CHAPTER 12
Military Service Overview
Elihu Zimet and Charles L. Barry

MILITARY CYBERPOWER is the application of the domain of cyberspace to operational concepts to accomplish military objectives and missions including humanitarian assistance and disaster relief (HA/DR); achieve stability, security, transition, and reconstruction (SSTR); and influence operations, as well as warfighting. Military operations such as administration, personnel management, medical care, and logistics are also enhanced with cyber tools. The growth in information technology and cyberspace has provided the military with new capabilities but has also provided new challenges, including balancing the need for new operational concepts to meet increasingly important military missions that now include appropriate and balanced use of soft and hard power with the need to jointly structure the military to accomplish these missions, including the connectivity to coalition partners. Unintended risks and vulnerabilities, especially the increased dependence of the military on civilian cyberspace capabilities, products, and services, need careful assessment to be effectively managed.

This chapter begins with a broad introduction to military cyberpower and a discussion of military operational constructs including information operations (IO), influence operations (mostly soft power), network-centric operations (NCO), intelligence operations, and the normal business and administrative use of cyberspace, followed by a discussion on military networks. Next is an overview of steps taken throughout the Department of Defense (DOD) to achieve joint network integration across the Services. Following this is an overview of current Service positions and approaches to cyberpower. The chapter concludes with observations on the DOD Global Information Grid (GIG), which is the principal common network backbone for the Services in the implementation of NCO.

Two points are made upfront. First, the growth and globalization of cyber-space technology and the corresponding need for adaptive information-based operational concepts to meet new military missions that include the use of both hard and soft power, from warfighting to HA/DR and SSTR, form the basis of the need for a military cyberpower strategy. The need to jointly structure the military to perform these operations and accomplish these missions, including the connectivity to coalition partners, provides an enduring challenge. Operational concepts such as the effectiveness of NCO in irregular warfare scenarios are still being tested.

Second, a single comprehensive network architecture designed to promote maximum connectivity and user pull based on an open commercial backbone will need separation from the secure connectivity required for sensor-to-weapon operations. The development of the GIG, the Combined Enterprise Regional Information Exchange System (CENTRIXS) program for information exchange among combined allied forces, and new technology initiatives is poised to address the issue of comprehensive networks, but not all technology objectives of these programs may be met, and vulnerabilities may exist. In the meantime, the military requires secure closed (separated) networks as well as fully connected open networks. The military also needs to wrestle with existing legacy systems to integrate them into the GIG, to leave them as standalone systems, or to terminate them.

The possession of accurate and timely knowledge and the unfettered ability to distribute this as information have always been a sine qua non of warfighting. As cyberspace has developed—particularly in the area of networked computer- based information systems such as the Internet,[1] global cellular-based networks with text messaging, personal digital assistants such as the Blackberry, and global satellite and cable networks (including radio and TV)—its impact on military operations has transformed operational concepts such as NCO and IO with the addition of new tools and procedures. In parallel with, indeed almost outpacing, the development of cyberpower in the military has been the global impact of cyberspace on all the levers of power (diplomatic/political, information, military, and economic) as well as the empowerment of individuals and groups and states. The Internet has also provided a "virtual safe haven" for nonconventional threats for the military including nonstate actors, terrorists, and criminal groups.

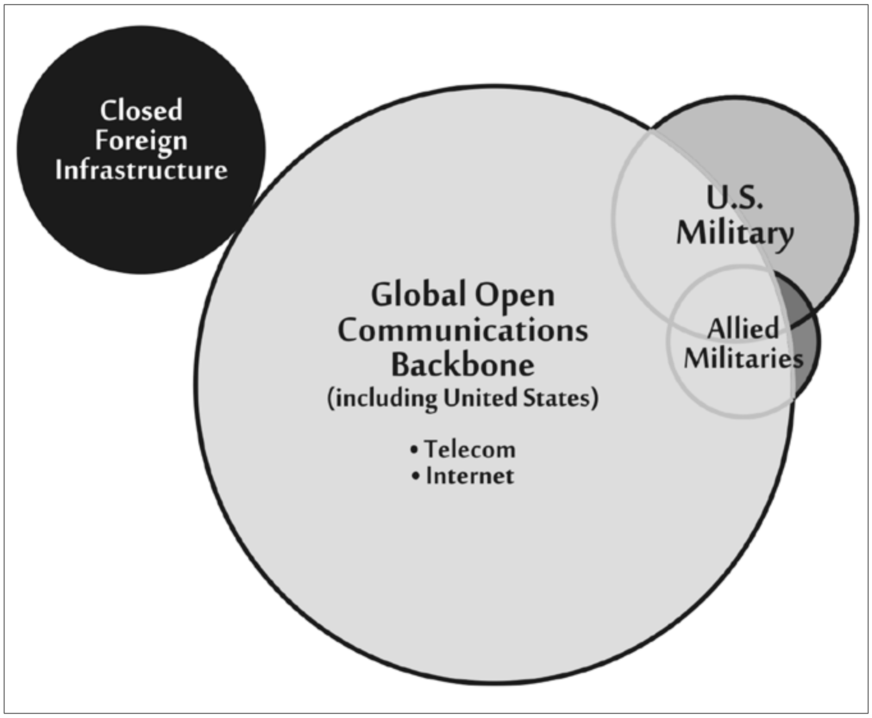
In the post–World War II industrial era, U.S. military superiority was structured on industrial strength; superior technology in platforms, weapons, and command, control, communications, computers, intelligence, surveillance, and reconnaissance (C^4ISR); and a robust military infrastructure. As we have moved from the industrial to the information age, however, the diffusion of information technology has tended to change some of the parameters of warfighting, and not always to our advantage. Precision weapons and NCO have given the United States a decided advantage on the battlefield, but in irregular warfare, we have had setbacks. While the United States was the developer of the cyberspace infrastructure, it is now open and available to all who possess the means to access it. The concepts of NCO and IO are also readily available, although there is a high cost of entry in developing significant capabilities. Cyberspace is a tool amenable to asymmetric warfare because it can be used anonymously, so deterrence and retribution are difficult; its immediate effects are nonlethal, so the risk of escalation is reduced. Cyberspace can also cause lethal effects (for example, by disrupting control systems, causing things to blow up) in IO as well as NCO. For example, a computer network attack on an unprotected supervisory control and data acquisition control system of a power plant could lead to catastrophic damage to power generators and transformers.

Cyberspace has become a pillar of our national (and international) infrastructure. The military owns its tanks, ships, and aircraft but it has only limited impact on the commercially provided connectivity (such as fiber optics and satellites) that the information superhighway depends upon. Figure 12–1 characterizes the communications backbone for connectivity.

The military use of the communications backbone of cyberspace falls into three regions on this chart. The military is a general user of the global communications backbone. Due to the risks and vulnerabilities inherent in operating in an open architecture, the military has its own specific secure networks for warfighting, as shown in the shaded area outside the large circle, but it also uses networks that rely on commercial connectivity where the military controls the nodes, access, and traffic on the networks (the area of overlap of the military and the open network, for example, the Secret Internet Protocol Router Network and Secure Telephone Units). The area of overlap between the U.S. military and allied militaries represents information exchange between combined forces and the joint combat commands region to region for global operations. A single, common, global, multinational data network is being developed as the CENTRIXS program. Security technology to allow information exchange among separate, simultaneous communities of interest across common network transport remains a significant challenge.

While the military establishment and the defense industrial base have been subjected to continuous probing, disruptions, and hacking attacks, the concepts and impact of cyberwar are only now being developed in terms of military organization, operational concepts, joint doctrine, rules of engagement, and training and education.

Figure 12-1 Cyberspace Connectivity



A considerable volume of literature continues to be produced on both the structure and implications of military cyberpower. This chapter attempts to link the capabilities enabled by cyberspace to both military missions and operational concepts. The military domain of cyberspace is characterized in two broad regimes that often require different attributes. The first regime is an open network in which collaboration, information-sharing, and situational awareness are principal measures of performance and connectivity is an essential driver. While operating within the timelines of an enemy is still essential, more latency in information transmittal is usually tolerated than in a sensor-to-shooter engagement, and shared knowledge gains in importance relative to speed of operations. The second regime employs closed, secure networks in which speed of operation, assured delivery, and integrity of information are paramount.

The concept of an open or closed network as used in this chapter is at best an abstraction in that these terms are really reference states and do not exactly correspond to actual employed networks. In fact, open networks are usually capable of supporting some secure transmissions, and some closed networks use the communications backbone. An open network is defined here as one that is open to any user who wants to dial in or log on. Security is usually provided by password protection, encryption, and computer and network protection tools. The principal measures of performance are connectivity, availability, and bandwidth. The Internet and telecom are examples (although not all of the Internet is open, and the communications backbone is also used for secure transmissions). A closed network has access by only designated nodes and is air-gapped from open networks. Principal measures of performance for closed networks are security, availability, and assuredness. An example of a closed network is the Joint Worldwide Intelligence Communications System.

Structure of Military Cyberpower

Military cyberpower is defined here as the application of operational concepts, strategies, and functions that employ the tools of cyberspace to accomplish military objectives and missions. Often, cyberpower is employed in support of operations in other domains such as maritime operations. However, at times joint cyberpower will be employed to prevail against an opponent in a contest wholly within cyberspace itself.

In order to develop this definition further, military cyberpower is represented as a pyramid in figure 12–2, where it is seen conceptually as resting on the foundation of cyberspace.

The base of the triangle is the domain of cyberspace including types of networks (open and closed) and their required attributes. Concepts such as the use of hard and soft power are broadly related to the appropriate use of networks in cyberspace for specific military missions. The second level of the triangle that is enabled by cyberspace is military cyberpower operational concepts, strategies, and functions that include NCO and IO but also the administrative function of operations including, for example, logistics, planning, training, procurement, and personnel. The apex of the triangle is “cyber-power: military missions” involving the use of cyberpower in prosecuting phase zero to phase five operations in the joint campaign plans.

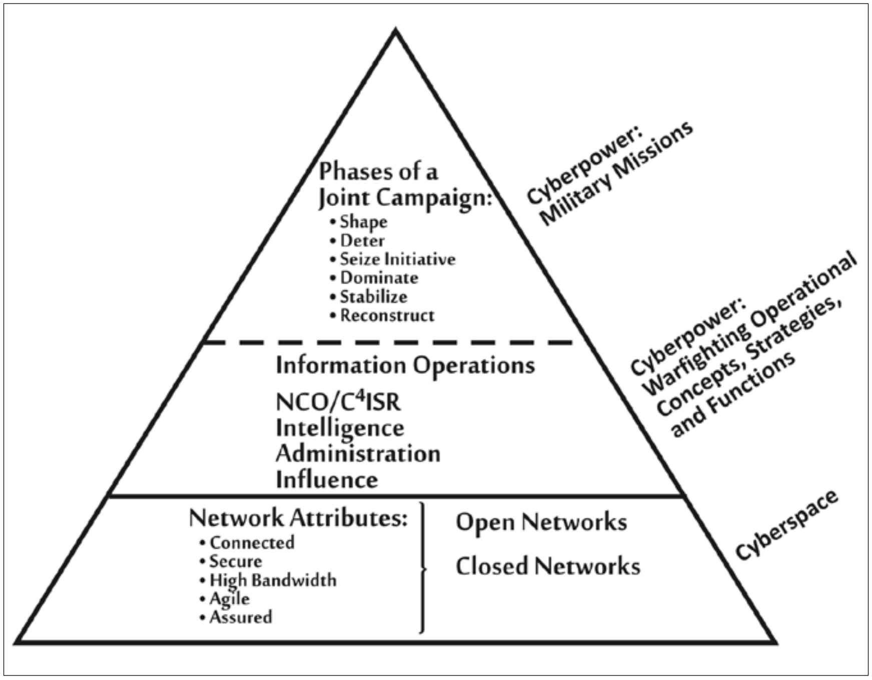
Military Missions and Joint Campaign Plans

The metrics for military effectiveness are the achievement of objectives and the execution of missions. The particular framework to examine the role of cyberpower in executing military missions chosen for this discussion is taken from the six phases (phase zero to phase five) of the joint campaign planning process.[2] This planning process now covers a campaign from prehostilities to reconstruction and is at the strategic rather than tactical level of objectives. Two caveats in the use of the joint campaign phases need to be mentioned. The first is that the phases are not entirely dissimilar from each other.

For example, phase two, “seizing the initiative,” and phase three, “decisive operations,” have much in common in terms of tactics and techniques. The second caveat is that the phases overlap in time as in a “three-block war”[3] in which full-scale military action, peacekeeping, and humanitarian assistance take place simultaneously within three city blocks. Despite these caveats, the phases are useful in showing the appropriate and balanced use of soft and hard power with the appropriate uses of cyberpower at each phase:

- phase zero, shaping countries at strategic crossroads
- phase one, deterring aggression
- phase two, seizing the initiative and assuming freedom of action
- phase three, performing decisive operations and achieving full spectrum superiority
- phase four, transitioning to stability operations and establishing security (including civil security and the rule of law) and restoring essential services
- phase five, engaging in reconstruction and enabling civil authority.

Figure 12-2 Military Cyberpower/Cyberspace Support to Operational Concepts, Strategy and Functions



Military Cyberspace Operational Constructs

The Capstone Concept for Joint Operations (CCJO) broadly describes how future joint forces are expected to operate across the range of military operations in 2012–2025 in support of strategic objectives.[4] In order to enable accomplishment of its particular objectives, the CCJO defines three fundamental actions taken by the joint force:

- establishing, expanding, and securing reach (this includes virtual reach through the use of cyberspace, as well as physical and human reach)
- acquiring, refining, and sharing knowledge
- identifying, creating, and exploiting effects.

For the objectives of this chapter and the exploration of military cyber- power, the above operations and actions are translated into the enabling (and synchronizing) hard power and soft power cyberspace concepts that support them. These are:

- information operations
- NCO, a transformational warfare concept whose scope, doctrine, and technologies are still under development and whose broad utility is still subject to debate. The debate on the effectiveness of NCO is discussed in chapter 11 in this volume, “Military Cyberpower.”
- normal and routine business and administrative functions using cyberspace-based tools

- intelligence operations using cyberspace-based tools
- influence operations using cyberspace-based tools.

Information Operations

Information operations comprise electronic warfare (EW), psychological operations (PSYOPS), computer network operations (CNO), military deception, and operations security.[5] In turn, CNO includes computer network attack, computer network defense, and computer network exploitation. Capabilities that support IO include information assurance, physical security, physical attack, counterintelligence, and combat camera. There are also three military functions: public affairs, civil military operations, and defense support to public diplomacy specified as related capabilities for IO. The relationship of IO to cyberpower is not straightforward due to the eclectic nature of IO as well as the support and related capabilities. Some elements of IO such as EW might be considered in the realm of conventional weapons. PSYOPS, however, is integrated in cyberpower influence operations, while the other elements of IO are supportive of both hard and soft power.

Network-centric Operations

Network-centric operations represent 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 concepts of network-centric warfare (NCW) were originally applied to hard power concepts, in particular strike warfare and air defense, but, taken broadly, can also be applied to other mission areas and the appropriate and balanced use of soft power and hard power. As a comparison, an Australian view of NCO is provided by Fewell and Hazen, who define *network-centric warfare* as:

> the conduct of military operations using networked information systems to generate a flexible and agile military force that acts under a common commander's intent, independent of the geographic or organizational dis- position of the individual elements, and in which the focus of the Warfighter is broadened away from the individual, unit or platform concerns to give primacy to the mission and responsibilities of the team, task group or coalition.[6]

While this definition is consistent with U.S. definitions, there is concern that in the implementation of NCO by our allies (many of whom have tailored versions of NCO), the ability to fight jointly may be compromised by nonintegrated technologies and different command and control structures. In order to head off such eventualities, DOD engages in a number of cooperative forums on interoperability with our most dependable allies, such as the North Atlantic Treaty Organization (NATO) and the cluster of so-called five eyes fora—the American, British, Canadian, and Australian Armies Standardization Program, the Multinational Interoperability Council, the Combined-Communications Electronics Board, and others. A main theme for most of these interoperability groups is multinational command and control, or determining the technologies and procedures for common information-sharing.

The tenets of NCO as articulated by DOD are that:

- 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.[7]

While fairly broad in nature, these tenets imply military operations in which the principal measures of performance relate to an enhanced speed of operations and function within an opponent's observe-orient-decide-act loop. These tenets are compatible with the elements of IO in that both embrace cyberspace and deal with military operations, yet their taxonomies are quite different, with IO structured by operations and NCO defined by capability. Alternatively, IO is characterized by functionality while NCO is identified with speed of operations, connectivity, shared decisionmaking, and effectiveness. It is fair to question whether, if NCO is the enabling concept of military cyberpower, the military is best organized to utilize this growing facet of modern warfighting and has the tools to be agile, execute, and adapt.

Business and Administrative Functions

Normal and routine business and administrative functions are cyberspace-dependent components of military operations that deal with administrative rather than warfighting and SSTR dimensions. This bureaucratic element of operating the military includes the planning, programming, budgeting, and execution cycle; logistics; training and education; medical care in the field and ashore; procurement; and personnel actions and records. The principal metrics for business and crisis response networks apply here with a strong emphasis on security and information assurance.

Intelligence Operations

Intelligence operations are a major military responsibility that relies heavily on cyberspace for information retrieval and information processing and dissemination—right place, right person, right time, and right quality.

Influence Operations

Influence operations have grown in importance as the military mission set has expanded to include nation-shaping, stabilization, and reconstruction and the threat set has expanded to include counterinsurgency. The United States must now deal with the multilateral nature of the modern world rather than the two- superpower world of the past.

Service Visions and Implementation

DOD Goal of Integrating Services

Military networks, beginning with the earliest connectivity technologies— telegraph, telephone, radio, and now the Internet and private intranets—have followed Service and agency organizational structures and funding channels, connecting users along organizational lines: Service staffs with agency staffs, field units with higher headquarters, and the Pentagon with all of its subelements.

As the potential of cyberspace blossomed, DOD was getting serious about genuine joint integration across all the Services, and jointness was soon coupled with the concept of net-centric operations. Service-oriented networks had to blend into a DOD-wide capability. Successive Office of the Secretary of Defense (OSD) and Joint Staff strategic documents have called for more and better joint interoperability and networks, culminating in the drive for network- centric operations and warfighting as the emergent core of U.S. military strategy. The rapid growth and convergence of information and telecommunications technologies offer significant opportunities for creating network-enabled joint operational capabilities.

Achievement of DOD-wide network integration and operational netcentricity is a work in progress, with DOD on the cusp—perhaps just the leading edge—of that transition. Most of the communications and data exchange— strategic, operational, and tactical—in Iraq, Afghanistan, and elsewhere remains hierarchical, push broadcast, system constrained, and user limiting. Investment in modern computing and telecommunications systems alone will not create the desired transformation, which will require a far more capable global backbone, unrestrained information-sharing among commands, and truly interoperable networks wherein every authorized user can access directly and instantly any information or other user on the network. With unrelenting dedication of resources and commitment and some luck, DOD may see that goal become a reality in a decade or so.

DOD's bureaucratic processes, procedures, and organizational culture have not evolved as quickly as technology to take full advantage of the potential for network integration and interoperability. Significant Service centered cultural and programmatic biases remain, and they reinforce one another as obstacles to collaborative investments in cross-department networking capabilities. However, it is a mistake to attribute parochialism to the military departments alone; the OSD staff, Joint Staff, agencies, and combatant commands (COCOMs) all seek to protect their own organizational priorities. Breaking down such barriers is the greatest challenge to networking all of DOD.

The scope of the network integration enterprise is huge. DOD data systems are comprised of approximately 3.5 million computers running thousands of applications over some 10,000 local area networks on 1,500 bases in 65 countries worldwide, connected by 120,000 telecom circuits supporting 35 major network systems over 3 router-based architectures transmitting unclassified, secret, and top secret level information—and that is just the fixed site profile. The most important and technologically challenging networks are those of the warfighters—deployed sea, air, land, special operations, and space forces performing missions around the world—and their supporting intelligence networks.

DOD divides its networking enterprise into three mission areas: business, operational, and intelligence. Intelligence networks are not wholly managed by DOD but are shared with other intelligence agencies. DOD business network integration arguably is equally as important as operational integration, yet it enjoys comparatively little attention. Most analysis concentrates on operations, the core of NCO.

DOD has made considerable progress toward joint networking, overcoming much parochial resistance and bureaucratic inertia and many technological obstacles along the way. Sustained emphasis on joint education, a wealth of commercial experience, and the Internet's ubiquitous presence in everyday life have been major factors in propelling a cultural shift toward broader sharing and collaboration and the breaking down of old paradigms. Most members of the military, including its leaders, demand to be connected 24/7/365 to whatever systems and users they believe essential to their mission—irrespective of parent Service, agency, or allied nation.

Across DOD, numerous commands, staffs, agencies, and contractors are committed to the goal of integrating command, control, communications, and computers (C^4) capabilities. Many billions of dollars have been spent, and ultimately hundreds of billions will have been invested. A lot of network integration is already in place, although it is still mainly *within* the Services and Defense agencies and along hierarchical lines. Incompatibilities abound. There is less progress across joint forces, especially at the tactical level. The networking and global connectivity that does exist is local. Few mobile users at the tactical level enjoy reliable, sustained Internet-based enterprise services such as real-time intelligence. However, primary joint networks do exist and have become the strategic and operational backbone of deployed forces. The interoperability goal is recognized and accepted, but as budgets tighten, all Services can be expected to cling first to internal priorities rather than joint integration when it comes to information technology (IT) and telecommunications investments. That resistance will be dampened by the forcing mechanism of essential connectivity, which drives commanders to insist on joint architectural standards so they can be continuously and reliably "plugged in" with whomever and wherever required.

Key obstacles to network integration include an unwieldy standards process, limited investment in enabling or replacing Service legacy systems, residual Service parochialism, independent-minded COCOMs, a noncollaborative culture across the officer corps, and the fact that DOD is still very much on the front end of a long timeline. Bringing the requisite technologies, processes, and systems into being will take a lot more time and investment.

In sum, DOD will get there, though budget pressures seem destined to slow progress in network integration as elsewhere. The main—and usually unrecognized—obstacle is time. It simply will take at least another 10 years of hard work, intense investment, and strong top-down emphasis before full net- centricity and network integration are achieved.

Network Integration Management at DOD

Two principal staffs driving network integration for DOD are the Assistant Secretary of Defense for Networks and Information Integration (ASD[NII]), who is also the DOD Chief Information Officer (CIO), and the Joint Staff J6 (JS J6), Director for Command, Control, Communications, and Computers, who is also the Joint Community CIO.

Under ASD (NII)/DOD CIO is the Defense Information Systems Agency (DISA), which is the operating agency responsible for DOD network operations and management worldwide. DISA is collocated with the Joint Task Force for Global Network Operations (JTF–GNO).

On the operational side, U.S. Joint Forces Command (USJFCOM) is responsible for joint force integration, including network interoperability. In this capacity, USJFCOM consolidates and harmonizes network requirements of the COCOMs and works with the JS J6 to ensure that investments in network systems include interoperability criteria as part of any approved system design.

The Services are responsible for training and equipping their forces to be joint network capable. That means investing in systems that meet interoperable protocols and common standards promulgated by OSD (NII) for their forces. There are substantial costs to meeting these requirements, and the Services routinely must make tradeoffs among priorities as they allocate investments. While the Services give every indication of full commitment to achieving network integration as soon as possible, timelines are not hard and fast, and funding is a major factor in determining progress.

The COCOMs are the managers of operational networks characterized by the architecture, standards, and systems established by DOD and provided by the Services, DISA, and JTF–GNO. Most COCOM communications and information networks are traditional hierarchical systems tethered to fixed locations, relay sites, or satellites. These are managed by the COCOM J6, who coordinates for Service requirements through the Joint Staff J6 as well as through the COCOM's subordinate component commands.

Under the 2002 Unified Command Plan, U.S. Strategic Command (USSTRATCOM) is assigned responsibility for information operations and global C^4ISR, including the responsibility to operate and defend the global information grid. USSTRATCOM's operational arm for maintaining the GIG is JTF–GNO. The roles of DISA and JTF–GNO are similar and overlapping, which is reflected in the dual-hatting of their commander. In essence, JTF–GNO is a component command of USSTRATCOM, uniquely provided by a defense agency rather than a military department.

Many external actors are as influential in network integration as in other high-priority and costly DOD programs. Congress is keenly interested in the successful achievement of joint operational capabilities, as is evident in the continued emphasis on the goals of the Goldwater-Nichols Department of Defense Reorganization Act some 20 years after its adoption. Congressional focus on the high cost of IT systems in DOD and across the government is apparent from the 1996 Clinger-Cohen Act and a host of related legislation that seeks to ensure we can define the return on IT investments. Other external actors are industry, the policy analysis community, and international bodies such as NATO, where similar integration architectures and standards have been defined and are the subjects of considerable investment. A new arrival whose architectures and standards are not yet well defined is the interagency cluster of departments that increasingly need to network with DOD at all operational levels.

Key Guiding Documents

The number of directives and internal guidance documents issued over the past several years is one way to measure how seriously DOD takes the makeover from platform-centered operations to net-centered operations. A broad and consistent stream of authoritative guidance establishes both legitimacy and logic. It also indicates that top-level DOD management is driving toward this goal as hard as they can.

Joint Vision 2020 and Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6212.01B, "Interoperability and Supportability of National Security Systems and IT Systems" (2000); the 2003 Transformation Planning Guidance and 2006 Quadrennial Defense Review (gearing up for renewal in 2009); the Joint Technical Architecture Version 6.0, Joint Battle Management Command and Control Roadmap, and CJCSI 3170.01C, "Joint Capabilities Integration and Development System," in 2003; and the Strategic Planning Guidance and DOD Architecture Framework in 2004 are all essential references for understanding the depth of DOD-wide commitment, management engagement, and investment in network integration. These same documents also signal the complexity and magnitude of the undertaking.

Earlier foundational underpinnings beyond DOD show that the Federal Government at large has acknowledged the advent of the information age and accepted the need for government as well as industry to bring its practices into the new era. This indicates that DOD overall and not merely its military operational side must achieve network integration. Above all, there has to be a clear link between IT investment and outcomes—the return on that investment for the taxpayer. The pivotal legislation and executive regulator policies in this regard are the Clinger-Cohen Act of 1996; the Office of Management and Budget Circular A–130, "Management of Federal Information Resources," and the Information Assurance Initiative (2000 National Defense Act) of 2000; and the E-Government Act of 2002.

Role of U.S. Joint Forces Command

USJFCOM is tasked with identifying the C^4 requirements of the joint com- munity. The command negotiates with the other joint commands to define a single, coherent set of required capabilities that can be passed to the service providers. Although flexibility and agile designs are desired, the reality is that bringing a requirement into operational use by a large force is time- and resource-intensive. Therefore, it is essential that required capabilities not be too transient or subject to frequent redefinition.

COCOMs sometimes press for standards to be loosened to encompass new and possibly immature technologies that have worked for them. In some cases, the systems may already have been procured for a pending operational requirement. USJFCOM does not yet exercise sufficient oversight to ensure that such "add-on" network systems do not actually move DOD *away* from its goal of networked forces. For example, a unique new system procured for a limited operational need by U.S. Pacific Command (USPACOM) may not be compatible with systems in use by U.S. Central Command (USCENTCOM) or U.S. European Command. However, some of the forces assigned to USPACOM for that operation may soon be ordered to USCENTCOM's area of responsibility. USJFCOM's role in achieving network interoperability is to adjudicate such inconsistencies to ensure a set of common technical standards acceptable across the joint operational user community.

USJFCOM has a primary role as well in achieving integration with inter- agency and multinational users. Typically, fewer close allies and agencies are involved in major combat operations than in stability operations; however, the network integration requirements for combat are more critical. The U.S. norm is for coalition combat operations, in which some allies provide niche capabilities, more partners from outside a COCOM's area of responsibility participate, and a higher level of interoperability is needed. USJFCOM has to meld multinational and interagency requirements as it does for joint operations, focusing on key allies and agencies across the range of military operations. USJFCOM then oversees these requirements as they are fed into the acquisition process, just as it does for joint matters.

The Joint Interoperability Test Command (JITC) is a test and evaluation organization established under DISA to advance global net-centric testing in support of joint operational capabilities. Its mission is to provide agile and cost- effective test, evaluation, and certification services to support rapid acquisition and fielding of global net-centric warfighting capabilities. Most of its projects are related to networks—standards, transport, services, applications, and platform integration. JITC works with industry and allies as well as DOD to certify interoperability and advance solutions as rapidly as possible.

Service Visions and Implementation

Current Service actions make clear that the tools of cyberspace have already had a significant impact on Service operational concepts and doctrine, systems development and technology, and organizational structure. There are also indications that the Services recognize that beyond being just a tool to enhance the effectiveness of conventional warfighting, cyber has changed the environment in which conflicts are played out. Cyberspace has changed the threat environment as well, creating new vulnerabilities and introducing a new level of global transparency to the execution of internal and external affairs. There is significant agreement among the Services as to the inherent capabilities of cyberpower in the networking, information/knowledge, and people/social domains. As an example, all the Services recognize the importance of cyber- dedicated educational and training facilities. But there are also major points of disagreement among the Services as to definitions and taxonomy of cyberspace, including its scope and frameworks. In addition, different organizational structures are being implemented within each Service to address this rapidly evolving source of both military opportunity and threat vulnerability. To further complicate the issue, different voices within the individual Services present diverse visions of the role of cyberpower and of their Service's role (usually that of leadership) within that vision.

Discerning substantive from semantic differences between the Service views of cyberspace and cyberpower is difficult. For example, discussion occurs about whether cyberspace is a domain in its own right and what the boundaries are between virtual and physical reality. What has become apparent is that engagements can be "fought" solely in cyberspace without resorting to the conventional domains. An example is a cyber attack on an opponent's military or civilian information networks that disrupts military connectivity and warfighting capability or degrades the country's basic infrastructures. In the emerging war of ideas and ideology, events in cyberspace are eventually manifested in the physical world. For example, the virtual haven of cyberspace has allowed terrorist organizations to recruit, plan, and execute physical acts of terrorism.

From a Service operational point of view, General James Cartwright, USMC, has critically pointed to the division of military cyberspace operations among three fiefdoms.[8] Under this approach, Joint Functional Component Command- Net Warfare is responsible for attack and reconnaissance, the Joint Task Force for Global Network Operations manages network defense and operations, and the Joint Information Operations Warfare Center oversees electronic warfare and influence operations. Strategic communications are overseen by USSTRATCOM. In addition to divisions in joint military cyberspace operations, there are potential Service and DOD C^{4}ISR interoperability issues as OSD proceeds with the development of the GIG and the Services proceed with implementations of NCW architectures.

Table 12–1 highlights Service concepts, architectural approaches, a small subset of service systems, and new organizational initiatives.

Table 12-1 Summary of Service Cyber Programs

Service	Concepts	Architecture	Systems	Organization
Air Force	Cyberspace as a warfighting domain	C^2 Constellation	Assurance, data integration, global information grid (GIG)	Cyberspace Command
Army	Information and cognition as a domain	LandWarNet	Future Combat System, Warfighter Information Network– Tactical, GIG	1st Information Operations Command, Network Enterprise Technology Command
Navy	Information operations, network- centric operations	FORCEnet	Navy Marine Corps Intranet (NMCI), GIG	Naval Network Warfare Command
Marine Corps	Net-centric operations and warfare	Marine Air-Ground Task Force–Information Operations	NMCI, GIG	Marine Corps Systems Command

Air Force

The Air Force has put cyberpower on an even footing with spacepower and air combat and has defined cyberspace as a "fifth dimension."[9] The Air Force considers cyberspace superiority an imperative and establishes the proposition that it is the prerequisite to effective U.S. military operations in all other warfighting domains. In a discussion on what it calls the "five myths" of cyberspace and cyberpower, the Air Force asserts the following:

- The intelligence collector and the information service provider should be separate organizational functions and not dual-hatted.
- The domain of cyberspace goes well beyond the Internet. The Air Force considers cyberspace a physical domain, through interlinking by the electromagnetic spectrum and electronic systems, rather than a virtual domain.
- The battle to achieve cyber superiority in any conflict must be fought in a distributed network rather than from one location where there may be a central coordinating element.
- The control of cyber weapons effects are controllable and the targeting and collateral damage issues are no different than with effects created by explosive or kinetically destructive means.
- Defense of the cyberspace domain requires a holistic network approach rather than just increased security at each individual node.

The Air Force Transformation Flight Plan describes the C^2 Constellation initiative as the centerpiece of the Service's NCW implementation efforts:

The Air Force is transitioning from collecting data through a myriad of independent systems (such as Rivet Joint, AWACS [airborne warning and control systems], JSTARS [joint surveillance target and attack radar systems], and space-based assets) to a C2 Constellation capable of providing the Joint Force Commander with real-time, enhanced battlespace awareness. It will provide Ground Moving Target Indicator capabilities along with focused Air Moving Target Indicator capabilities for Cruise Missile Defense. Additionally, every platform will be a sensor on the integrated network. Regardless of mission function (C^2, Intelligence, Surveillance, and Reconnaissance [ISR], shooters, tankers, etc.), any data collected by a sensor will be passed to all network recipients. This requires networking of all air, space, ground, and sea-based ISR systems, command and control nodes, and strike platforms to achieve shared battlespace awareness and a synergy to maximize the ability to achieve the Joint Forces Command's (JFC's) desired effects.[10]

The Air Force has also introduced a significant organizational change by standing up the Cyberspace Command as the 8th Air Force at Barksdale Air Force Base. The command's mission is to prepare for fighting wars in cyberspace by defending national computer networks, running critical operations, and attacking adversary computer networks.

Army

Jeff Smith of the Army's Network Enterprise Technology Command envisions a future in which soft power and the human/social impact of cyberpower are matched with a hard power that also is transformed by cyber. Smith considers that cognition is the actual goal of military strength, which is at a level above information (which in turn is at a level above cyberspace). Cognition refers to aspects of the human element, including leadership/behavior, understanding/decisionmaking, and problem-solving/adapting. Cyberspace is considered a subset of networks which in turn is related to information and finally cognition. In this paper, Smith collapses air/space, land, and sea into one physical environment and cognition into a second environment. His thesis is that Army doctrine, organization, training, materiel, leadership and education, personnel, and facilities are almost exclusively focused on the physical rather than the cognitive, which is the more important.

The Army implementation of NCO, LandWarNet, comprises the Service's information infrastructure and is its contribution to the GIG. LandWarNet consists of all globally interconnected Army information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand—supporting warfighters, policymakers, and support personnel. It includes all Army communications and computing systems, software (including applications), data security, and other associated services. The Future Combat System (FCS), a principal development program for NCO, is a modular construct of a reconfigurable family of systems capable of providing mobile, networked C^4 functionalities; autonomous robotic systems; precision direct and indirect fires; airborne and ground organic sensor platforms; and adverse weather reconnaissance, surveillance, targeting, and acquisition.[11] The Warfighter Information Network-Tactical (WIN–T) is the Army's tactical digital communications system for providing advanced commercial-based networking capabilities under the umbrella of the GIG. The WIN–T network C^4ISR support capabilities goals are for a network that is secure, survivable, seamless, and capable of supporting multimedia tactical information systems.[12] FCS is managed by the Army, with Boeing as a lead systems integrator. The Government Accountability Office, which reviews the program annually, has questioned the technical maturity of WIN–T and the Joint Tactical Radio System in terms of Army acquisition goals.[13]

Navy

The Navy perspective on cyberpower shows a structure incorporating the elements of IO and NCW. The Navy Marine Corps Intranet (NMCI) addresses the communications network and the business and administrative functions of cyberpower in the Navy and Marine Corps.[14] The Naval Network Warfare Command includes a Navy IO core competency, which supports the combat commander's ability to shape and influence potential adversary decisionmakers' thinking prior to conflict, resulting in deterrence of hostilities; enable decisive nonkinetic (effects-based operations) to complement kinetic warfare and defeat the adversary if conflict should ensue; and engage in continuing postconflict shaping/influence operations to maintain stability. To accomplish these goals, the Navy must develop an effective structure for IO force development, integration, planning, command and control, and execution in the joint environment.

FORCEnet is the Department of the Navy's implementation strategy for performing network-centric operations. The Chief of Naval Operation's accepted definition of FORCEnet is "the operational construct and architectural frame- work for naval warfare in the information age that integrates warriors, sensors, networks, command and control, platforms and weapons into a networked, distributed combat force that is scalable across all levels of conflict from seabed to space and sea to land."[15] The Naval Research Advisory Committee defines FORCEnet as "a portfolio of programs to enable the gathering, processing, transportation, and presentation of actionable information in support of all aspects of joint and combined naval operations."[16] Unlike the Army's WIN–T, FORCEnet is not a specific program but rather an architecture or a group of programs that serves as the organizing principle as the Naval enablement of the GIG. The NMCI is a key component of FORCEnet and has the goal of providing the Navy and Marine Corps with a full range of network-based information services on a single intranet. NMCI has the goal of providing secure, universal access to integrated voice, video, and data communications. Eventually, the massive NMCI network will link more than 400,000 workstations and laptops for 500,000 Navy and Marine Corps users across the continental United States, Hawaii, Cuba, Guam, Japan, and Puerto Rico. Under NMCI, the program office and the prime contractor control the layout, distribution, and analysis of the system. The prime contractor, Electronic Data Systems, owns all the IT assets and leases them to the government.

In the Navy Strategic Studies Group's (SSG's) study on "Convergence of Sea Power and Cyber Power," an even broader definition of cyberpower is given:

> an unconstrained interaction space—for human activity, relationships and cognition—where data, information, and value are created and exchanged— enabled by the convergence of multiple disciplines, technologies, and global networks—that permits near instantaneous communication, simultaneously among any number of nodes, independent of boundaries.

The SSG looks to a future with a more complex world driven by many emerging challenges. Cyberpower is seen to converge with the conventional seapower concepts and to transform conventional Navy roles in sea control, power projection, naval presence (both physical and virtual), strategic lift, and strategic deterrence.

Marine Corps

The Marine Corps has focused its cyberpower vision on net-centric operations and warfare (NCOW) and is developing a Marine Air-Ground Task Force Information Operations (MAGTF-IO) strategy for operational implementation. The future MAGTF–IO aims to enable decentralized decisionmaking that promotes taking advantage of fleeting battlefield opportunities. MAGTF–IO is a cyber strategy, a process, and ultimately a system of systems by which the Marine Corps will develop current and future capabilities and programs in order to achieve NCOW and implement the FORCEnet functional concept of providing robust information-sharing and collaboration capabilities. MAGTF–IO is the functional and conceptual equivalent of the other Service net-centric concepts of LandWarNet (Army) and C^2 Constellation (Air Force). It will also be integrated with NATO through the NATO NET Enabled Capability and be able to facilitate "coalitions of the willing" as needed. It entails a seamless, scalable, modular capability that is relevant across the full spectrum of military operations, from major combat operations to irregular warfare operations to humanitarian assistance operations.

DOD Implementation

Management and development of information-based technology and systems are spread through the Services. The Office of Force Transformation[17] provided an overall vision for NCO, but the Services develop their own systems in conjunction with the development of the Global Information Grid. A consideration of the GIG is essential in a discussion of military cyberpower because the GIG was mandated by DOD Directive 8100.1, "Global Information Grid Overarching Policy," in September 2002 as the physical implementation of the principles of NCW.

While all the Services recognize the GIG as the umbrella network under which they will operate, there is no commonality among them as to network architecture or their approaches to NCW. This circumstance requires that issues of interoperability be properly addressed. Each Service has special requirements, such as submarine communication for the Navy and mobile networked command and control for the Army. There are also areas where commonality should be sought, such as in aviation connectivity. How well the Services (as well as agencies such as members of the Intelligence Community) will develop their C^4ISR NCW programs to interface seamlessly with the GIG remains to be seen.

The Defense Information Systems Agency heads the GIG project under the leadership of the CIO of the ASD (NII)/DOD. The formal definition of the *global information grid* is "the globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating and managing information on demand to war fighters, policy makers, and support personnel."[18] The architecture for the GIG relies on Internet protocol (IP) and will depend largely on the commercial transmission infrastructure and on commercial information and network management technology.[19]

The vision and proposed architecture of the GIG are very challenging both from the standpoint of technology development and from the reliance on commercial systems to achieve information assurance. The National Security Agency (NSA) has been tasked by the ASD(NII)/DOD CIO to develop an end- to-end information assurance perspective for the GIG.[20] NSA recognizes that information assurance needs to be an embedded feature designed into every system in the GIG and that this requires a shift from today's model, which consists predominantly of link encryption and boundary protection between multiple discrete networks. In order to accomplish the GIG objectives, DOD will need to impact the commercial technologies and standards that will comprise the GIG architecture.

As noted earlier, the Services are all pursuing alternative networking architectures under the umbrella of the GIG. The GIG promises to provide a network based on commercial protocols, software and hardware for both tactical and strategic communications, data links to operate in an environment of forces on the move, and the ability to continue to operate effectively during network attacks and failures. Shortfalls exist in the GIG development to meet certain Service-specific needs. For example, with a mobile infrastructure, the Army will require protocols for a mobile ad hoc networking capability. However, commercial industry is moving toward an all-IP core network (IP version 6). The Navy may also experience shortfalls from the eventual GIG development. For example, the communications requirements for ships at sea depend on continuous high-capacity, low-latency connectivity to be provided by the transformational satellite program that is persistently being delayed for cost and technology reasons. Even when it is completed and the Navy develops suitable shipboard terminals, the Service's communications capacity will remain limited by capacity and satellite communications interruptions caused principally by antenna blockage. Also, the GIG programs do not address the challenging problem of communicating with submarines at speed and depth.[21] Another quandary for the introduction of communications systems under the GIG umbrella is funding new systems to replace legacy systems that do not fit into the new architecture. For example, Army officials must determine how to transition the Joint Network Node, a commercial, IP-based mobile communications system deployed to soldiers in Iraq, to the WIN–T.[22]

Challenges and risks also are associated with the use of commercial products such as Microsoft Windows and Office, which are typically released with bugs. DOD does not have access to the proprietary codes to receive the patches that remedy the bugs. Additionally, commercial-off-the-shelf computers, routers, and servers often have "trap doors" for maintenance that can provide system access to hackers. Internet gateways for the Nonsecure Internet Protocol Router Network and other government unclassified networks have offered venues for attackers to exploit and disrupt. Even secure systems with multiple users are susceptible to the insider threat. The access to and the sharing of information with Internet portals have benefits, risks, and limitations that must be managed, especially for SSTR and information-sharing with other nations, international organizations, and nongovernmental organizations (NGOs).

An additional concern relating to the use of commercial products is the outsourcing of IT providers of both products and services in network operations and management in crisis situations. This practice could lead to issues such as embedded trojan horses in foreign-built equipment and software. National constraints limiting international vendors during a crisis could result in supply problems. Finally, there is a trend toward the global IT infrastructure (including IT products, services, and networks such as global Internet, cellular, telecoms, cable, and satellites) being taken over by foreign ownership that may not be friendly to U.S. policy and needs, especially the need to ensure continuity of operations during a crisis.

The full implementation of a joint, interconnected force via the GIG is still in the future. Other issues relating to multinational military actions with coalition operations as well as civil-military operations in support of HA/DR and SSTR operations will also need to be addressed. Issues to be overcome include the lack of an NCO organizing principle and architecture between the Services; related interoperability issues among Services, civil agencies, coalition partners, international organizations, and NGO communities; the impact of a changing threat environment with irregular warfare; new technology developments; the need for high bandwidth, agile connectivity, and security; and the costs associated with implementation.

Conclusion

Knowledge and information exchange have always been essential to warfighting. As cyberspace technology has evolved over the past few decades, the military has adapted the technology to its traditional warfighting paradigms of land, air-, space-, and seapower. Rather than developing its own information and communications technology knowledge base and systems, the military has relied extensively on commercial systems and increased dependence on commercial services globally, including the use of the Internet to support some elements of command and control.[23] In addition to the Internet, the military is a user of commercial products such as wireless networking, cellular phones, personal digital assistants, telecommunications, and satellite and cable-based networks, radio, and television. While it has developed the concepts of network-centric warfare to integrate land, air-, space-, and seapower, it has maintained the conventional warfighting principles of strike warfare, air superiority, and air and missile defense structured to increase the speed and timeliness of operations, to operate more effectively in extended areas of coverage, and to enhance precision. This utilization of cyberpower enhances our hard power capabilities and defines the attributes of the network to support these operations. The evolutionary growth of these capabilities has maintained the existing organizational, management, and acquisition structure of the Services in dealing with technological advances in cyberspace. Similarly, military information operations have maintained their organizational principles even in the face of the extraordinary impact that radical groups have exhibited by their adaptation of the Internet to recruit, plan, finance, and influence. Rather than speed of operations, the defining metrics here are large-scale connectivity, user pull, and collaboration. This is being accomplished by making more effective use of emerging information and communications technology and changing operations to support the increased importance of HA/DR and SSTR in phases zero, four, and five, as well as warfighting in phases one, two, and three.

In this chapter, military cyberpower has been described in terms of three dimensions: military requirements or missions as described by the joint war- fighting phases; military information-based capabilities or operational concepts, including NCO, IO, military administration, intelligence collection, and influence operations; and the dimension of cyberspace, including open and closed architectures employing dedicated networks, the Internet, military tactical radios, commercial radio/TV, and telecommunications. Ideally, an integrated cyberspace architecture can be envisioned that supports all military requirements and military information-based capabilities. It would need to be reliable, available, and survivable under attack and would also need to be scalable and provide high bandwidth. While optimal, such an integrated architecture may provide multiple unforeseen vulnerabilities and introduce unacceptable cost and capability risks. A single open architecture designed to promote maximum connectivity and user pull based on IP may need separation from the secure connectivity required for sensor-to-weapon NCO operations. The GIG and new technology initiatives are poised to address these issues but may not meet all technology objectives of these programs. In the meantime, the military requires secure closed networks that restrict users and have highly controlled access arrangements and stringent security protection, as well as fully connected open networks. The military also needs to wrestle with existing legacy systems, many of which will not be interoperable with the GIG.

There is no question that the Services are already adapting to and leveraging the new environment in communications and information provided by the exponential growth in cyberspace connectivity and information storage and processing. However, risks and vulnerabilities have been introduced—especially the increased dependence of the military on civilian cyberspace capabilities, products, and services—that need careful assessment to be effectively managed. The Services are also experiencing growing pains as they deal with a different world order and the impact of new technology coupled with their evolving and changing missions in this environment including HA/DR, SSTR, and influence operations.

There is significant agreement among the Services as to the inherent capa- bilities of cyberpower in the networking, information/knowledge, and people/ social domains. There are also currently points of disagreement among the Ser- vices as to definitions and taxonomy of cyberspace, including scope, frameworks, and leadership.

Within each Service, different organizational structures are being imple- mented to address this rapidly evolving source of both military operational op- portunities and to defend against and respond to threat vulnerability.

While all the Services recognize the GIG as the umbrella network under which they will operate, there is no commonality among them as to network architecture or their approaches to NCO. This approach will only succeed if issues of interoperability are properly addressed.

The GIG has been mandated as the physical implementation of the principles of NCO. The vision and proposed architecture of the GIG are challenging both from the standpoint of technology development and from the reliance on commercial systems to achieve information assurance.

[1] Defining the Internet broadly, this includes email and the World Wide Web as well as military and government Internet protocol–based networks. These include networks that have access to the Internet architecture—for example, the Nonsecure Internet Protocol Router Network—and those that do not—such as the Secret Internet Protocol Router Network and Joint Worldwide Intelligence Communications System, which are secure networks.

[2] Department of Military Strategy, Planning, and Operations, "Campaign Planning Primer AY 07," U.S. Army War College, 2006, available at <www.carlisle.army.mil/usawc/dmspo/Publications/Campaign%20Planning%20Primer%20AY07.pdf>.

[3] The "three-block war" concept is credited to General Charles Krulak, former Commandant of the Marine Corps.

[4] Department of Defense, "Capstone Concept for Joint Operations," Version 2.0, August 2005, available at <www.dtic.mil/futurejointwarfare/concepts/approved_ccjov2.pdf>.

[5] Joint Publication 3–13, *Information Operations* (Washington, DC: The Joint Staff, February 13, 2006), available at <www.dtic.mil/doctrine/jel/new_pubs/jp3_13.pdf>.

[6] M.P. Fewell and Mark G. Hazen, "Network-Centric Warfare—Its Nature and Modeling," Australian Defence Science and Technology Organisation, September 2003, available at <www.dsto.defence.gov.au/publications/scientific_record.php?record=3310>.

[7] David S. Alberts and John J. Garstka, "Network-centric Warfare: Department of Defense Report to Congress," July 2001, available at <www.dodccrp.org/files/ncw_report/ report/ncw_cover.html>.

[8] Josh Rogin, “Cartwright: Cyber Warfare Strategy ‘Dysfunctional’,” U.S. Air Force Aim Points, February 12, 2007, available at <http://aimpoints.hq.af.mil/display.cfm?id= 16609>.

[9] Lieutenant General Robert J. Elder, Jr., “The Fifth Dimension: Cyberspace,” briefing, Headquarters, U.S. Air Force.

[10] *The Air Force Transformation Flight Plan* (Washington, DC: Headquarters, U.S. Air Force, November 2003), B–6, available at <www.af.mil/library/posture/AF_TRANS_ FLIGHT_PLAN-2003.pdf>.

[11] *United States Army 2003 Transformation Roadmap* (Washington, DC: Department of the Army, November 2003), B–3, available at <www.army.mil/2003transformationroadmap/>.

[12] Warfighter Information Network–Tactical Operational Requirements Document, November 1999, available at <www.fas.org/man/dod-101/sys/land/docs/WIN-T5NOV. htm>.

[13] Government Accountability Office, “Defense Acquisitions: Key Decisions to Be Made on Future Combat System,” Report to Congressional Committees 07–376, March 16, 2007, available at <www.gao.gov/new.items/d07376.pdf>.

[14] Kenneth Jordan, “The NMCI Experience and Lessons Learned: The Consolidation of Networks by Outsourcing,” Case Studies in National Security Transformation No. 12 (Washington, DC: Center for Technology and National Security Policy, September 2007), available at <www.ndu.edu/ctnsp/Case%20Studies/Case%2012%20%20The%20NMCI%20Experience%20and%20Lessons%20Learned.pdf>.

[15] Richard W. Mayo and John Nathman, “Sea Power 21 Series, Part V: Turning Information into Power,” U.S. Naval Institute *Proceedings* (February 2003), 42.

[16] Naval Research Advisory Committee, “Naval S&T in FORCEnet Assessment,” Report 04–2, July 2004, 15, available at <www.onr.navy.mil/nrac/docs/2004_rpt_navy_st_ forcenet.pdf>.

[17] Office of Force Transformation, *The Implementation of Network-Centric Warfare* (Washington, DC: U.S. Government Printing Office, January 2005), available at <www.maxwell.af.mil/ au/awc/awcgate/transformation/oft_implementation_ncw.pdf>.

[18] The *global information grid* is defined in DOD Directive 8100.1, “Global Information Grid Overarching Policy,” September 19, 2002, available at <www.dtic.mil/whs/directives/ corres/pdf/810001p.pdf>. See also David S. Alberts and Richard E. Hayes, *Power to the Edge: Command and Control in the Information Age* (Washington, DC: Department of Defense Command and Control Research Program, June 2003), 187.

[19] Alberts and Hayes, 196.

[20] “Global Information Grid,” National Security Agency Web site, available at <www.nsa.gov/ia/industry/gig.cfm?MenuID=10.3.2.2>.

[21] National Research Council, *FORCEnet Implementation Strategy* (Washington, DC: National Academies Press, 2005).

[22] Frank Tiboni, “Army Stuck in a WIN–T Quandary,” *FCW.com*, February 2006, available at <www.fcw.com/article92437-02-27-06-Print>.

[23] Center for Technology and National Security Policy, *Report to the Congress: Information Technology Program* (Washington, DC: Center for Technology and National Security Policy, January 2006).