Order Code RL32411

CRS Report for Congress
Received through the CRS Web

Network Centric Warfare: Background and Oversight Issues for Congress

June 2, 2004

Clay Wilson
Specialist in Technology and National Security
Foreign Affairs, Defense, and Trade Division

Network Centric Warfare: Background and Oversight Issues for Congress

Summary

Network Centric Warfare (NCW) is a key component of DOD planning for transformation of the military. NCW relies on computer processing power and networked communications technology to provide a shared awareness of the battle space for U.S. forces. Proponents say that a shared awareness increases synergy for command and control, resulting in superior decision-making, and the ability to coordinate complex military operations over long distances for an overwhelming war-fighting advantage. NCW technology saw limited deployment in Afghanistan and, more recently, increased deployment in Operation Iraqi Freedom (OIF). Several DOD key programs are now underway for deployment throughout all services.

Congress may be concerned with oversight of the DOD organization and the individual services as they transform through NCW programs that are intended to promote a management style and culture with joint objectives. Oversight may involve a review of service efforts to improve interoperability of computer and communications systems, and may also involve questions from some observers about whether DOD has given adequate attention to possible unintended outcomes resulting from over-reliance on high technology. Updates may also be required on emerging threats that may be directed against increasingly complex military equipment.

The background section of this report describes technologies that support NCW, and includes (1) questions about possible vulnerabilities associated with NCW; (2) a description of directed energy weapons, and other technologies that could be used as asymmetric countermeasures against NCW systems; (3) descriptions of some key military programs for implementing NCW; (4) a list of other nations with NCW capabilities; and, (5) a description of experiences using NCW systems in recent operations involving joint and coalition forces. The final section raises policy issues for NCW that involve planning, budget, network interoperability, acquisition strategies, offshore outsourcing, technology transfer, asymmetric threats, coalition operations, and U.S. military doctrine.

Appendices to this report give more information about the global network conversion to Internet Protocol version 6 (IPv6), and possible perverse consequences of data-dependent systems.

This report will be updated to accommodate significant changes.

Contents

List of Tables

Network Centric Warfare: Background and Oversight Issues for Congress

Introduction

This report provides background information and discusses possible oversight issues for Congress on DOD's strategy for implementing network centric warfare (NCW). NCW forms a central part of the Administration's plans for defense transformation. Possible issues for Congress are whether to approve, modify, or reject the Administration's plans for implementing NCW. Congress' decisions on this issue could affect future U.S. military capabilities, the composition of U.S. defense spending, and the ability of U.S. military forces to operate in conjunction with allied military forces. Additionally, while proponents argue that NCW may improve both the efficiency and effectiveness of combat operations, others argue that questions remain about (1) the interoperability of information systems for joint and coalition forces, (2) a shortage of available bandwidth to support NCW operations, and (3) possible unexpected outcomes when using data-dependent systems.

Background

Defense Transformation

Defense transformation involves large-scale, discontinuous, and possibly disruptive changes in military weapons, organization, and concepts of operations (i.e., approaches to warfighting) that are prompted by significant changes in technology or the emergence of new and different international security challenges.[1] Many observers believe that a U.S. military transformation is necessary to ensure U.S. forces continue to operate from a position of overwhelming military advantage in support of national objectives.[2] The administration has stated that DOD must transform to achieve a fundamentally joint, network centric, distributed force structure capable of rapid decision superiority. To meet this goal, DOD is building doctrine, training, and procurement practices to create a culture of continual transformation that involves people, processes, and systems.

---

[1] For more information, see CRS Report RL32238, *Defense Transformation: Background and Oversight Issues for Congress*.

[2] U.S. Department of Defense, *Transformation Planning Guidance*, April 2003.

Definition of Network Centric Warfare

The network centric approach to warfare is the military embodiment of information age concepts. Studies[3] have shown that networking enables forces to undertake a different range of missions than non-networked forces, by improving both efficiency and effectiveness of operations. NCW uses computers and communications to link people through information flows that depend on the interoperability of systems used by all U.S. armed forces. NCW involves collaboration and sharing of information to ensure that all appropriate assets can be quickly brought to bear by commanders during combat operations.[4] Procurement policy to support NCW is also intended to improve economic efficiency by eliminating stove-pipe systems, parochial interests, redundant and non-interoperable systems, and by optimizing capital planning investments for present and future information technology systems. Objectives of NCW include the following:

(1) Self-synchronization, or doing what needs to be done without traditional orders;
(2) Improved understanding of higher command's intent;
(3) Improved understanding of the operational situation at all levels of command; and,
(4) Increased ability to tap into the collective knowledge of all U.S. (and coalition) forces to reduce the "fog and friction" commonly referred to in descriptions of fighting.[5]

DOD describes its strategy for implementing NCW in a publication titled, "Network Centric Warfare: Creating a Decisive Warfighting Advantage," released in January 2004 by the Office of Force Transformation. Key elements for implementation include the following:

(1) Refine the rules and theory of NCW through simulation, testing, experimentation, and combat experience.

---

[3] Network Centric Operations is a theory that is being tested as part of an ongoing research program. The Office of Force Transformation (OFT) and the Command and Control Research Program (CCRP) of the Office of the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD/C3I) have been collaborating to develop metrics to support Transformation related experiments, studies, and analyses. To date the effort has been led by RAND, with support from Evidence Based Research, Inc. (EBR), and participation of the government sponsors. The theory posits that the application of information technologies has a positive impact on military effectiveness. Independent variables include networking, information sharing, collaboration, etc. Dependent variables include speed of command and force effectiveness. Dr. Kimberly Holloman, Evidence Based Research, Inc., *The Network Centric Operations Conceptual Framework*, Presentation at the Network Centric Warfare 2004 Conference, Washington, D.C., Jan. 20, 2004, [http://www.oft.osd.mil/library/library.cfm?libcol=2].

[4] U.S. Department of Defense, *Report on Network Centric Warfare*, 2001, [http://www.defenselink.mil/nii/NCW/ncw_sense.pdf] , and Ret. Admiral Arthur Cebrowski, *Speech to Network Centric Warfare 2003 Conference*, Jan. 2003, [http://www.oft.osd.mil].

[5] "Fog" is the term that describes the uncertainty about what is going on during a battle, while "Friction" is the term that describes the difficulty translating a commander's intent into battlefield actions.

(2) Apply NCW theory enterprise-wide in DOD.
(3) Accelerate networking in the joint force.
(4) Accelerate deployment of network centric concepts and capabilities.
(5) Experiment with network centric concepts to develop new ways to conduct NCW.
(6) Address challenges of using NCW with coalition forces.
(7) Develop appropriate doctrine and tactics for NCW.

Some argue that, as new concepts and technologies are proven valid over time, NCW may extend to become a stabilizing deterrence against future conflict. For example, if adversary targets are neutralized by NCW systems before they can engage in fighting with U.S. forces, then the battle can be finished before it has really begun.[6] Others argue that wealthy countries now have a temporary advantage which may be reduced as NCW technology becomes less expensive and as technical knowledge spreads to other nations and terrorist groups.[7] Some argue that to maintain its advantage, the United States must continue to refine the uses of technology to increase flexibility and adaptability for both joint and coalition NCW operations.

Technologies that Support NCW

Some observers have said that the price of entry into NCW operations is the construction of a network of sensors. For example, aircraft and other platforms become sensors as they are given new capabilities to communicate and combine data, and many weapons are no longer considered simple munitions, but also become part of the system of sensors, as they are guided to their targets until they explode.[8] This section discusses key components of a NCW system.

Network Architectures. NCW is highly dependent on the interoperability of communications equipment, data, and software to enable networking of people, sensors, and manned and unmanned platforms. Parts of NCW technology rely on line-of-sight radio transmission for microwave or infrared signals, or laser beams. Other parts of the technology aggregate information for transmission through larger network trunks for global distribution via fiber optic cables, microwave towers, or both low-altitude and high-altitude satellites. The designs for this technology must enable rapid communications between individuals in all services, and rapid sharing of data and information between mobile platforms and sensors used by all military services.[9] The

---

[6] Dr. Kimberly Holloman, Evidence Based Research, Inc., *The Network Centric Operations Conceptual Framework*, Presentation at the Network Centric Warfare 2004 Conference, Washington, D.C., Jan. 20, 2004,[http://www.oft.osd.mil/library/library.cfm?libcol=2].

[7] Scott Renner, C2 Information Manager, MITRE Corporation, *Building Information Systems for NCW*, 4th Annual Multinational C4ISR Conference, Mclean, Virginia, May 6, 2004.

[8] Frederick Stein, Senior Engineer, MITRE Corporation, *Presentation on Network Centric Warfare Operations*, 4th Annual Multinational C4ISR Conference, McLean, Virginia, May 6, 2004.

[9] For more information about military network interoperability issues, and the Global

(continued...)

architectures must also have the ability to dynamically self-heal and re-form the network when one or more communications nodes are interrupted.

Perhaps the most widely-known U.S. military networks are the Non-Classified Internet Protocol Router Network, and the Secret Internet Protocol Router Network (NIPRNET and SIPRNET.) The architectures for these networks isolate transmission of classified SIPRNET messages away from the civilian Internet, while a large percentage of less-secure NIPRNET traffic is reportedly routed through the civilian Internet.[10] In the past, some military units reportedly have used special encryption technology to enable SIPRNET communications to be sent through the NIPRNET.[11]

Satellites. Satellites are crucial for enabling mobile communications in remote areas, as well as for providing imagery, navigation, weather information, a missile warning capability, and a capability to "reach back" to the continental United States for added support. The Global Positioning System (GPS), consisting of 28 navigation satellites, helps identify the location of U.S. forces, as well as target locations for launching U.S. weapons, such as cruise missiles. The United States maintains 6 orbital constellations for Intelligence, Surveillance, and Reconnaissance (ISR): one for early warning, two for imagery, and three for signals intelligence. However, despite the number of military satellites, the Defense Information Systems Agency (DISA) reported that up to 84 percent of the satellite communications bandwidth provided to the Operation Iraqi Freedom (OIF) theater was supplied by commercial satellites.[12]

Radio Bandwidth. Digitization of communications is a key part of the DOD programs associated with military force transformation. Digital technology makes more efficient use of spectrum bandwidth for communications than does analog technology. However, since 1991, there has been an explosive increase in demand for bandwidth, due to efforts to speed up the delivery of digital information. Defense officials remain concerned about whether the radio bandwidth supply available through DOD systems will grow adequately to keep up with increasing military demand in the future (see more at Bandwidth Limitations, below).

---

[9] (...continued)
Information Grid, see CRS Report RS21590, *Defense Program Issue: Global Information Grid, Bandwidth Expansion*.

[10] Seventy percent of NIPRNET traffic reportedly is routed through the civilian Internet, Christopher Dorobek and Diane Frank, *DOD may pull key net from the Internet*, InsideDefense, Dec. 26, 2002, [http://www.insidedefense.com].

[11] Dan Caterinicia, "Marines Tunnel to SIPRNET," FederalComputerWeek.com, Dec. 9, 2002, [http://www.fcw.com].

[12] DOD satellites could not satisfy the entire military demand for satellite bandwidth, and therefore DOD has become the single largest customer for commercial satellite services. DOD sometimes leases commercial satellite bandwidth through DISA, and at other times bypasses the process to buy directly from industry. Bypassing DISA may reduce interoperability and increase redundancies. Jefferson Morris, "GAO: DOD Needs New Approach to Buying Bandwidth," *Aerospace Daily*, Dec. 12, 2003; "DISA Chief Outlines Wartime Successes," *Federal Computer Week*, June 6, 2003.

Unmanned Vehicles (UVs). UVs, also known as Unmanned Aerial Vehicles (UAVs), Ground Vehicles (UGVs), and Underwater Vehicles (UUVs), are primarily used for surveillance, however their mission is evolving to also include combat.[13] During OIF, approximately 16 Predator and 1 Global Hawk UAVs were in operation, and all were controllable remotely via satellite link from command centers in the continental United States. UVs each require a large amount of bandwidth for control and for transmission of reconnaissance images, and UVs also serve as nodes that can relay messages through the NCW network.[14]

Computer Processor Chips. Gordon Moore's Law of Integrated circuits predicts that every 18 months, computer chips evolve to become twice as dense and twice as fast for about the same cost, meaning they become almost 4 times as powerful every 18 months. Industries that use computer technology rely on Moore's Law as a guide for investing in future technology systems. Many future NCW concepts now being developed by DOD also rely on the continued evolution in computer processing power, and may also be affected by advances in other technologies, such as nanotechnology.

Nanotechnology. New materials developed through nanotechnology may eventually change battlefield equipment in ways hard to imagine. Weapons may become smaller and lighter, and new miniaturized network sensors may detect, locate, identify, track, and target potential threats more efficiently.[15] DOD currently uses nanotechnology to create a heat-resistant coating that extends the life of propulsion shafts for warships, and as an additive to boost the performance of rocket propellant. Some observers believe that nanotechnology may eventually alter fundamental concepts of warfare, perhaps even more than the invention of gunpowder.[16]

In June 2003, MIT opened the Institute for Soldier Nanotechnologies in Cambridge, Massachusetts. The Institute was funded in March 2002 by a $50 million grant from the Army, and will seek to develop technologies such as a handheld device that detects chemical or biological weapons, or a flexible yet bulletproof exoskeleton that could reduce the weight of a soldier's equipment and protective gear by 50 pounds, while also adding biomedical sensors linked to mobile networks. Other

---

[13] The two key programs for UAV development are the USAF's X-45 and the Navy's carrier-capable X-47. Both projects are under the Joint Unmanned Combat Air System (J-UCAS) program, which is led by DARPA. DOD believes that merging these two projects will lead to greater efficiencies and reduced acquisition costs. Adam Herbert, "New Horizons for Combat UAVs," *Air Force Magazine*, Dec. 2003.

[14] For more information about UVs, see CRS Report RS21294, *Unmanned Vehicles for U.S. Naval Forces: Background and Issues for Congress*.

[15] Edward A. Smith, "Network Centric Warfare: Where's the Beef?," Submission to the *U.S. Naval War College Review*, 2000,[http://www.dodccrp.org/].

[16] According to statements reportedly made by Dr. Clifford Lau, DOD Office of Basic Research, nanotechnology will affect every aspect of weaponry, communications, and the welfare of soldiers. Barnaby Feder, "Frontier of Military Technology is the Size of a Molecule," *New York Times*, Apr. 8, 2003, p.C2.

countries are also making advances in nanotechnology.[17] However, in 2000, Asian countries produced nearly 25,000 Ph.D. graduates in fields related to nanotechnology, while the United States produced fewer than 5,000.[18]

Software. Software is an important component of all complex defense systems used for NCW. GAO has recommended that DOD follow best practices of private sector software developers to avoid the kinds of schedule delays and cost overruns that have plagued many Pentagon programs that depend on complicated software.[19] Many observers of the software industry believe that globalization of the economy dictates a global process for software development. In keeping with the GAO recommendation, contractors for DOD often outsource software development to other, smaller private firms, and in some cases, programming work may be done by offshore companies. This raises questions about the possibility of malicious computer code being used to subvert DOD computer systems. However, Robert Lentz, the U.S. Defense Department's director of information assurance, reportedly has stated that DOD is currently investigating ways to strengthen policy mechanisms to increase DOD confidence in the security of both foreign and domestic software products.[20] (See Outsourcing and Technology Transfer, below.)

Questions About NCW

While the United States has the ability to exploit advances in computer information processing, networking, satellites, radio communications, and other technologies, some observers question whether the United States military places too much emphasis on technology, and others question whether information itself may be overrated as a useful military asset (See Appendix B, Perverse Consequences of Data-Dependent Systems).

However, technology is only one of the underpinnings of NCW. Other observers state that NCW requires changes in behavior, process, and organization to convert the advances of Information Age capabilities into combat power. Through new uses of NCW technologies, rigid constructs are transformed into dynamic constructs that can provide new and advantageous flexibility for actions in combat. Sometimes, however,

---

[17] "Chinese, U.S. scientists make headway in nano-wire research," *People's Daily Online,* Feb. 1, 2004,

[18] For more information about nanotechnology, see CRS Report RS20589, *Manipulating Molecules: The National Nanotechnology Initiative*.

[19] U.S. General Accounting Office, *DEFENSE ACQUISITIONS: Stronger Management Practices Are Needed to Improve DOD's Software-Intensive Weapon Acquisitions*, GAO-04-393, Mar. 2004.

[20] It is virtually impossible to find unauthorized and malevolent code hidden deep within a sophisticated computer program module that may have originated from a company in one of more than a half-dozen countries commonly used for software outsourcing. Mark Willoughby, "Hidden Malware in offshore products raises concerns," *Computerworld*, Sept. 15, 2003 [http://www.computerworld.com].

people may initially not fully utilize the capabilities of the new systems because they are not yet comfortable with the required changes in behavior.[21]

Advantages of NCW. Emerging literature supports the theory that power is increasingly derived from information sharing, information access, and speed. This view has been supported by results of recent military operational experiences[22] showing that when forces are truly joint, with comprehensively integrated capabilities and operating according to the principles of NCW, they can fully exploit the highly path-dependent[23] nature of information age warfare. Some resulting military advantages of NCW operations include the following:

(1) Networked forces can consist of smaller-size units that can travel lighter and faster, meaning fewer troops with fewer platforms and carrying fewer supplies can perform a mission effectively, or differently, at a lower cost.

(2) Networked forces can fight using new tactics. During OIF, U.S. Army forces utilized movement that was described by some as "swarm tactics." Because networking allows soldiers to keep track of each other when they are out of one another's sight, forces could move forward in Iraq spread out in smaller independent units, avoiding the need to maintain a tight formation. Using "swarm tactics," unit movements are conducted quickly, without securing the rear. All units know each other's location. If one unit gets into trouble, other independent units nearby can quickly come to their aid, "swarming" to attack the enemy from all directions at once. Benefits may include the following: (1) fewer troops and less equipment are needed, so waging war is less expensive; (2) it is harder for an enemy to effectively attack a widely dispersed formation; (3) combat units can cover much more ground, because they do not have to maintain a formation or slow down for lagging vehicles; (4) knowing the location of all friendly units reduces fratricide during combat operations; and (5) swarming allows an attack to be directed straight into the heart of an enemy command structure, undermining support by operating from the inside, rather than battling only on the periphery.

(3) The way individual soldiers think and act on the battlefield is also changing. When a unit encounters a difficult problem in the field, they radio the Tactical Operations Center, which types the problem into an online chat room, using

---

[21] Frederick Stein, Senior Engineer, MITRE Corporation, "Presentation on Network Centric Warfare Operations," 4th Annual Multinational C4ISR Conference, McLean, Virginia, May 6, 2004.

[22] John Garstka, "Network-Centric Warfare Offers Warfighting Advantage," Signal Forum, *Signal Magazine*, May 2003.

[23] Path-dependence means that small changes in the initial conditions will result in enormous changes in outcomes. Therefore, a military force must define initial conditions that are favorable to their interests, with the goal of developing high rates of change that an adversary cannot outpace. Dan Caterinicciа and Matthew French, "Network-centric warfare: Not there yet," *Federal Computer Week*, June 9, 2003 [http://www.fcw.com/fcw/articles/2003/0609/cov-netcentric-06-09-03.asp].

Microsoft Chat software. The problem is then "swarmed" by experts who may be located as far away as the Pentagon.[24]

(4) The sensor-to-shooter time is reduced. Using NCW systems, soldiers in the field have the capability to conduct an "on site analysis" of raw intelligence from sensor displays, rather than waiting for return analysis reports to arrive back from the continental United States.[25]

Information Overrated. Some observers state that Information Age technology is making time and distance less relevant, and that information increases the pace of events and the operational tempo of warfare.[26] However, other observers believe that networking for information exchange is not a sufficient substitute for combat maneuver, and that information superiority and situational awareness are not the most significant components of combat power. As in a chess game, these observers believe it is knowing the next move to make that is the key to success in battle, for example, through correct analysis of an anticipated enemy movement and tactics.[27]

Other observers also state that huge information resources may be overrated as an asset for creating effective military operations, and that important military decisions may not always lend themselves to information-based rational analysis.[28] They argue that discussions of military transformation have overwhelmingly focused on the rewards of information, and that the military services, national security establishment, and intelligence community have not thoroughly studied the risks associated with data-dependent military doctrine.[29] Some of the issues raised by these observers include:

---

[24] Joshua Davis, "If We Run Out of Batteries, This War is Screwed," *Wired Magazine*, June 2003, [http://www.wired.com/wired/archive/11.06/battlefield.html].

[25] For example, one UAV equipped with multiple sensors can survey the same area as ten human sentries, or one could monitor areas contaminated with radiological, chemical or biological agents without risk to human life. Today, DOD has in excess of 90 UAVs in the field; by 2010, this inventory is programmed to quadruple. U.S. Department of Defense, Office of the Secretary, *Unmanned Aerial Vehicles Roadmap 2002-2007*, Dec. 2002.

[26] David Alberts, John Garstka, Frederick Stein, *Network Centric Warfare*, DOD Command and Control Research Program, Oct. 2003, p.21.

[27] Lt. Colonel Edmund Blash, USAR, "Network-Centric Warfare Requires a Closer Look," Signal Forum, *Signal Magazine*, May 2003.

[28] Martin Burke, *Information Superiority Is Insufficient To Win In Network Centric Warfare*, Joint Systems Branch, Defense Science and Technology Organization, 2001, [http://www.dodccrp.org/events/2000/5th_ICCRTS/cd/papers/Track4/024.pdf].

[29] Michael Schrage, *Perfect Information and Perverse Incentives: Costs and Consequences of Transformation and Transparency*, Security Studies Program Working Paper, Massachusetts Institute of Technology, E38-600, May 2003, p.15.

(1) Quantitative changes in information and analysis often lead to qualitative changes in individual and organizational behavior that are sometimes counter-productive.[30]

(2) Reliance on sophisticated information systems may lead to management overconfidence.[31]

(3) An information-rich, opportunity-rich environment may shift the value of the information, redefine the mission objectives, and possibly increase the chances for perverse consequences. (See Appendix B, Perverse Consequences of Data-Dependent Systems.)

Underestimating the Adversaries. Some observers have wondered whether proponents of NCW are making overstated claims, similar to exaggerated expectations that led to the recent dot-com stock run-up and crash. They believe that the DOD model for network centric operations may underestimate an enemy's ability to deceive sensors, or block information needed for NCW. One of the vulnerabilities cited by observers may be the fact that DOD has openly published plans for using NCW technologies in future warfare. Just like the Maginot Line before World War I, an enemy now has time to plan ways to avoid our strengths and attack our weaknesses.[32]

Interoperability. Some question whether the U.S. military can achieve true network and systems interoperability among all services. According to statements reportedly made by Army Major General Marilyn Quagliotti, vice director of the Defense Information Systems Agency (DISA), "We are still developing stovepipe systems, [and] they are still getting through our governance structure." An example cited is the Global Command and Control System (GCCS) which currently runs under 16 different databases, with multiple architectures specified for different military branches and divisions. However, DISA reportedly will soon field GCCS Version 4.0, with a new architecture designed to use only one master database.[33]

DOD reportedly intends to integrate the network architectures of systems used by all branches of the military to create a network centric capability linked to the Global Information Grid (see below). To help accomplish this integration, the DOD Joint Staff has created a new Force Capability Board (FCB) to monitor NCW programs for mismatches in funding, or mismatches in capability. When an issue is

---

[30] Dr. Kimberly Holloman, Evidence Based Research, Inc., *The Network Centric Operations Conceptual Framework,* Presentation at the Network Centric Warfare 2004 Conference, Washington, D.C., Jan. 20, 2004, [http://www.oft.osd.mil/library/library.cfm?libcol=2].

[31] Michael Schrage, *Perfect Information and Perverse Incentives: Costs and Consequences of Transformation and Transparency*, Security Studies Program Working Paper, Massachusetts Institute of Technology, E38-600, May 2003, p.4.

[32] Alfred Kaufman, "Be Careful What You Wish For: The Dangers of Fighting with a Network Centric Military," J*ournal of Battlefield Technology*, Vol 5, No.2. July 2002, and "Networking in an Uncertain World," *Journal of Battlefield Technology*, Vol 5, No.3, Nov. 2002.

[33] Dawn S. Onley, "Franks credits technology with decisive wins," *Government Computer News*, Feb. 23, 2004, p.28.

detected, the FCB reports to the Joint Requirements Oversight Council, which then provides information during budget deliberations at the Pentagon.[34]

Bandwidth Limitations. Some observers question whether communications bandwidth supply can be made adequate to match growing future military needs. When the supply of bandwidth becomes inadequate during combat, military operations officers have sometimes been forced to subjectively prioritize the transmission of messages. They do this by literally pulling the plug temporarily on some radio or computer switching equipment in order to free up enough bandwidth to allow the highest-priority messages to get through. This can delay, or cancel other messages or data transmissions, which are placed into in a lower priority. Latency, or delays in information updates resulting from a bandwidth shortage, could theoretically leave some units attempting to fight the red display icons on their computer screens, rather than the enemy, who might change position faster than screen image information can be updated.

By the year 2010, the Congressional Budget Office estimates that the supply of effective bandwidth in the Army is expected to fall short of peak demand by a ratio of approximately 1 to 10.[35] According to former Assistant Secretary of Defense for Networks and Information Integration (ASD/NII), Paul Stenbit, the primary barrier to achieving the NCW Internet paradigm is finding ways to meet the demand for bandwidth. Communications infrastructure must have enough bandwidth to allow, for example, several people at different locations in the battlefield to pull the same problem-solving data into their computer systems at the same time, without having to take turns sharing and using the same available, but limited bandwidth.[36]

Space Dominance. The United States is now highly-dependent on space assets for communications, navigation, imagery, weather analysis, and missile early-warning systems. The United States has enjoyed space dominance during previous Gulf conflicts largely because its adversaries simply did not exploit space, or act to negate U.S. space systems. However, the United States cannot rely on this same advantage in the future, and we may expect less-technically advanced nations and non-

---

[34] Brigadier General Marc Rogers, Director Joint Requirements and Integration Directorate/ J8, for U.S. Joint Forces Command, in U.S. Congress, House Armed Services Subcommittee on Terrorism, Unconventional Threats and Capabilities, Hearing on Military C4I Systems, Oct. 21, 2003 [http://www.cq.com], and Rich Tuttle, "New Organization to Stress Importance of Network Programs," *Aerospace Daily*, Jan. 30, 2004,

[35] Anticipated hardware improvements by 2010 will shift the existing bandwidth bottleneck from the brigade level to the corps level. If the Joint Tactical Radio System (JTRS) performs as the Army projects, the new radio may provide more than enough bandwidth for the lower tactical levels of command, with a margin for growth of demand beyond 2010. However, at the division and corps level, the projected demand is still expected to be much greater than the likely supply. U.S. Congressional Budget Office, *The Army's Bandwidth Bottleneck*, Aug. 2003, [http://www.cbo.gov].

[36] In certain situations, some commanders had access to only one communications channel. If someone else was using it first, the commander had to wait until it was free for him to use. Matthew French, "Bandwidth in Iraq a subject of debate," *Federal Computer Week*, Oct. 20, 2003, p.43.

state actors to employ electronic jamming techniques, or launch attacks against satellite ground facilities.[37] A non-state group could possibly also take advantage of space-based technology by leasing satellite bandwidth, or purchasing high-resolution imagery from suppliers in the Soviet Union, China, or other countries that own and operate space assets.

In the future, satellites will be used for Space Based Radar (SBR), which will provide persistent views of the battlefield, including accurate terrain information needed for mapping. However, there is growing doubt within the intelligence community about the long-term future of satellite-based ISR. As enemies become more diverse and more unconventional, they may begin to utilize different technologies, such as fiber optics, that are beyond the reach of satellite sensors.[38]

Outsourcing and Technology Transfer. An increase in offshore outsourcing of high tech jobs, including computer programming and chip manufacturing, may enable a transfer of knowledge and technology that may eventually threaten U.S. global technical superiority and undermine current NCW advantages.[39] The Gartner Group research firm has reported that corporate spending for offshore information technology (IT) services will increase from $1.8 billion in 2003 to more than $26 billion by 2007, with half of the work going to Asian countries such as India and China.[40]

Contracting for national defense is reportedly among the most heavily outsourced of activities in the federal government.[41] Within DOD, the ratio of private sector jobs to civil service jobs is nearly five to one, and has been increasing far in excess of non-defense-related agencies. While outsourcing may have been initially motivated by

---

[37] Testimony from the hearing on Army Transformation, Senate Armed Services Committee, Subcommittee on Airland, Mar.12, 2003, CQ.com,[http://www.cq.com/aggregatedocs.do].

[38] Three additional constellations of U.S. satellites are also used for electronic eavesdropping on enemy radio, cell phone, and microwave transmissions. There are also 2 constellations (totaling 6 satellites) of secret photo-reconnaissance satellites that transmit visible light images, infrared images, and radar images. Loren Thompson, "Satellites Over Iraq," *Intelligence, Surveillance, and Reconnaissance Journal*, vol.3, no.1, March 2004, p.20.

[39] In 2003, of the 2,027 doctorates awarded by U.S. universities for electrical engineering and computer science, 63 percent were earned by foreign nationals. Of the 15,906 master's degrees awarded in these same fields, 56 percent were earned by non-U.S. residents. Eric Chabrow and Marianne McGee, "Immigration and Innovation," *Information Week*,Feb. 23, 2004, p.20.

[40] Paul McDougall, "Optimizing Through Outsourcing," *Information Week*, Mar. 1, 2004, p.56. For more information, see CRS Report RL30392: *Defense Outsourcing: The OMB Circular A-76 Policy*.

[41] Ann Markusen, Director, Project on Regional Industrial Economics, University of Minnesota, "Statement Made to David Walker, Chairman Commercial Activities Panel, GAO, June 5, 2001 and Pender M McCarter, "500,000 U.S. IT Jobs Predicted to Move Overseas by Year-end 2004; IEEE Sees Continued Loss in U.S. Economic Competitiveness, National Security," *IEEE-USA News*, July 21, 2003, [http://www.ieeeusa.org/releases /2003/072103pr.html].

cost-reduction, the new trend is for more high-level research and development (R&D) work to be done offshore, partly due to the growth in education and technology talent now found among foreign workers. For example, as early as 1998, Intel Corporation, Microsoft Corporation, and other IT vendors opened R&D facilities in Beijing and other parts of Asia. Microsoft reportedly has 200 Ph.D. candidates and 170 researchers currently working in its Asia R&D facilities.[42]

Technology transfer also occurs for the manufacture of high-technology equipment used to support NCW operations. For example, only 20 percent of the thermal batteries used in U.S. missiles, guided artillery, and guided bombs are produced by domestic suppliers, while 80 percent of these devices are produced by a foreign supplier. Night-vision infrared devices that have formerly given U.S. forces a tremendous military advantage are now manufactured with materials and components that come almost entirely from foreign sources.[43]

However, a recent study by DOD concluded that utilizing foreign companies as sources for high-technology equipment does not affect long-term military readiness, and that for the majority of high-technology items, several domestic suppliers are available to meet DOD needs.[44] In addition, some observers believe that U.S. high-technology companies must retain flexibility to align their business operations as necessary to meet customer needs. For example, as the skill sets of foreign workers increase, customers of high-technology suppliers gain expanded options for lower-cost access to technical talent. Observers have stated that companies that ignore outsourcing trend do so at the peril of their long-term competitiveness.[45]

Asymmetric Threats to Counter NCW

The term "asymmetric", when referring to strategies in warfare, is often intended to describe attacks launched by a weaker, or less-well-equipped enemy, as they learn to exploit a stronger opponent's vulnerabilities. Technology has provided an asymmetric advantage for U.S. forces in recent conflicts. However, asymmetry sometimes leads to unanticipated outcomes. For example, video images showing the overwhelming power of the U.S. military in recent urban conflicts have been on

---

[42] Patrick Theobald and Sumner Lemon, "R&D Starts to Move Offshore," *Computerworld*, vol. 38, no. 9, Mar. 1, 2004, p. 1.

[43] Research into technology for newer, more efficient versions of night vision systems has been almost entirely eliminated within the United States. Publication of the House Armed Services Committee. "The U.S. Military 'Owns the Night' on the Battlefield, But Not for Long, Says Industry Pioneer, *Manufacturing & Technology News*, Oct. 3, 2003.

[44] U.S. Department of Defense, Office of the Deputy Undersecretary of Defense for Industrial Policy, *Study on Impact of Foreign Sourcing of Systems*, Jan. 2004.

[45] For more information on DOD outsourcing, see U.S. General Accounting Office *Information Technology: DOD Needs to Leverage Lessons Learned from Its Outsourcing Projects*, GAO-03-371, Apr. 2003. The Information Technology Association of America (IITA) has justified U.S. companies' move to outsource work in order to ensure cost advantage and customer proximity. Ashu Kumar, "U.S. IT Body Backs Outsourcing, Warns Against Restrictions," *ZDNetIndia*, Aug. 26, 2003, [http://www.zdnetindia.com/print.html?iElementId=88394].

display in the global news media. Such images, resulting from the technological efficiency of U.S. forces, may have given terrorist organizations such as Al Qaeda added power to spread rhetoric, recruit more members, and gain more indigenous loyalty.[46]

Asymmetric countermeasures may include actions taken by an enemy to bypass NCW sensors, or to negate the usefulness of high technology weapons. Some examples may include (1) suicide bombings; (2) hostile forces intermingling with civilians used as shields; (3) irregular fighters and close-range snipers that swarm to attack, and then disperse quickly; (4) use of bombs to spread "dirty" radioactive material, or (5) chemical or biological weapons.

Persons associated with terrorist groups are sometimes found to have received advanced education in high-technology, and may also have knowledge of how to use technology in an asymmetric attack against the supporting infrastructure for NCW.[47] For example, Khalid Sheikh Mohammed, who was arrested in 2003 for possible links with Al Qaeda, reportedly studied engineering at a university in North Carolina. A student at the University of Idaho, who was recently arrested for alleged terrorist connections, was studying in a Ph.D. program for cyber security,[48] and several of the 9/11 terrorists reportedly had degrees in technology.

Possible uses of technology to launch asymmetric attacks against NCW systems may include (1) directed energy devices used to jam satellite signals;[49] (2) directed

---

[46] The 2004 annual meeting of the World Economic Forum featured a session that analyzed the methods of the Al Qaeda organization from a business perspective. At the Forum, Aart J. de Geus, Chairman and Chief Executive Officer, Synopsis, U.S.A., reportedly stated, "The response of the U.S. has legitimized [Bin Laden's] approach." As a result, some analysts now believe that Al Qaeda is becoming a virtual organization, while creating new links to local franchises. It is these new local groups that are now carrying out terrorist attacks, rather than Al Qaeda itself, and these smaller, local groups are more difficult for the U.S. military to anticipate, locate, and engage. Summary of the Annual Meeting, *Business Lessons from Terrorists*, World Economic Forum, January 21-25, 2004, [http://members.weforum.org/pdf/Session_Summaries2004/084e.pdf].

[47] See also CRS Report RL32114, *Computer Attack and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress.*

[48] Interview with Richard Clarke, *Frontline: Cyberwar*, March 18, 2003, [http://www.pbs.org].

[49] A group of Iranians last summer reportedly jammed a U.S.-built commercial satellite broadcasting pro-rebel information into that Middle Eastern country. The specific transponder that was carrying the broadcast was disrupted for about two weeks by Iranians operating at a teleport in Cuba, according to industry sources. Amy Butler, "Heavy DoD Reliance On Commercial SATCOM Prompts Questions of Protection," *Defense Daily*, Apr. 13, 2004.

energy devices that could theoretically burn out computer circuits at a distance,[50] and (3) malicious computer code to subvert controls for complex weapons.

Cyber Attacks Against Military Computers

DOD has taken steps to block access to some of the communications ports that link the NIPRNET and the civilian Internet. However, in October 2003, an intrusion by a civilian hacker forced a NIPRNET website to be taken offline temporarily.[51] Other hackers have also used the civilian Internet to successfully penetrate military computers, causing measurable damage,[52] and forcing portions of the military computer network to shut down temporarily.[53]

There is growing controversy about whether the U.S. military should use general purpose "open source" commercial computer software for the command, control, and communications functions in advanced defense systems for tanks, aircraft and other complex equipment. An example is the popular computer operating system known as "Linux", which is labeled "Open-Source" software because it has been developed by a worldwide community of contributing programmers who continuously add new features by building on each others' openly-shared source code. Subscriptions are purchased for commercial technical support of different versions of "open source" software. In contrast, the code for proprietary, or "Closed-Source" commercial-off-the-shelf (COTS) software products, such as Microsoft Windows, is not openly disclosed to the public.

NSA has researched a secure version of Linux, but it is not clear that all military computer systems are restricted by results of that research.[54] Some experts believe that open-source software violates many security principles, and may be subverted by adversaries who could secretly insert Trojan horse malicious code to cause complex defense systems to malfunction. Other computer experts disagree, stating that precisely because Linux is openly reviewed by a worldwide community of contributing programmers, it has security that cannot easily be compromised by a foreign agency.

A recent study by the Defense Information Systems Agency (DISA) states that DOD currently uses a significant variety of open-source computer software programs,

---

[50] Directed energy weapons could include a High-Energy Microwave device (HPM), activated by a chemical explosion. Such a bomb-driven device, the size of a suitcase and using a specially-shaped antenna, could theoretically direct a narrow-beam energy pulse that could damage a computer within a distance of 1 kilometer. Prof. Robert Harney, Naval Postgraduate School, *personal communications,* April 12, 2004.

[51] MARADMIN, "Marine Corps Announcement of website Breach," Oct. 15, 2003, [http://www.insidedefense.com].

[52] Brooke Masters, "Briton Indicted as Hacker," *Washington Post,* Nov. 13, 2003, p. A11, [http://www.washingtonpost.com/wp-dyn/articles/A45963-2002Nov12.html].

[53] U.S. Attorney's Office, District of New Jersey, Public Affairs Office, Nov. 11, 2002, [http://www.usdoj.gov/usao/nj/publicaffairs/NJ_Press/files/mc1112_r.htm].

[54] See NSA Security Enhanced Linux, [http://www.nsa.gov/selinux/index.cfm].

and concluded that open-source software is vital to DOD information security. This is partly because many information security tools used by DOD are built using open-source code, and effective counterparts are not available from closed-source COTS products. The study also states that DOD Web services and DOD software development would be disrupted without continued use of open-source software. This is because many tools that are basic to web design and software development are based on open-source code.[55]

Experts at the Naval Post Graduate School reportedly have stated that "software subversion" can only be avoided by using "high-assurance" software that has been proven to be free of any malicious code.[56] Because of the added development rigor and test procedures required for such proof, high-assurance software would cost considerably more than open-source software.[57]

Key Military Programs

The following are key programs related to NCW that are identified in the DOD budget as Program Elements (PE) for Research, Development, Test and Evaluation (RDT&E). Figures for FY2005 and beyond are estimates.

Net Centricity. The Net Centricity program is intended to support information technology activities for network-centric collaboration. Horizontal Fusion is a component that determines how quickly DOD and intelligence community programs can be extended to a net-centric operational environment. The GIG Evaluation Facility is a component that tests interoperability of key systems in an end-to-end manner, including the Joint Tactical Radio System (JTRS) and the Global Information Grid Bandwidth Expansion (GIG BE) programs.

---

[55] DISA, "Use of Free and Open-Source Software (FOSS) in the U.S. Department of Defense," Mitre Report No. MP 02 W0000101, Version 1.2, Oct. 2002, p. 20, [http://unix.be.eu.org/docs-free/dodfoss.pdf].

[56] Alexander Wolfe, "Green Hills calls Linux "Insecure" for Defense," *EETimes*, Apr. 9, 2004, [http://eetimes.com/showArticle.jhtml?articleID=18900949] and Charles J. Murray, April 19, 2004, "Linux: Unfit for National Security?," *EETimes*, [http://eetimes.com/showArticle.jhtml?articleID=18901858].

[57] Research at the Naval Postgraduate School has resulted in new security tools for protecting against unauthorized computer and network intrusions. The new technology has been licensed to Lancope Inc. of Alpharetta, Georgia, which has created a new commercial version of the intrusion detection tool, called "StealthWatch." The license was granted because the Naval Postgraduate School intended that the technology become more developed through marketing in the commercial world. William Jackson, "Hasta La Vista, Attacks," *Government Computer News*, vol.23, no.6, Mar. 22, 2004, p.27.

Table 1. PE 0305199D8Z Net Centricity.[58]

($ in Millions)

	FY2003	FY2004	FY2005 (est.)	FY2006 (est.)	FY2007 (est.)	FY2008 (est.)	FY2009 (est.)
Total PE Cost	—	—	214.225	216.015	219.464	231.226	236.086
Horizontal Fusion			206.422	207.815	210.864	222.126	226.586
GIG Evaluation			7.800	8.200	8.600	9.100	9.500

DOD Global Information Grid (GIG). The GIG supports DOD and related intelligence community missions and functions, and enables sharing of information between all military bases, mobile platforms, and deployed sites. The GIG also provides communications interfaces to coalition, allied, and non-DOD users and systems. Older messaging systems, such as the Defense Message System (DMS), Global Command and Control System (GCCS), and the Global Combat Support System (GCSS) will all be made accessible via the GIG.[59]

DOD is planning, by 2008, that military communications equipment use the new Internet Protocol version 6 (IPv6) as the standard for all transmission through the Global Information Grid (GIG), and for all DISN systems that will interoperate with the GIG.[60] The new IPv6 protocol will reportedly offer greater message security and better tracking of equipment, supplies, and personnel through use of digital tags (See Appendix A, The Transition from Internet Protocol Version 4 (IPv4) to IPv6).

Key service network architectures for implementing the GIG are the Air Force C2 Constellation, Marine Corps Integrated Architecture Picture, Navy ForceNet, and Army LandWarNet.[61] These network architectures will become fully interoperable to help realize the full potential of NCW.

---

[58] DOD RDT&E Budget Item Justification, PE 0305199D8Z, Appropriation/Budget Activity, RDT&E Defense-Wide, BA 7, Feb. 2004, [http://www.defenselink.mil/comptroller/defbudget/fy2005/budget_justification/pdfs/rdtande/OSD_BA7/ZZN-70305199D8Z_Net_Centricity__R-2(co)R-2A__Feb_2004.pdf].

[59] Dawn Onley, "Old DOD Net is Key to New Global Grid," *Government Computer News* Mar. 8, 2004, [http://www.gcn.com].

[60] Staff, "DOD Now Preparing for Rapid Move to IPv6, Hi-Tech Chief Says," *LookSmart*, July 2, 2003, [http://www.findarticles.com/cf_dls/m0PJR/13_1/110307574/p1/article.jhtml].

[61] For more information about the GIG, see CRS Report RS21590, *Defense Program Issue: Global Information Grid, Bandwidth Expansion (GIG-BE)*.

Table 2. Global Information Grid (GIG) Systems Engineering and Support/T62, DII PE 0302019K.[62]

($ in Millions)

	FY2003	FY2004	FY2005 (est.)	FY2006 (est.)	FY2007 (est.)	FY2008 (est.)	FY2009 (est.)
GIG Systems Engineering	2.328	2.423	2.517	2.581	2.652	2.713	2.777

Air Force Advanced Tactical Targeting Technology (AT3). The AT3 system combines information collected by an airborne network of sensors to identify the precise location of enemy air defense systems. The system relies on coordination of information from different systems aboard multiple aircraft.[63]

Table 3. Sensor and Guidance Technology (AT3), PE 0603762E [64]

($ in Millions)

	FY2003	FY2004	FY2005 (est.)
Air Force AT3	11.023	5.815	0.0

Air Force Link 16. Tactical Data Links (TDLs) are used in combat for machine-to-machine exchange of information messages such as radar tracks, target information, platform status, imagery, and command assignments. The purpose of this program element is to insure the interoperability of Air Force TDLs. TDLs are used by weapons, platforms, and sensors of all services. Other TDLs include Link 11, Situational AwarFY2eness Data Link (SADL), and Variable Message Format (VMF).

---

[62] DISA RDT&E Budget Estimate, FY2005, R-1 Exhibit, Defense-Wide/07 R-2a, DII PE 0302019K, P.109,[http://www.defenselink.mil/comptroller/defbudget/fy2005/budget_justification/pdfs/rdtande/DISA.pdf].

[63] Hampton Stephens, "USAF Will Begin Air-Defense Targeting Demonstration In FY-04," June 27, 2003, [http://www.idga.org/iowa-robot/document.html?topic=196&document=30568].

[64] DOD Fiscal Year 2005 Budget Estimates, RDT&E Budget Item Justification Sheet (R-2 Exhibit) BA3, Defense Wide, February 2004, PE 0603762E, p. 338, [http://www.defenselink.mil/comptroller/defbudget/fy2005].

Table 4. Link 16 Support and Sustainment, PE 0207434F.[65]

($ in Millions)

	FY2003	FY2004	FY2005 (est.)	FY2006 (est.)	FY2007 (est.)	FY2008 (est.	FY2009 (est.)
Total PE Cost	50.535	70.481	141.012	218.743	228.009	161.909	153.606

Navy Cooperative Engagement Capability (CEC). The CEC system links Navy ships and aircraft operating in a particular area into a single, integrated air-defense network in which radar data collected by each platform is transmitted on a real-time (i.e., instantaneous) basis to the other units in the network. Each unit in the CEC network fuses its own radar data with data received from the other units. As a result, units in the network share a common, composite, real-time air-defense picture. CEC will permit a ship to shoot air-defense missiles at incoming anti-ship missiles that the ship itself cannot see, using radar targeting data gathered by other units in the network. It will also permit air-defense missiles fired by one ship to be guided by other ships or aircraft.[66]

Table 5. Develop and Test CEC, PE 0603658N [67]

($ in Thousands)

	FY2003	FY2004	FY2005 (est.)
Navy CEC	106,020	86,725	103,452

Army Force XXI Battle Command Brigade and Below (FBCB2). FBCB2, used with Blue Force Tracker computer equipment, is the U.S. Army's main digital system that uses the Tactical Internet for sending real-time battle data to forces on the battlefield. During OIF, this system was used in some Bradley Fighting Vehicles and M1A1 Abrams tanks, and effectively replaced paper maps and routine reporting by radio voice communication. The computer images and GPS capabilities allowed tank crews to use Blue Force Tracker to pinpoint their locations, even amid Iraqi sand storms, similar to the way pilots use instruments to fly in bad weather.[68]

---

[65] Department of the Air Force FY2005 Budget Estimates, RDT&E, Descriptive Summaries, Vol. II, BA4-6, Feb. 2004, [http://www.saffm.hq.af.mil/FMB/pb/2005/rdtande/RDT&E%20FY2005%20PB%20Volume%201.pdf].

[66] For more information, see CRS Report RS20557, *Navy Network-Centric Warfare Concept: Key Programs and Issues for Congress*.

[67] DOD Budget Fiscal Year 2005, RDT&E Programs (R-1), PE 0603658N, RDT&E Programs (R-1), February 2004, P. N-5, [http://www.defenselink.mil/comptroller/defbudget/fy2005].

[68] Frank Tiboni and Matthew French, "Blue Force Tracking Gains Ground," *Federal Computer Week*, vol.18, no.7, Mar. 22, 2004, p. 49.

Table 6. Develop and Test FBCB2, PE 0203759A [69]

($ in Thousands)

	FY2003	FY2004	FY2005 (est.)
Army FBCB2	59,887	47,901	23,510

Joint Tactical Radio System (JTRS). DOD has determined that future military radio frequency communications systems should be developed in compliance with the JTRS architecture. JTRS is a family of common, software-defined, programmable radios that will initially become the Army's primary tactical radio for mobile communications, including radios that are capable of communicating via satellite. The new JTRS devices will have routers built-in to support networks in the battlefield, with the capability to dynamically re-form communications links whenever one or more nodes or routers are interrupted.[70] Reportedly there is some disagreement among planners about whether the military should use laser-based communications or JTRS radio waves for the space-to-ground communications link. Currently, the military services use different radio waveforms that have yet to be made interoperable.[71]

Table 7. Develop and Test JTRS, PE 0604280 (A,N,F) [72]

($ in Thousands)

	FY2003	FY2004	FY2005 (est.)
Army JTRS	62,892	133,293	121,400
Navy JTRS	19,231	88,601	78,624
Air Force JTRS	13,667	38,096	49,856
Total: Army, Navy, Air Force	95,790	259,990	249,880

Joint Unmanned Combat Air Systems (J-UCAS). The J-UCAS program combines the efforts previously conducted under the DARPA/Air Force Unmanned Combat Air Vehicle (UCAV) program and the DARPA/Navy Naval UCAV (UCAV-N) program, for a common architecture to maximize interoperability.

---

[69] DOD Budget Fiscal Year 2005, RDT&E Programs (R-1), PE 0203759A, RDT&E Programs (R-1), Feb. 2004, p. A-10, [http://www.defenselink.mil/comptroller/defbudget/fy2005].

[70] Stephen Trimble, "Pentagon Adds 'Network Router' to List of JTRS Missions," *Aerospace Daily*, vol. 206, no 13, Apr. 17, 2003.

[71] Susan Menke, "$200 Billion: One Estimate of What DOD Must Spend to Go Net-Centric," *Government Computer News*, Mar. 2, 2004, [http://www.gcn.com/vol1_no1/daily-updates/25112-1.html].

[72] DOD Budget FY2005, RDT&E Programs (R-1), RDT&E Programs (R-1) , PE 0604280, Feb. 2004, pp. A-6, N-7,F-5, [http://www.defenselink.mil/comptroller/defbudget/fy2005].

Table 8. Prove the Basic Technological Feasibility of J-UCAS, Advanced Technology and Risk Reduction, PE 0603400D8Z.[73]

($ in Millions)

	FY2004	FY2005 (est.)	FY2006 (est.)	FY2007 (est.)	FY2008 (est.)	FY2009 (est.)
Risk Analysis	0.0	284.617	77.785	—	—	—

Table 9. Prove the Operational Value of J-UCAS, Advanced Component and Prototype Development, PE 0604400D8Z [74]

($ in Millions)

	FY2004	FY2005 (est.)	FY2006 (est.)	FY2007 (est.)	FY2008 (est.)	FY2009 (est.)
Development	0.0	422.873	667.307	380.105	1043.498	986.156

Other Nations and NCW Capability

Military organizations worldwide are creating responses to the challenges of information age warfare. Some countries, such as Sweden which uses the term Network-Based Defense, may view NCW concepts and the promise of more efficiency and effectiveness through networking with coalition partners, as a way to reduce military budgets.[75] Denmark, Norway and the Netherlands have all adopted the term Network Centric Warfare; Australia uses the term Network-Enabled Warfare; the U.K. uses the term Network-Enabled Capability; and, the armed forces of the Republic of Singapore uses the term Knowledge-Based Command and Control.[76] Observers have reported that units of the Chinese military have been using computer systems for on-line tactical simulation exercises. The simulation involved networking and multi-media presentations to train commanders and troops in an on-line classroom, where battles are fought using an "electronic sand table", and results are judged for scoring. Officers and troops could also exchange messages and share information via the

---

[73] DOD RDT&E Budget Item Justification, Appropriation/Budget Activity, Defense Wide RDT&E BA 4, PE 0603400D8Z, Feb. 2004, [http://www.defenselink.mil/comptroller/defbudget/fy2005/budget_justification/pdfs/rdtande/OSD_BA3/M-30603400D8Z_J-UCAS__R-2(co)_R-2a__Feb_2004.pdf].

[74] DOD RDT&E Budget Item Justification,Appropriation/Budget Activity, Defense Wide RDT&E BA 4, PE 0604400D8Z, Feb. 2004, [http://www.defenselink.mil/comptroller/defbudget/fy2005/budget_justification/pdfs/rdtande/OSD_BA4/ZE-40604400D8Z_J-UCAS__R-2(co)_2a(co)_R-3(co)_R-4(co)_4a__Feb_2004.pdf].

[75] Frederick Stein, Senior Engineer, MITRE Corporation, "Presentation on Network Centric Warfare Operations,"4th Annual Multinational C4ISR Conference, Mclean, Virginia, May 6, 2004.

[76] John Garstka, "Network-Centric Warfare Offers Warfighting Advantage," Signal Forum, *Signal Magazine*, May 2003,

network.[77] The NCW capabilities under development by other countries include technologies similar to what is described for joint U.S. forces in this report.

NATO is currently building a capability for dynamic interoperability with U.S. forces in the future and is developing a framework for high-technology warfare using the combined forces of multiple nations, called NATO Network Enabled Capabilities, similar to the U.S. military's Joint Vision 2020.[78] Other NATO initiatives for coalition operations include the Multinational Interoperability Program, the Cross System Information Sharing Program, and the Multi-functional Air-based Ground Sensor Fusion Program.[79]

NCW Technology in Recent Military Operations

OIF might be more accurately characterized as a transitional, rather than transformational operation, because NCW technology was not fully deployed in all units during OIF, and some systems were not user-friendly.[80] Some observers feel that OIF proved the effectiveness and potential of network enhanced warfare,[81] while others believe that it is hard to interpret the NCW experiences objectively, partly because the review process may sometimes be distorted by the internal military bias that favors force transformation. Still others point out that the latest experiences using NCW technology may be misleading because recent U.S. adversaries were weak and incompetent, including Panama (1990), Iraq (1991), Serbia (1999), and Afghanistan (2001).[82]

---

[77] Gao Zhongqi and Zhu Da, "Regiment of Nanjing MAC Improves Training Efficiency Via Network," *PLA Daily*, Feb. 5, 2004.

[78] "NATO Network Enabled Capability (NNEC), " Times staff, Mar. 3, 2003, "NATO Starts 'Transformation' Process," *NavyTimes.com*, Feb. 5, 2004, [http://www.navytimes.com/].

[79] Dag Wilhelmsen, Manager of NATO C3 Architecture, "Presentation on Information Sharing Effectiveness of Coalition Forces Operations," 4th Annual Multinational C4ISR Conference, McLean, Virginia, May 6, 2004.

[80] Some argue that OIF experiences validate Admiral Cebrowski's view that technology is not NCW, but rather only the enabler of NCW. Loren B. Thompson, CO Lexington Institute, "ISR: Lessons of Iraq," Defense News ISR Integration Conference, Nov. 18, 2003. See also CRS Report RL31946: *Iraq War: Defense Program Implications for Congress.*

[81] Lt. General William Wallace, Commander Combined Arms Center, in U.S. Congress, House Armed Services Subcommittee on Terrorism, Unconventional Threats and Capabilities, Hearing on Military C4I Systems, Oct. 21, 2003, [http://www.cq.com].

[82] Some traditional virtues such as air superiority, may be under emphasized. The review process may exaggerate the role of "jointness" and special operations, according to Loren B. Thompson, Analyst at the Lexington Institute, "ISR: Lessons of Iraq, Defense News ISR Integration Conference," Nov. 18, 2003. "The Iraqis made so many mistakes it would be foolish to conclude that defeating them proved the viability of the new strategy," Dan Caterinicia and Matthew French, "Network-Centric Warfare: Not There Yet," *Federal Computing Week*, June 9, 2003, [http://www.fcw.com/fcw/articles/2003/0609/cov-netcentric-06-09-03.asp].

Network Communications. Increased networking during OIF reportedly allowed U.S. forces to develop a much improved capability for coordinating quick targeting. In Operation Desert Storm in 1991, coordinating efforts for targeting required an elapsed time of as much as four days. In Operation Iraqi Freedom, U.S. forces reduced that time to about 45 minutes.[83] During April 2003, the Marine Corps Systems Command compiled comments from some soldiers about their experiences using several new communications systems during combat operations in Iraq. Comments from soldiers and other observers follow:

(1) Several communicators, operations officers, and commanders reportedly stated that they felt generally overloaded with information, and sometimes much of that information had little bearing on their missions. They stated that they received messages and images over too many different networks, requiring them to operate a large number of different models of communications equipment.[84]

(2) Some troops stated that when on the move, or when challenged by line-of-sight constraints, they often used email and "chat room"[85] messages for communications (This usually required linking to a satellite).

(3) Force XXI Battle Command, Brigade and Below (FBCB2), with Blue Force Tracker, reportedly received widespread praise from troops for helping to reduce the problem of fratricide. Blue Force Tracker (BFT) is a generic term for a portable computer unit carried by personnel, vehicles, or aircraft that determines its own location via the Global Positioning System, then continuously transmits that data by satellite communications. The position of each individual unit then appears as a blue icon on the display of all other Blue Force Tracker terminals, which were used by commanders on the battlefield, or viewed at remote command centers. Clicking on any blue icon would show its individual direction and speed. A double-click reportedly would enable transmission of a text message directly to that individual unit, via satellite.

Satellites. Satellite communications played a crucial role for transmitting message and imagery data during OIF operations, and also enabled a capability for U.S. forces in the field to "reach back" to the continental United States for support. However, a growing dependence on space communications may also become a critical vulnerability for NCW.

(1) During the OIF conflict, communications trunk lines, including satellite transmissions, were often "saturated", with all available digital bandwidth used up. The peak rate of bandwidth consumed during OIF was

---

[83] Dan Caterinicia and Matthew French, "Network-Centric Warfare: Not There Yet," *Federal Computing Week*, June 9, 2003, [http://www.fcs/com].

[84] Matthew French, "Technology a Dependable Ally in Iraq War," *Federal Computer Week*, vol. 18, no.8, Mar. 29, 2004, p. 46.

[85] John Breeden, "Bantu Sails with the Navy," *Government Computer News*, May 26, 2003, p. 1.

approximately 3 Gigabits-per-second, which is about 30 times the peak rate consumed during Operation Desert Storm in 1991. DOD satellites cannot satisfy the entire military demand for satellite bandwidth, and therefore DOD has become the single largest customer for commercial or civilian satellite services. DOD sometimes leases commercial satellite bandwidth through DISA, and at other times bypasses the process to buy directly from industry. However, bypassing DISA may reduce interoperability between the services, and may increase redundancies. [86]

(2) Commercial satellites were used to supplement military communications, which did not have enough capacity, despite the fact that a number of military satellites were moved to a better geostationary orbital position for both Afghanistan and Iraq.[87]

Radio Bandwidth and Latency. Some problems with delayed arrival of messages during OIF may have occurred due to unresolved questions about managing and allocating bandwidth. Sometimes, when demand for bandwidth was high, NCW messages with lower priority were reportedly dropped deliberately so that other messages with a higher priority could be transmitted.[88]

(1) The speed with which U.S. forces moved, a shortage of satellite communications, and the inability to string fiber nationwide hampered efforts to provide adequate bandwidth. At times, some commanders were required to share a single communications channel, forcing them to wait to use it whenever it became free.[89]

(2) Brigade-level command posts could view satellite and detailed UAV images, but battalion-level commanders, and lower command levels, could not view those same images. The lower-level commands are where greater detail is critical to fighting successfully.

(3) Although the Army has invested in military-only decision-support systems, some of the planning and collective decision-making during OIF was handled through email and chat-rooms that soldiers were familiar with, that

---

[86] Jefferson Morris, "GAO: DOD Needs New Approach to Buying Bandwidth," *Aerospace Daily*, Dec. 12, 2003 and "DISA Chief Outlines Wartime Successes," *Federal Computer Week*, June 6, 2003,

[87] Brigadier General Dennis Moran, U.S. Central Command/ J6, in U.S. Congress, House Armed Services Subcommittee on Terrorism, Unconventional Threats and Capabilities, *Hearing on Military C4I Systems*, Oct. 21, 2003, [http://www.cq.com] .

[88] U.S. Congressional Budget Office, *The Army's Bandwidth Bottleneck*, Aug. 2003, [http://www.cbo.gov], and Lt. General William Wallace, Commander Combined Arms Center, in U.S. Congress, House Armed Services Subcommittee on Terrorism, Unconventional Threats and Capabilities, *Hearing on Military C4I Systems*, Oct. 21, 2003, [http://www.cq.com].

[89] Matthew French, "Bandwidth in Iraq a Subject of Debate," *Federal Computer Week*, Oct.r 20, 2003, [http://www.fcw.com/fcw/articles/2003/1020/tec-iraq-10-20-03.asp].

were "user-friendly" and reliable, that were available when other systems experienced transmission delays, and that required little or no training.[90]

Air Dominance. UAVs sometimes carry thermal cameras that can see through darkness or rain. These reportedly gave military planners so much confidence when orchestrating raids, they often skipped the usual time-consuming rehearsals and contingency planning.[91] However, without early air dominance, UAVs and other Intelligence Surveillance and Reconnaissance (ISR) aircraft could not have been used to provide information needed for NCW systems. UAVs, and other support aircraft, such as refueling support tankers, were nearly defenseless and reportedly could not have operated deep in Iraqi air space without early air dominance.

Operations in Iraq with Coalition Forces. Using NCW technology with coalition forces resulted in reduced fratricide during OIF. However, during OIF, coalition assets reportedly operated as separate entities, and coalition forces were often locked out of planning and execution because most information was posted on systems accessible only to U.S. forces. For example, most major air missions, that supposedly used NCW technology for coalition operations, involved only U.S. aircraft.[92]

Policy for sharing of classified information requires a separate contract agreement between the United States and each coalition partner. DOD currently maintains 84 separate secure networks for NCW coalition operations; one for each coalition partner. This is because U.S. National Disclosure Policy restricts what information may be released to coalition partners.[93] In addition, each coalition partner nation has a corresponding policy for release of its own sensitive information. As a result of these policies, operations planning information was spread to coalition forces using a manual process, and the transfer of data fell behind combat operations.[94] A secure single network is required to efficiently share information among multiple partners, with a capability to dynamically add and subtract coalition partners. DOD has initiated a program called "Network Centric Enterprise Services" (NCES, also known as "Horizontal Fusion") to make information immediately available to any coalition partners who need it, while also providing strong security through network

---

[90] U.S. Congressional Budget Office, *The Army's Bandwidth Bottleneck*, Aug. 2003, [http://www.cbo.gov].

[91] "In Iraq, Soldiers Wage War Via Computer," *Baltimore Sun/A.P.*, Jan. 4, 2004.

[92] Lt. General Daniel Leaf, Vice Commander for U.S. Air Force Space Command, in U.S. Congress, House Armed Services Subcommittee on Terrorism, Unconventional Threats and Capabilities, *Hearing on Military C4I Systems*, Oct. 21, 2003,[http://www.cq.com].

[93] Each coalition partner must agree to protect classified military information that the United States shares with them. DOD Directive 5230.11, June 16, 1992, implements the October 1, 1988 "National Policy and Procedures for the Disclosure of Classified Military Information to Foreign governments and International Organizations," or the National Disclosure Policy, within the Department of Defense, [http://www.dtic.mil/whs/directives/corres/pdf/d523011_061692/d523011p.pdf].

[94] Meagan Scully, "Out of Touch: Policies, Technology Hindered Data-Sharing with Allies in Iraq," *ISR Journal*, vol. 3, no. 4, May 2004, p. .32.

encryption technologies and dynamic access controls.[95] However, this technical solution may not affect the differences in the individual policies that restrict information sharing among coalition partners.

Oversight Issues for Congress

Potential oversight issues for Congress pertaining to NCW include the following.

Sufficient Information for Effective NCW Oversight

Does Congress have sufficient information about the full scope of the Administration's strategy for implementing NCW to conduct effective oversight of this effort? Are programs critical for NCW adequately identified as such in the DOD budget? Does the Administration's plan for defense transformation place too much, too little, or about the right amount of emphasis on NCW? Is the strategy for implementing NCW paced too quickly, too slowly, or at about the right speed? Does the Administration's strategy for implementing NCW programs call for too much, too little, or about the right amount of funding? How are "network centric" items identified separately in the budget line items?

Sufficiently Joint NCW Planning

Is the Administration's strategy for implementing NCW sufficiently joint? Is there an overall DOD information architecture, or enterprise architecture? Do the current service network architectures — Army LandWarNet, Navy ForceNet, Air Force C2 constellation — allow systems to work together through the GIG, or do they enforce parochialism along service boundaries that is inconsistent with the Joint cyber environment?

Military Support for Transformation and NCW

What is the level of support within the military for the objectives of transformation and NCW? Observers reportedly state that flag officers, and technical officers at lower levels, both have a strong interest in being able to operate in an integrated manner and a net-centric environment.[96] However, a recent study concluded that while the strongest base of support for transformation is the senior

---

[95] Cheryl Roby, Deputy Secretary of Defense, OASD, NII, "Information Sharing Challenges in Coalition Operations," presentation at the 4th Annual Multinational C4I Conference, McLean, Virginia, May 4, 2004 and Matthew French, "Dod Blazes Trail for Net-centric Strategy," *FCW.com*, June 9, 2003, [http://www.fcw.com/fcw/articles/2003/0609/news-dod-06-09-03.asp].

[96] Brigadier General Marc Rogers, Director Joint Requirements and Integration Directorate/J8, for U.S. Joint Forces Command, in U.S. Congress, House Armed Services Subcommittee on Terrorism, Unconventional Threats and Capabilities, *Hearing on Military C4I Systems*, Oct. 21, 2003, [http://www.cq.com].

officers, the junior military officers do not see transformation as something that is important to them.[97]

Effects of NCW on U.S. Defense Spending

What are possible effects of NCW on the composition of U.S. defense spending? What other programs might have to be reduced to pay for NCW programs? Hardening high technology systems against possible threats from a technically sophisticated enemy is expensive. NCW systems that are not hardened may not perform well, or may be destroyed after a cyber attack, or an attack involving a directed energy weapon.

Networking with Coalition Forces

What are implications for future NCW operations with coalition forces and foreign countries? How well are coalition forces adapting to NCW? Is it possible to give Allies access to C4ISR information to improve collaboration during high-speed combat operations, while still protecting other information that is sensitive or classified? Will differences in the national disclosure policies for each coalition nation restrict sharing of necessary information among all partners during training operations, and if so, will this threaten the effectiveness of training? Will U.S. analysts or warfighters be overwhelmed by the vast increase in information that will flow if all coalition NCW networks are seamlessly linked to the U.S. NCW network? A subset of the same issues that affect DOD operations with coalition partners may also affect coordination with U.S. first-responders during domestic attacks by terrorists. Should DOD networks also be extended to first-responders who may need support during possible widespread attacks involving nuclear bombs or biological weapons; for example, geo-spatial images from UAVs monitoring domestic areas? Should policy allow domestic first responders to input or view important data during such an attack, even though some may not have clearances?

---

[97] Research by Mahnken and Fitzsimmons, 2003, measured attitudes of military officers in supporting the Administration's planned transformation process. The study argues that broad support within the officer corps is a key element in force transformation. Results indicated that (1) a majority of officers believed that tanks, manned aircraft, and aircraft carriers would still be important in twenty years, (2) a vast majority were unwilling to reduce current force structure in order to invest in new approaches to warfare, (3) officers were confident in the U.S. ability to deal effectively with threats, (4) officers were unclear about future military challenges and the requirements for a transformed force to deal with those challenges, and (4) that service affiliation remains the strongest determinant of officer attitudes. The study also concluded that the strongest base of support for transformation appears to come from the senior officer ranks, while the junior officers do not see transformation as something that is important to them. The study goes on to say that "the lack of a truly compelling rationale for major change, and the absence of an effort to market that rationale to the broad officer corps, suggest little reason for transformation's advocates to be optimistic." The study included focus groups and a survey of 1,900 students attending seven different U.S. military education institutions, such as the Naval War College. Thomas Mahnken and James Fitzsimmonds, "Revolutionary Ambivalence: Understanding Officer Attitudes toward Transformation," *International Security*, vol. 28, no. 2, Fall 2003, pp. 112-148.

Value of NCW Information

Is information overrated as an asset for NCW? How thoroughly has the administration studied the risks associated with data-dependent military doctrine? Several observers have argued that DOD plans for NCW stress only the rewards of information without including adequate analysis of the risks associated with possible over-reliance on data-driven systems. Some elite network centric corporations with state-of-the-art systems that offer "information superiority" have experienced perverse results, and sometimes even catastrophic economic losses (See Appendix B, Perverse Consequences of Data-Dependent Systems). Congress could encourage DOD to examine the economics of information in order to avoid similar perverse consequences on the battlefield that may be created by "information abundance."[98]

NCW Technology Transfer

Does the Administration's strategy pay sufficient attention to possible national security issues related to technology transfer? Technology transfer and offshore outsourcing may increase the number of foreign-nationals who are experts in newer Internet technologies and software applications (See Appendix A, The Transition from IPv4 to IPv6.)

Asymmetric Threats against NCW

Does the Administration's strategy for implementing NCW pay sufficient attention to asymmetric threats and growth of technology skills in other countries? How is DOD working with industry to find ways to protect software against cyber threats, including those possibly related to offshore outsourcing of R&D and information technology services? Several policy options that may reduce risk to the effectiveness of NCW due to growth of technology skills in foreign countries may include (1) encourage companies to maintain critical design and manufacturing functions inside the U.S., (2) encourage highly skilled individuals to relocate to areas in the U.S. where industries are in need of technical professionals, or (3) encourage U.S. high technology workers to update and increase their set of job skills.[99]

---

[98] Modern portfolio theory, Baysian analysis, and Monte Carlo simulation are quantitative tools that can be used to examine when and where the benefits of information transparency consistently outweigh the costs. Michael Schrage, "Perfect Information and Perverse Incentives: Costs and Consequences of Transformation and Transparency," Security Studies Program Working Paper, Massachusetts Institute of Technology, E38-600, May 2003.

[99] Paul J. Kostek, Chair American Association of Engineering Societies, "Globalization vs Outsourcing and Their Impact on Competitiveness," Oct. 30, 2003, [http://www.planetee.com/Forums].

Acquisition Strategies for NCW Technologies

Does the Administration's strategy for implementing NCW incorporate the right technologies and acquisition strategy? Future research into areas such as nanotechnology will likely lead to radically new innovations in material science, fabrication, and computer architecture. However, the basic research to develop new technologies requires high-risk investment, and increasingly involves international collaboration. To maintain a U.S. military advantage for NCW may require stronger policies that encourage education in science and high-technology, and that nurture long-term research that is bounded within the United States private sector, universities, and government laboratories.[100]

(1) Technologies: Is DOD making sufficient investments for R&D in nanotechnology? Nanoscience may fundamentally alter military equipment, weapons, and operations for U.S. forces, and possibly for future U.S. adversaries. Does the Administration's plan pay sufficient attention to creating solutions to meet bandwidth requirements for implementing NCW? Latency, which is often caused by a bandwidth bottleneck, is an important complaint of fighters, "once the shooting starts." How do messages that are either dropped, lost, or delayed during transmission alter the effectiveness of Network Centric Operations?

(2) Acquisition: All DOD acquisition programs require a key performance parameter for interoperability and for successful exchange of critical information.[101] Development of some weapons in the past has rendered them obsolete by the time they are finally produced, sometimes 15 to 20 years later. Admiral Arthur Cebrowski (retired), director of the Office of Force Transformation reportedly wants program development cycles brought in line with those of commercial industry, which are typically measured in months and years, instead of decades.[102] How does the traditional DOD long acquisition cycle keep up with new commercial developments for high technology?[103]

---

[100] Gerald Borsuk and Timothy Coffey, "Moore's Law: A Department of Defense Perspective," Defense Horizons, Center for Technology and National Security Policy, National Defense University, No. 30, July 2003.

[101] Lt. General Daniel Leaf, Vice Commander for U.S. Air Force Space Command, in U.S. Congress, House Armed Services Subcommittee on Terrorism, Unconventional Threats and Capabilities, *Hearing on Military C4I Systems*, Oct. 21, 2003, [http://www.cq.com].

[102] Keith Phucas, "The New Military: Proposing Change," *Norristown, Pennsylvania Times-Herald*, Nov. 28, 2003.

[103] The Army Science Board recently completed a study of high-risk technologies that will be developed as part of the Army Future Combat System (FCS) program. The study identifies 7 major technology areas that will be emphasized throughout the FCS incremental acquisition strategy: joint interoperability, network survivability, bandwidth efficiency, smart antennas, software, transparent battle space, and systems reliability, [https://webportal.saalt.army.mil/sard-asb/ASBDownloads/FCS-Exec-Briefing.pdf].

NCW Doctrine

Is DOD developing doctrine and training programs for NCW sufficient to keep pace with rapid changes in technology? NCW enables the military to fight with smaller units, moving rapidly using "swarming tactics". While smaller size combat forces supports DOD concepts for NCW, several critics have argued that some of the soldiers taken prisoner during OIF may have been spared if DOD had fielded a larger force.[104] Therefore, while NCW may enable swarming of smaller military units, it is not clear whether terrorists or other adversaries can use similar tactics even more effectively to counter some U.S. tactics. Does doctrine for NCW also stress civilian casualty prevention and protection, or does the goal of overwhelming force in minimum time overrule those policy choices? What are the changing requirements for finding and recruiting personnel who are qualified to operate high-technology NCW equipment? Finally, if terrorist groups become more local and smaller in size, will law-enforcement activities, coupled with good intelligence, displace military operations as a more effective pre-emptive strategy for the future, partly because it may be seen as less controversial?

Related Legislation

P.L. 108-136, The National Defense Authorization Act for Fiscal Year 2004. This act requires the Secretary of Defense to submit to Congress, in support of the Department of Defense budget for FY2006, a report on the activities carried out for the development of high-speed, high-bandwidth communications capabilities for support of network-centric operations by the Armed Forces. The report shall include the following: (1) A description of the joint R&D activities, and (2) An analysis of the effects on recent military operations of limitations on communications bandwidth and access to radio frequency spectrum. Reports shall also be submitted to the House and Senate Armed Services Committees for implementation of management for the JTRS program, and for development of the FBCB2 Blue Force Tracking System.

H.R. 3911: This bill proposes to make ineligible for the receipt of Federal grants, Federal contracts, Federal loan guarantees, and other Federal funding, any companies that have outsourced jobs during the previous five years to companies outside the United States, when those services were previously performed within the United States. Outsourcing for purposes of national security is exempted from this proposed legislation. On 3/4/2004, the bill was referred to the House Committee on Government Reform.

---

[104] Ralph Peters, "Shock, Awe and Overconfidence," *Washington Post*, Mar. 25, 2003, p. A. 9.

Appendix A

The Transition from Internet Protocol Version 4 (IPv4) to IPv6

The U.S. military now uses several transport protocols for digital communications, including Internet Protocol version 4 (IPv4). However, by 2008, DOD is planning to convert digital military communications to use the new Internet Protocol version 6 (IPv6) as the standard for all transmission through the Global Information Grid (GIG), and for all systems that are part of the Defense Information System Network (DISN) that will interoperate with the GIG. However, the transition from IPv4 to IPv6 may go more smoothly for the U.S. military and for the Internet infrastructure that supports global commerce in other countries, than for the commercial Internet infrastructure within the United States, which may continue using the older IPv4 protocol for a longer time because it is so firmly embedded.

Because the new communications infrastructures that support Internet technology in other countries will be built using newer equipment, much talent for managing IPv6 technology may eventually belong to many technicians and programmers who reside in countries where the United States may have political differences. Research has shown that regional agglomeration of technical expertise increases active sharing of tacit knowledge among groups of innovators.[105] Some of that tacit knowledge may also include sharing of information about newly-discovered vulnerabilities for the IPv6 technology.

What follows is a brief explanation of some technical differences between IPv4 and IPv6, and a discussion of possible economic and security issues related to the coming transition to the new Internet protocol.

Technical differences between IPv4 and IPv6. Information is sent through the Internet using packets (approximately 4000 digital bits per packet), and which include the address of the sender and the intended destination. Internet Protocol version 4 (IPv4) has been used globally since before 1983. However, IPv4 information packets are designed to carry an address in a 32-bit field, which means that IPv4 can only support approximately 4,000,000,000 Internet devices (computers, routers, websites, etc.). With Internet access expanding globally, and with more types of equipment now using Internet addresses (e.g. cell phones, household appliances, and PDAs) the number of Internet addresses needed for connected equipment could soon exceed the addressing capacity of the IPv4 protocol.

---

[105] Geographic concentration of information technology employment increases labor productivity among IT workers. Findings from research indicate that geographic proximity matters most where tacit knowledge plays an important role in the generation of innovative activity, and tacit knowledge does play an very important role during the early life cycle of an information technology system. Christian Le Bas and Frederic Miribel, "Is the Death of Distance Argument Relevant: The Agglomeration Economies Associated with Information Technology Activities," [http://www.ish-lyon.cnrs.fr/labo/walras/Objets/Membres/Miribelebas_paper.pdf], p. 20.

For example, slightly more than 3 billion of the 4 billion possible 32-bit IPv4 addresses are now allocated to U.S.-operated ISPs. In contrast, China and South Korea, with a combined population of more than 1.3 billion, are allocated 38.5 million and 23.6 million respectively. Therefore, Asian counties are especially interested in the possibilities that come with adoption of IPv6.

Internet Protocol version 6 (IPv6) quadruples the size of the address field from 32 bits to 128 bits (IPv1-IPv3, and IPv5 reportedly never emerged from testing in the laboratory). IPv6 could theoretically provide each person on the planet with as many as 60 thousand trillion-trillion unique Internet addresses. Theoretically, by switching to IPv6, humanity will never run out of Internet addresses. IPv6 is also believed to be more secure than IPv4 because it offers a feature for encryption at the IP-level.

However, several drawbacks may slow the global adoption of the IPv6 standard. Switching to IPv6 means that software applications that now use Internet addresses need to be changed. Every Web browser, every computer, every email application, and every Web server must be upgraded to handle the 128-bit address for IPv6. The routers that operate the Internet backbone now implement IPv4 via computer hardware, and cannot route IPv6 over the same hardware. By adding software to route IPv6 packets, the routers will operate more slowly, which may cripple the Internet. Alternatively, upgrading and replacing the hardware for millions of Internet routers would be very costly.

IPv4 also uses a technology feature called Natural Address Translation (NAT) which effectively multiplies the number of IP address that may exist behind any single firewall. This technology trick is widely employed within the United States, and its usage also adds an extra layer of security to both commercial networks and home PC networks that have a router. NAT allows a home user to connect multiple PCs to their home network, so they all can share a single IPv4 address behind the router/firewall. By using NAT, it is possible, and certainly much cheaper, to put off or ignore the problem of running out of IPv4 addresses. At least temporarily, in the United States, most technologists prefer sticking with NAT rather than switching over to IPv6.

Also, despite the new feature that allows IP-level encryption, there may be new security problems associated with converting to IPv6. Whenever new code is deployed onto computers, undiscovered bugs are usually soon discovered through study and repeated experimentation by hackers. Therefore, IPv6 is sure to hold security surprises that the designers have simply not found through extensive testing. And because switching over to IPv6 will be a global undertaking, some of the newly discovered security problems could possibly become critical, and even threaten the functioning of the Internet itself.

IPv6 also offers other technical advantages over IPv4. For example, IPv6 makes peer-to-peer communication between individual computers much easier than with IPv4. This will make applications like Internet telephony and next generation multi-media groupware work much more smoothly.

Technology Divide. The opportunity to leapfrog past older Internet technology may someday result in increased expertise in newer technology for technicians and engineers who reside outside the United States. For example,

countries such as India, North Korea, Iran, Pakistan, and Iraq that are now building new communications infrastructures for Internet commerce, may initially adopt the latest network switching equipment using the newer IPv6 technology, and thus leapfrog over IPv4.

Meanwhile, industries in the United States, which are already heavily invested in older IPv4 technology, may remain tied to IPv4 using the NAT technology for a longer time. This is because NAT can extend the useful life of older IPv4 applications, and can defer the cost of conversion by transferring that cost to the ISPs, who would then set up gateways to translate between all IPv4 and IPv6 Internet traffic going into and out of the United States. The U.S. could then become divided from the technology used in the rest of the world, at least for a while, by an IPv4/IPv6 difference that is similar to the U.S./metric divide we see today.[106]

Possible Vulnerabilities

U.S. military forces, to save time and expense, sometimes connect staff at multiple locations to the DOD secure SIPRNET network by using an encryption technique known as tunneling, which lets users traverse a non-secure network to access a top-secret one. For example, Marine Corps staff recently began using tunneling through the non-classified NIPRNET to extend the DOD classified SIPRNET to 47 sites in the Marine Forces Pacific Command.[107] However, during OIF as much as seventy percent of NIPRNET traffic reportedly was routed through the civilian communications infrastructure. This means that when there is need for a high volume of U.S. military communications, security may be partly dependent on reliability of IPv6 equipment found in the civilian infrastructure and in commercial satellites.[108]

Countries with emerging communications infrastructures, and purchasing the latest commercial network equipment, may also be the home countries of those best able to exploit IPv6 technical vulnerabilities. If this includes countries where the United States may be involved in military activity, hostile groups with appropriate technical knowledge of IPv6 vulnerabilities may be positioned to attempt to interfere with U.S. military communications.

---

[106] Simson Garfinkel, "The Net Effect," Jan. 7, 2004, [http://www.simson.net/pubs.php].

[107] Dan Caterinicia, "Marines Tunnel to SIPRNET," *FederalComputerWeek*, Dec. 9, 2002, [http://www.fcw.com].

[108] Christopher Dorobek and Diane Frank, "Dod May Pull Key Net from the Internet," *InsideDefense*, Dec. 26, 2002, [http://www.insidedefense.com].

Appendix B

Perverse Consequences of Data-Dependent Systems

The Office of Force Transformation [http://www.oft.osd.mil/] has indicated that DOD must continue to refine the rules and theory of network centric warfare through simulation, testing, and experimentation. This section describes that although some experiences have shown that networking may increase certain advantages in warfare, other experiences may also indicate that relying on information systems can sometimes lead to unexpected results.

Information-Age warfare is increasingly path-dependent, meaning that small changes in the initial conditions will result in enormous changes in outcomes. Speed is an important characteristic for NCW because it enables a military force to define initial conditions favorable to their interests, and then pursue a goal of developing high rates of change that an adversary cannot outpace.[109] To this end, whenever data-links are employed between military units and platforms, digital information can be shared and processed instantaneously, which produces a significant advantage over other military units that must rely on voice-only communications.

Examples that illustrate this advantage are found in several training exercises conducted in the 1990's between Royal Air Force jets equipped with data-links, referred to as Link-16, and U.S. Air Force jets with voice-only communications. A series of air-to-air engagements showed that the RAF jets were able to increase their kill ratio over the U.S. jets by approximately 4-to-1. Other training engagements, involving more than 12,000 sorties using 2-versus-2, or 8-versus-16, aircraft showed that jets equipped with Link-16 increased their kill ratio by 150 percent over those aircraft having voice-only communications. Similar results were seen in training exercises involving Navy and Army units equipped with new networking technology.[110]

However, some observers believe that important military decisions may not always lend themselves to information-based rational analysis.[111] They argue that the military services, national security establishment, and intelligence community have not thoroughly studied the risks associated with a data-dependent military doctrine.

Issues raised by these observers include the following:

---

[109] Dan Caterinicciа and Matthew French, "Network-centric Warfare: Not There Yet," *Federal Computer Week*, June 9, 2003, [http://www.fcw.com/fcw/articles/2003/0609/cov-netcentric-06-09-03.asp].

[110] John Garstka, "Network-Centric Warfare Offers Warfighting Advantage," Signal Forum, *Signal Magazine*, May 2003.

[111] Martin Burke, *Information Superiority Is Insufficient To Win In Network Centric Warfare*, Joint Systems Branch, Defence Science and Technology Organisation, 2001, [http://www.dodccrp.org/events/2000/5th_ICCRTS/cd/papers/Track4/024.pdf].

(1) Information flows may be governed by a diminishing marginal utility for added effectiveness. Quantitative changes in information and analysis may lead to qualitative changes in individual and organizational behavior that are sometimes counter-productive.

(2) An information-rich, opportunity-rich environment may shift the value of the information, redefine the mission objectives, and possibly increase the chances for perverse consequences.

In 1999, large-scale army experimentation with better visualization of the battlefield resulted in surprises such as requests for up to five times the normally-expected amounts of ammunition. Instead of concentrating on only critical targets, the experimental army units were overwhelmed with the vast array of potential targets they could now see. The unprecedented requests for larger quantities of ammunition caused logistical failures. More information did not assure better decision-making, but rather it exposed doctrinal flaws.[112]

A similar effect was observed in later experiments conducted as part of the Network Centric Operations Conceptual Framework. Ammunition was expended at a faster rate, possibly because more information creates a target-rich environment. These observations imply a possibly greater demand for logistics support.[113]

Issues raise by other observers of data-driven systems are:

(3) Reliance on sophisticated information systems may lead to management overconfidence.

(4) Different analytical interpretations of data may lead to disagreements among commanders about who is best situated to interpret events and act on them.

The past economic under-performance of many hedge fund organizations and other technology firms that have employed very sophisticated network centric management techniques may serve as examples to caution DOD against over-reliance on data-driven military information systems. For example, Long-Term Capital Management (LTCM), a highly-leveraged multi-billion dollar hedge fund, and Cisco Systems, a well-respected high-tech firm, both used sophisticated systems to track market conditions and expand their data-driven "situational awareness" to gain and maintain competitive advantage. However, in 1998 a U.S. government-led consortium of banks bailed out LTCM after its trading losses put the entire world's financial system at risk of meltdown. Also, in 2001 Cisco was forced to take a $2.25 billion inventory write-down. While there is yet no professional consensus explaining

---

[112] Robert R. Leonhard, *Principles of War for the Information Age*, (Novato, CA: Presidio Press, 2000) p. 156, and p.224.

[113] Dr. Kimberly Holloman, Evidence Based Research, Inc., "The Network Centric Operations Conceptual Framework," Presentation at the Network Centric Warfare 2004 Conference, Washington, D.C., Jan. 20, 2004, [http://www.oft.osd.mil/library/library.cfm?libcol=2].

these poor performance problems, many analysts agree that the presumed excellence of information systems may have invited managerial over-reliance, and that over-reliance led to overconfidence. Executives may have ignored unambiguous external signals in favor of their own networked data.[114]

Finally, some believe that more information imposes a higher degree of accountability on actions. Failure to minimize casualties or protect civilians may be digitally reviewed and used to politicize flawed military decisions.

These observers suggest that modern portfolio theory, Bayesian analysis, and Monte Carlo simulation are three quantitative tools that military decision makers should explore if they want the benefits of information transparency to consistently outweigh its costs. These tools could answer questions, such as: (a) if information were to be managed as a portfolio of investment risks much as asset classes like equities, fixed income, and commodities, how would commanders diversify to maximize their returns; (b) what information asset classes would they deem most volatile; (c) what information would they see as most reliable; and (d) which information classes would be co-variant, and which would be auto-correlated?[115]

---

[114] Michael Schrage, "Perfect Information and Perverse Incentives: Costs and Consequences of Transformation and Transparency," Security Studies Program Working Paper, Massachusetts Institute of Technology, E38-600, May 2003, p.4.

[115] Michael Schrage, "Perfect Information and Perverse Incentives: Costs and Consequences of Transformation and Transparency," Security Studies Program Working Paper, Massachusetts Institute of Technology, E38-600, May 2003, p.15.