THE CHALLENGE AND PROMISE OF NETWORK-CENTRIC WARFARE

Mr. John Luddy
Adjunct Fellow

February 2005

1600 Wilson Boulevard, Suite 900
Arlington, VA 22209
Tel : 703.522.5828 Fax : 703.522.5837
www.lexingtoninstitute.org mail@lexingtoninstitute.org

THE CHALLENGE AND PROMISE OF NETWORK-CENTRIC WARFARE

Mr. John Luddy

EXECUTIVE SUMMARY

In recent years the 'Revolution in Military Affairs' has given way to 'Transformation' as the guiding rationale for most U.S. national security developments. Since the late 1990s, the ability to wage "network-centric warfare" has become identified as a goal of transformation. Both terms are broad enough to be used, and abused -- imprecise and sometimes grandiose language has led some to see "network-centric" as part strategic panacea, and part silver bullet. Its reality and potential are each more complicated.

Network-centric warfare (NCW) now has a track record. Practical application in Afghanistan and Iraq has given analysts enough data and experience to begin to evaluate its successes, weaknesses, and prospects for improvement. These first clashes in the war on terror have shown that NCW works. Albeit against markedly inferior military forces, American forces were able to integrate information and communications systems and procedures to accomplish more with less, and faster, than would have been possible even a decade ago. Sorties per target destroyed; speed of the "target observed-target destroyed" sequence; relatively little collateral damage; aggregate numbers of U.S. forces required -- by these and other measures, both conflicts show that NCW is the right objective for American military planning.

By their very nature, and especially in the early going, major shifts in orientation are always more about challenges, risks, and shortfalls than about smooth, flawless implementation. As expressed in unit-level after-action reports, top-level Defense Department reviews, and numerous outside analyses, it is clear that the promise of NCW is accompanied by a range of challenges. Understanding, resolving, and accounting for these challenges will enhance NCW as a tool in America's war on terror.

THE CHALLENGE AND PROMISE OF NETWORK-CENTRIC WARFARE

Mr. John Luddy

INTRODUCTION

Networking amounts to getting the right information, faster, to the right forces -- who in turn can take the right action, faster, against the right objective. It shortens what is often called the 'kill chain' -- detect, decide, attack, assess -- and reduces the amount of resources required to move through each link. This is how the Pentagon's Office of Force Transformation describes network-centric warfare:

> *NCW represents a powerful set of warfighting concepts and associated military capabilities that allow warfighters to take full advantage of all available information and bring all available assets to bear in a rapid and flexible manner. The tenets of NCW are:*
>
> - *A robustly networked force improves information sharing.*
> - *Information sharing enhances the quality of information and shared situational awareness.*
> - *Shared situational awareness enables collaboration and self-synchronization, and enhances sustainability and speed of command.*
> - *These, in turn, dramatically increase mission effectiveness.*

The goal of network-centric operations (NCO) is to enable forces to accomplish their objectives more efficiently: faster; with fewer troops in harm's way; and with fewer and lighter weapons and other equipment to bring to, sustain, and maneuver in the battlespace. With timely and accurate intelligence, commanders can decide faster, deploy a force of the optimal size and characteristics, command and control that force better, and stay one step ahead of enemy forces. Network-centric operations can improve all of these functions.

In early October 2001, not quite a month after the 9/11 attacks on the World Trade Center, the Pentagon and in Pennsylvania, U.S. and British ships and aircraft introduced the 21st century (and the Taliban) to network-centric operations. With a striking blend of old and new technology, operating throughout the electromagnetic spectrum and across the range of operations, from ground forces to air and sea platforms and into space, U.S. forces in both conflicts used networked information to achieve huge efficiencies in combat. The "kill chain" against enemy targets was reduced in many cases from hours to minutes, and information about the location of enemy and friendly forces was relayed and tracked just as quickly. In Afghanistan, the deployment of American ground troops was minimal; in Iraq, a force one-quarter the size of the 1991 Desert Storm coalition defeated the Iraqi regime in 21 days, with only 161 troops killed in action. In both theaters, the incidence of civilian casualties and other collateral damage was minimal.

It is risky to draw too many conclusions from the Coalition's success against Taliban and Iraqi troops, simply because both adversaries were inferior in every way. One does not slight the American warfighter to observe that this was not a close fight between evenly-matched forces. In military parlance, enemy forces created very little "friction" and "fog" for U.S. Central Command (CENTCOM) to contend with during major combat operations. Yet as the ongoing conflict in both theaters makes clear, NCO may improve what technology already does, but it cannot do things technology cannot -- such as occupy ground, protect patrolling troops from exploding mines and improvised explosive devices, or give skittish locals the feeling of security they need to come out and vote. Key aspects of leadership and the "art of war," such as intelligence, training, and command initiative, can be assisted by a network, but they cannot be replaced by one. Likewise, while network-centric operations are sustained by information and data, they have not reduced combat leadership to a process of quantitative calculations. In short, as a technology-based process, networking can neither replace, nor succeed without, many other less tangible, human aspects of waging war.

NETWORK-CENTRIC WARFARE IN ACTION: EXAMPLES

Small ground units, strategic bombers, precision weapons = close air support. One lingering image from Afghanistan illustrates NCW's potential, even when using old technology: a Special Forces soldier on horseback sends targeting data from his laptop computer to a 40-year old B-52H Stratofortress, which delivers a devastating blow to massed Taliban forces in less than 20 minutes. In operations against the Taliban and Iraqi forces, B-52s and other aircraft were armed with the Joint Direct Attack Munition (JDAM), a 2000-pound bomb with a receiver that uses in-flight updates from Global Positioning System satellites to strike within a few feet of their aim points. Special Operations Forces on the ground used binoculars equipped with laser range finders to determine a target's exact location, and then transmitted precise coordinates to the bombers above them. Bomber crews could then program JDAMs and deliver them to targets within minutes of identification.

This ability to network real-time cueing from maneuvering ground forces and a range of other sensors to the aircraft and, in turn, to the bombs themselves, put massive, accurate, and close-in fire support at the disposal of U.S. and Coalition troops. Often the enemy was hit with lethal and accurate firepower, not from an armored division and thousands of U.S. troops, or massed formations of aircraft, but by handfuls of soldiers transmitting electrons to a single aircraft. Strikes that took hours to coordinate in Desert Storm a decade earlier were carried out in Afghanistan and Iraq as quickly as 45 minutes from the time a target was identified. Many carrier-based strike missions were not even targeted until the aircraft were underway.

Long-range UAVs, controlled from afar = strategic intelligence, surveillance and reconnaissance (ISR). Flying at altitudes of up to 60,000 feet, at high speed, the Air Force's experimental, high-flying, long-range Global Hawk unmanned aerial vehicle (UAV) provided constant coverage of wide areas of territory and added significantly to the

imagery provided by satellites and other surveillance aircraft. With its synthetic aperture radar, electro-optical camera, and infrared (IR) and other sensors, Global Hawk saw through most environmental and battlefield conditions, and provided thousands of images for use in bomb damage assessment, fire support, and general reconnaissance.

From a networking standpoint, Global Hawk showed two especially unique capabilities: it was controlled through a communications network based from ground stations thousands of miles away, in Europe and California; and it flew not only pre-planned flight paths, but also in real time to locations as required by various missions. Global Hawk continues to fly responsive border surveillance missions in Iraq, providing closer follow-up reconnaissance when other assets point to suspicious activity.

Responsive UAVs, in support of maneuver forces. The lower-altitude Predator UAV played a network-centric role by linking with RC-135 Rivet Joint, U-2, and E-8C Joint STARS ground surveillance aircraft to enhance the battlefield picture for commanders. The Predator's radar and IR sensors allowed it to see through bad weather and at night. Its video capability allowed it to transmit live images to command centers, other aircraft, or tactical controllers on the ground. These features made it invaluable to reconnaissance and maneuver forces engaged in combat with a moving enemy, or aircraft seeking to locate mobile targets. They also allowed the Predator, like Global Hawk, to add considerably to the overall battlefield picture available to commanders.

Predator's unique network-centric contribution was in serving as "eyes and ears" for maneuvering ground forces. For example, in March 2002, Special Operations teams in Operation Anaconda in Afghanistan were linked directly to Predators, which they used to essentially "walk point," identifying possible enemy locations or conversely, indicating when the way ahead was clear. By networking with Predator, forces could move faster than if they had been forced to deploy their own scouts to detect threats in their path, and could better employ supporting fires during their advance.

Operational Shortcomings

Although the successes and great potential of the network-centric approach are evident in Afghanistan and Iraq, there were still blind spots, capability gaps, and outright mistakes; including fratricide, undetected and missed targets, and civilian collateral damage. Weaknesses in network-centric operations lay at each end of the operational spectrum -- at the strategic level, the Department of Defense (DoD) has acknowledged that, although network-centric linkages functioned over large areas and time-spans, there was no overarching "network" that continually linked operations throughout each theater.

Many aircraft had no on-board ability to transmit and receive satellite communications, forcing them to rely on links to the E-3 Airborne Warning and Control System (AWACS). In general, the continuing inability of various sensor platforms to communicate with each other, with strike platforms, and with command centers was a major obstacle to achieving comprehensive and reliable network-centric operations. At the tactical level, there were notable instances of fast and accurate supporting fires (B-52s and B-1s with JDAMs) and immediate and responsive reconnaissance (Predator), but communications to and among

ground units were often hampered by a lack of bandwidth over which to transmit signals. (This was true in Afghanistan even though DoD had purchased all available commercial satellite communications bandwidth in the region prior to attacking the Taliban.)

There was wide variance among ground units in the types and quality of their communications equipment, which not only hampered their ability to communicate with each other at times, but forced commanders to consider this incompatibility when assigning missions to different units. Where true networking existed, the efficiency and effectiveness of American forces improved notably, but they were not networked everywhere or always. Thus, while ground forces -- even individual troopers -- served as excellent "sensors" feeding into the overall operating picture for commanders, a complete picture often did not flow as well back to the field. This may be the single biggest flaw in NCW developments to date: senior commanders are inundated with information while maneuver commanders get too little operationally useful information, or they get it too late or not at all. Technology gaps; glitches inherent in all information technology systems; insufficient training; all these factors contribute to the problem. Fortunately, these shortcomings were not disastrous, especially against unsophisticated foes; just as fortunately, they have provided real-world tests that can help guide further progress.

THE WAY AHEAD

Because the conflicts in Afghanistan and Iraq demonstrated the promise of networking, lessons learned in these conflicts are shaping policy, organization and procurement decisions throughout the U.S. military establishment. Today analysts grade the performance of technology, weapons, command structures and entire departments on their ability to conduct and contribute to network-centric operations.

Defense-wide Initiatives

Secretary of Defense Donald Rumsfeld established the Office of Force Transformation (OFT) soon after the 9/11 attacks, in October 2001. Noting the positive effects of networking in the conflicts in Afghanistan and Iraq, OFT in 2003 issued "Transformation Planning Guidance" for the Services to use as they adapt procurement and organizational activities to a 21st century network model. Though far from complete, a network-centric focus now runs through many of the plans and activities of the Services. Throughout 2004, OFT conducted case studies across a range of operations and training exercises to examine the ways in which networking can improve various aspects of warfare. Air-to-ground, ground-to-ground, maritime, information, and special operations are each being studied. The results of these studies appear to validate network-centric operations and should help to guide subsequent networking developments.

In addition to developing common plans and operational concepts for NCW, DoD faces an ongoing challenge in developing interoperable systems, and bringing them on line at the same time. The Joint Staff's new Force Capability Board tracks network-oriented programs across individual service acquisition systems, identifies cases where funding or

capability levels are mismatched, and then advises the Joint Staff's Joint Requirements Oversight Council so that these issues can be addressed in the budget process.

The Defense Department has several communications initiatives underway designed to link equipment of forces across service lines and operational mediums. The Global Information Grid (GIG) is a joint effort to allow for integrated, interoperable, network-centric and knowledge-based warfare for the Services. Each Service contributes its own network architecture -- for example, the Navy's ForceNet and Air Force's ConstellationNet (discussed below) -- to form the combined grid. By 2008, DoD plans to establish Internet Protocol version 6 as the standard for transmission on the GIG, which will allow information on more units, individuals, and equipment to transit the Internet, and in more secure message format. With advanced fiber-optic and switching technology, GIG should help to meet U.S. forces' enormous and growing demand for frequency bandwidth.

The Transformational Communication System is an effort to establish virtually unlimited bandwidth capacity, which will allow distributed secure communications in a layered (ground and space) network. At the user-equipment level, the new Joint Tactical Radio System will develop a family of affordable, high-capacity, interoperable and scaleable tactical radios to provide both line-of-sight and beyond-line-of-sight C4I capabilities to warfighters.

U.S. Joint Forces Command (JFCOM)

From the warfighter perspective, DoD has focused its major network-centric developments at Joint Forces Command, which has responsibility for organizing, integrating, and training joint forces that then fight under command of the regional combatant commands (such as CENTCOM). JFCOM has particular focus on information technology concept development and experimentation. By shaping military standards and designing common architectures, JFCOM seeks to improve the level of interoperability and assimilation of common information technology tools.

Since the Services still retain acquisition authority for actual hardware, JFCOM works closely with the combatant commands, the Services, and defense agencies to set future joint requirements prior to acquisition decisions. JFCOM is also attempting to bridge the looming gap in networking capabilities between U.S. and international forces. This year, JFCOM conducted an experiment with major allies (Australia, Canada, the United Kingdom and Germany), in an effort to resolve policy and procurement obstacles to future coalition information sharing.

Air Force

With recent conflicts' emphasis on ISR and long-range strike, the Air Force has a full slate of network-oriented programs and improvements underway. The lessons from these conflicts have fueled a new push for better and more varied UAV options. Predator will continue to be armed with Hellfire air-to-ground missiles, and with a new "Small Diameter Bomb" weapon now in development. Also planned are datalinks embedded into new and existing ordnance -- such as the Small Diameter Bomb, Joint Air to Surface Standoff

Missiles and Joint Standoff Weapon -- so that individual weapons will have their own internet address to which ground forces can connect to control them.

The Air Force has also taken a range of institutional steps to better organize for network-centric operations. The service created the position of Deputy Chief of Staff for Warfare Integration, and has established an Air Force Command and Control, Intelligence, Surveillance and Reconnaissance Center (AFC2ISRC). This center maintains a Technology Transition Office to monitor transformational developments outside the Air Force, and an Experimentation Office that conducts wargames and other experiments to review and validate doctrine, operations and platform integration.

This summer, the AFC2ISRC conducted Joint Expeditionary Force Experiment 2004 with the Army to develop better connections between air and ground operations. Out of this exercise came an Air Force plan for establishing a layered network-centric architecture by 2020. Called "ConstellationNet," it will serve as the Air Force piece of the GIG, and will include a variety of satellite and airborne surveillance and command and control (C2) platforms, linked to combat aircraft, unmanned combat air vehicles, and support aircraft. The nerve center of ConstellationNet will be the E-10A Multi-sensor Command and Control Aircraft (MC2A) which will provide targeting and battle management command and control. ConstellationNet will be interconnected by the Link 16 datalink system, which provides real-time, jam-resistant secure transfer of digital communications, navigation, and identification information across a shared communication link, giving all those on the network the same real-time situational awareness.

Navy

The Navy's "ForceNet" is a strategic, conceptual effort intended to capture all aspects of network-centric operations and serve as the Navy's part of the GIG. This approach links sensors, weapons, command and control, and people to other Navy and joint forces. As with other network-centric efforts, ForceNet attempts to combine information, weapons systems, and units to effect rapid and decisive action. At the same time, ForceNet serves as the organizing principle for the Navy's evolving doctrine for network-centric operations. Naval Network Warfare Command is the organization implementing ForceNet for the fleet, and setting the future parameters of network connectivity that new weapons systems and upgrades must meet.

Whereas ForceNet embodies Navy networking in the broadest sense, the Navy's cooperative engagement capability (CEC) is an approach specifically to defensive operations that has been in development for several years. It is designed to link legacy and new platforms alike, binding sensors, fire-control, and weapons systems together into a defensive network for theater air and missile defense, and ship self-defense missions. It collects sensor data from a range of systems, and exchanges that data itself -- not set tracks, which are harder to coordinate -- among fire-control systems and weapons platforms across an entire force. This data set, collected from more sources, thus creates a clearer target 'track;' the track itself can be provided to a platform (an Aegis destroyer, for example) which can launch an interceptor missile even if the launching ship has not tracked the target itself. This makes more interceptors available, more quickly, from more platforms.

Reflecting DoD's interest in joint and multi-functional networking, CEC is intended to expand into a Joint Composite Tracking Network (JCTN), which will include the Patriot, Terminal High Altitude Area Defense, and AWACS sensors in the CEC network. Ultimately, CEC/JCTN could form an essential part of the GIG, extending a larger defensive net over maritime, air and ground forces.

Army

The Army is approaching network-centric operations with a broad plan, a specific networking concept for technology, and some specific technologies, all developing simultaneously. Looking ahead, the "Objective Force" is the Army's plan for organizing, manning, equipping and training forces for the future. These forces are intended to be more lethal, survivable, and sustainable across a wide range of military operations from major theater wars to counterinsurgency and counterterrorism missions.

As with other network-centric approaches, much of the Objective Force effort rests on technology. Working jointly with the Defense Advanced Products Research Agency and an industry team, the Army has embarked on the "Future Combat Systems" (FCS) program to identify promising systems and technologies, and the best ways to integrate platforms and soldiers into the Objective Force. A network of sensors, platforms, and command-and-control links, connected with high-bandwidth, high-speed communications, will provide maneuver units and individual soldiers the accurate and timely situational awareness they need. The Warfighter Information Network-Tactical (WIN-T) will be the communications backbone of the FCS. The WIN-T network will provide mobile, secure, multimedia C4ISR support capabilities to tactical information systems across the battle area.

In Operation Iraqi Freedom, the Force XXI Battle Command Brigade and Below "Blue Force Tracker" gave commanders the locations of some friendly forces, thereby helping to avoid friendly-fire incidents. During operations in Iraq, hundreds of the laptop-sized Blue Force Tracker units replaced paper maps and routine radio checks as a real-time, accurate method to maintain common situational awareness among rapidly-moving ground forces. In a promising example of joint information sharing, U.S. Marine and other coalition forces were provided with a number of Blue Force Tracker systems and were in turn able to connect to the Army network.

The Role of Industry and Congress

Operations in Afghanistan and Iraq have shown industry that networking works, as well as where it can be improved. With network-centric doctrine and policy taking hold, Pentagon planners -- and budgets -- are encouraging more investment in interoperability. Companies are now working with JFCOM, their Service customers, and each other to make the systems they develop better able to network. They are aided by the Department's gradual move away from a conservative requirements-based procurement process toward a more flexible and aggressive capabilities-based approach. Capabilities-based procurement encourages innovation by allowing system integrators to include network-enabling technology as it becomes available.

JFCOM has challenged industry to build systems with as much non-proprietary technology as possible. One welcome and innovative industry development has been the creation of an organization designed to foster common technology standards and protocols across different companies. The Network Centric Operations Industry Consortium, established September 2004, includes 30 of the largest defense contractors. By identifying and recommending operating standards, it aims to encourage technology that can be shared, or is at least compatible, across different companies' products.

Congress has shown increasing interest in network-centric operations. In the summer of 2003 -- one year into the operations in Afghanistan and Iraq -- Congress passed the Fiscal Year 2004 Defense Authorization Act, which included a provision requiring the Secretary of Defense to report to Congress on the military's activities in the area of high-speed, high-bandwidth communications in support of network-centric operations. The report is due Spring 2005, when the Pentagon's Fiscal Year 2006 budget request arrives on Capitol Hill. It is required to include analyses of joint research and development activities, and the effects on military operations of limited communications bandwidth. Congress has supported, and even increased, the Defense Department's requests for research and development spending across the defense budget.

OUTSTANDING ISSUES

The network-centric paradigm is an enormous step forward in military thinking. But future enemies are going to find ways to defend against networked forces, and even the best network cannot solve or avoid every challenge U.S. forces will face. Growing reliance on network-centric operations should not blind the U.S. military and DoD to its inherent technical, operational, strategic and cultural limitations. Regardless of the particular weapons and other systems that emerge during this process, several broad objectives must be pursued.

Technical Limitations

Bandwidth is the information-carrying lifeblood of any network, and network-centric operations devour signal bandwidth. As technology proliferates and expectations for information "right now" increase, network-centric operations will constantly require more and more communications bandwidth. This means that the Services and industry must make constant efforts to manage bandwidth more efficiently, with better communications technology, and with command-and-control systems that are better able to prioritize and manage signal flow.

Because networks begin with sensors, they will always be vulnerable to jamming by moderately sophisticated foes. Even the least capable enemy will be able sometimes to use deception or concealment to foil sensors, particularly with the coverage gaps that currently exist. An adept opponent may find ways to attack the networks themselves. Because technology is always vulnerable, and frequently fragile, networks must be tough, flexible and redundant.

False or incomplete technical information can distort or impede network effectiveness. Since most sensors and communications links run through space platforms or aircraft, networked operations have benefited from the freedom of action U.S. air dominance provides. Space-based sensors and communications assets today face no significant anti-satellite (ASAT) threat. Should surface- or air-to-air threats be present, and in the likely eventuality that ASAT threats emerge, network operations may become suddenly vulnerable. Even now, active jamming efforts and other interference can threaten the flow of information.

As battle lines become blurred in a fast moving conflict or an insurgency, one of network-centric operations' greatest weaknesses -- the ability to distinguish friend from foe -- will become even more difficult. "Persistent" (day/night, all-weather) coverage from space based systems like Space-Based Radar (SBR) will narrow these gaps, but it will be several years before SBR and aircraft together are able to provide nearly persistent coverage over large areas of operations.

Operational Limitations

From a commander's perspective, more information generally is better than less. However, a somewhat ironic difficulty can arise when commanders at different levels became inundated with information from different sensors and sources. Information may become intoxicating, turning tactical challenges into quantitative equations and distracting commanders from such basic military principles as initiative and decisiveness. Too much information may cause commanders to 'tune out.' Ultimately, the appropriate information -- not just data -- must be matched to the differing requirements of tactical commanders and theater commanders.

Networks allow for collaborative planning throughout the chain of command, which can develop more effective plans faster. But the same collaboration allows senior level commanders to micromanage. Military operations rely on a properly functioning chain of command, where commanders at each level have a manageable span of control and can focus on operations at their appropriate level. As real-time battlefield information passes before senior commanders, there will be a temptation to over-direct small units and lose focus on broader objectives. One of the U.S. military's greatest strengths is the initiative of small-unit commanders; if these commanders grow accustomed to centralized control from above, they may grow hesitant and indecisive.

As forces become more accustomed to high-quality, real-time information, there is a risk that they will be hesitant or even paralyzed without it. For example, networking enabled some remarkably responsive close air support in Afghanistan and Iraq, and raises expectations for conflicts in the future. But because technology can and will fail, our military must have an ongoing commitment to mastering basic soldiering skills -- such as map-and-compass navigation, communications and the accurate verbal call for fire support -- even when the optimal 'network' is not there to facilitate them. DoD and the Services must also be able to compensate when forces show up without connectivity with the network, or lose it during operations.

Strategic Limitations

Network-centric operations can make information flow faster, and forces operate more efficiently. But there are aspects of strategy that have little to do with speed and efficiency. In fact, the drive toward using fewer and lighter forces could place network-centric operations in direct conflict with important strategic objectives. In every conflict, there is a tradeoff -- or at least a sequence -- between striking and destroying targets, and seizing and holding ground. "Strike" forces are generally ineffective as "stability" forces.

Current operations in Iraq illustrate that efficient, lethal light and medium forces may kill targets and topple an enemy, but securing a peaceful outcome -- the war's strategic objective -- requires the presence of ordinary troops and heavy armor. In most of Iraq, U.S. strategic interests are being achieved by relatively low-tech means. This is not an argument against network-centric operations, but it does suggest that they may do very well in the initial stages of a conflict while being marginally useful in achieving the conflict's larger strategic objectives.

Cultural Limitations

Network-centric operations require technology, but they ultimately rely on people and organizations. As technology improves, the military must make similar advances in its institutions, processes, and culture. Analysts and practitioners alike agree that the human aspects of military operations -- training, doctrine, and leadership development -- still need to change.

Training. In a network-centric campaign, system operators are more closely engaged in tracking, supporting and controlling the forces actually in combat. To be most effective, these 'rear-echelon' operators must see frontline forces as more than arrows and symbols on a screen. They must be trained to understand what combat elements are experiencing. Personnel at all levels must enhance their fluency with the data and hardware that hold the network together, both to make the best use of various network capabilities, and to troubleshoot or work around glitches that surely will occur. Military forces in the field should become comfortable with relying on "reachback" capabilities, such as C4ISR systems whose controllers may reside in CONUS, and who may even be commercial providers. With small units and even individual troopers fully participating in the C4ISR loop, sufficient C4ISR training must extend far lower in the chain of command, to even the most junior ranks. While U.S. forces operate jointly to a great extent today, greater networking will bring even greater jointness. As the Pentagon seeks to develop common systems and links across the Services, joint communications and operations training must keep pace.

Doctrine. By making the military forces more flexible, precise, and rapid, network-centric capabilities enable most traditional military operations to happen more efficiently. In Afghanistan, networking presented new ways to use traditional tools -- for example, using heavy bombers in close-air support missions. In the next major conflict, networks will present options that we cannot predict today, and they will also create methods of shaping the strategic environment short of actual hostilities that have yet to be imagined. In and of

itself, connectivity presents opportunities to apply people and technology differently -- this will in turn cause doctrine and tactics to change more rapidly than in the past. All of this will challenge military doctrine to keep pace, so that leaders' awareness of, and aptitude for, networking matches the tools at their disposal. From Service academies and career-level schools, to specialized courses and on-the-job-training, the doctrine that guides military operations must be thorough enough to include networking as it is, and flexible enough to capture new military applications as they develop.

Leadership. As with any military concept, the success of network-centric operations will depend on leadership. It requires a commitment to change, and forceful direction, to bring disparate Service interests and functional areas (space, air, sea and land) together to function through a common network. As they try to blend common systems, from command-and-control to acquisition, leaders must innovate and foster innovation in their subordinates. Having the entire chain of command networked together will present tempting opportunities to scrutinize their subordinates' every action, but leaders will have to find the right balance between leadership and micromanagement. Above all, leaders must function while awash in information. Managing huge amounts of real-time information -- the obvious product of a more networked force -- will test leaders' ability to operate with speed and decisiveness. The least tangible but most important test of network-centric warfare will be whether or not the right information, to the right degree of detail, gets to commanders and units at the appropriate level, and in the right period of time. Even when it does not, maneuver commanders must keep focused on what they need to know to act, and theater commanders will need to keep their broad strategic objectives from being lost in mountains of detail.

Intelligence

Network-centric operations depend on comprehensive intelligence collection, management and analysis. The greatest limitation facing NCW is the constant challenge to get actionable intelligence. One widely noted shortfall in recent operations was the lack of persistent (day/night, all-weather) battlespace sensor coverage. More and better UAVs will improve this situation, as will more capable sensor suites on manned aircraft such as the Navy's P-3C Orion and the Air Force's E-10A MC2A. Ultimately, a constellation of SBR satellites will provide the most significant sensor improvement in decades -- but the Pentagon still has to prove that SBR can be integrated with other assets, tasked effectively and responsively by warfighters, strategic analysts and planners, and acquired on a realistic schedule and budget. Finally, no advance in technology or its efficient use can compensate for inadequate human intelligence (HUMINT). In the drive toward increased network-centric operations, and better and faster sensors, the need for accurate HUMINT should not be neglected.

Networked Coalitions

As the U.S. defense establishment increases its network-centric focus, the failure thus far of even the most technologically advanced allies to do likewise could prove a serious obstacle to the success of future coalition efforts. A number of nations -- Sweden, Denmark, Norway, Australia, and the United Kingdom -- are exploring networked operations in one form or another. Sweden has transitioned its forces to a network-centric

organizational concept, and the United Kingdom and France have acquisitions underway that fit a network-centric model. But these efforts are very limited. Coalition members are transitioning to providing "niche" capabilities rather than trying to match the U.S. system for system. Future coalitions will have to incorporate varying levels of technological sophistication, and account for it in training, exercises, doctrine and resources. If U.S. forces become unable to reliably communicate with allied militaries, the current assumption that a coalition effort will be more politically viable (and save U.S. lives and treasure) could be turned on its head -- U.S. leaders might well be justified in fighting alone.

This dilemma must be avoided. The United States must make every effort to encourage its allies to pace their network-centric modernization with its own, perhaps with carefully constructed joint ventures between U.S. and foreign companies. A "NATO standard" for communications protocols and software would be a good start. From there, procurement and deployment benchmarks should be established.

Acquisition Reform

Ironically, the most daunting obstacle to achieving a fully networked force is the same acquisition process that will make it possible. There is general consensus that platforms and systems must be joint, interoperable, and built as much as possible around common technology. In reality, industry, Service and Congressional priorities will surely clash from time to time.

For the U.S. military to continue its progress toward a network-centric way of war, Congress must be an active and constructive partner. Congress must move more aggressively to support policies and enact budgets that help to shorten procurement cycles, and adopt capabilities-based acquisition for as many systems as possible. Individual members must resist political pressure to protect legacy programs from changes or even termination, because those changes may be necessary to produce network-capable systems.

Many aspects of the procurement process work to discourage industry from adopting network-centric thinking. Traditional single-Service procurement leads companies to develop and sell equipment in relative isolation with little concern for interoperability. Systems built by different manufacturers are often unable to communicate and share data. Companies also have legitimate concerns about exposing proprietary technology and information to their competitors.

Both Congress and industry must be willing to expose their processes, technology, laws and regulations to new thinking, and reform each where necessary. The Secretary of Defense, with White House backing, must continue to bring vision and leadership to bear as a unifying force in the acquisition process.

CONCLUDING OBSERVATIONS

Much of what needs to get done to advance network-centric warfare is underway. Most military leaders, DoD civilians, industry leaders and analysts appear to understand the potential, and the remaining challenges, they face. Estimates vary as to the amount of time DoD will need to field a fully networked force. Optimists suggest that comprehensive network-centric operations will be possible four to five years from now, during the middle years of the Fiscal Year 2008 Future Years Defense Plan 2008-2012, which many observers believe will reflect the Bush Administration's comprehensive plan for "transformation." Others suggest that it will take a decade or two before the government and the industrial base adapt sufficiently. Certainly it is in the nature of transformation that the process will never be complete, even after network-centric operations are the norm.

Network-centric operations were applied unevenly, and imperfectly, in Afghanistan and Iraq, but those campaigns have validated the concept's potential. They have provided real-world learning opportunities to correct gaps, fix problems, and chart a course before U.S. forces are tested again, by potentially far more capable adversaries. While these victories do not validate "network-centric operations" as *the* reason for success, there is no doubt that networking has vastly improved U.S. operations. American forces were able to integrate information and communications systems and procedures to accomplish more, with less, and faster, than would have been possible against a similarly capable enemy even a decade ago. In the speed with which U.S. forces covered great distances, the efficiency and flexibility with which targets were destroyed, the rarity of collateral damage, the relatively small coalition force required, and the opponents' astonishingly unequal casualty rate -- these and other metrics show that enhancing NCW is a worthy objective for American military planning.

John Luddy is an Adjunct Fellow at the Lexington Institute. From 1995 to 2002, he served as national security aide to three U.S. Senators and in the Office of the Secretary of Defense. He is president of Vector Solutions, a defense consulting company based in McLean, Virginia.