The Maxwell Papers

A Cyberspace Command and Control Model

Joseph H. Scherrer
Colonel, USAF
and
William C. Grund
Lieutenant Colonel, USAF

Air War College
Maxwell Paper No. 47

Air University
Allen G. Peck, Lt Gen, Commander

Air War College
Maurice H. Forsyth, Maj Gen, Commandant
Daniel Baltrusaitis, Col, PhD, Dean of Research
Lawrence E. Grinter, PhD, Series Editor
George J. Stein, PhD, Essay Advisor

Air Force Research Institute
John A. Shaud, Gen, PhD, USAF, Retired, Director

Air University Press
Bessie E. Varner, Deputy Director
Jeanne Shamburger, Content Editor
Andrew Thayer, Copy Editor
Nedra O. Looney, Prepress Production
Daniel Armstrong, Cover Design
Daniel Armstrong, Illustrations
Mary J. Moore, Quality Review

Please send inquiries or comments to
Editor
The Maxwell Papers
Air War College
325 Chennault Circle, Bldg. 1401
Maxwell AFB, AL 36112-6006
Tel: (334) 953-7074
Fax: (334) 953-1988
http://www.au.af.mil/au/awc/awcgate/awc-mxwl.htm

AIR UNIVERSITY

AIR WAR COLLEGE

A Cyberspace Command and Control Model

JOSEPH H. SCHERRER
Colonel, USAF

and

WILLIAM C. GRUND
Lieutenant Colonel, USAF

Air War College
Maxwell Paper No. 47

Air University Press
Maxwell Air Force Base, Alabama

August 2009

01-Frontmatter.indd 1 10/19/09 1:35:20 PM

This Maxwell Paper and others in the series are available electronically at the Air University Research Web site http://research.au.af.mil and the AU Press Web site http://aupress.au.af.mil.

Disclaimer

Opinions, conclusions, and recommendations expressed or implied within are solely those of the authors and do not necessarily represent the views of Air University, the United States Air Force, the Department of Defense, or any other US government agency. Cleared for public release: distribution unlimited.

01-Frontmatter.indd 2 10/19/09 1:35:21 PM

Foreword

As the nation's most technologically advanced service, the Air Force relies absolutely on cyberspace to perform its war-fighting missions. Underpinning this competency is the ability to command and control cyberspace operations, something the authors argue is in need of a fresh approach if the Air Force is to effectively fly, fight, and win in cyberspace.

The authors assert that the lack of an effective cyberspace C2 structure critically reduces the responsiveness to combatant and joint task force commanders and increases the difficulty of integrating cyberspace capabilities into operational plans and execution. The traditional military hierarchies currently used for cyberspace C2 do not have the agility to deal with the high velocity of change that characterizes cyberspace. Instead, the authors argue for flexible organizational structures to match the complexity and pace of the cyberspace operational environment.

As with all Maxwell Papers, the Air War College publishes this study in the spirit of academic freedom and open debate. We encourage your engagement on the issues the paper raises and solicit your responses.

MAURICE H. FORSYTH
Major General, USAF
Commandant, Air War College

01-Frontmatter.indd 3 10/19/09 1:35:22 PM

01-Frontmatter.indd 4 10/19/09 1:35:22 PM

About the Authors

Col Joseph H. Scherrer, USAF, is a communications and information officer. He has commanded three communications squadrons, served on the Joint Staff, and participated in multiple contingency operations, including Deny Flight, Provide Promise, Deliberate Force, Joint Forge, Southern Watch, and Enduring Freedom. While on the Joint Staff, he led the Joint Staff team that produced the first *National Military Strategy for Cyberspace Operations*. Colonel Scherrer graduated from the Air War College with distinction in May 2009 and currently is the commander of the 75th Mission Support Group, Hill AFB, Utah. He is married to the former Dina Leite Moraes of Rio de Janeiro, Brazil.

Lt Col William C. Grund, USAF, is a communications and information officer. He has commanded two communications squadrons, served on the PACAF and Joint Staffs, and participated in multiple contingency operations including Southern Watch, Noble Eagle, and Enduring Freedom. While at PACAF, he brought the PACAF Network Operations and Security Center (NOSC) to initial operational capability (IOC), and at the Joint Staff, he coauthored the *National Military Strategy for Cyberspace Operations*. Following graduation from the Air War College in May 2009, Colonel Grund assumed command of the 379th Communications Squadron, Al Udeid AFB, Qatar. He is married to the former Teresa Sue Archambault. They have three children: Carl (14), Patrick (11), and Krista (10).

01-Frontmatter.indd 5 10/19/09 1:35:22 PM

01-Frontmatter.indd 6 10/19/09 1:35:23 PM

Introduction

Although the concept of command and control (C2) is firmly embedded in US war-fighting doctrine, organization, technology, and operations, a definitive method for cyberspace C2 has not been established across the joint force. This is despite ample evidence that the joint force is not optimally organized for C2 of cyberspace operations. Ongoing intrusions to the tune of six million per day and massive exfiltration of information remain unabated. Attacks appear to be growing ever more sophisticated and difficult to detect. In addition, the armed forces' offensive capabilities are unnecessarily segmented, being that both the legal authorities and technical capabilities are wholly enabled by agencies other than the Department of Defense (DOD). This situation critically reduces the responsiveness to combatant and joint task force commanders and increases the difficulty of integrating cyberspace capabilities into operational plans and execution.

The central thesis of this paper is that any approach to cyberspace command and control must be founded on the nature of the cyberspace domain itself. To investigate this proposal, this study examines possible alternatives for cyberspace C2 that are based on the nature of the strategic environment, the nature of the cyberspace domain itself, and the way in which conflict must be approached in this domain in order to improve the armed forces' ability to successfully compete in cyberspace. The paper provides background on the pertinent threats arising in cyberspace; the definition of cyberspace; and the nature of the strategic environment, cyberspace, and competition in cyberspace. Next, a review of C2 models and associated organizational forms, including the current DOD approach, is presented. A set of cyberspace C2 criteria is then derived, followed by an analysis of the models in light of the criteria. Using the results of the analysis, implications for C2—with particular emphasis on organizational structure—are addressed.

Background

In late 2005, several media outlets published reports of a DOD code-named computer intrusion set titled Titan Rain.

02-Text.indd 1 10/19/09 1:38:22 PM

These reports outlined a concerted and lengthy effort by supposed Chinese computer hackers who were systematically infiltrating DOD systems across the globe. Their intrusions were described as efficient and rapid: "They would commandeer a hidden section of a hard drive, zip up as many files as possible and immediately transmit the data to way stations in South Korea, Hong Kong or Taiwan before sending them to mainland China. They always made a silent escape, wiping their electronic fingerprints clean and leaving behind an almost undetectable beacon allowing them to re-enter the machine at will. An entire attack took 10 to 30 minutes."[1]

These intrusions resulted in huge amounts of data being transferred outside the United States to ultimate destinations unknown. While the actual types and specifics of the data lost remain classified, suffice it to say they included operationally and tactically relevant information that could assist an adversary. More disturbing is that the intrusions could take place at all and that it normally takes the DOD quite a long time to even notice an intrusion has taken place. This does not bode well for a zero-day intrusion, which is integrated into a more conventional type of an attack. The point of the zero-day attack would be to slow our response down long enough to give our adversary an asymmetric advantage, with the end result being dominance over US forces.

To meet these and other intrusion attempts, the DOD has relied upon an exceedingly hierarchical and authority-lacking organizational C2 structure. This has led to a system that finds itself in a reactive, defensive crouch vice one that can execute active defense measures to preempt unrelenting intrusions while keeping cyberspace available and allowing freedom of action for users and war fighters. More specifically, the military is using the traditional template of assigning responsibility, without adequate authority, to a single combatant command (COCOM), United States Strategic Command (USSTRATCOM). As this paper shows, it is widely recognized that cyberspace is declared, at the highest levels, as the newest domain of warfare. However, unlike the other war-fighting domains, cyberspace responsibilities are assigned to a COCOM vice a "service equivalent." Service equivalent means that primary air responsibilities reside with the Air Force, land operations with the Army, and maritime activities with the Navy and Marine Corps.

02-Text.indd 2 10/19/09 1:38:23 PM

For these domains, no one COCOM executes operational responsibilities across other COCOMs' lines of authority and responsibility. Nor do the various service chiefs attempt to direct air, land, or maritime operations within a different COCOM. This is not so with cyberspace; for this domain, the military treats a domain of warfare organizationally different while utilizing conventional C2 structures that result in significant C2 challenges.

However, functional component commands do exercise combatant command authority over assets of all the services, not unlike geographical combatant commanders do once they are assigned or attached forces. But the similarity ends there. Unlike the functional commands, USSTRATCOM does not enjoy the ability to command and control the services' cyberspace forces in a unified manner to ensure cyberspace superiority.

Nowhere is this borne out more than in the military's own documentation regarding C2 of cyberspace. Joint Task Force-Global Network Operations (JTF-GNO), the DOD's operational and tactical command for cyberspace, published the *Joint Concept of Operations* [CONOPS] *for Global Information Grid Network Operations* [GIG NETOPS] in 2006. In this document, JTF-GNO published a chart (fig. 1) designed to help guide it in deciding when and how it might intervene and exercise C2 over the GIG during an event.[2] Based on the chart, the DOD is using traditional, geographically based thinking in an attempt to delineate artificial C2 boundaries when the global nature of cyberspace argues against this approach.

Criteria / Incident	CROSSES THEATER BOUNDARY	IMPACTS MULTIPLE COCOMS	IMPACTS OTHER AGENCIES	BEYOND THEATER CAPABILITIES	GLOBAL EVENT?

Figure 1. **JTF-GNO matrix to manage incidents**. (Reprinted from USSTRATCOM, *Joint Concept of Operations for Global Information Grid NetOps* [version 3], 4 August 2006.)

02-Text.indd 3 10/19/09 1:38:23 PM

Some might claim that cyberspace is purely an enabler best viewed as a functional area. Even if this were true, the current command structure does not reconcile with the nature of the domain. Unlike the US Transportation Command, the US Joint Forces Command, or other functional COCOMs which are organized around their functional area, cyberspace is relegated to one of many missions under the USSTRATCOM umbrella.

Further complicating the picture is a recent secretary of defense–directed organizational change. In a November 2008 memo, Secretary Robert Gates directed the USSTRATCOM commander to "place [JTF-GNO] under the operational control of Commander, Joint Functional Component Command [for] Network Warfare [JFCC-NW])."[3] This arrangement further creates gaps and seams as the DOD attempts, through a traditional, hierarchical approach, to exercise C2 over the cyberspace domain. Instead, the environment in which cyberspace is embedded necessitates a C2 structure that recognizes, embraces, and takes advantage of the nongeographic nature of cyberspace.

The cyberspace environment can best be characterized by the acronym VUCA: volatility, uncertainty, complexity, and ambiguity. As this paper illustrates, rapid technological advances and increases in the use and pervasiveness of cyberspace coupled with aggressive adversaries create a volatile environment. The DOD, along with the rest of the world, is uncertain about the future uses and exploitations that will occur in cyberspace and the impact to our military and society should the current intrusions we suffer from advance in a destructive manner. Furthermore, the domain's technological aspects and usage make it difficult to understand. All of these factors, along with the challenges of attributing cyberspace intrusions, combine to create an environment of frustrating ambiguity. The correct military response lies in establishing a C2 structure for this new domain so that the armed forces can not only execute day-to-day defense but also fight through future intrusions in time of war.

02-Text.indd 4 10/19/09 1:38:23 PM

Cyberspace: A Definition

To begin a discussion on cyberspace, one must first define and reach a common understanding of the term. Much writing on this topic has occurred over the past decade as cyberspace matured and as the DOD realized that a new domain and form of warfare had materialized.

The term *cyberspace* has come to be accepted universally as what we, as humans, created and now inexorably rely upon both in a military and civilian sense. It was first coined by the novelist William Gibson in his 1982 story titled "Burning Chrome" and then published in his 1984 novel *Neuromancer*.[4] However, his definition differs greatly from our current understanding of the concept. To wit, he defines *cyberspace* as "a consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts. . . a graphic representation of data abstracted from banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the nonspace [*sic*] of the mind, clusters and constellations of data. Like city lights, receding."[5] As one can quickly tell, Gibson's idea of cyberspace hardly applies to our reality. Like the Joint Publication (JP) 1-02, *Department of Defense Dictionary of Military and Associated Terms*, definition of cyberspace, the universal understanding of cyberspace does not include a description of a "consensual hallucination," "unthinkable complexity," or "lines of light." Although we have embraced the term *cyberspace*, the DOD quickly rejected the definition submitted by its creator.

Enamored with the possibilities of cyberspace, the term was employed in many contexts with many different meanings and definitions. The accepted DOD definition as published in JP 1-02 prior to August 2006 states that *cyberspace* is the "notional environment in which digitized information is communicated over computer networks."[6] Once again, the concept of a "notional environment," that is, one that does not exist except in one's mind, is encountered. As there are very real, physical pieces to cyberspace, this definition does not accurately describe it. However, efforts to properly define it or discuss the very nature of cyberspace in any type of official capacity were met throughout the past decade with indifference or outright stonewalling.

02-Text.indd 5 10/19/09 1:38:24 PM

In 2003 the president of the United States recognized the importance of cyberspace to the nation and attempted to define it in the *National Strategy to Secure Cyberspace* as "composed of hundreds of thousands of interconnected computers, servers, routers, switches, and fiber optic cables that allow our critical infrastructures to work."[7] While an admirable effort, coordinated across the entire US government, this definition deals mainly with hardware aspects of the domain and fails to recognize that cyberspace is, in fact, a domain and does not really add more to the discussion past the definition provided by the DOD in JP 1-02.

A significant breakthrough occurred with the publication of the 2006 *Quadrennial Defense Review (QDR)*. The *QDR* is the fulfillment of the statutory requirement in 10 *US Code*, section 118, which requires the DOD to "conduct a comprehensive examination (to be known as a 'quadrennial defense review') of the national defense strategy, force structure, force modernization plans, infrastructure, budget plan, and other elements of the defense program and policies of the United States with a view toward determining and expressing the defense strategy of the United States and establishing a defense program for the next 20 years. Each such quadrennial defense review shall be conducted in consultation with the Chairman of the Joint Chiefs of Staff."[8] This high-level document, a coordinated effort across the entire Joint Staff, acknowledged cyberspace is, in fact, a domain not unlike the traditional domains of warfare (air, land, sea). However, the *QDR* in a sense backed into the declaration of cyberspace as a domain by treating it as a fait accompli. It uses the term *cyberspace* as a de facto domain as passages pulled from the document illustrate.

- "Capabilities to locate, tag and track terrorists in all domains, including *cyberspace*."[9]
- "Contribute to the nation's response to and management of the consequences of WMD attacks or a catastrophic event, such as Hurricane Katrina, and also to raise the level of defense responsiveness in all domains (e.g., air, land, maritime, space and *cyberspace*) if directed."[10] (emphasis added)

02-Text.indd 6 10/19/09 1:38:24 PM

Having treated cyberspace as a domain, the *QDR* did not find it necessary to define the domain, leaving that for follow-on efforts. However, it did create the necessary, official environment to begin shaping the discussion toward cyberspace being officially declared as a domain of warfare with all the associated challenges and opportunities.

Immediately building upon the efforts of the *QDR* and driven by foreign intrusions against the Nonsecure Internet Protocol Router Network, the Joint Staff's Communications and Information Directorate (J-6) led a chairman of the Joint Chiefs of Staff–directed, staffwide effort to develop a strategy to deal with cyberspace. As part of the effort to create the first-ever *National Military Strategy for Cyberspace Operations* (*NMS-CO*), the authors arrived at a DOD-wide coordinated definition of *cyberspace* as "a domain characterized by the use of electronics and the electromagnetic spectrum to store, modify and exchange data via networked systems and associated physical infrastructures."[11] As Dr. Kamal T. Jabbour, senior scientist for information assurance at the Air Force Research Laboratory in Rome, New York, accurately points out,

> The word "domain" instead of "environment" carries legal implications under the laws of armed conflict. "Electronics and the electromagnetic spectrum" refer to the wave-particle duality of radiation which, when modulated with information, creates a signal. "Data and networked systems" refer to digital information and application programs, and the computers and networks on which they exist, in other words data and applications, at rest and in motion.[12]

Cyberspace consists of more than the Transmission Control Protocol/Internet Protocol (TCP/IP)–based Internet, though to be sure, it is the Internet that currently dominates what most people think of as cyberspace. There are thousands of protocols, software architectures, and hardware implementations that comprise cyberspace. This includes networks not based on the Internet Protocol, such as specialized military networks, networks not connected to the Internet, and networks that use different or proprietary communications protocols. Examples include Link 16 networks that use a time division multiple access method and standardized message formats and the Signaling System 7 protocol, which ties together the world's telephone switch network. The point here is that cyberspace is more than just Internet-based computer networks.

02-Text.indd 7 10/19/09 1:38:24 PM

Building upon the definition provided by the *NMS-CO*, the Office of the Secretary of Defense staff continued to refine the definition and finally arrived at the current definition which is incorporated into JP 1-02 and is the *official* DOD definition of cyberspace: "A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[13] This definition is sufficient to enable further discussion about cyberspace, its place within the traditional domains of warfare, and the need to establish effective command and control structures enabling the military to operate effectively within and through the domain.

The Nature of Cyberspace

One central and vital point must be understood: the value of cyberspace is derived from the information that flows through it. This continuous, massive exchange of information has made cyberspace indispensable to modern civilization and, thus, central to modern military operations. The volume of global Internet traffic per year, estimated to range from 3,000 to 5,000 petabytes (10^{15} bytes) and the fact that overall Internet traffic is growing at 50 to 60 percent yearly, are enough to provide ample support for this assertion.[14] This phenomenon results from a combination of technological, economic, and sociological factors and gives rise to a rich, dynamic, and ever-growing web of human-to-human, human-to-machine, and machine-to-machine interactions. New applications, such as Web 2.0 or social networking, digital television streaming, and the "executable Internet" promise to open innovative avenues to conduct commerce, stay in touch, and fight wars. The armed forces would do well to anticipate disruptive threats to emerge from cyberspace given the domain's facility to generate innovation and create crosscutting change.

Innovation and change are hallmarks of cyberspace. It is important to understand that the cyberspace infrastructure, like the information that flows through it, does not remain static. The technologies and architectural approaches that comprise cyberspace will continue to change over time,

02-Text.indd 8 10/19/09 1:38:24 PM

meaning that the fabric of cyberspace itself will evolve. Advances in electronics engineering, fabrication, integration, and production; improved computing architectures, networking, and information exchange methods; and emerging nanotechnologies and biotechnologies promise to transform today's cyberspace into ever more potent forms with more powerful capabilities for information transmission, storage, processing, and depiction. Another critical point is that cyberspace will continue to become increasingly complex, especially in terms of scale and control. Cyberspace is comprised of billions of devices—each with its own hardware, software, and purpose—with billions to follow. This results in an extremely heterogeneous systems environment that is becoming less and less amenable to direct and pervasive human control. From a military standpoint, this evolutional reality drives an enduring requirement for aggressive science and technology research that will in turn translate into systematic alignment and fielding of effective cyberspace operational capabilities.

Cyberspace: A Man-Made Domain of Warfare

Cyberspace is both linked to and distinguished from air, land, sea, and space in that it is a man-made domain established through the use of electronic technology and software, firmware, and hardware programs specifically designed to manipulate electromagnetic energy into encoded signals. In one sense, cyberspace is exactly like the other physical domains in that it relies on a scientific reality—in this case the electromagnetic spectrum—that is governed by physical laws (e.g., Maxwell's equations). However, cyberspace differs from the other domains in that technology is an essential factor for its existence. Cyberspace is a man-made domain in the sense that the transmission of encoded electromechanical signals is only possible through the use of human designed, manufactured, and organized electronics-based technology.

Cyberspace is also similar to the other domains in that it is globally distributed, which adds to the C2 complexities. Unlike the other domains, cyberspace is owned by commercial, state, or private interests. It is not as some would say a "global commons" or "a natural asset outside national jurisdiction such as the oceans, outer space, and the Antarctic."[15]

02-Text.indd 9 10/19/09 1:38:24 PM

Within some areas of the DOD the term *global commons* has taken on a sort of buzzword status and is used to support strategic concepts that have US military forces engaged in the protection of access to the global commons. Except for very narrow situations such as public cable access or amateur radio frequencies, the principles of sovereignty, property rights, and commercial enterprise apply to cyberspace, which, in turn, under US and international law, place constraints on when and how military force can be used in cyberspace.

The effort to classify cyberspace as a part of the global commons is best viewed as a movement to internationalize its control and subject it to supranational legal regimes. This controversy centers largely around the Internet, which since 1992 has been overseen by a consortium of commercial, governmental, academic, and research organizations under the auspices of the Internet Society. In addition, the Internet Corporation for Assigned Names and Numbers (ICANN), which controls the assignment of Internet address space and is contracted to the US Department of Commerce to perform this task on behalf of all Internet users, has come under fire from both commercial and governmental interests as to whether ICANN has the authority to accept or reject the establishment of new domains. The Internet Society and ICANN exemplify the regulatory and standards complexity that accompany operations in cyberspace.

Cyberspace is also distinguished from the other domains by its potential to drive extremely high operational speeds. Whereas operations in the other domains are subject to much lower limits on speed due to gravitational, hydrodynamic, astrophysical, propulsive, and ballistic forces, cyberspace operations can occur at much higher speeds. For instance, the transmission of optical signals has been registered at two-thirds the speed of light, which is orders of magnitude faster than speeds achieved in the other domains.[16] Practical examples include AT&T's 40-gigabit-per-second transmission capability on its Internet backbone and the 1.2 seconds it takes for a one-way, end-to-end, geosynchronous satellite transmission.[17] The speed at which events occur in cyberspace serves to transform the classic time-space planning factor by reducing the tyrannies of time and distance. With innovations occurring

02-Text.indd 10 10/19/09 1:38:25 PM

continuously, the upper limit of operational speed in cyberspace will only continue to increase.

However, increased operational speed is not automatic and is attenuated by a number of factors. Perhaps most obviously, speed is affected by machine failures and faults. In addition, just as in the other domains, adversary operations and effectiveness of friendly planning, decision making, and operational processes place a drag on operational speed. Unless cyberspace operations are thoroughly augmented with technological automation—to include more precise and cogent methods for producing situational awareness and moment-by-moment domain understanding—the human-induced latency associated with planning and decision making will negatively impact operational tempos, resulting in a failure to capitalize on the potentially high speeds afforded by the domain.

Another limitation on operations is the difficult task of tracing and attributing malicious activity in cyberspace. Adversaries conduct attacks using multiple nodal hops and diverse network paths that can transit many national boundaries. Even if an attack is successfully traced, it becomes another task altogether to correlate the attack to the actor who initiated it, all of which takes time. In addition, anonymity is readily achieved using obfuscation, masquerade, and deception techniques. With sufficient expertise, especially when augmented by knowledge available in the Internet, cyberspace becomes a sanctuary where information exchanges are conducted in secrecy and large-scale attacks can be launched with low probability of attribution. This affords a tremendous asymmetric advantage to a cyberspace attacker.

Asymmetric advantage is also associated with the ease at which cyberspace can be accessed. Operating in cyberspace is an inexpensive proposition as compared to the costs of entry to compete militarily in the other domains, especially air and space. Commercial computing technology and connectivity can be readily obtained along with extremely sophisticated attack and exploitation tools. Successfully competing in cyberspace is not restricted solely to nation-states. Organized crime and extremist organizations increasingly exhibit the type of agility and innovation previously reserved for state-run military-intelligence establishments to conduct

02-Text.indd 11 10/19/09 1:38:25 PM

sophisticated technical operations. As the scale and reach of cyberspace capabilities grow, nonstate actors should be expected to increasingly use cyberspace as an asymmetric offset to a state's conventional forces and technical means, while state actors will gain skill in the conduct and integration of cyberspace operations with operations in air, land, sea, and space. Because of its dependence on cyberspace, the United States is especially vulnerable to such operations.

Another intricacy of the cyberspace domain is that very little in the way of international law exists with regard to its use. Unlike the other domains, from a legal standpoint, cyberspace is not yet considered a "place" as such, and therefore traditional territorial-based law for international conduct does not apply cleanly to the domain. Given the speed and general anonymity with which information flows, it is difficult to clearly delineate a state's territorial boundary in cyberspace at any given moment. Such a capability would require the instantaneous mapping of electronic traffic flows to precise geographic points as well as the technical and procedural means to identify and police such flows. In addition, since cyberspace is based on an open-access philosophy that is embedded within the protocols and architecture upon which it is built, "fencing off" the domain into territorial sections would require a massive reengineering of its fundamental architecture. So the legal problem is as much conceptual and technical as it is legal, which confounds the search for a solution. In the meantime, in the international arena, it can be said that all actors have tremendous freedom of action in cyberspace.

Cyberspace—US Legal Authorities

Within the US government, legal authorities for cyberspace are distributed among several different departments, agencies, and commissions. The *United States Code* prescribes defense in Title 10, commerce in Title 15 (technical standards–making), law enforcement in Title 18, intelligence gathering in Title 50, and communications regulation in Title 154 (Federal Communications Commission). In addition, the National Security Council has oversight responsibility for cyberspace policy making, and Congress shapes the cyberspace legal environment through law making,

02-Text.indd 12 10/19/09 1:38:25 PM

legislative language, and funds appropriation. In contrast to the international arena, domestically, cyberspace operations must adhere to legal regimes concerned with law enforcement, intelligence gathering, and use of military force.[18] Issues germane to cyberspace operations include homeland defense and posse comitatus; right to privacy, eavesdropping, and the Foreign Intelligence Surveillance Act; and the right of self-defense under Article 51 of the United Nations charter.

With regard to the inherent right of self-defense, of particular interest is the question of when a cyber attack becomes an act of military aggression as opposed to espionage. Certainly, there have been large-scale cross-border cyberspace intrusions (e.g., Estonia and Georgia), but in those cases neither the United Nations nor the North Atlantic Treaty Organization moved to declare the event an act of military aggression. A Schmitt Analysis yields two factors making such a declaration problematic: presumptive legitimacy and responsibility, which get to the issue of attribution.[19] Presumptive legitimacy holds that "State actors have a monopoly on the legitimate use of kinetic force, while other non-kinetic actions—attacks through or in cyberspace—are often permissible in a wider set of circumstances; actions that have not been the sole province of nation-states are less likely to be viewed as military." Also, "if a state takes visible responsibility for any destructive act, it is more likely to be characterized as a traditional military operation."[20] Therefore, this ambiguity makes it much more difficult to declare a cyber event an attack. As compared to the other operational domains, such grey areas in international law afford both state and nonstate actors considerable cover to conduct wide-ranging cyberspace operations with potentially severe effects. However, if an event were classified as an attack, a response by a nation-state, including one that uses cyberspace, would have to adhere to the law of armed conflict tenets of military necessity, distinction, proportionality, and chivalry. In this regard, the legal requirements for military operations in cyberspace are no different than operations in air, land, sea, and space.

Further regulatory-like influence is exercised in the technical arena by industry consortiums and standards-making bodies. This complex of legal, regulatory, and standards

02-Text.indd 13 10/19/09 1:38:25 PM

structures—while facilitating free enterprise, respect for privacy, and property rights—creates inherent hurdles, obstacles, and barriers for the conduct of cyberspace operations. To be sure, thoughtful change is always an option to reduce complexity when it comes to the conduct of cyberspace operations, but the most pragmatic approach is for military practitioners to acknowledge this complexity, incorporate it into their plans, find ways to increase cooperation with others who have interests in cyberspace, and use existing structures to the best military advantage while working to implement positive change.

Defending Cyberspace

Perhaps the most significant asymmetric advantage afforded to an adversary is derived from the difficulty of defending a globally distributed, highly technical domain. Cyberspace is comprised of literally hundreds of millions of addressable devices that use both network communications protocol stacks and computer software and hardware stacks. Add to this the ubiquity of the electromagnetic spectrum, and the immensity of the defensive task becomes clear. Report after report of intrusions and growing attack sophistication provide irrefutable evidence that—at the moment—cyberspace operations favors the offense.

The preceding analysis of cyberspace characteristics reveals the multidimensional nature of cyberspace. Fundamentally, cyberspace is a man-made, evolving, and technological domain firmly rooted in the scientific reality of electromagnetics. It relies on electronic devices, including communications switches and computer processors, to transmit and process modulated signals. Cyberspace is not a global commons but rather is owned, although the standards which underpin its technological fabric are largely a cooperative enterprise. In addition, cyberspace is based on an architecture designed for efficient and resilient data exchange. These three factors—commercial electronics, ownership, and ease of data exchange—have given rise to a situation wherein both access to the domain and acquisition of sophisticated data manipulation tools are inexpensive. Skilled practitioners can use access and tools to great operational effect, given the speed and anonymity

02-Text.indd 14 10/19/09 1:38:26 PM

at which events occur under the cover of a complex maze of international and domestic legal, regulatory, and standards frameworks. Given that cyberspace operations currently favor the offense, cyberspace, properly used, can deliver an asymmetric advantage to both state and nonstate actors. For nation-states, cyberspace operations promise to be another powerful component of joint warfare; however, the armed forces must move out to achieve domain mastery to make the promise a reality.

Cyberspace is an enabler of globalization; rapid technological innovation; and faster decision making, product development, and service-delivery cycles.[21] These factors all serve to shift and undermine the status quo not only in business but also in government policy making and social discourse. If an organization is to prosper, premiums must be placed on knowledge about the environment and the speed with which organizations can act to take advantage of opportunities or deal with challenges. Richard A. D'Aveni describes this situation as hypercompetition. *Hypercompetition* is "an environment characterized by intense and rapid competitive moves, in which competitors must move quickly to build new advantages and [simultaneously] erode the advantages of their rivals."[22] Organizational survival hinges on the capacity for strategic and operational flexibility, leadership agility, and the ability to employ aggressive strategies to radically shift the status quo and destroy competitor advantage. Experimentation, rapid learning, and adaptation are prized, while penalties can be severe for slow and inappropriate responses.

Hypercompetition is a strong metaphor for the fundamental task of the armed forces—fighting and winning the nation's wars in a VUCA operational environment. From a war-fighting standpoint, hypercompetition evokes concepts, like full-spectrum dominance, the Clausewitzian Trinity, and operational art, that conceive of warfare as an intensely competitive struggle against cunning adversaries where measure is met by countermeasure in a lethal struggle to gain supremacy.[23] In a similar manner, cyberspace operations exemplify the hypercompetitive metaphor as these operations are conducted in the very domain that drives the hypercompetitive reality. The armed forces are de facto competitors in this domain in much the

02-Text.indd 15 10/19/09 1:38:26 PM

same way as commercial industry is, with the additional component of combat.

In cyberspace, competition moves at a rapid rate, in part due to the speed at which technology changes. Therefore, any competitive advantage achieved in cyberspace is tenuous and transient, and military superiority must be viewed as temporary, local, and continually at risk. Just as successful business organizations must have the ability to quickly conceive of and employ technological solutions to challenges arising in and from the domain, so must the armed forces, especially in terms of cyber defense. Success requires the armed forces to effectively deal with rapid change and complexity in order to achieve efficacy in support of national security priorities—requirements that are especially pertinent for cyberspace operations.

Command and Control and the Cyberspace Domain

Command and control is often misunderstood and not surprisingly so. Surveys of C2 literature reveal a wide variety of definitions, approaches, and models. In order to provide a common intellectual framework for understanding the C2 models to be discussed, this section describes how the term *command and control* emerged. In addition, particular attention will be paid to the match of organizational form to C2. Of central importance to this discussion is W. Ross Ashby's law of requisite variety, which states that an organization's internal regulatory mechanisms must be as diverse as the environment within which it is embedded.[24] Building on Ashby, Henk Volberda further asserts that the ability to deal with a hypercompetitive threat is directly related to how well an organization is structured internally to match the environment.[25] An organization with variety is capable of adapting appropriately to its environment or adapting its environment to the benefit of the organization. In the VUCA environment, careful consideration is needed to ascertain which organizational model will perform best, as the choice will directly affect the C2 method deployed to support the organization's mission. Choices must be made between stability and flexibility, specialization and generalization, and centralization and decentralization.[26] Too much internal complexity, and

02-Text.indd 16 10/19/09 1:38:26 PM

operating costs go up. Too little, and the organization will not produce the requisite variety needed to survive. It is clear that the correct choice of organizational form is critical to achieving cyberspace superiority.

After establishing a common understanding of C2, three main models for C2, with important variants, are presented: (1) the historical-traditional model (which includes the current DOD approach to cyberspace C2), (2) the cybernetic-systems model, and (3) the cognitive-psychological model. These models are also linked to the positive and negative characteristics of the hierarchical, heterarchical, and hybrid organizational forms. These three approaches are then vetted in terms of enduring C2 criteria, with particular focus on C2 organization and authorities. A recommendation is then made on a cyberspace C2 approach and what actions must be taken to implement it.

Historical-Traditional Model

The roots of the modern understanding of C2 can be traced to the industrial revolution with its requirements for the direction of large organizations engaged in complex mass-production processes. From this viewpoint, C2 is synonymous with the hierarchic organizational form and the emergence of the professional bureaucracy. Early organizational pioneers such as Max Weber, Frederick Taylor, and Frank and Lillian Gilbreth studied bureaucratic organization, work design, work measurement, standardization, and production control in order to best take advantage of the division of labor and specialization of tasks, thereby increasing production output and efficiency. Alfred P. Sloan is credited with establishing the modern hierarchical form of industrial organization with his divisional structure.[27] This structure emphasizes strict hierarchical command chains, centralized finance and planning, cross-divisional integration at the corporate level, and tight control of and reporting on highly prescribed production activities. This basic construction endures not only in the business arena but also in the organization of the armed forces, as seen in the plan employed to mobilize for and conduct the Second World War, the Defense Reorganization Act of 1947, and the Goldwater-Nichols Act of 1987.[28]

02-Text.indd 17 10/19/09 1:38:26 PM

From a technical perspective, the development of C2 as an organizational function reached new heights during the Second World War. The challenges brought on by the war resulted in the intensified development and use of mathematical methods to work on complex military C2 problems such as antiair defense, dynamic ballistic-firing solutions, large-scale logistics movements, and production and resource allocation decisions. During this period and shortly thereafter, statistical methods, operations research, linear programming, control theory, and systems analysis were applied to these problems on a nearly wholesale basis. In addition, the use of the first computers allowed mathematicians to solve more and more complex problems in less time. With the aid of computers, advanced computational methods were developed for simulation and forecasting of future results and to increase the efficiency of a hierarchical organization's processes. The increasing use of computers to actually perform organizational control functions contributed to the identification of C2 as inherently technology-enabled, thereby serving to blur the distinction between the purposes of command and control. In essence, the two were viewed as synonymous. Further evolution of C2 occurred during the Cold War as increasingly sophisticated and comprehensive computerized command and control systems were developed.

The Cold War ushered in yet another era of scientific development, given the need to ensure positive control of the destructive power of nuclear weapons and their delivery platforms, inform procurement decisions for increasingly complex weapon systems, manage the development and production of these systems, model and simulate nuclear warfare scenarios, and direct the actual conflict. With regard to nuclear conflict, it was quickly recognized that nuclear-armed jet bombers, and soon thereafter ballistic missiles, dramatically reduced the time to detect and intercept Soviet equivalents. This drove the need for a responsive and reliable C2 system, one based on state-of-the-art communications and computing technology. Due to the consequences of nuclear conflict and the requirement to retain tight control of its inherent destructive power, the function of command—the authority to direct military forces—was seen as inextricably tied to the organizational, procedural, and technical

02-Text.indd 18 10/19/09 1:38:26 PM

apparatus that allowed command to be exercised. To address this situation, the military designed and implemented a tightly coupled C2 system composed of computerized command, control, and communications systems and highly specified operational procedures that were in turn reinforced by rigorous training, exercise, and inspection standards. This highly prescribed and vertically integrated C2 system resulted in positive weapons control, assured receipt of orders, and high launch probability from the order to launch at the presidential level to the turning of keys in missile silos.

Historical-traditional C2 is virtually synonymous with the hierarchical organizational form, which has performed well during the industrial age and for modern government bureaucracies (fig. 2). Hierarchical organizations have a pyramidal structure and are characterized by specified superior-subordinate chains of command, specialization by function, uniform policies covering rights and duties, standardized procedures for each job, a career based on promotions for technical competence, impersonal relations, and all coordination being done from a level above the work being coordinated.[29] They reduce transaction costs by increasing scale and by placing control of resources into the hands of top-level managers and are well matched to stable, predictable environments and large-scale production. Hierarchies take advantage of the division of labor and economies of scale for known, structured problems where there is less of a requirement to coordinate and share information across functional lines of authority. Position, rank, and experience are of paramount importance with regard to power relationships, decision-making authority, and control of resources. Power and decision-making authority are concentrated at the top of the hierarchy and decrease as one moves to the lower levels of the organization.

Hierarchies also create "stovepipes," which are vertical, tightly coupled component organizations that are optimized for narrowly focused functions (e.g., intelligence, logistics, maintenance, etc.). The systems that support hierarchies are built and controlled by these stovepipes, making interoperability difficult to achieve. This, in turn, drives the need for systematic coordination and integration if the organization is to achieve its overall purpose. Information flow in a hierarchy is necessarily aggregated and filtered as it

02-Text.indd 19 10/19/09 1:38:27 PM

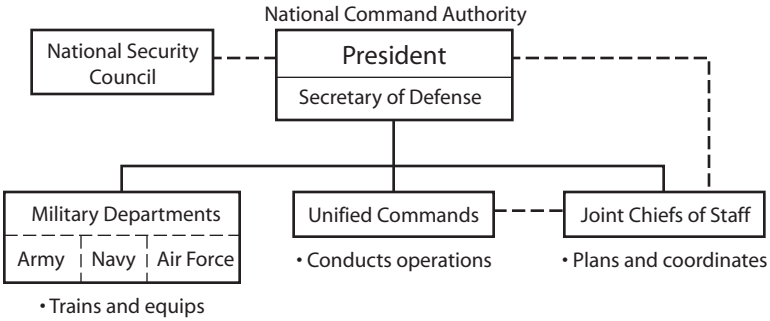

Figure 2. **National Command Authority**. (Adapted from JP-1, *Doctrine for the Armed Forces of the United States*, 14 May 2007, II-5.)

moves up the organization. Lower-level elements therefore have the most detailed local knowledge of the environment, whereas leaders at the top of the hierarchy have a broader picture of the global environment in which the organization operates. Courses of action are constructed globally at the highest command level and are progressively distilled down at each subordinate layer of command. Information flows within a hierarchy are largely confined to the stovepipes that created the information. There is little incentive to share information given that it is a source of knowledge—and therefore power—within the organization. Given the time it takes for information to flow from the bottom of the organization to the top, decision-making time horizons and perspectives are different between levels, yielding an asymmetry of decision-making focus. For the top of the pyramid, the longer time horizon and the higher position in the hierarchy result in decisions that are larger in scope and longer in term.

The historical-traditional military C2 model is closely tied to the hierarchical form. However, despite its success, the effectiveness of the hierarchical form is challenged by environmental complexity, accelerating change, and hypercompetition. Hierarchies are slow to respond to environmental changes in part due to the restricted, up-and-down flow of information. Although hierarchies can sometimes react quickly to narrowly defined crises, they can lack the requisite variety to respond appropriately. Horizontal communication is hampered, and

02-Text.indd 20 10/19/09 1:38:28 PM

functional loyalties of stovepipes inhibit communication, problem solving, and coordination. The focus on efficiency means functional components can make decisions that benefit them rather than the organization as a whole. Interests become entrenched, and the organization as a whole resists change. Experience and position can be more prized than knowledge, leading to poor decisions or lack of acceptance of new ideas.

Fast-forward to today, and it is readily apparent that the definition of C2 in JP 1-02 is at least partially a product of this industrial-age, nuclear-era understanding of the concept. The DOD, for example, defines *command and control* as "the exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. Command and control functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission."[30] Rooted in this definition are the traditional-historical notions of hierarchy, authority, and management of scale, complexity, and force. This understanding results in a distinct military approach to C2 that tightly couples its functions for the purpose of controlling military force in a hierarchical organization.

With regard to current DOD organization for cyberspace C2, at the top of the hierarchy is USSTRATCOM. USSTRATCOM is tasked, via the *Unified Command Plan* (*UCP*), to defend the armed forces' global information grid, the military-only portion of cyberspace. This means that USSTRATCOM has the combatant command authority to operate and defend the GIG. Indeed, USSTRATCOM states that part of its mission is "to ensure US freedom of action in space and cyberspace."[31] To accomplish this mission, it established two subordinate commands—the Joint Functional Component Command for Network Warfare and Joint Task Force-Global Network Operations. The JFCC-NW is responsible for coordinating and executing offensive operations enabled by the National Security Agency's (NSA) exploitative cyberspace operations. The JTF-GNO executes its mission to operate and defend military cyberspace through the issuance of various operational and defensive orders to

02-Text.indd 21 10/19/09 1:38:28 PM

subordinate commands. These orders direct GIG configuration changes, defensive measures, and reporting requirements. Until recently, these two organizations, while reporting to USSTRATCOM, were separate. However, understanding the lack of synergy and C2 difficulties encountered by "splitting" offense and defense, the DOD acted to remedy this with the November 2008 secretary of defense memo that placed JTF-GNO under the operational control of JFCC-NW.[32] Interestingly, the commanders of both the JTF-GNO and JFCC-NW maintain their current dual-hatted roles: the three-star commander of JTF-GNO is also the Defense Information Systems Agency commander, and the three-star commander of the NSA is also the JFCC-NW commander.

Within the USAF, the top-level organization for cyberspace now resides with Twenty-fourth Air Force under Air Force Space Command. Through Twenty-fourth Air Force, the USAF operates and defends its portion of cyberspace through its Air Force Network Operations command. It is from this organization that all operational and defensive actions are directed for Air Force cyberspace. AFNETOPS executes C2 of cyberspace through two Network Operations and Security Centers (NOSC). Each NOSC is assigned certain Air Force bases and is fully responsible for operating and defending the cyberspace that affects these bases. Agreements between the NOSCs and base communications squadron delineate responsibilities and help to ensure that the two organizations do not duplicate work. The implications for this arrangement are that wing commanders have lost control of the base-level computer network and have no say in the decisions regarding its operations and defense. Rather, these decisions are now made at AFNETOPS or the NOSCs. Another challenge arises when a squadron deploys to another combat command, thereby falling within that COCOM's authority.

Figure 3 shows the dual chain of command a communications squadron operates under in a deployed, wartime environment. Unlike the air, land, sea, and space domains, there is no discussion of combatant, operational, or tactical command as one expects regarding a domain of warfare. Instead, there are two lines of command authority directing the cyberspace activities of a base communications squadron

02-Text.indd 22 10/19/09 1:38:28 PM

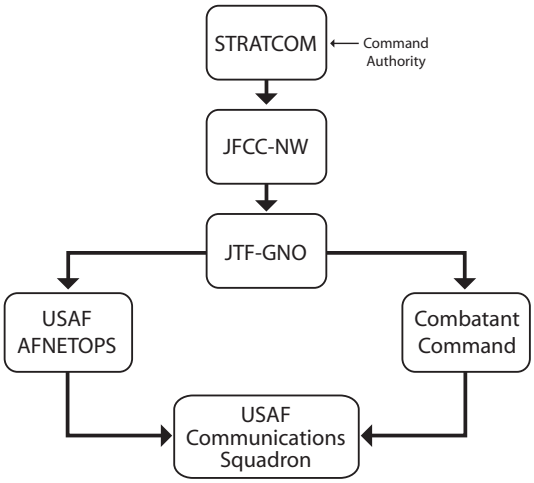

Figure 3. Current DOD cyberspace C2

in a deployed environment. This arrangement not only causes confusion and duplication of effort but also violates the principle of warfare known as unity of command. Compounding the confusion is the fact that the Air Force NOSCs, which direct all activity on AF networks, are outside of the combatant command's chain of command. Further, the COCOM is outside the functional line regarding how the Air Force operates, trains, and equips its forces. In the final analysis, the DOD, services, and COCOMs have established a traditional-hierarchical C2 structure that undermines unity of command, conflates the roles of the services and combatant commands, and—most critically—hamstrings the armed forces' ability to rapidly adapt to events and innovations arising in the cyberspace domain. This situation unnecessarily constrains freedom of action and prevents the agility needed to successfully operate in the domain.

In order to exercise cyberspace C2, legal authority must be assigned to a commander. Under the current cyberspace C2 construct, the authorities of the COCOMs and services overlap and are poorly defined, further complicating C2. The new *UCP* attempts to clarify some of these authority issues by clearly breaking out cyberspace operations as a new responsibility for the USSTRATCOM commander. Specifically, the new *UCP* states that

02-Text.indd 23 10/19/09 1:38:28 PM

USSTRATCOM is responsible for synchronizing planning for cyberspace operations, and will do so in coordination with other combatant commands, the Services, and as directed, appropriate U.S. government agencies. USSTRATCOM's specific responsibilities include:

(a) Directing Global Information Grid operations and defense.

(b) Planning against designated cyberspace threats.

(c) Coordinating with other combatant commands and appropriate U.S. government agencies prior to the generation of cyberspace effects that cross areas of responsibility.

(d) Providing military representation to U.S. national agencies, U.S. commercial entities, and international agencies for matters related to cyberspace, as directed.

(e) Advocating for cyberspace capabilities.

(f) Integrating theater security cooperation activities, deployments, and capabilities that support cyberspace operations, in coordination with the geographic combatant commanders, and making priority recommendations to the Secretary.

(g) Planning OPE [operational preparation of the environment], and as directed, executing OPE or synchronizing execution of OPE in coordination with the geographic combatant commanders.

(h) Executing cyberspace operations, as directed.[33]

At first glance, this appears to show that USSTRATCOM is in charge of the operation and defense of cyberspace, or at least the GIG. However, in lengthy joint staff–tank sessions, a new phrase was defined, and it becomes a critical point for this new *UCP*. Specifically, the tank defined the phrase "synchronize planning" to mean "Combatant Commanders charged with synchronizing planning lead a global collaborative planning process that includes other Combatant Commanders, Services, Combat Support Agencies, and applicable Defense agencies and Field Activities in support of a designated global mission or campaign plan. The phrase 'synchronizing planning' pertains specifically to planning efforts only and does not, by itself, convey authority to execute operations or direct execution of operations."[34]

This shows that disagreement remains between USSTRATCOM, the other combatant commands, and the services regarding overall authority for conducting cyberspace operations. The issue at hand is whether USSTRATCOM ought to have the authority to direct cyberspace operations within another COCOM's area of responsibility. Although the 2008 *UCP* attempts to resolve some of this disagree-

02-Text.indd 24 10/19/09 1:38:29 PM

ment by specifically mentioning cyberspace and assigning the mission to USSTRATCOM, it stops short of assigning USSTRATCOM the full authority to conduct cyberspace operations across the globe by the inclusion of the phrase "synchronize planning." In effect, this phrase allows the other combatant commands and services to disregard USSTRATCOM directives with which they disagree. There remains no clear authority for cyberspace C2.

This attempt to bring cyberspace operations under the command of a single COCOM will also cause other issues. For example, cyberspace activities such as network maintenance fall under the purview of the respective service, not a combatant command.[35] However, in a recent memorandum, the secretary of defense recently approved a definition for *cyberspace operations* as "the employment of cyber capabilities where the primary purpose is to achieve military objectives or effects in or through cyberspace. Such operations include computer network operations and activities to operate and defend the Global Information Grid."[36] The memorandum goes on to state that (1) the term *cyberspace operations* is consistent with the language used in the *National Military Strategy for Cyberspace Operations*, presidential directives, and the 2008 *Unified Command Plan*; (2) the methodology used for defining *cyberspace operations* is consistent with other joint operational definitions; and (3) *cyberspace operations* should encompass current computer network operations and activities to operate and defend the Global Information Grid.[37]

The first two points are significant because they show an attempt to forestall any further complaints or objections about this definition by declaring cyberspace operations to be fully consistent with all salient documentation currently published. The second point establishes cyberspace operations as an official DOD definition, to be incorporated into JP 1-02. However, the third point is significant because it states that network attack and network defense fall under cyberspace operations and include activities to "operate and defend the GIG." When viewed in light of the 2008 *UCP*, it appears that operations and maintenance activities, legally a service responsibility, are now assigned to a COCOM. This creates a situation wherein two separate entities—USSTRATCOM and the services—could validly claim the

02-Text.indd 25 10/19/09 1:38:29 PM

authority to direct military cyberspace operations in accordance with Title 10 of the *US Code* and DOD guidance. Some would argue that USSTRATCOM can avoid this issue by labeling all its cyberspace directives as defensive in nature, which is well within their purview, versus operations and maintenance, the purview of the services. However, it is inevitable that the services will protest this situation as an encroachment on their congressionally mandated Title 10 authorities to organize, train, and equip forces.

The current arrangement for cyberspace C2 mixes authorities and, as such, will continue to constrain the ability of the armed forces to conduct responsive cyberspace operations. The issues associated with USSTRATCOM, other combatant commands, and service prerogatives must be dealt with and call for a complete rethinking of the DOD's approach to cyberspace C2.

We argue that such an understanding of C2 is inappropriately restrictive for the cyberspace domain. What is needed is an approach to C2 that allows more flexibility to conceptualize and match the fundamental purpose of C2 to the environment in which it is exercised. Toward this end, we follow Berndt Bremer and George Orr, who view the purpose of C2 as the direction and coordination of operations to produce desired effects according to the commander's intent through the positioning of forces at the time and place they are needed.[38] From this perspective, effective command seeks to gain competitive advantage by controlling the military power distribution.[39] Control is achieved by gathering information about the operational environment, synthesizing the information to understand what actions must be taken, and translating that understanding into orders and direction that are executed through one's forces.[40] This understanding of C2 emphasizes goal, adversary (environment), and process rather than specification of authority, command chains, and organizational structure which unnecessarily limit—perhaps catastrophically—the action required of the C2 system. Given this understanding, we examine other alternatives for cyberspace C2 and commensurate organizational forms.

02-Text.indd 26 10/19/09 1:38:29 PM

Systems Theory and the Cybernetic-Systems Model

First articulated by biologist Ludwig von Bertalanffy in his book *General Systems Theory*, systems theory offers principles and methods with which to study the interactions, relationships, and structure of any set of interacting entities (a system).[41] Systems theory therefore takes a holistic perspective instead of a reductionist one: the behavior of a system is understood from the interactions of its parts rather than a detailed understanding of each of its parts. It is directed toward the analysis of "any group of objects that work in concert to produce some result. This could be a single organism, any organization or society, or any electro-mechanical or informational artifact."[42] Based on Bertalanffy's study of biologic organisms, two basic principles characterize systems theory. "First, all phenomena can be viewed as a web of relationships among elements, or a system. Second, all systems, whether electrical, biological, or social, have common patterns, behaviors, and properties that can be understood and used to develop greater insight into the behavior of complex phenomena."[43] Systems theory also endeavors to understand the interactions, processes, relationships, and macro behavior of the interdependent parts as a whole. Especially important are the complexity of the relationship of systems to their environments and the ability of systems to adjust to changes in the environment. Systems theory includes the following key traits:

- A system is a dynamic, complex, and interdependent whole, interacting as a structured functional unit.
- A system is holistic, exhibiting emergent properties not possible to detect by analysis of individual parts.
- A system is a community situated within an environment.
- Energy, materiel, and information flow among the different elements that compose the system.
- The elements of the system are differentiated and perform specialized functions.

02-Text.indd 27 10/19/09 1:38:29 PM

- Energy, materiel, and information flow from and to the surrounding environment via semipermeable membranes or boundaries.
- Energy, materiel, and information are transformed into outputs through processes by which the goals are achieved.
- Systems are often composed of entities seeking equilibrium but can exhibit other types of behavior (e.g., chaotic, oscillating).
- Systems are regulated through feedback.
- Systems can comprise parts of larger systems.
- A system is goal seeking, meaning that systemic interaction must result in some goal or final state.
- Systems exhibit equifinality, alternative ways of attaining the same objectives (convergence), and multifinality, attaining alternative objectives from the same inputs (divergence).[44]

The cybernetic-system model is the dominant C2 paradigm for nearly all researchers and systems builders and either explicitly or implicitly informs all C2 models (see fig. 4). A cybernetic system is composed of three fundamental components: (1) sensors that accept input from the environment, (2) processors that accept the input and transform it, and (3) output mechanisms that take the processed information and use it to change the behavior of the system. The cybernetic aspect of military operations is readily apparent given that these operations are a process by which a commander (sensor and processor) directs forces (people, processes/organizations, and technology organized into a system to produce output) to achieve comparative advantage over an adversary (interaction with the environment) through maneuver and the application of firepower (output and feedback). The science of cybernetics observes internal and external interactions "guided by the principle that numerous different types of systems can be studied according to principles of feedback, control, and communications."[45] Also key to understanding the concept of cybernetics is the idea of self-regulation. When a system senses a change in the environment, that information is used to adjust the behavior according to

02-Text.indd 28 10/19/09 1:38:30 PM

the goal of the system. The system then monitors the environment to ascertain if either the internal or external change has successfully aligned with the system's goal.

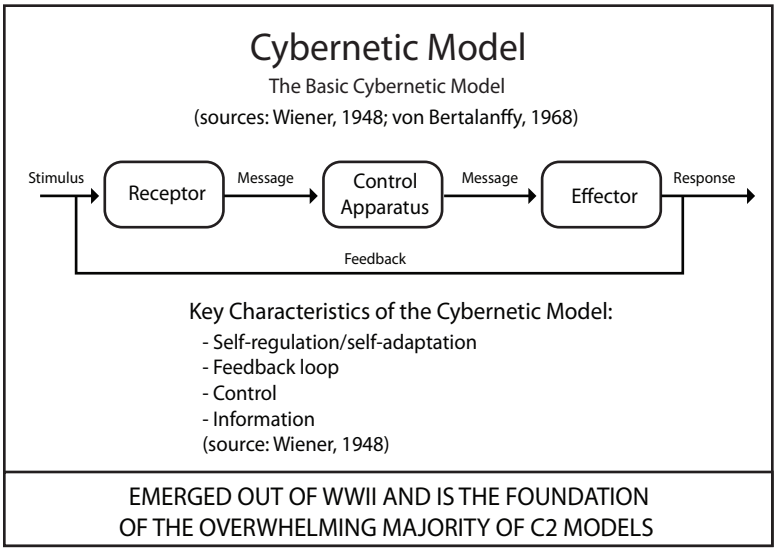

Figure 4. **The Cybernetic Model**. (Adapted from Norbert Wiener, *Cybernetics: Or the Control and Communication in the Animal and the Machine* [Cambridge, MA: MIT Press, 1948]; and Ludwig von Bertalanffy, *General Systems Theory: Foundations, Development, and Applications* [New York: George Braziller, 1968].)

Management cybernetics applies the principles of cybernetics and systems theory to organizations. Pioneered by Stafford Beer in 1959, management cybernetics examines the problems of control and decision making and the development of models in terms of the organization's goals; inputs, transformation of inputs, and outputs; regulation, control, and feedback; and capability to generate a variety of responses to environmental challenges.[46] Beer's Viable System Model (fig. 5) is an abstracted cybernetic description applicable to any organization that is a viable system and capable of autonomy. Beer developed the Viable System Model as a conceptual tool for designing, implementing, and reengineering organizations to improve an organization's ability to adapt

02-Text.indd 29 10/19/09 1:38:30 PM

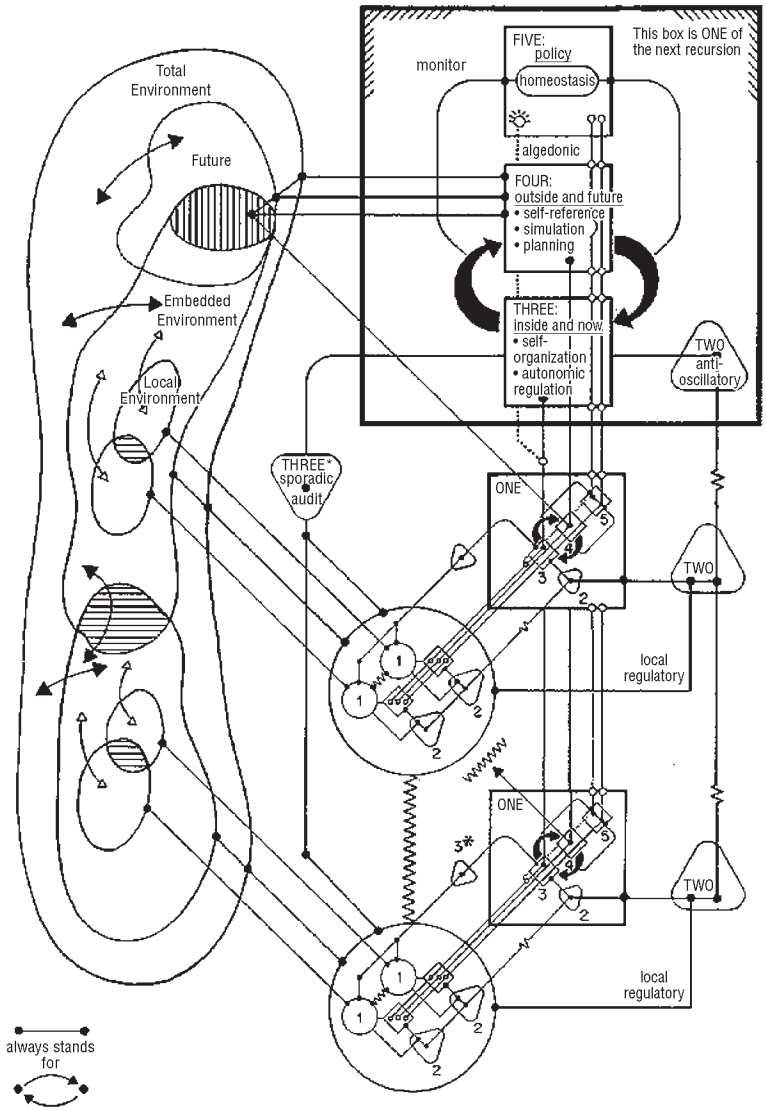

Figure 5. **Viable System Model**. (Adapted from Stafford Beer, *Brain of the Firm* [London: Penguin Press, 1972].)

and survive in its environment.[47] Beer's model examines five major elements that an organization depends on to achieve its purpose: (1) operations, (2) coordination between elements in the organization, (3) activity and resources that optimize the organization in relation to its environment, (4) the organization's environment, and (5) normative rules and regulations. The model then diagnoses the information flows that tie all the elements together in terms of sufficiency and richness. Multichannel robustness is especially emphasized as it allows the organization's structures and processes to work and deal with changes in the environment. Control, regulation, and communication are also optimized according to what the organization must do to be successful in its current operations, for its future, and in terms of its long-term identity and values.

Models Derived from Complexity Theory

The principles of cybernetics and systems theory have in turn informed the development of complexity theory. Complexity theory is a special application of systems theory, founded on biological science and the behavior of living organisms. It can be defined as "any system featuring a large number of interacting components, whose aggregate activity is nonlinear and typically exhibits hierarchical self-organization and evolving behavior when placed under stress from its environment."[48] From an organizational standpoint, complexity theory is used to explain how organizations adapt and survive in their environments.[49] John H. Holland, a complex and nonlinear systems pioneer, cites such characteristics as self-organization, emergent behavior, dispersed control, and adaptability as hallmarks of a complex organization. He describes complex adaptive systems as having the following qualities:

- Many agents acting in parallel in an environment produced by their interactions with other agents in the system.
- Because the agent is constantly acting and reacting to the other agents' actions, nothing in its environment is fixed.

02-Text.indd 31 10/19/09 1:38:31 PM

- Control is highly dispersed, therefore any coherent behavior there might be in the system has to arise from competition and cooperation among the agents themselves.
- Many levels of organization, with agents at one level serving as building blocks for the next level up.
- Constant rearrangement of the building blocks as a result of learning, experience, evolution, and adaptation.
- All anticipate the future to some degree, making attempts at prediction on the basis of models of their environment.
- All have niches they can exploit. Filling up one niche often opens up new ones that can be exploited, so the system never reaches equilibrium.
- Some dimensions can be improved upon but never optimized.
- The richness of the interactions within the system allows the system as a whole to undergo spontaneous self-organization.[50]

Self-organization is a process of attraction and repulsion in which the internal organization of a system, normally an open system, increases in complexity without being guided or managed by an outside source. Emergence is the process of deriving new and coherent structures, patterns, and properties as an organization works to fit itself to the environment. Emergent phenomena occur due to the pattern of interactions between the elements of the system over time and are observable at a macro level, even though they are generated by micro-level elements. Emergence is also related to dispersed control in that decisions are made by a variety of elements in the system rather than a central governor. Adaptability, or homeostasis, is the regulation of a system's internal environment so as to maintain a stable, constant condition in relation to environmental changes.

As a model for organizations, complexity theory has had a major impact on modern organizational theory. Some would even argue that cyberspace, despite being nonbiological, manifests such emergent properties. In fact, from an overall war-fighting standpoint, the United States

02-Text.indd 32 10/19/09 1:38:31 PM

Marine Corps (USMC) elevated complexity theory as its fundamental viewpoint for war fighting and explicitly views war-fighting organizations as complex systems.[51] The Marine Corps based its doctrinal decision on John Boyd's "Organic Design for Command and Control" (fig. 6) in support of its all-important maneuver warfare doctrine. However, viewing Boyd's design as simply a model for maneuver warfare diminishes its conceptual sophistication as a much broader model for organizational complexity in the face of complex operating environments. In this regard, Boyd was well ahead of his time and, in fact, has much in common with Stafford Beer and his Viable System Model.

Boyd's model more closely resembles a heterarchy. As an organizational form, a heterarchy more closely matches the requirements of a viable system or a complex adaptive system. A heterarchy is well suited to handling challenges from the environment that call for flexibility and adaptability. In a heterarchy, authority is laterally rather than vertically distributed and has no fixed superior decision-making chain. Heterarchies are characterized by interdependent relationships, dense information nets, and distribution of decision-making power. Organizational members participate in decision making regardless of their functional role, position, or rank. The premium for decision-making authority is based on knowledge and competence in solving problems rather than rank or time served in the organization. In addition, heterarchies process more information and use it more effectively than hierarchies. Communications channels are dynamic and are created and modified to reflect the needs of a particular situation or event. This ability to dynamically adapt to changing situations can be viewed as a way of employing requisite variety. The emphasis on knowledge contributes to the capacity of a heterarchy to generate a variety of solutions to problems that face the organization. Heterarchies have a greater ability to quickly integrate information from multiple sources and achieve flexibility to adapt to changing circumstances. A member of a heterarchy can be connected to any other members without needing to go through or get permission from anyone. In this way, a heterarchy distributes privilege and decision making among participants, in contrast to a hierarchy, which assigns more power and privilege to the members

02-Text.indd 33 10/19/09 1:38:31 PM

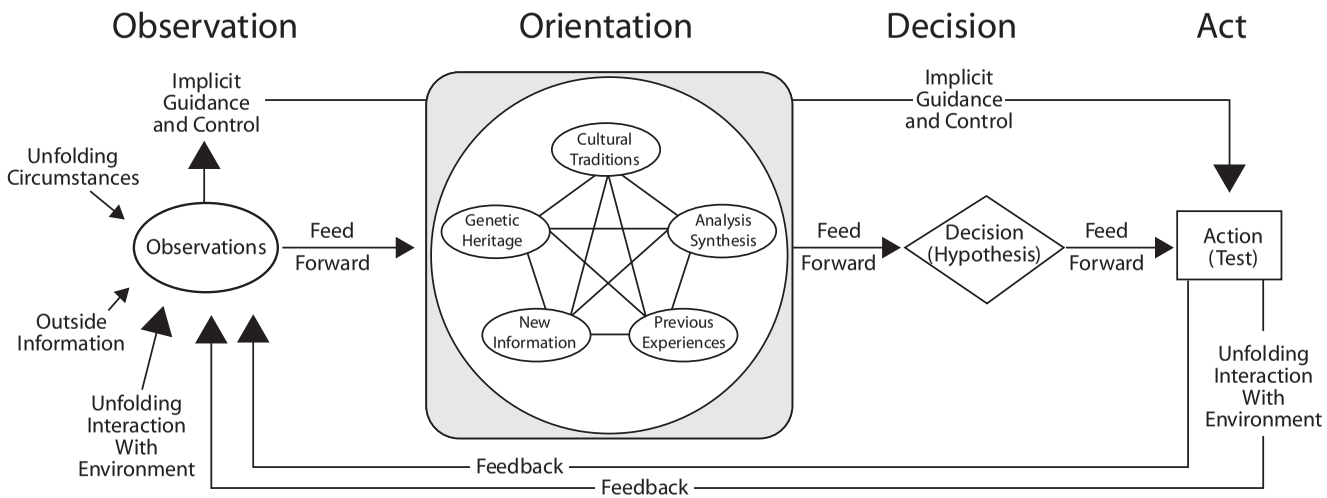

Figure 6. **Organic Design for Command and Control**. (Reprinted from John Boyd, "Organic Design for Command and Control," unpublished briefing, 1987.)

higher in the structure. Heterarchies include these distinctive features:

- Temporary associations out of a pool of people are emphasized rather than permanent structures and changing people.
- Overlap of responsibility is viewed as an advantage.
- Knowledge is resident throughout the organization and valued wherever it exists.
- Lateral communication is preferred over vertical communication.
- Strategic nodes can emerge at any place in the organization based on environmental contingencies and where the requisite knowledge to solve the problem exists.
- Upper levels of the organization are viewed as orchestrators of communication rather than solely agents of control, monitoring, and resource allocation.
- Strategy is a product of contributions across the network rather than formulation and dissemination by higher headquarters.

There are downsides to cybernetics, systems theory, and heterarchies. Save for Boyd's theories, the major criticism of cybernetics and systems theory is that they do not explicitly incorporate human agency or moral factors. The human aspects of interaction, cognition, and relationships and the moral and emotional aspects of conflict and cooperation are perceived to be immaterial to the function of the system and its output. In effect, these approaches reduce humans to mere parts or black boxes, making the models necessarily incomplete. With regard to complexity theory, its concrete scientific applications are so constrained (e.g., cellular behavior) that the generalization of the theory to broader classes, especially complex systems, is called into question. With regard to heterarchies, a significant investment of time, energy, and administrative and technical support infrastructure is needed to maintain the dense communications nets required to keep information flowing at the volumes required for effective collaboration,

02-Text.indd 35 10/19/09 1:38:32 PM

coordination, and action. In addition, the bias toward consensus in decision making in heterarchies creates the potential for confusion, sluggish response (although the response may be perfectly appropriate, it is too late to address the need), and gridlock. Finally, the lack of a central governor or prescribed chain of authority in a heterarchy results in difficulty in achieving global optimization, long-term plans of action, and predictable performance.

Cognitive-Psychological Models

As a remedy to the issues associated with cybernetics-systems models, several efforts have been made to address cognitive and psychological factors in command and control. Carl Builder's "Command Concept C2" is one such effort.[52] Builder's analysis is "driven by the need to separate the *intellectual* performance of the commander from the *technical* performance of the C2 system." (emphasis added) He further states that the "essence of command lies in the cognitive processes of the Commander."[53] Builder places emphasis on preparation for battle using the C2 system rather than orchestration and improvisation. In addition, he views information as important when developing the command concept, but real-time information is not especially relevant to altering the outcome of a conflict. In this regard, Command Concept C2 diverges dramatically from the cybernetic-systems view, which holds that information is essential to adaptation. However, in the end, Builder's theory is cybernetic in nature as he claims that "the formulation and transmission of the commander's concept could be considered as the content of the C2 system."[54] This means that the Command Concept C2 would have to be integrated into an overall C2 model, which in all likelihood would be cybernetic.

Another cognitive-psychological approach has been formulated by Ralph Stacey that incorporates relationship psychology to account for human interaction.[55] Stacey is a proponent of complexity theory but believes it has been misapplied. His approach is in part a reaction to the functionalist point of view embedded in all systems thinking, exemplified by his opinion that "the radical potential of theories of chaos and dissipative structures for organization

02-Text.indd 36 10/19/09 1:38:32 PM

theory tends to be obscured by simulations of this kind because the agents in the system are treated in an impersonal way." Instead, he takes a constructivist approach and proposes organizations as "complex responsive processes" based on interacting themes, conversations, and relationships. In other words, members of the organization continuously build an organizational narrative and thereby shape and reshape the power relationships and actions that the organization takes to deal with its environment. Stacey's approach is not so much a model as it is a competing philosophical viewpoint that places human interaction at the center of organizations. It is human-to-human interaction that exercises "ordinary daily human freedom. . . to weave actions into and around the system. . . in order to cope" with the environment and "get things done."[56] Stacy presents a compelling case, but at the moment it remains a theoretical one. Although models for complex responsive processes could emerge over time, for now the theory remains just that—theory.

The Hybrid Form

Both hierarchies and heterarchies have strengths and weaknesses. A critical weakness of hierarchies is that their top-down, authority-driven structure does not have the requisite variety to respond to the VUCA cyberspace environment. On the other hand, heterarchies lack a mechanism to provide for global direction and predictable performance. Another organizational option is to combine the strengths of both and minimize their weaknesses in order to provide the means to resolve the need for control and direction on the one hand and flexibility and adaptation on the other. A hybrid organization, properly designed, employs the best attributes of hierarchy and heterarchy. Command and control in a hybrid organization moves away from the traditional C2 model by uncoupling command from control.[57] Command involves the making of strategy and setting conditions for action through planning, resourcing, and facilitating information flow throughout the organization. Control is not a function of command but emerges as a function of organizational structure; resource, information, and knowledge flows;

02-Text.indd 37 10/19/09 1:38:32 PM

and the environment (which includes adversaries).[58] Beer's Viable System Model exemplifies this approach.

From a military standpoint, a key example of the hybrid form was during World War I on the Western Front when the German army formally implemented storm trooper tactics to break the stalemate of trench warfare with its lethal concentration of industrial age firepower. The Germans relied heavily on *Auftragstaktik*, or mission-type orders, as an approach to operations wherein "a military commander gives their subordinate leaders a clearly defined goal (the mission) and the forces needed to accomplish that goal with a time within which the goal must be reached. The subordinate leaders then implement the order independently. The subordinate leader is given, to a large extent, the planning initiative and a freedom in execution which allows flexibility in execution. Mission-type tactics free higher leadership from tactical details."[59]

To be sure, *Auftragstaktik* is a way of increasing the autonomy of the military organization, its capacity to maneuver quickly, and the initiative of its individual members in the face of a more complex and deadly battlefield environment. In effect, it patches around the inflexibility of a standard hierarchical organization and in its own way uniquely addresses the Clausewitzian realities of emotion, chance, and friction in the VUCA environment. Even though mission-type orders are institutionalized as part of US war-fighting doctrine, this does not go nearly far enough to allow the armed forces to succeed in the hypercompetitive cyberspace domain.[60] Although not touted as such, the concept of network-centric warfare has the potential to move the armed forces toward a hybrid organizational form more in tune with the requirements of a VUCA cyberspace environment. To do this, network-centric warfare should not be viewed as a "value proposition" or "new form of warfare" but rather as a way to increase the requisite variety of military organizations to deal with the VUCA environment.[61] Quite simply, an organization that is networked and provisioned with rich information flows, reconfigurable (and highly automated) processes, knowledge-based practitioners, and—especially key—control flexibility will display a greater capacity to successfully adapt to internal and external threats and exploit emerging opportunities. This type of organization

02-Text.indd 38 10/19/09 1:38:32 PM

blends the best of the hierarchical and heterarchical organizational forms and best applies to the cyberspace domain.

Criteria for Cyberspace Command and Control

Based on the above analysis, we argue that the historical-traditional model of C2 is inappropriately restrictive for the cyberspace domain. What is needed is an approach to C2 that allows more flexibility to conceptualize and match its fundamental purpose to the environment in which it is exercised. As stated previously, we use Bremer and Orr, who view the purpose of C2 as the direction and coordination of operations to produce desired effects according to the commander's intent through the positioning of forces at the time and place they are needed.[62] In addition, we adopt the positions of Builder and Georgiy Levchuk et al., and indirectly Volberda, who all advocate the conceptual delinking of command from control. In this view, the role of command is to continually survey the internal and external environments and ensure the organization's inputs, processes, interactions, and information flows are calibrated properly to achieve the organization's goals. Command involves the surveying, contemplating, and monitoring of the organization's fitness to the environment, and—when necessary—directing adjustments to the organization's structure in order to assure ongoing performance and survival. On the other hand, control is distributed throughout the organization and supported by dense nets of information flows, interactions, and knowledge-based decision making and engagement within the organization and with the environment.

The environment in which cyberspace operations are conducted produces certain mandatory requirements for the armed forces to successfully compete in the domain. The VUCA strategic environment; the speed, multidimensional complexity, and rapid technological innovation characteristic of cyberspace; and the nature of competition and change in cyberspace call for a C2 function that can continually match this environment and impact the environment itself for the benefit of the objectives for which cyberspace operations are employed. We propose seven criteria for cyberspace C2 that, if met, will place the armed forces in a position to

02-Text.indd 39 10/19/09 1:38:32 PM

best orchestrate cyberspace operations. These criteria include speed, adaptability, alertness, flexibility, responsiveness, resilience, and efficiency.

Speed is the sine qua non of cyberspace operations. Two types of speed are needed to compete in the cyberspace domain. First, the cyberspace C2 function and the technology that supports it must be capable of operating at speeds that enable appropriate responses and preventive actions. The speeds required will be variable but should incorporate the potential to achieve two-thirds the speed of light, which is built into the infrastructure of the domain itself. Second, cyberspace organizations must exhibit a speed of adaptation, planning, innovation, and implementation that meets or exceeds the rate of introduction of new attack vectors; novel tactics, techniques, and procedures; and technological innovation and implementation. This type of speed is necessarily slower than the information flows that transit cyberspace; however, without it, cyberspace C2 would not be capable of the adaptation needed to maximize the opportunity offered by the raw speed of the domain.

The hypercompetitive nature of cyberspace is characterized by continuous change and innovation. This requires an adaptable organization that is able through its C2 capability to (1) correctly perceive and appropriately deal with the external environment, (2) maintain high levels of information exchange and cooperation within the organization in order to formulate options, and (3) dynamically restructure processes, decision-making relationships, and behaviors to effectively implement change options to deal with the external environment. In terms of war fighting, cyberspace C2 must be adaptable in the face of all types of threats, across the entire range of military operations, and at all levels of war—strategic, operational, and tactical. The criteria of alertness, flexibility, responsiveness, and resilience are driven by the requirement for speed and are directly related to adaptability.

Alertness refers to timely awareness of existing or anticipated changes internal to the organization or in the operating environment.[63] It implies a multidimensional understanding of the current and projected status of the cyberspace domain in relation to the larger operational

02-Text.indd 40 10/19/09 1:38:33 PM

environment. Alertness also includes the capacity for situational awareness of the technical parameters that comprise the cyberspace infrastructure. Particularly important is the anticipation of adversary action and innovation, areas that require the intense application of intelligence operations. In addition, it points the organization toward the threats and opportunities associated with emerging capabilities and innovations and how the organization might deal with a threat or capitalize on an opportunity.[64]

According to Volberda, control flexibility is "the degree to which an organization has a variety of managerial capabilities and the speed at which they can be activated to increase the control capacity of management and improve the controllability of the organization."[65] Flexibility, then, can be viewed as the governor of adaptability and management's most important C2 task. Without it, an organization could fail to adapt or perhaps yield to a series of mindless adaptations that lead to disintegration. It follows that cyberspace C2 must be flexible enough to continue to operate in new or changed scenarios rather than remaining set in static configurations.

Responsiveness refers to the change capacity of an organization's processes once it is found that adjustments must be made to positively adapt to internal or external threats and opportunities.[66] Responsiveness relates to the development of variety in the choice and design of C2 processes in order to ensure that information inputs and decisions are transformed into the effects needed for a particular situation appearing in the environment. Responsive processes must be rapidly reconfigurable (polymorphic), automated where possible, and supported by appropriate levels of information, knowledge, competence, resources, and a cultural bias in the organization that understands and supports the need for change.

Resilience is the ability of cyberspace C2 to withstand attack or other forms of significant shock and discontinuity. A resilient cyberspace C2 capability would enable an organization to continue to operate, adapt, and survive in the VUCA cyberspace environment in the face of damage, degradation, disruption, or destruction.

Cyberspace C2 efficiency relates to how well information, time, and resources are used throughout the organization to feed processes and decision making in order to produce

02-Text.indd 41 10/19/09 1:38:33 PM

the desired output in the fastest, most economical, and highest quality way. In practice, cyberspace C2 efficiency can also reduce the deployed footprint, decrease the demand for scarce resources, and leverage economies of scale across time and space. Achieving cyberspace C2 efficiency requires a well-designed technical architecture, high-volume yet appropriately tailored and calibrated information flows, multidimensional situational awareness, and well-trained and educated practitioners.

To be sure, this set of criteria is abbreviated. However, the criteria are based on solid academic research and the practical experience of today's operational environment, and therefore for our purposes they are sufficient to begin to relate the requirements of the cyberspace domain to the choice of an appropriately matched C2 model. If one assumes that C2 is as essential for cyberspace operations as it is in any other war-fighting domain, the question at hand becomes what is the best form of C2 to exercise command and achieve desired military results in cyberspace? Although it stands to reason that cyberspace operations share similar C2 elements as other war-fighting domains such as organization; technical systems; and tactics, techniques, and procedures, we assert that the most effective C2 method for cyberspace operations will be heavily influenced by the nature of the domain itself and the environment within which it exists.[67]

Evaluation of Models

To arrive at a decision regarding which C2 model to recommend, we developed a straightforward decision matrix to evaluate each model based upon the seven criteria described earlier. We chose the decision matrix because we felt this tool would help us arrive at a quantitative decision even though the evaluation of how each model met the criteria is subjective. We will explain later how we arrived at each of our evaluations.

We grouped the various C2 constructs discussed earlier into three bins for the purpose of evaluation. These groupings centered on hierarchical, heterarchical, and hybrid C2 models. The matrix is filled in using a scale of 1 to 5, with 1 being the least effective and 5 being the most effective. We

02-Text.indd 42 10/19/09 1:38:33 PM

did not weight any criteria higher than any other because we felt each item was equally important to the evaluation of the C2 models (see fig. 7).

	Hierarchical	*Heterarchical*	*Hybrid*
Speed	3	4	5
Adaptability	1	3	3
Alertness	3	5	5
Flexibility	1	3	3
Responsiveness	3	5	5
Resilience	5	1	5
Efficiency	3	3	4
Totals	19	24	30

Figure 7. Decision matrix

As previously discussed, the hierarchical model is not quick to react to change in the environment nor is it a very quick method to disseminate orders from top to bottom. This is due to the necessary vetting and approval process that a hierarchical organization employs. The heterarchical model is very quick due to its distributed nature and reliance upon very distributed decision making. However, unlike the hierarchical model, there is a significant loss in uniform, homogenous decision making and synchronized, macro-oriented direction. The hybrid model, while not as quick to disseminate orders, still retains lower-level decision-making authority, which enables local C2 of an issue while still incorporating the best aspects of a hierarchical command structure. This allows time to be used most efficiently at multiple layers within this model due to each organization working its level of the action.

A heterarchical system is adaptable, depending upon the local organization. How the lower echelons of command decide to adapt to a certain situation results in a disjointed and inconsistent effort across the spectrum, as one organization will adapt to a changing environment one way while another adapts differently. While there should be resilient communication flows between the organizations' best practices and past lessons learned, this does not mean that

02-Text.indd 43 10/19/09 1:38:33 PM

these will necessarily be incorporated. In contrast, the hierarchical C2 structure is adaptable only so far as the parent command allows. In today's remote, deployed environment, commanders far removed from the scene may not fully understand the problem set or the need to deviate from established parameters. Additionally, the downward-directed adaptation may fall well short in time and purpose of what is needed at the local level and may not be feasible across the entire cyberspace domain. The hybrid C2 structure results in an organization that can adapt as the situation presents itself while still conforming to an established set of goal-oriented guidelines.

Assuming a level playing field (sufficient and similar technologies deployed across the three models), we believe that all three models can achieve similar levels of alertness. The technological advances of the last decade enable commanders in all domains of warfare to be cognizant of the lowest level of tactical events on the battlefield. So it can be with cyberspace. It is feasible for any C2 structure within cyberspace to be aware of the lowest-level event, to monitor it, and to direct actions mitigating the seriousness of the event. We could not discern a difference between the three models worthy of distinction.

As with adaptability, the hybrid model is the most flexible of the three. As stated before, combining the best attributes of each allows for a C2 structure that can change based upon localized mission requirements while still preserving a similar enough structure that it retains strong similarities to others. The hierarchical model, again, will flex as much as parent commands allow, which may not be enough for the situation and may not apply or be useful to the entire hierarchical C2 structure. The same adaptability detractors for the heterarchical model apply here as well.

Assuming proper intelligence and warning, a hierarchical model can be highly responsive. To pretend otherwise would be to dismiss centuries of warfare and all relevant examples. There are, obviously, instances where intelligence and warning were not available or properly utilized (the attack at Pearl Harbor as an example); however, this is not indicative of the entire C2 model. Likewise, a heterarchical model can also be exceptionally responsive across the entire range. Once again, one does run into the disjointed

02-Text.indd 44 10/19/09 1:38:34 PM

approach that a heterarchical model would employ across the entire cyberspace domain. As also mentioned before, the hybrid model would enjoy the benefits of being responsive to an event while working within the hierarchical guidance.

Both the hybrid and hierarchical models would prove to be resilient. By virtue of their nature, these two models enjoy the advantages of parent command structures enabling higher-level commands to implement initiatives to deal with eventualities. These types of issues could range from the physical destruction of a site to the failure of a local organization to implement certain actions designed to protect the entire cyberspace domain. However, a heterarchical organization could benefit from a resilient command structure that would enable it to survive multiple failures (regardless of source, duration, or effect) without serious degradation of the domain.

Assuming a level playing field, all of these C2 models can be efficient—there is no salient feature of the models that causes any to be unnecessarily inefficient. The heterarchical model could be the most inefficient of all three. While it can execute with minimal overhead, the disparate nature of the model results in increased overhead in training variances coupled with technical variances. The hierarchical model is likewise inefficient in that it seeks an overall approach to events and can be inefficient in allocation of resources and command guidance to deal with cyberspace events. The hybrid model incorporates the strengths of both as it enables C2 that is as efficient as the other attributes of the domain and C2 model allow.

Recommendations

The current hierarchical C2 structure which serves other domains well does not work at optimal levels for exercising global C2 of our newest domain—cyberspace. Accordingly, our research and analysis point to a new model to be embraced by the DOD—a hybrid model. To be sure, this model possesses its own unique weaknesses, and it will take time and effort to fully vet this new approach. Nevertheless, the hybrid model is the strongest of the three we analyzed for cyberspace C2. Figure 8, shown below, is how we envision

02-Text.indd 45 10/19/09 1:38:34 PM

the command and informational relationships in this new model. It is important to note the difference between the command and informational connections. We believe it is essential in the hybrid model that information about the domain as a whole, as well as specific incidents, is shared quickly and without prejudice so that commanders at all levels can take the necessary actions within their span of control. Important to note is that information flows exist at and between all levels of the C2 model and across current organizational lines. These flows enable the advantages discussed previously by allowing all levels of command to tackle problems simultaneously while also ensuring a unified higher headquarters command approach. Perhaps most importantly for this model, the power to respond to and deal with events is placed in the hands of personnel who have the best knowledge, no matter their rank. Teams are then rapidly formed, disbanded, and reformed as events continue to ebb, peak, and flow.

The next model (fig. 9) shows a basic organizational element of the hybrid model. We envision that these organiza-

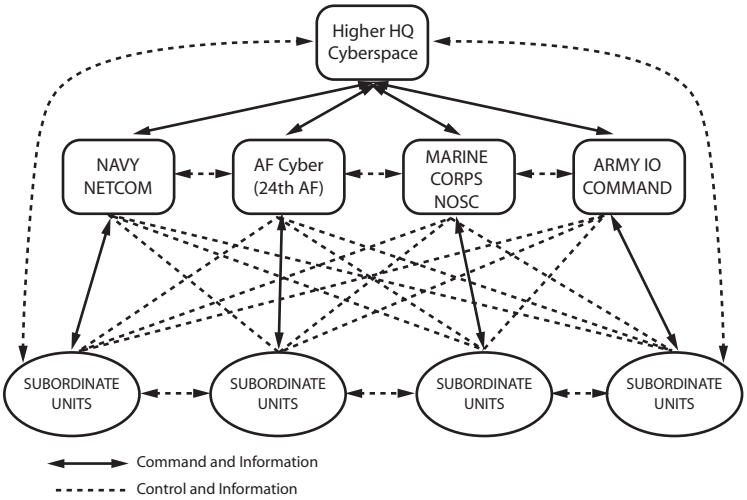

Figure 8. Proposed hybrid C2 model

02-Text.indd 46 10/19/09 1:38:34 PM

tions will utilize this basic model and its method of command and control to become part of a learning organization where all levels are informed and cognizant of events and activities, regardless of where these occur.

In order to successfully implement the hybrid model, it will be necessary to identify, recruit, and develop a new set

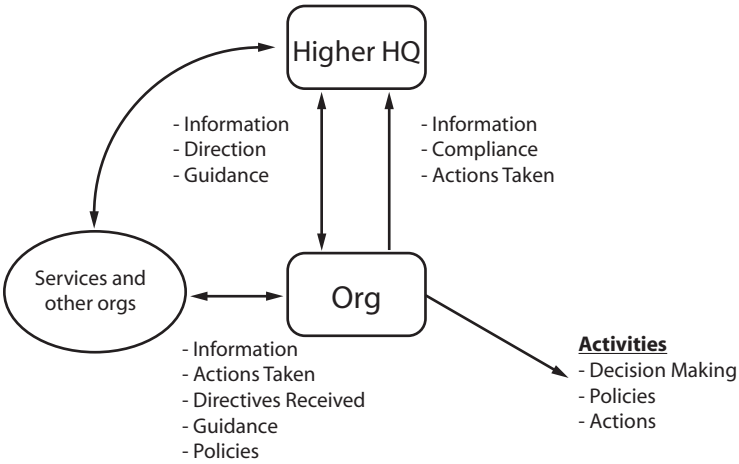

Figure 9. Organizational implementation of the hybrid C2 model

of "cyberspace warriors" who receive not only the unique training demanded of this domain but also the training and education regarding the new C2 model and how they are to operate within it. As author Col Thomas Hammes, USMC, states in his groundbreaking treatise on fourth-generation warfare (4GW), it will be necessary to "select and promote intelligent, innovative people and ensure that they are free to experiment and fail—provided they learn from those failures."[68] Not only is this important in 4GW, it will also be important to cyberspace in order to enable "a creative member [to] literally tap the world for information, ideas, and techniques that apply to his or her mission."[69] This will also require reeducating a whole new cadre of leaders who understand the importance of unconstrained information flow and how command must be employed in a highly adaptive organization.

02-Text.indd 47 10/19/09 1:38:35 PM

There will also be a need to increase resource assignment in this domain. In order to establish these robust information links where data, intelligence, and information regarding the domain are passed effortlessly and seamlessly, resources will need to be applied to enable this connectivity. Not only will large and redundant communications links need to be installed but also the necessary hardware and software to take advantage of these increased sources of information. These resources must be implemented such that these organizations embrace the new technologies which enable fast, adaptive processes using distributed, recombinant—and evolutionary—capability based on threat and environmental changes. We must continue to move to an autonomic technological infrastructure focusing on speed and "smart automated" infrastructure management.

Additionally, organizations will have to produce new doctrine and guidance on how to deal with the new information available to all. *Joint Vision 2020*, originally published in 2000, is on target—information superiority and the use of it is a requirement for successful cyberspace dominance as is network-centric warfare, properly understood. History is replete with examples of information being available but not acted upon with disastrous results (e.g., Maj Gen Joseph Hooker at Chancellorsville).

Changes in higher-level, presidential-granted authorities will also be required. While the 2008 *UCP* is a positive step forward, the lines of authority are still confused, ill defined, and ultimately inappropriate for cyberspace C2. It is necessary in the hybrid model to set the parameters for organizations to exercise their authority in a productive, collaborative fashion. This could require the movement away from the investiture of the cyberspace domain into a multirole functional combatant command and toward a domain-oriented command where the power of cyberspace can be maximized. This would also fulfill the tenants of unity of command and unity of effort, two long-enduring principles of warfare.

Another area to address is how joint and coalition forces will implement and work within this construct. One option to investigate further to organize and employ joint forces in accordance with the hybrid model is a joint force cyberspace component commander (JFCCC). A JFCCC will con-

02-Text.indd 48 10/19/09 1:38:35 PM

solidate the planning and operations functions currently performed by the various J-6 staffs across the combatant commands and place them in a full-time operational command structure. Additionally, it will elevate the cyberspace domain on par with similar functional components such as the joint force air, land, and maritime component commanders. Given that events are occurring continuously in cyberspace, it is possible that the JFCCC could be established as a global, full-time component of USSTRATCOM. Following this logic, it would be necessary to extend the cyberspace C2 model on a worldwide basis and ensure additional linkages to the operational level. To this end, one can conceive of "cyberspace coordination elements" or "directors of cyber forces–forward" embedded within the other combatant commands and service components. This is an area for further investigation as the DOD moves to adopt the hybrid model for cyberspace C2.

Conclusion

Based on the results of this study, it is clear that for the armed forces to have any realistic chance of success in cyberspace, they must acknowledge that the hybrid form is best matched to respond to the hypercompetitive, complex, and technological nature of the cyberspace domain. The hybrid form necessarily moves the armed forces away from the doctrinal superficialities of organizational wiring diagrams and traditional military-bureaucratic biases toward hierarchies and vertical control. Instead, with the hybrid form, cyberspace C2 is established upon a force that prizes knowledge ahead of rank and experience and that is bound together by rich, ubiquitous information flows that connect all participants at all levels of the cyber fight. It is able to achieve high operating speeds both in terms of the raw potential of information transfer and in terms of adaptation, planning, dynamic restructuring, decision making, innovation, and implementation. Such an organization is also able to handle the continuous change that is characteristic of the domain.

With the hybrid form, the cyber force is intrinsically postured to meet emerging threats at all levels of war due to its alertness, flexibility, responsiveness, and resilience. C2

02-Text.indd 49 10/19/09 1:38:35 PM

is based on a pervasive understanding of the internal and external operating environments, where decision makers translate deep situational awareness into anticipatory operational responses, scaled and tailored technologically and procedurally to the situation. Cyber leaders demonstrate war-fighting skill according to their ability to decisively calibrate the control needed to deal with an event and improve the controllability of the organization in the face of novel, fast-developing situations arising from the larger operational environment. These leaders are also the guarantors of the principle of variety in the choice, design, resilience, and efficiency of C2 processes. In the hybrid model, the cyber leader is the governor of cyberspace C2.

If the case for the hybrid form is convincing, the next step is to implement it throughout the DOD. In that regard, a JFCCC is a potential solution, providing a solid doctrinal basis for war-fighting organizations while also setting the stage to go beyond traditional doctrinal notions of C2 as applied to the exacting requirements of the cyberspace domain. The JFCCC organization must embody the very essence of the hybrid model wherein processes are rapidly reconfigurable, automated, and supported by a well-designed technical architecture, high-quality information flows, deep awareness, and thoroughly educated practitioners. The JFCCC must be simultaneously global, regional, and local in focus, an objective that will be achieved through the very structure, processes, practice, and governance of the hybrid form itself.

To be sure, some will question whether the hybrid model can work within the strict, hierarchical environment of the US military. True, our argument for a "new" cyberspace C2 approach is not exactly new. It has been echoed throughout the military literature since the onset of the "information revolution" in the 1990s, and the DOD has been wrestling with it for much of that time.[70] In the organizational development literature, the recognition goes back to the 1960s. However, what is new and what this study has shown is that the evidence for the need to move to the hybrid model is irrefutable—theory has merged with practice. The nature of the hypercompetitive cyberspace domain is such that the DOD *must* change its approach if cyberspace military superiority is to be achieved now and into the future. One need

02-Text.indd 50 10/19/09 1:38:35 PM

only recognize the astonishing number of computer network intrusions and data exfiltrations to understand the scope of the threat. Even our most sophisticated weapons systems are not exempt. Increasingly sophisticated cyber weaponry is readily available on hacker Web sites, and attack anonymity is easily achieved, making attribution and response problematic. Offensive overmatch is the rule, given that our defenses are largely reactive—engineered to respond after attacks have already occurred—if they are detected at all. As the world's most technologically advanced military, the armed forces are absolutely dependent on cyberspace to perform their war-fighting, intelligence, and business missions. The interdependent joint team cannot fight without cyberspace.

That is why, at its heart, this study is an urgent call for radical cyberspace C2 reform across the DOD. In order to meet the challenge of cyberspace operations today and into the future, the armed forces must move away from their traditional, hierarchical C2 structure. Instead, they must embrace the hybrid model and the opportunities for war-fighting performance offered by the establishment of a JFCCC structured along the lines of the model. We further call upon all cyberspace leaders to fight and overcome the endemic bureaucratic pathologies that mitigate against the needed change. Nothing less than the armed forces' ability to fight and win the nation's wars is at risk.

Notes

1. Nathan Thornburgh, "The Invasion of the Chinese Cyberspies (And the Man Who Tried to Stop Them)," *Time.com*, 29 August 2005, http://www.time.com/time/magazine/article/0,9171,1098961,00.html.

2. USSTRATCOM, *Joint Concept of Operations for Global Information Grid NetOps* (version 3), 4 August 2006. (Information extracted is unclassified.)

3. Hon. Robert M. Gates, secretary of defense, to secretaries of the military departments; chairman of the Joint Chiefs of Staff; under secretary of defense for policy; under secretary of defense for intelligence; assistant secretary of defense for networks and information integration; commander, US Strategic Command; and director, National Security Agency, memorandum, 12 November 2008.

4. *Wikipedia*, s.v. "Cyberspace," http://en.wikipedia.org/wiki/Cyberspace (accessed 15 November 2008).

5. Ibid.

02-Text.indd 51 10/19/09 1:38:35 PM

6. James M. Liepman, "Cyberspace: The Third Domain," *The Wright Stuff* 2, no. 23, 13 December 2007, 6, http://www.au.af.mil/au/aunews/archive/2007/0223.html.

7. Pres. George W. Bush, *National Strategy to Secure Cyberspace* (Washington, DC: The White House, February 2003), vii.

8. 10 *US Code*, sec. 118, "Quadrennial Defense Review," 8 January 2008, http://uscode.house.gov/uscode-cgi/fastweb.exe?getdoc+uscview+t09t12+54+0++%28QDR%29%20%20AND%20%28%2810%29%20ADJ%20USC%29%3ACITE%20AND%20%28USC%20w%2F10%20%28118%29%29% 3ACITE%20%20%20%20%20%20%20%20%.

9. Department of Defense, *Quadrennial Defense Review* (Washington, DC: Department of Defense, February 2006), 23.

10. Ibid., 37.

11. Chairman of the Joint Chiefs of Staff, *National Military Strategy for Cyberspace Operations*, December 2006, ix.

12. Dr. Kamal T. Jabbour, *50 Cyber Questions Every Airman Can Answer* (Rome, NY: Air Force Research Lab, 2008), 3.

13. Joint Publication (JP) 1-02, *Department of Defense Dictionary of Military and Associated Terms*, April 2001 as amended through 17 March 2009, 141.

14. University of Minnesota, "Minnesota Internet Traffic Studies," http://www.dtc.umn.edu/mints, 2008; and Andrew Odlyzko, "Threats to the Internet: Too Much or Too Little Growth?" *Internet Evolution*, 25 February 2008, http://www.internetevolution.com/author.asp?section_id=592&doc_id=146747.

15. United Nations, *Glossary of Environment Statistics: Studies in Methods*, series F, no. 67 (New York: United Nations, 1997).

16. This is the speed of light through glass.

17. OC-768 supports rates of 40 gigabits per second on a fiber-optic carrier using dense wavelength division multiplexing. The 1.2-second calculation is using quadrature amplitude modulation, a method of conveying data in which the amplitude of two transmission waves which are 90 degrees out of phase with each other is changed. These changes represent the data signal.

18. Thomas C. Wingfield and James B. Michael, *An Introduction to Legal Aspects of Operations in Cyberspace*, Technical Report no. NPS-CS-04-005 (Monterey, CA: Naval Postgraduate School, 28 April 2004).

19. Ibid., 11–12.

20. Ibid., 12.

21. Thomas L. Friedman, *The World Is Flat: A Brief History of the 21st Century* (New York: Farrar, Straus & Giroux, 2005).

22. Richard A. D'Aveni, *Hypercompetition: Managing the Dynamics of Strategic Maneuvering* (New York: Free Press, 1994), 217.

23. JP 1-02, *Department of Defense Dictionary*, defines *full spectrum dominance* as "the cumulative effect of dominance in the air, land, maritime, and space domains and information environment that permits the conduct of joint operations without effective opposition or prohibitive interference" (223); Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1989); and JP 3-0, *Joint Operations*, 2006, II-5.

02-Text.indd 52 10/19/09 1:38:36 PM

24. William Ross Ashby, *Introduction to Cybernetics* (London: Chapman & Hall, 1957).

25. Ibid.; Thomas R. Burns and George M. Stalker, *The Management of Innovation* (London: Tavistock Publications, 1961); and Henk W. Volberda, "Toward the Flexible Form: How to Remain Vital in Hypercompetitive Environments," *Organization Science* 7, no. 4 (July–August 1996): 359–74.

26. Marshal Van Alstyne, "The State of Network Organization: A Survey in Three Frameworks," *Journal of Organizational Computing* 7, no. 3 (1997): 83–151.

27. John C. Wood, *Alfred P. Sloan, Jr.: Critical Evaluations in Business and Management* (New York: Routledge, 2003).

28. Mark Skinner Watson, *Chief of Staff: Prewar Plans and Preparations* (Washington, DC: Center for Military History, 1991); US Congress, *National Security Act of 1947 (Public Law 253, 80th Congress, July 26, 1947, 61 Stat. 495) as amended* (Washington, DC: Government Printing Office [GPO], 1953); and US Congress, *Goldwater-Nichols Department of Defense Reorganization Act of 1986* (Washington, DC: GPO, 1986).

29. Gareth Morgan, *Images of Organization* (Thousand Oaks, CA: Sage Publications, 2006).

30. JP 1-02, *Department of Defense Dictionary*, 103.

31. USSTRATCOM, "USSTRATCOM Vision, Mission, Priorities," http://www.stratcom.mil/mission.

32. Gates to secretaries of the military departments et al., memorandum.

33. Robert M. Gates, *Unified Command Plan 2008* (Washington, DC: US Department of Defense, 3 October 2008). Document was signed on 23 December 2008.

34. Ibid., 30.

35. Lt Col Sam Arwood, "Cyberspace as a Theater of Conflict: Federal Law, National Strategy and the Departments of Defense and Homeland Security" (graduate research project, Air Force Institute of Technology, 2007), 15–16.

36. Gen James E. Cartwright, vice-chairman of the Joint Chiefs of Staff, to deputy secretary of defense, memorandum, 29 September 2008.

37. Ibid.

38. Berndt Brehmer, "Understanding the Functions of C2 Is the Key to Progress," *The International C2 Journal* 1, no. 1 (2007): 211–32, http://www.dodccrp.org/html4/journal_v1n1.html.

39. George E. Orr, *Combat Operations C3I: Fundamentals and Interactions* (Maxwell AFB, AL: Air University Press, 2004).

40. Brehmer, "Understanding the Functions of C2," 211–32.

41. Ludwig von Bertalanffy, *General Systems Theory: Foundations, Development, and Applications* (New York: George Braziller, 1968).

42. *New World Encyclopedia*, s.v. "Holism: Systems Theory," http://www.newworldencyclopedia.org/entry/Holism (accessed 1 February 2008).

43. Ervin Laszlo, "The Meaning and Significance of General Systems Theory," *Behavioral Science* 20, no. 1 (1974): 9–24.

44. *Wikipedia*, s.v. "Systems thinking," http://en.wikipedia.org/wiki/Systems_thinking (accessed 11 July 2009).

02-Text.indd 53 10/19/09 1:38:36 PM

45. David A. Mindell, "Cybernetics: Knowledge Domains in Engineering Systems" (research paper, Massachusetts Institute of Technology, Fall 2000), http://web.mit.edu/esd.83/www/notebook/Cybernetics.PDF.

46. Stafford Beer, *Cybernetics and Management* (London: English University Press, 1959).

47. Stafford Beer, *Brain of the Firm* (London: Penguin Press, 1972).

48. Luis M. Rocha, "Complex Systems Modeling: Using Metaphors from Nature in Simulation and Scientific Models," *BITS: Computer and Communications News*, Computing, Information, and Communications Division, Los Alamos National laboratory, November 1999, http://informatics.indiana.edu/rocha/complex/csm.html.

49. Philip Anderson, "Complexity Theory and Organization Science," *Organization Science* 10, no. 3 (May–June 1999): 216–32.

50. John H. Holland, *Hidden Order: How Adaptation Builds Complexity* (New York: Basic Books, 1995), 10–34.

51. United States Marine Corps, Marine Corps Doctrine Document 1, *Warfighting*, 1997.

52. Carl H. Builder, Steven C. Bankes, and Richard Nordin, *Command Concepts: A Theory Derived from the Practice of Command and Control* (Monterey, CA: National Defense Research Institute, RAND Corporation, 1999).

53. Ibid., xiv.

54. Ibid.

55. Ralph D. Stacey, Douglas Griffin, and Patricia Shaw, *Complexity and Management: Fad or Radical Challenge to Systems Thinking?* (New York: Routledge, 2000).

56. Ibid., 6, 60.

57. Georgiy M. Levchuk, Feili Yu, Krishna R. Pattipati, and Yuri Levchuk, "From Hierarchies to Heterarchies: Application of Network Optimization to Design of Organizational Structures," *Proceedings of the 2003 International Command and Control Research and Technology Symposium,* Washington, DC, June 2003, 2.

58. Ibid.

59. Thomas H. Barth, "Auftragstaktik: A Leadership Philosophy for the Information Age" (monograph, School of Advanced Military Studies, Fort Leavenworth, KS, 1995).

60. Chairman of the Joint Chiefs of Staff, Joint Publication 3-0, *Operations,* 2006.

61. Arthur K. Cebrowski and John J. Gartska, "Network-Centric Warfare: Its Origins and Future," *US Naval Institute Proceedings* 124, no. 1 (January 1998): 28–35.

62. Brehmer, "Understanding the Functions of C2," 211–32.

63. Clyde W. Holsapple and Xun Li, University of Kentucky, "Understanding Organizational Agility: A Work-Design Perspective" (paper presented at the 13th International Command and Control Research and Technology Symposia, 17–19 June 2008, Seattle, WA).

64. V. Sambamurthy, A. Bharadwaj, and V. Grove, "Shaping Agility through Digital Options: Reconceptualizing the Role of Information Technology in Contemporary Firms," *MIS Quarterly* 27, no. 2: (2003): 236–63.

65. Henk W. Volberda, *Building the Flexible Firm: How to Remain Competitive* (Oxford: Oxford University Press, 1999), 100.

02-Text.indd 54 10/19/09 1:38:36 PM

66. Ibid., 104–5.

67. Thomas R. Burns and George M. Stalker, *The Management of Innovation* (London: Tavistock Publications, 1961).

68. Col Thomas X. Hammes, USMC, *The Sling and The Stone: On War in the 21st Century* (St. Paul, MN: Zenith Press, 2006), 274.

69. Ibid., 275.

70. Authors: The DOD has seen many approaches to cyberspace, none of them all encompassing or entirely satisfying. They include command and control warfare (C2W); command, control, communications, and intelligence (C3I); command and control intelligence, surveillance, and reconnaissance (C2ISR); command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR); information warfare; the various iterations of information operations; and network-centric warfare.

02-Text.indd 55 10/19/09 1:38:36 PM

02-Text.indd 56 10/19/09 1:38:37 PM

Abbreviations

COCOM	combatant command
CONOPS	concept of operations
C2	command and control
DOD	Department of Defense
4GW	fourth-generation warfare
GIG	global information grid
ICANN	Internet Corporation for Assigned Names and Numbers
JFCCC	joint force cyberspace component comander
JFCC-NW	Joint Functional Component Command for Network Warfare
JP	joint publication
JTF-GNO	Joint Task Force-Global Network Operation
NETOPS	network operations
NMS-CO	*National Military Strategy for Cyberspace Operations*
NOSC	Network Operations and Security Center
NSA	National Security Agency
QDR	*Quadrennial Defense Review*
TCP/IP	Transmission Control Protocol/ Internet Protocol
UCP	*Unified Command Plan*
USMC	United States Marine Corps
USSTRATCOM	United States Strategic Command
VUCA	volatility, uncertainty, complexity, and ambiguity

03-abbreviations.indd 57 10/19/09 1:38:58 PM