Military Perspectives on Cyberpower

edited by **Larry K. Wentz**
Charles L. Barry
Stuart H. Starr

PUBLISHED BY THE CENTER FOR TECHNOLOGY AND NATIONAL SECURITY POLICY AT THE NATIONAL DEFENSE UNIVERSITY
WASHINGTON, DC
July 2009

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
JUL 2009		**00-00-2009 to 00-00-2009**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Military Perspectives on Cyberpower	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **National Defense University,Center for Technology and National Security Policy,300 5th Avenue SW,Washington,DC,20319**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

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

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**128**	

This book was published by *the National Defense University Center for Technology and National Security Policy, Fort Lesley J. McNair, Washington, DC. CTNSP publications are available online at* www.ndu.edu/ctnsp/publications.html.

Contents

Glossary v
Preface xi

Chapter 1

Military Service Cyber Overview 1
Elihu Zimet and Charles L. Barry

Chapter 2

A Unified Field Theory for Full-Spectrum Operations: Cyberpower and the Cognitive Domain 29
Jeffrey G. Smith, Jr.

Chapter 3

Navy Operations to Achieve Military Power in Cyberspace: A Draft Concept for Navy Computer Network Operations 73
Michael A. Brown

Chapter 4

The Air Force in Cyberspace: Five Myths of Cyberspace Superiority 87
Forrest B. Hare and Glenn Zimmerman

Chapter 5

Marine Corps Cyberspace in Support of MAGTF C2: By Many a Marine, With a Single Vision 97
John L. Cloninger

About the Authors 113

Glossary

Abbreviation	Meaning
ABCA	American, British, Canadian, and Australian
ACC	Air Combat Command
AEHF	Advanced Extremely High Frequency
AOR	Area of Responsibility
ASD(NII)	Assistant Secretary of Defense (Networks and Information Integration)
BDA	Battle Damage Assessment
C2	Command and Control
C4	Command, Control, and Communications
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance
CCEB	Combined Communications-Electronics Board
CCJO	Capstone Concept for Joint Operations
CDS	Cross Domain Solution
CENTCOM	Central Command
CENTRIXS	Combined Enterprise Regional Information Exchange System
CG	Commanding General
CID	Center for Information Dominance
CIO	Chief Information Officer
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CMO	Civil Military Operations
CMOS	Cognitive Model of the Simulation
CNA	Computer Network Attack
CND	Computer Network Defense
CNE	Computer Network Exploitation
CNO	Computer Network Operations

Abbreviation	Meaning
COCOM	Combatant Commander
COA	Course of Action
COC	Combat Operations Center
COG	Center of Gravity
COI	Community of Interest
CONOPS	Concept of Operations
CT	Cryptological Technicians
CTI	Cryptological Technicians (Interpretive)
CTN	Cryptological Technicians (Networks)
CTR	Cryptological Technicians (Collection)
CTT	Cryptological Technicians (Technical)
DIRSUP	Direct Support
DISA	Defense Information Services Agency
DOD	Department of Defense
DOTMLPF	Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, Facilities
DR	Disaster Relief
EDS	Electronic Data Systems
EW	Electronic Warfare
EUCOM	European Command
FCS	Future Combat Systems
FIOC	Fleet Information Operations Center
FM	Field Manual
FOS	Family of Systems
GCM	GIG Content Manager
GDP	Gross Domestic Product
GEM	GIG Enterprise Management
GIG	Global Information Grid
GND	GIG Network Defense
GPS	Global Positioning System
HA	Humanitarian Assistance

Abbreviation	Meaning
HW	Hardware
I&W	Indications & Warning
IA	Information Assurance
ICT	Information Communications Technology
IED	Improvised Explosive Device
IO	Information Operations
IP	Internet Protocol
IPE	Intelligence Preparation of the Environment
ISAF	International Security Assistance Forces (Afghanistan)
ISR	Intelligence, Surveillance, and Reconnaissance
IT	Information Technology
JBMC2	Joint Battle Management Command and Control
JCIDS	Joint Capabilities Integration and Development System
JC3IEDM	Joint Consultation Command and Control Information Exchange Model
JFC	Joint Force Commander
JFCC-NW	Joint Functional Component for Network Warfare
JFCOM	Joint Forces Command
JIC	Joint Integrating Concept
JIOWC	Joint Information Operations Warfare Center
JITC	Joint Interoperability Test Command
JNN	Joint Network Node
JS	Joint Staff
JSTARS	Joint Surveillance Target Acquisition System
JTA	Joint Technical Architecture
JTF	Joint Task Force
JTF-GNO	Joint Task Force–Global Network Operations
JTRS	Joint Tactical Radio System
JWICS	Joint Worldwide Intelligence Communications System
LAN	Local Area Network

Abbreviation	Meaning
MAGTF-IO	Marine Air-Ground Task Force-Information Operations
MANET	Mobile, Ad Hoc Network
MCEITS	Marine Corps Enterprise Information Technology Services
MCSC	Marine Corps Systems Command
MCNOSC	Marine Corps Network Operations and Security Command
MEF	Marine Expeditionary Force
MHQ	Maritime Headquarters
MNF-I	Multi-National Force – Iraq
MOP	Measure of Performance
MOC	Maritime Operations Center
MSC	Major Subordinate Command
MUOS	Mobile User Object System
NATO	North Atlantic Treaty Organization
NCAT	Navy Cyber Attack Team
NCDOC	Navy Cyber Defense Operations Command
NCES	Net Centric Enterprise Services
NCO	Net Centric Operations
NCOE	Net Centric Operational Environment
NCOW	Net Centric Operations and Warfare
NCW	Net Centric Warfare
NECC	Naval Expeditionary Combat Command
NIOC	Navy Information Operations Command
NIPRNET	Non-classified Internet Protocol Router Network
NGOs	Non-government Organizations
NMCI	Navy Marine Corps Intranet
NNEC	NATO Net Enabled Capability
NNWC	Naval Network Warfare Command
NSA	National Security Agency

Abbreviation	Meaning
NSC	Network Service Center
NWDC	Naval Warfare Development Center
OE	Operational Environment
OGA	Other Government Agencies
OIF	Operation Iraqi Freedom
OMB	Office of Management and Budgeting
OODA	Observe, Orient, Decide, Act
OPSEC	Operations Security
OSD	Office of the Secretary of Defense
PA	Public Affairs
PACOM	Pacific Command
PDA	Personal Digital Assistant
PSYOP	Psychological Operations
QDR	Quadrennial Defense Review
RDT&E	Research, Development, Test & Evaluation
RF	Radio Frequency
SCADA	Supervisory Control and Data Acquisition
SIPRNET	Secure Internet Protocol Router Network
SOF	Special Operations Force
SOS	System of Systems
SPG	Strategic Planning Guidance
SSG	Strategic Studies Group
SSTR	Stability, Security, Transition, and Reconstruction
STRATCOM	Strategic Command
STU	Secure Telephone Unit
SW	Software
TACTOM	Tactical Tomahawk
TCA	Transformational Communications Architecture
TD	Target Development
TMOS	Technical Model of the Situation
TOE	Table of Organization and Equipment

Abbreviation	Meaning
TRADOC	Training and Doctrine Command
TPG	Transformational Planning Guidance
TSAT	Transformational Satellite Program
TTPs	Tactics, Techniques, and Procedures
UCP	Unified Command Plan
UOC	Unit Operations Center
USFFC	US Fleet Forces Command
VA	Vulnerability Assessment
VCJCS	Vice Chairman Joint Chiefs of Staff
WIN-T	Warfighter Information Network–Tactical

Preface

During the course of nearly two years, the Center for Technology and National Security Policy (CTNSP), National Defense University (NDU), has conducted extensive research to identify and explore major cyber issues. These activities were performed in response to a request in the 2006 Quadrennial Defense Review (QDR). The result of that research is documented in a book entitled *Cyberpower and National Security*.

As part of that research, CTNSP convened several workshops to address challenges in cyberspace, cyberpower, cyberstrategy, and institutional factors. Several representatives from the military Services participated extensively in those workshops. During those workshops, a variety of cyber issues emerged about the roles of the Services in the areas of roles and missions and the creation of needed intellectual capital. As a consequence, we turned to each of the Services and asked if they could contribute to the public debate on these cyber issues.

Subsequently, each of the Services identified volunteers who graciously generated white papers to illuminate the cyber debate. It must be emphasized that the individual white papers have not been reviewed by their Services. They constitute the individual opinions of the contributors who sought to identify and explore the key cyber challenges that the Services must address. In addition, to put those contributions in context, Dr. Elihu Zimet and Dr. Charles Barry from CTNSP have written an initial chapter that provides a framework for the Service chapters. In that chapter, they briefly summarize the major findings and recommendations from the individual authors.

We are delighted to present these white papers in this volume. We trust they will help to identify and address many of the key cyber issues that the national security community must confront during the coming decade.

Chapter 1

Military Service Cyber Overview

Elihu Zimet and Charles L. Barry

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

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

Two observations are made up front. First, the growth and globalization of cyberspace technology, and the corresponding need for adaptive

information-based operational concepts to meet new military missions that now include the use of both hard and soft power from warfighting to HA/DR and SSTR, required development of a military cyberpower strategy. The need to jointly structure the military to perform new operations and accomplish new missions, including the connectivity to coalition partners, creates an enduring challenge. Operational concepts such as the effectiveness of NCO in irregular warfare scenarios are still being tested.

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

Introduction

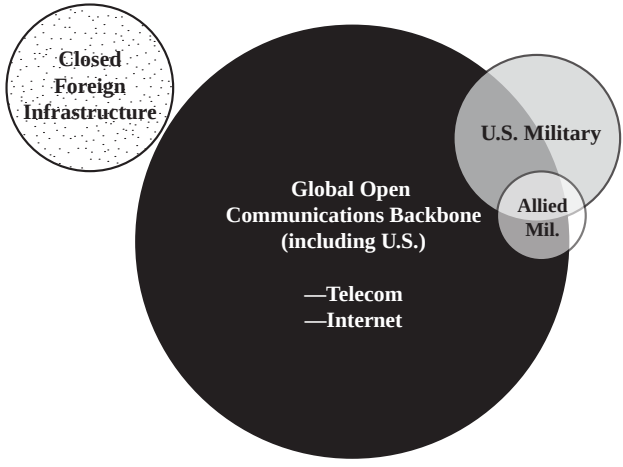
The possession of accurate and timely knowledge and the unfettered ability to distribute it as information has always been a *sine qua non* of warfighting. As cyberspace has developed, particularly in the area of networked, computer-based, information systems such as the Internet,[1] the introduction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

In the post–World War II industrial era, U.S. military superiority was structured on industrial strength, superior technology in platforms, weapons, and C4ISR, and a robust military infrastructure. As we have

moved from the industrial to the information age, however, the diffusion of information technology has tended to change some of the parameters of warfighting, not always to our advantage. Precision weapons and NCO have given the United States a decided advantage on the battlefield, but in irregular warfare we have had setbacks. While the United States was the developer of the cyberspace infrastructure, it is now open and available to all who possess the means to access it. The concepts of NCO and IO are also available to all, although there is a high cost of entry in developing significant capabilities. By its nature, cyberspace is a domain amenable to asymmetric warfare, because it can be used anonymously so that deterrence and retribution are difficult, and its immediate effects are usually non-lethal, so the risk of escalation is reduced. Cyberspace can also cause lethal effects (e.g., by disrupting control systems, causing things to blow up) in IO as well as NCO. For example, a computer network attack on an unprotected Supervisory Control and Data Acquisition (SCADA) control system of a power plant could lead to catastrophic damage to power generators and transformers.

Cyberspace has become a pillar of our national (and international) infrastructure. The military owns its tanks, ships, and aircraft but has only limited impact on the commercially provided connectivity (e.g., fiber optic, satellite) on which the "information superhighway." Figure 1 depicts the communications backbone for connectivity.

Figure 1. Cyberspace Connectivity



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

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

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

The concept of an "open" or a "closed" network as used in this chapter is at best an abstraction, in that these terms are really reference states and do not exactly correspond to actual employed networks. If fact, open

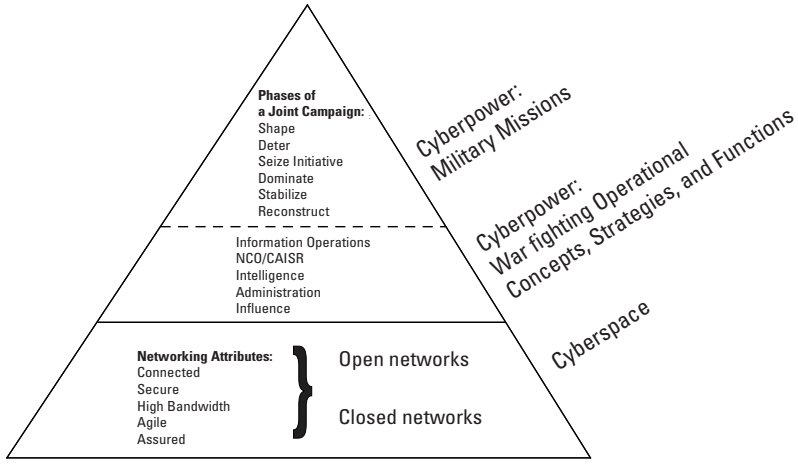
networks are usually capable of supporting some secure transmissions, and some closed networks use the communications backbone. An open network is defined here as one that is open to any user who wants to dial in or log on. Security is usually provided by password protection, encryption, and computer and network protection tools. The principal measures of performance are connectivity, availability, and bandwidth. The Internet and telecom are examples (although not all of the Internet is open, and the communications backbone is also used for secure transmissions). A closed network has access by only designated nodes and is "air-gapped" from open networks. Principal measures of performance for closed networks are security, availability, and assuredness. An example of a closed network is the Joint Worldwide Intelligence Communications System (JWICS).

The Structure of Military Cyberpower

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

To develop this definition further, military cyberpower is represented as a pyramid as, shown in figure 2. Military cyberpower is then seen conceptually as resting on the foundation of cyberspace.

Figure 2. Military Cyberpower—Cyberspace Support to Operational Concepts, Strategy and Functions to Achieve Military Missions



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

Military Missions: Joint Campaign Plans

The metrics for military effectiveness are the achievement of objectives and the execution of missions. The particular framework to examine the role of cyberpower in executing military missions chosen for this discussion is taken from the six phases (zero to 5) of the joint campaign planning process.[2] This planning process now covers a campaign from pre-hostilities to reconstruction and is at the strategic rather than tactical level of objectives.

Two caveats in the use of the joint campaign phases need to be mentioned. The first is that the phases are not entirely dissimilar from each other. For example phase 2, "seizing the initiative," and phase 3, "decisive operations," have much in common in terms of tactics and techniques. The second caveat is that the phases overlap in time as in a "three block war,"[3] in which full-scale military action, peacekeeping, and humanitarian assistance may take place simultaneously within three city blocks. Despite these caveats, the phases are useful in showing the appropriate and balanced use of soft and hard power with the appropriate uses of cyberpower at each phase. The six phases are listed below.

- Phase Zero, shaping countries at strategic crossroads,
- Phase One, deterring aggression,
- Phase Two, seizing the initiative and assuming freedom of action,
- Phase Three, performing decisive operations and achieving full spectrum superiority,
- Phase Four, transition to stability operations and establish security (including civil security and the rule of law) and restore essential Services, and
- Phase Five, engage in reconstruction and enable civil authority.

More detail on the nature of these phases can be found in references 3 and 4.

Military Cyberpower Operational Constructs

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

- Establish, expand, and secure reach (this includes virtual reach through the use of cyberspace, as well as physical and human reach),
- Acquire, refine and share knowledge, and
- Identify, create, and exploit effects.

For the objective of this paper, and exploration of military cyberpower, the above operations and actions are translated into the enabling (and synchronizing) hard power and soft power cyberspace concepts that support them. These, to be described in more detail below are:

- IO,
- NCO, a transformational warfare concept whose scope, doctrine, and technologies are still under development, and whose broad utility is still subject to debate,
- Normal and routine business and administrative functions using cyberspace-based tools,
- Intelligence operations, using cyberspace-based tools, and
- Influence operations, using cyberspace-based tools.

Information Operations

Information operations comprise electronic warfare (EW), psychological operations (PSYOP), computer network operations (CNO), military deception, and operations security (OPSEC).[5] In turn, CNO includes computer network attack (CNA), computer network defense (CND), and computer network exploitation (CNE). Capabilities that support IO include information assurance (IA), physical security, physical attack, counterintelligence, and combat camera. There are also three military functions: public affairs (PA), civil military operations (CMO), and defense support to public diplomacy specified as related capabilities for IO. The relationship of IO to cyberpower is not straightforward due to the eclectic nature of IO as well as the support and related capabili-

ties. Some elements of IO, such as EW, might be considered in the realm of conventional weapons. PSYOP, however, is integrated in cyberpower influence operations, while the other elements of IO are supportive of both hard and soft power.

Network Centric Operations

Network centric operations represent a powerful set of warfighting concepts and associated military capabilities that allow warfighters to take full advantage of all available information and bring all available assets to bear in a rapid and flexible manner. The concepts of NCW were originally applied to hard power concepts, in particular strike warfare and air defense, but taken broadly can also be applied to other mission areas and the appropriate and balanced use of soft and hard power. As a comparison, an Australian view of NCO is articulated by Fewell and Hazen, who describe network-centric warfare as follows:

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

While this definition is consistent with U.S. definitions, there is concern that in the implementation of NCO by our allies (many of whom have tailored versions of NCO), the ability to fight jointly may be compromised by non-integrated technologies and different command and control structures. To head off such eventualities, DOD engages in a number of cooperative forums on interoperability with our most trusted and dependable allies, such as NATO and the cluster of so-called "five eyes" fora—the ABCA Armies Standardization Program (for American, British, Canadian, and Australian Armies and as of 2006, includes New Zealand),[7] the Multinational Interoperability Council, the Combined-Communications Electronics Board (CCEB), and others. A main theme for these interoperability groups is multinational command and control, or determining the technologies and procedures for common information sharing.

The tenets of NCO as articulated by DOD are:[8]

- A robustly networked force improves information sharing,
- Information sharing enhances the quality of information and shared situational awareness,

- Shared situational awareness enables collaboration and self-synchronization, and enhances sustainability and speed of command,
- These, in turn, dramatically increase mission effectiveness.

While broad in nature, these tenets imply military operations in which the principal MOPs relate to an enhanced speed of operations and operation within an opponent's OODA loop (the cycle of observe, orient, decide, and act). These tenets are compatible with the elements of IO, in that both embrace cyberspace, and both deal with military operations. However, the two taxonomies are quite different, with IO structured by operations and NCO defined by capability. Alternatively, IO is characterized by functionality, while NCO is characterized by speed of operations, connectivity, shared decision making, and effectiveness. It is fair to question that, if NCO is the enabling concept of military cyberpower, is the military best organized to utilize this growing facet of modern warfighting, and does it have the tools to be agile, to execute, and to adapt?

Normal and Routine Business and Administrative Functions

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

Intelligence Operations

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

Influence Operations

Influence operations have grown in importance as the military mission set has expanded to include nation shaping, stabilization, and reconstruction and the threat set has expanded to include counter-insurgency. The United States must now deal with the multi-sided nature of the modern world rather than the two super-power world of the past.[9]

Service Visions and Implementation

DOD's Goal of Integrating the Services

Moving from theory to practice, it is no surprise that military networks, beginning with the earliest connectivity technologies—telegraph, telephone, radio, and now the Internet and private intranets—have followed Service and agency organizational structures and funding channels, connecting users along organizational lines: Service and agency staffs, field units with higher headquarters, and the Pentagon to all of its subelements.

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

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

DOD's bureaucratic processes, procedures, and organizational culture have not evolved as quickly as technology to take full advantage of the potential for network integration and interoperability. Significant Service-centered cultural and programmatic biases remain, and they reinforce one another as obstacles to collaborative investments in cross-department networking capabilities. However, it is a mistake to attribute parochialism

to the military departments alone; the OSD staff, Joint Staff, agencies, and combatant commands all seek to protect their own organizational priorities. Breaking down such barriers is the greatest challenge to networking all of DOD.

The scope of the network integration enterprise is huge. DOD data systems comprise approximately 3.5 million computers running thousands of applications over some 10,000 Local Area Networks (LANs) on 1,500 bases in 65 countries worldwide, connected by 120,000 telecom circuits supporting 35 major network systems over three router-based architectures transmitting unclassified, secret, and top secret information. And that is just the fixed-site profile. The most important and technologically challenging networks are those of the warfighters—deployed sea, air, land, Special Operations Forces (SOF), and space forces performing missions around the world, and their supporting intelligence networks.

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

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

Across DOD there is heavy investment in integrating command, control, computing, and communications capabilities, with numerous commands, staffs, agencies, and contractors committed to the goal. Many billions have been spent, and ultimately hundreds of billions will have been invested. A lot of network integration is already in place, although it is still mainly *within* the Services and Defense agencies and along hierarchical lines. Incompatibilities abound. There is less progress across joint forces, especially at the tactical level. What does exist is local in terms of networking and global connectivity. Few mobile users at the

tactical level enjoy reliable, sustained, Internet-based enterprise services, such as real-time intelligence. However, primary, joint networks do exist and have become the strategic and operational backbone of deployed forces. The interoperability goal is recognized and accepted, but, as budgets tighten, all Services can be expected to cling to internal priorities rather than joint integration when it comes to information technology (IT) and telecommunications investments. That resistance will be dampened by the forcing mechanism of essential connectivity, which drives commanders to insist on joint architectural standards so they are assured of being continuously and reliably "plugged in" with whomever and wherever required.

Key obstacles to network integration include an unwieldy standards process, limited investment in enabling or replacing Service legacy systems, residual Service parochialism, independent-minded CoComs, a non-collaborative culture across the officer corps, and simply the fact that DOD is still very much on the front end of a long time line. A lot more time and investment must pass to bring the requisite technologies, processes, and systems into being.

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

Network Integration Management at DOD

Two principal staffs driving network integration for DOD are the Assistant Secretary of Defense for Networks and Information Integration (ASD(NII)) who is also the DOD Chief Information Officer (CIO), and the Joint Staff J-6, Director for Command, Control, Communications and Computers (JS J-6), who is also the Joint Community CIO.

Under ASD(NII)/DOD CIO is DISA, which is the operating agency responsible for DOD network operations and management worldwide. The Joint Task Force-Global Network Operations (JTF-GNO), which supports computer network defense, is currently housed with DISA in Arlington, VA.

On the operational side, Joint Forces Command (JFCOM) is responsible for joint force integration, including network interoperability. In this capacity, JFCOM consolidates and harmonizes network requirements of the combatant commands and works with the JS J-6 to ensure invest-

ments in network systems include interoperability criteria as part of any approved system design.

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

The Combatant Commands (CoComs) are the managers of operational networks characterized by the architecture, standards, and systems established by DOD and provided by the Services, DISA, and JTF-GNO (STRATCOM). Most CoCom communications and information networks are traditional hierarchical systems tethered to fixed locations, relay sites, or satellites. These are managed by the CoCom J-6, who coordinates for Service requirements through the JS J-6 as well as through the CoCom's subordinate component commands (e.g., land, air, maritime, SOF).

Under the Unified Command Plan (UCP) 2002, STRATCOM is assigned responsibility for information operations and Global C4ISR, including responsibility to operate and defend the GIG. STRATCOM's operational arm for maintaining the GIG is JTF-GNO. The roles of DISA and JTF-GNO are similar and overlapping, which is reflected in the dual-hatting of their commander. In essence, JTF-GNO is a component command of STRATCOM, uniquely provided by a defense agency rather than a military department.

In network integration, no less than other high priority and costly DOD programs, there are many influential external actors. Congress is keenly interested in the successful achievement of joint operational capabilities, as is evident in the continued emphasis on Goldwater-Nichols goals some 20 years after the Act. Congress is also very focused on the high cost of IT systems in DOD and across the government, evident by the 1996 Clinger-Cohen Act and a host of related legislation since that seeks to ensure we can define the return on IT investments. Other external actors are industry, the policy analysis community, and international bodies, such as NATO, where similar integration architectures and standards have been defined and are the subjects of considerable investment. A new arrival not yet well defined is the emergent interagency cluster of Departments that

increasingly need to network with DOD at all operational levels (e.g., the Department of Homeland Security).

Key Guiding Documents

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

Joint Vision 2020 and CJCSI 6212.01B Interoperability and Supportability of National Security Systems and IT Systems (2000); the 2004 Transformation Planning Guidance (TPG) and 2006 Quadrennial Defense Review (QDR—now gearing up for renewal in 2009); the Joint Technical Architecture (JTA) version Six, JBMC2 Roadmap and CJCSI 3170.01C (JCIDS) in 2003; and, the Strategic Planning Guidance (SPG) and DOD Architecture Framework in 2004. All these are essential references for understanding the depth of DOD-wide commitment, management engagement, and investment in network integration. These same documents also signal the complexity and magnitude of the undertaking.

Earlier foundational underpinnings beyond DOD show that the Federal government at large has acknowledged the advent of the Information Age and accepted the need for government as well as industry to bring its practices into the new era. This indicates that DOD overall, and not merely its military operational side, must achieve network integration. Above all, there has to be a clear link between IT investment and outcomes, i.e., the return on investment for the taxpayer. The pivotal legislation and executive regulator policies in this regard are the Clinger-Cohen Act and EO 13011 (Federal Information Technology) (1996); OMB Cir. A-130 (Management of Federal Information Resources) and the Information Assurance Initiative (2000 National Defense Act) in 2000; and the E-Government Act of 2002.

The Role of Joint Forces Command (JFCOM)

JFCOM has been given the task of identifying the C4 requirements of the joint community. JFCOM negotiates with its co-equal joint commanders to define a single, coherent set of required capabilities that can be passed to the Service providers. Although flexibility and agile designs are desired, the reality is that bringing a requirement into operational use by a large force is time and resource intensive. Therefore it is essential

that required capabilities not be too transient or subject to frequent redefinition.

CoComs sometimes press for loosening standards to encompass new and perhaps immature technologies they have discovered work for them. In some cases the systems may already have been procured for a pending operational requirement. JFCOM as yet does not exercise sufficient oversight to ensure such add-on network systems do not actually move DOD *away* from its goal of networked forces. For example, a unique new system procured for a limited operational need by PACOM may not be compatible with systems in use by CENTCOM or EUCOM. However, some of the forces assigned to PACOM for that operation may soon be ordered to CENTCOM's AOR. JFCOM's role in achieving network interoperability is to adjudicate such inconsistencies to ensure a set of common technical standards acceptable across the joint operational user community.

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

The Joint Interoperability Test Command (JITC)

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

Service Visions and Implementation

It is apparent from current service actions that the tools of cyberspace have already had a significant impact on Service operational

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

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

From a Service operational point of view, General James Cartwright, Vice Chairman Joint Chiefs of Staff (VCJCS) (and former Commander, USSTRATCOM) has critically pointed to the division of military cyberspace operations among three fiefdoms.[10] Under this approach, Joint Functional Component Command-Net Warfare (JFCC-NW) is responsible for attack and reconnaissance, the JTF-GNO manages network defense and operations, and the Joint Information Operations Warfare Center (JIOWC) oversees electronic warfare and influence operations. Strategic

Communications are overseen by STRATCOM. In addition to divisions in joint military cyberspace operations, there are potential Service and DOD C4ISR interoperability issues as OSD proceeds with the development of the GIG and the Services proceed with implementations of NCW architectures.

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

Table 1. Summary of Service Cyber Programs

Service	Concepts	Architectures	Systems	Organization
USAF	Cyberspace as a Warfighting Domain	C2 Constellation	Assurance, Data Integration, GIG	Cyberspace Command
USA	Information and Cognition as a Domain	LandWarNet	FCS, WIN-T, GIG	1st IO Command, NETCOM
USN	IO, NCO	FORCEnet	NMCI, GIG	NETWARCOM
USMC	NCOW	MAGTF-IO	NMCI, GIG	MCSC

Air Force Vision and Implementation

The Air Force has put cyberpower on an even footing with Space Power and Air Combat and has defined cyberspace as a "Fifth Dimension."[11] In the chapter by Lt Col Forrest Hare and Col Glenn Zimmerman, the Air Force considers cyberspace superiority an imperative and establishes the proposition that cyberspace Superiority is the prerequisite to effective US military operations in all other warfighting domains. In a discussion on what the Air Force calls the "five myths" of cyberspace and cyberpower, the Air Force asserts the following:

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

- Defense of the cyberspace domain requires a holistic network approach rather than just increased security at each individual node.

The Air Force transformation Flight Plan[12] describes the C2 Constellation initiative as the centerpiece of the Air Force NCW implementation efforts:

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

The Air Force has also introduced a significant organizational change by standing up the provisional Cyberspace Command as the 8th Air Force at Barksdale Air Force Base. The mission of the Cyber Command is to prepare for fighting wars in cyberspace by defending national computer networks, running critical operations, and attacking adversary computer networks.[13]

Army Vision and Implementation

In a paper by BG Jeff Smith of the Army's Network Enterprise Technology Command, a future is envisioned in which soft power and the human/social impact of cyberpower is matched together with a hard power that also is transformed by cyber. Smith considers that cognition is the actual goal of military strength, which is at a level above information, which in turn is a level above cyberspace. Cognition refers to the human element, including: leadership/behavior, understanding /decisionmaking, and problem-solving/adapting. Cyberspace is considered a subset of networks, which in turn is related to information and finally cognition. In this paper, Smith collapses air/space, land, and sea into one physical environment and cognition into a second environment. His thesis is that Army

DOTMLPF is almost only focused on the physical and not enough on the cognitive, which is more important.

The Army implementation of NCO is called LandWarNet, which comprises the Army's information infrastructure and is the Army's contribution to the GIG. LandWarNet consists of all globally interconnected Army information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand—supporting warfighters, policymakers, and support personnel. It includes all Army communications and computing systems and services, software (including applications), data security services, and other associated services. The Future Combat System (FCS) is a principal development program in the Army for NCO. It is a modular construct of a reconfigurable family of systems capable of providing mobile, networked command and control, communication, and computer functionalities; autonomous robotic systems; precision direct and indirect fires; airborne and ground organic sensor platforms; and adverse-weather reconnaissance, surveillance, targeting, and acquisition.[14] The Warfighter Information Network-Tactical (WIN-T) is the Army's tactical digital communications system, which has the goal of providing advanced, commercial-based networking capabilities under the umbrella of the GIG. The WIN-T network C4ISR support capabilities goals are for a network that is secure, survivable, seamless, and capable of supporting multimedia tactical information systems.[15] FCS is managed by the Army, which employs Boeing as a lead systems integrator. The program is reviewed annually by the U.S. Government Accountability Office, which has questioned the technical maturity of WIN-T and the Joint Tactical Radio System (JTRS) in terms of Army acquisition goals.[16]

Navy Vision and Implementation

The Navy perspective on cyberpower shows a structure incorporating the elements of IO and NCW. The Navy Marine Corps Intranet (NMCI) addresses the communications network and the business and administrative functions of cyberpower in the Navy and Marine Corps.[17] The Navy formed the Naval Network Warfare Command, which includes a Navy IO core competency that supports the Combat Commander's ability to: shape and influence potential adversary decisionmakers thinking prior to conflict, resulting in deterrence of hostilities; enable decisive, non-kinetic (effects-based) operations to complement kinetic warfare and defeat the adversary, should conflict ensue; and engage in continuing post-conflict shaping/influence operations to maintain stability. To accomplish

these goals, the Navy must develop an effective structure for IO force development, integration, planning, command and control, and execution in the joint environment.

FORCEnet is the Department of the Navy's implementation strategy for performing network-centric operations. The Chief of Naval Operations' accepted definition of FORCEnet is "the operational construct and architectural framework for naval warfare in the information age that integrates warriors, sensors, networks, command and control, platforms and weapons into a networked, distributed combat force that is scalable across all levels of conflict from seabed to space and sea to land."[18] The Naval Research Advisory Committee defines FORCEnet as "a portfolio of programs to enable the gathering, processing, transportation, and presentation of actionable information in support of all aspects of joint and combined naval operations."[19] Unlike the Army's WIN-T, FORCEnet is not a specific program but rather an architecture, or at best a group of programs, that serves as the organizing principle for Naval enablement of the GIG. The NMCI is a key component of FORCEnet and has the goal of providing the Navy and Marine Corps with a full range of network-based information Services on a single intranet. NMCI has the goal of providing secure, universal access to integrated voice, video, and data communications. Eventually, the massive NMCI network will link more than 400,000 workstations and laptops for 500,000 Navy and Marine Corps users across the continental United States, Hawaii, Cuba, Guam, Japan, and Puerto Rico. Under NMCI, the program office and the prime contractor control the layout, distribution, and analysis of the system. The prime contractor, Electronic Data Systems (EDS), owns all the IT assets and leases them to the government.

In the Navy SSG's study on "Convergence of Sea Power and Cyber Power" an even broader view of cyberpower is taken. The SSG definition of cyberspace is:

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

The SSG looks to a future with a more complex world driven by many emerging challenges. Cyberpower is seen to converge with the conventional sea power concepts and to transform conventional Navy roles in

sea control, power projection, naval presence (both physical and virtual), strategic lift, and strategic deterrence.

Marine Corps

The Marine Corps has focused its cyberpower vision on net-centric operations and warfare (NCOW and is developing a Marine air-ground task force information operations (MAGTF-IO) strategy for operational implementation.

The future MAGTF-IO aims to enable decentralized decision making that promotes taking advantage of fleeting battlefield opportunities. MAGTF-IO is a cyber strategy, a process, and ultimately a system-of-systems by which the Marine Corps will develop current and future capabilities and programs to achieve NCO and Warfare (NCOW), and implement the FORCEnet functional concept of providing robust information sharing and collaboration capabilities. MAGTF-IO is the strategy by which the Marine Corps will implement the Naval FORCEnet functional concept and is the functional and conceptual equivalent to the other Service net-centric concepts of LandWarNet (Army) and C2 Constellation (Air Force). It will also be integrated with NATO through the NATO NET Enabled Capability (NNEC), and be able to facilitate "coalitions of the willing" as needed. It entails a seamless, scalable, modular capability that is relevant across the full spectrum of military operations from major combat operations, to irregular warfare operations, to humanitarian assistance operations.

DOD Implementation

Management and development of information-based technology and systems are spread through the Services. The Office of Force Transformation[20] provided an overall vision for NCO, but the Services develop their own systems in conjunction with the development of the GIG. A consideration of the GIG is essential in a discussion of military cyberpower, because the GIG has been mandated by DOD directive 8100.1 from the Deputy Secretary of Defense in September 2002 as the physical implementation of the principles of NCW.

While all three Military Departments recognize the GIG as the umbrella network under which they will operate, there is no commonality among the Services as to network architecture or their approaches to NCW. This approach requires that issues of interoperability be properly addressed. Each Service has special requirements, such as submarine communication for the Navy and mobile networked command and control for the Army. There are also areas where commonality should be sought,

such as in aviation connectivity. How well the Services (as well as agencies such as the intelligence agencies) develop their C4ISR NCW programs to interface seamlessly with the GIG remains to be seen.

DISA heads the GIG project under the leadership of the CIO of the ASD(NII). The formal definition of the GIG is "The globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating and managing information on demand to war fighters, policy makers, and support personnel."[21] The architecture for the GIG relies on internet protocol (IP) and will be largely reliant on the commercial transmission infrastructure and on commercial information and network management technology.[22]

The vision and proposed architecture of the GIG are very challenging, from the standpoint of both technology development and reliance on commercial systems to achieve information assurance. The National Security Agency (NSA) has been tasked by ASD(NII)/DOD CIO to develop an end-to-end information assurance plan for the GIG.[23] The NSA recognizes that information assurance needs to be an embedded feature designed into every system in the GIG, and that this requires a shift from today's model, which consists predominantly of link encryption and boundary protection between multiple discrete networks. To accomplish the GIG objectives, DOD will need to impact the commercial technologies and standards that will constitute the GIG architecture.

As noted above, the Services are all pursuing alternative networking architectures under the umbrella of the GIG. The GIG promises to provide a network based on commercial protocols, software, and hardware for both tactical and strategic communications, and data links to operate in an environment of forces on the move, and the ability to continue to effectively operate during network attacks and failures. Shortfalls exist in the GIG development to meet certain Service specific needs. For example, with a mobile infrastructure, the Army will require protocols for a mobile, ad-hoc, networking (MANET) capability. However, commercial industry is moving toward an all-IP core network (IPv6). The Navy may also experience shortfalls from the eventual GIG development. For example, the communications requirements for ships at sea depend on continuous, high-capacity, low-latency connectivity to be provided by the Transformational Satellite Program (TSAT) that is being delayed for cost and technology reasons. Even when it is completed and the Navy develops suitable shipboard terminals, the Navy's communications capacity will still be limited by capacity and satellite communications interruptions caused principally by antenna blockage. Also, the GIG programs do not address

the challenging problem of communicating with submarines at speed and depth.[24] Another quandary for the introduction of communications system that fit under the GIG umbrella is that of legacy systems that do not fit into the new architecture and funding for new systems. For example, Army officials must determine how to transition the Joint Network Node (JNN), a commercial, IP-based mobile communications system deployed to soldiers in Iraq, to the WIN-T.[25]

There are also challenges and risks associated with the use of commercial products, such as Microsoft Windows and Office in which the DOD does not have access to the proprietary codes that are typically released, with bugs that are later addressed with patches. Additionally, commercial off-the-shelf computers, routers, and servers often have "trapdoors" for maintenance that can provide system access to hackers. Internet gateways for NIPRNET and other unclassified government networks have provided opportunities for attackers to exploit and disrupt. Even secure systems with multiple users are susceptible to the insider threat. The access to and the sharing of information with Internet portals has benefits, risks, and limitations that must be managed, especially for SSTR operations and sharing with other nations, international organizations, and non-governmental organizations (NGOs). An additional concern relating to the use of commercial products is the outsourcing of IT providers, including both products and services in network operations and management in crisis situations. This could lead to issues such as embedded Trojan Horses in foreign-built equipment and software. National constraints limiting international vendors during a crisis could result in supply problems. Finally, there is a trend toward the global IT infrastructure, including IT products, services, and networks, such as global internet, Cellular, telecoms, cable, and satellites being taken over by foreign ownership that may not be friendly to U.S. policy and needs, especially during crisis.

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

Conclusions

Knowledge and information exchange have always been essential to warfighting. As cyberspace technology has evolved over the past few decades, the military has adapted the technology to its traditional warfighting paradigms of air, space, land, and sea power. Rather than developing its own information communications technology (ICT) knowledge base and systems, the military has developed an extensive reliance on commercial ICT and increased dependence on commercial services globally, including the use of the Internet to support some elements of command and control.[26] In addition to the Internet, the military is also a user of other commercial products, such as wireless networking, cellular phones, BlackBerries, telecoms, satellite and cable-based networks, radio, and TV. While it has developed the concepts of network-centric warfare to integrate air, space, land, and sea power, it has maintained the conventional warfighting principles of strike warfare, air superiority, and air and missile defense structured to increase the speed and timeliness of operations, operate more effectively in extended areas of coverage, and enhance precision. This utilization of cyberpower enhances our hard power capabilities and defines the attributes of the network to support these operations. The evolutionary growth of these capabilities has maintained the existing organizational, management, and acquisition structure of the military Services in dealing with technological advances in cyberspace. Similarly, military information operations have maintained their organizational principles, even in the face of the extraordinary impact that radical groups have exhibited by their adaptation of the Internet to recruitment, planning, financing, and influencing. Rather than speed of operations, the defining metrics here are large-scale connectivity, user pull, and collaboration. This is being accomplished by making more effective use of emerging ICT and changing operations to support the increased importance of HA/DR and SSTR in phases zero, four, and five as well as warfighting in phases one, two, and three.

In this chapter military cyberpower has been described in terms of three dimensions: military requirements or missions as described by the joint warfighting phases; military information-based capabilities or operational concepts including NCO, IO, military administration, Intelligence collection and influence operations; and the dimension of cyberspace, including open and closed architectures employing dedicated networks, the Internet, military tactical radios, commercial radio/TV, and telecommunications. Ideally, an integrated cyberspace architecture can be envisioned

that supports all the intersections of military requirements and military information-based capabilities. It would need to be reliable, available, and survivable under attack, and would also need to be scalable and provide high bandwidth. While ideal, such an integrated architecture may provide multiple unforeseen vulnerabilities and introduce unacceptable cost and capability risks. A single, open architecture designed to promote maximum connectivity and user pull based on IP may need separation from the secure connectivity required for sensor-to-weapon NCO operations. The development of the GIG and new technology initiatives are poised to address these issues, but not all technology objectives of these programs may be met. In the meantime, the military requires secure, closed networks, including restricted users, highly controlled access arrangements, and stringent security protection, as well as fully connected, open networks. The military also needs to wrestle with existing legacy systems, many of which will not be interoperable with the GIG.

There is no question that the military Services are already adapting to and leveraging the new environment in communications and information provided by the exponential growth in cyberspace connectivity and information storage and processing. However, risks and vulnerabilities have been introduced that need careful assessment to be effectively managed, especially the increased dependence of the military on civilian cyberspace capabilities, products, and services. The Services are also experiencing growing pains as they deal with a different world order and the impact of new technology, coupled with the evolving and changing missions of the Services in this environment, including HA/DR, SSTR and influence operations. In this chapter, comments were made about Service visions and implementation along with comments on the DOD GIG. These challenges to moving forward are briefly summarized below.

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

Within each Service, different organization structures are being implemented to address this rapidly evolving source of military operational opportunities and to defend against and respond to threat vulnerability.

While all three Military Departments recognize the GIG as the umbrella network under which they will operate, there is limited commonality among the Services as to network architecture or their approaches

to NCO. This approach will only succeed if issues of interoperability are properly addressed.

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

Notes

[1] Defining *Internet* broadly, this includes e-mail and the World Wide Web, as well as military and government Internet protocol (IP) based networks. These include networks that have access to the Internet architecture, e.g. NIPRNET, and those that do not, e.g. SIPRNET and JWICS, which are secure networks.

[2] "Campaign Planning Primer AY 07," Department of Military Strategy Planning and Operations, U.S. Army War College, 2006.

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

[4] "Capstone Concept for Joint Operations," Version 2.0, August 2005, available at DTIC.

[5] Joint Publication 3-13, *Information Operations*, February 13, 2006.

[6] M.P. Fewell and Mark G. Hazen, "Network-Centric Warfare—Its Nature and Modeling," Australian Defense Science and Technology Organization, http://www.dsto.defence.gov.au/cororate/reports/DSTO-RR-0262, September 2003.

[7] See ABCA, "Purpose and History," at http://www.abca-armies.org/History/Default.aspx

[8] Alberts and Gartska, DOD Report to Congress on Network-Centric Warfare, July 2001.

[9] In the book "Cyberpower and National Security", Potomac Press, January 2009, the chapters by Kramer and Wentz, and also by Starr, specifically address cyberpower aspects of influence operations and the role of the military.

[10] Josh Rogin, FCW.com, http://aimpoints.hq.af.mil/display.cfm?id=16609.

[11] Lt. General Bob Elder, "The Fifth Dimension: Cyberspace," briefing from Headquarters U.S. Air Force.

[12] The Air Force Transformation Flight Plan, Washington DC, November 2003, p. B-6.

[13] As noted by Kevin Fogarty, Defense Systems, October 13, 2008, "the cyberspace initiative will become an element of the numbered Air Force, one step down the organizational ladder from the top-level major commands and above wings and other independent groups."

[14] 2003 United States Army Transformation Roadmap, p. B-3.

[15] Warfighter Information Network-Tactical (WIN-T), Operational Requirements Document, November 1999.

[16] http://www.gao.gov/new.items/d07376.pdf, March 16, 2007.

[17] Kenneth Jordan, "The NMCI Experience and Lessons Learned," http://www.ndu.edu/ctnsp/pubs/CaseStudy%2012%20-%20NMCI.pdf.

[18] VADM Richard W. Mayo and VADM John Nathman, "Sea Power 21 Series, Part V: Turning Information into Power," *U.S. Naval Institute Proceedings*, February 2003, p. 42.

[19] NRAC report, "Naval S&T in FORCEnet Assessment," NRAC 04-2, July 2004, p. 15.

[20] "The Implementation of Network-Centric Warfare," Office of Force Transformation (Washington, DC: U.S. Government Printing Office, January 2005).

[21] GIG definition available on the DTIC site, http://www.dtic.mil/whs/directives/corres/html2/d81001x.htm. See also David Alberts and Richard Hayes, "Power to the Edge," Information Age Transformation Series CCRP Publication, June 2003, p. 187.

[22] Ibid., p. 196.

[23] http://www.nsa.gov/ia/industry/gig.cfm?MenuID=10.3.2.2.

[24] FORCEnet Implementation Strategy, Naval Studies Board, 2005.

[25] "Army Stuck in a WIN-T Quandary," Frank Tiboni, FCW.COM, http://www.fcw.com/article92437-02-27-06-Print, February 2006.

[26] Center for Technology and National Security Policy, National Defense University, "Information Technology Program: Report to Congress," January 2006.

Chapter 2

A Unified Field Theory for Full-Spectrum Operations: Cyberpower and the Cognitive Domain

Jeffrey G. Smith, Jr.

"Any war has its origin in the human brain."
Timothy L. Thomas, USACAC[1]

"We can get this generally right, and precisely wrong."
GEN Charles C. Campbell, Cdr, FORSCOM[2]

"The world has gone berserk; too much paperwork."
Bob Dylan[3]

Introduction

This chapter is the short story of two revolutions, one cyber, the other cognitive. One about which we're generally right; the other about which we're (so far) precisely wrong. One that is well underway, the other just stirring. One makes us merely competitive; the other has the potential to make us more secure.

Cyber's revolutionary ardor is already absorbed within "transformation," the means by which institutions achieve the broad and deep delivery of that which was once rare, uncommon, and controversial. In exchange for its undeniable advantages, we have generally agreed to tie a percentage of our GDP and defense force structure (and transformational efforts) to the furious wag of its evolutionary tail. We do so to preserve cyber's availability, while denying adversaries an intolerable cyber advantage. We do so because we are becoming "paperless ships," the presumption of cyber's availability now a part of our operational DNA. We do so because

we have no choice; the world has undergone an information refresh that has been as inexorable as the flow of tides; eventually, with notable exceptions, cyber will connect everyone to everything. We've placed our lot with cyber because our young soldiers deserve the same collaborative advantage while defending their nation that they enjoyed before joining the Service. We do so because the foot soldier in the employ of our adversary is enabled by the most sophisticated global network in history, at the cost of purchasing a peripheral.

Cyberspace, though, is preface (and subordinate) to a revolution that is stirring within and across our peer enterprises, a revolution in the way humans think, decide, solve, understand, organize, act, and behave collectively. The multi-disciplined fields of the cognitive arts and sciences are mapping the metaphysics of the human brain, where the will to wage war originates, where passions are born, character resides, decisions are made, plans conceived, judgment sits, threat and opportunity are modeled, the future simulated, and where, ultimately, human conflict is resolved. Within our Armed Forces, operationally engaged leaders are directing their brigade and regimental combat and special operations teams as if they were surgeons, with tailored teams, tools, and touch meant to shape psychological positions. Sun Tzu had a phrase for this cognitive approach to combat. He counseled his commanders, over-schooled in the physical arts, to "throw rocks at eggs."[4] Sun Tzu's elliptical, poetic guidance was his way of emphasizing the mental nature of the operational objective, often obscured by indiscriminate physical activity on the part of ignorant kings, ambitious generals, and desperate soldiers.

Despite the works of ancients, the precedents of history, and the evidence of our own ongoing operations, we remain institutionally reluctant to commit to a taxonomy for cognitive activities that embraces a revolution in the way we solve problems. This despite the profound difference in stakes between these two revolutions. Whereas cyber has potential to make us merely competitive, the cognitive revolution has potential to make us more secure. Where the consequences of cyber failure can be temporary and reversible, cognitive failures are often beyond retraction; indeed, cognitive consequences—both good and horrific—light the path that we know as history.

The author's objective is modest enough: to nudge our current battle command construct from its doctrinal position as "C2 function" overseeing largely physical operations within the expeditionary environment, to the cognitive operation at the core of our operational unified field theory, the objective of which is the collective brains of Blue (friendly), Gray (neu-

tral), and Red (adversarial) constituencies. Within Army Field Manual 3.0, under the title "Information Tasks," there is a tantalizing hint of the way forward. The mission of a new operational category called "information engagement" is to "influence the behavior of target audiences."[5] That effect, I believe, is the general objective of battle command, which ought to lend its name to the operation that achieves it. Battle command, as the Army's preeminent cognitive operation, will inspire nationwide efforts to earn the corollary to the catastrophic consequence of cognitive failure: that no other activity within our operational environment has more potential for revolutionary application than that within the cognitive domain. No other activity has such potential to make us more secure. All other operational activities, I believe, derive from it.

Within the proposed unified field theory, battle command is not an operation that is limited to a particular echelon, or Service, or Blue, Gray, or Red constituency. Indeed, it is an art that our enemy practices with at least equal vigor and intuition, if not study. It is an art that we'll expect of our Commander-in-Chief and a science whose practice must extend to Blue leaders at every level and operational location. It is increasingly clear that decisions made at departmental, agency, and national levels contributed directly to the difficulty of the expeditionary force to arrive at satisfactory states of accommodations among Blue, Gray, and Red constituents during the early stages of Operation *Iraqi Freedom*. Said another way, operational success depends on the exercise of wise, collective, cognitive activity by leaders at national, institutional, global, regional, and expeditionary levels. The inconsistent approach we take toward the education, organization, integration, and incorporation of those who are responsible for so much of our operational activity is certainly one of the indisputable findings of on-going operations.

The subject of this article, then, is battle command in the cognitive age. Although the terms and shapes of the unified field theory and its operational model are provisional, their insights are meant to apply equally to Blue, Gray, and Red constituencies, and tested over time against historical, current, and future operational circumstances. I've settled on cognition as the core activity within the operational environment (OE) because it is the mental activity from which the will to war originates, through which operational activity is organized, and by which war is resolved via a series of forced or negotiated accommodations among populations. The categories within the cognitive domain are not meant to echo the important taxonomical work of Benjamin Bloom, for it is the *collective* brain and its derived collective behavior that is of operational consequence within the

operational environment. The activities I've categorized within the cognitive domain are more likely the product of observation, whether those of operational genius (Sun Tzu, Alexander, Wellington, and Grant, among others), personal experience, or extensive discussion with veterans.

This chapter was commissioned by three sponsors. First, the Center for Technology and National Security Policy of The National Defense University solicited papers on cyberspace (its nature, power, and operations) from a Service perspective. The chapter is written from the perspective of those Forces responsible for land-based operations conducted among human populations. Second, LTG Sorenson, the Army G6, asked for an examination of whether the Army got cyberspace generally right with regard to its role in support of battle command (the Army's chief operational C2 construct). Third, General William S. Wallace, CG Training and Doctrine Command (TRADOC), requested that the work be placed in the context of his essential effort on what he calls the "human dimension."[6] This chapter is an excerpt from a longer, more deliberately argued effort influenced by joint concepts, fresh doctrine, the failures of my own personal experience, informal interviews, an angled view of much-travelled historical examples, and, finally, selected lessons learned from our Global War.

This chapter is not meant to represent a staffed position within the Army or any other Service. Instead, the model and theory sketched within the article are meant to form a doctrinal prequel, or taxonomical ancestry, from which, and by which, we can reexamine the basic insights of joint and service operational doctrine, disentangle the terms of their taxonomies, and recommend an early entry into the post-IT revolution, or the Age of Cognition. The remainder of the paper falls into five general parts. Part one defines assumptions and key terms. The second part is a dense abstract that describes the modified model of the operational environment, its derived field theory, and the full spectrum of its enabling operations. Part 3 provides historical precedent for battle command as the cognitive operation at the core of the operational environment (OE). Part 4 gives the cognitive domain and the metaphysical dimension a taxonomy of their own. Part 5 argues that revolution in cyber doesn't translate to cognitive revolution, but serves as preface to this more substantial revolution.

Assumptions and Key Terms

Assumptions

Thucydides, among others, declared the causes of war to be psychological (honor, fear, greed, and ambition).[7] The field theory proposed

within this paper rests on this single assumption. And if war begins in the human brain, then war is resolved there as well—in the minds of Blue, Gray, and Red constituents expressed as the collective wills of their populations (and subgroups). As the highest category of organized activity within the operational environment, operations move populations from the will to fight to the willingness to accommodate what were once mutually exclusive goals and objectives. The chief operation, then, is cognitive, directed toward the achievement of influence over human choice, specifically the decision to act in a particular way, on behalf of a particular constituency, and in support of particular objectives. It is from cognitive activity and in support of its objectives that the full spectrum of operational activities is derived and toward which its effects are directed.

Key Terms

- *Blue, Gray,* and *Red* are shorthand for the categories of humans encountered in the operational environment. These colors also represent the multiple shades within each primary color, each of which requires its own nuanced operational approach. The primary colors correspond roughly to the doctrinal categories of the situation (friendly, environmental, and enemy). Blue refers to those humans whose leaders are explicitly engaged in the development, promulgation, and implementation of the nation's (or group's) security strategy. Red denotes humans whose leaders are in organized opposition to Blue. Gray connotes humans whose leaders seek independence from, or accommodation with, Blue and Red, but will turn Red or Blue if sufficiently provoked or motivated. From the perspective of the individual constituent, all constituents are Blue.
- *Cognition* is derived from Sun Tzu's famous quotation "know yourself and your enemy, and you will never be in peril."[8] Sun Tzu presumed that to know is to act collectively—and wisely—on behalf of nations (or groups). Cognition comprehends five interrelated activities. First, to *shape* information into the Janus model of Threat and Opportunity. Second, to *form* a solution that counters the former and seizes the latter. Third, to *understand* personally and *adapt* to the continuously evolving Situation. Fourth, to translate personal understanding into *public*, broad-based activity. Fifth, to *lead* in order that Blue *behaves* is if One.
- *Battle Command* is the art and science of leveraging the full spectrum of operational activity to resolve differences among Blue,

Gray, and Red via a series of forced and negotiated accommodations. It is the only operational level that is accountable both for tactical outcomes and political objectives. It is the superior cognitive operation within the OE.

The Unified Field Theory's Central Idea and Abstract

The Central Idea

The central idea within the unified field theory is formlessness, or the ability of Blue to adapt the form of his solution to the continuously evolving shape of his situation (to conform to a continuously evolving shape implies the ability to change form continuously, hence the name). Formlessness requires four distinct and interrelated skills. First, the leader's ability (and the network's capability) to build a model of the situation from which the shape of threat and opportunity emerges, linked to local circumstance and national (or group) objectives. Second, the leader's ability (and the network's capability) to form elemental combinations that conform to the continuously evolving shapes of peril and opportunity. Third, the leader's ability (and network's capability) to form operational combinations across the spectrum of activity as part of integrated plans and orders. Fourth, the leader's ability (and the network's capability) to assemble, locate, identify, and modify the shape of physical and mental objects and project the consequences of their collisions.

The model of the situation forms the common core to all four activities. The model of the situation tells the interrelated fates of Blue, Gray, and Red in order to provide three outputs: (1) the shape of peril; (2) the shape of opportunity; (3) and the universal context within which all local activity is linked to the achievement of political objectives of the nation (or group). The model of the situation exists in two states. The technical model of the situation (TMOS) is a collaborative product presented in physical form meant to be broadly and simultaneously absorbed by leaders at every level and location. The TMOS translates input from across a vast collaborative Information Infrastructure (part human, part technological) into the story of relevant operational activity in order to recommend to leaders the means to resolve it favorably. The cognitive model of the situation (CMOS) is influenced by the TMOS, but exists within the brains of leaders. It is through the CMOS that leaders personally comprehend their situation, and understand the precise means by which they must conform to it. It is from the CMOS that leaders' intent emerges. It is through the CMOS that leaders observe the mental organs of their constituents, and

decide precisely how to modify the objects that reside within each. Finally, the CMOS continuously modifies the technical and human parameters of the TMOS to conform to the leaders' own cognitive landscape.

Formlessness also depends on the maturation of two revolutions, cognitive and cyber. The cognitive revolution enables leaders to perceive the metaphysical landscape within the OE, a mental landscape whose terrain is composed of the organs of the human brain: the moral, intellectual, creative, emotive, instinctive, spiritual, professional, and personal identities of Blue, Gray, and Red constituents. The shapes of objects within those organs determine the nature, duration, and resolution of operational activity and constitute the true target of operations. The mental nature of the OE, then, demands a much broader, more diverse and nuanced spectrum of elemental and operational combinations than one motivated by the physical goal of closing with and defeating an armed opponent. The cognitive revolution encourages leaders to shed doctrinal, imaginative, organizational, functional, and professional biases that seek to achieve false agility by fitting circumstances into pre-configured information, effects, organizational, and operational models. The cognitive revolution achieves actual agility by demanding that leaders conform to the situation in which they find themselves, requiring leaders to choose from a full spectrum of elemental and operational choices, combinations for which doctrine (and therefore the enemy) will quite often have no name. Without a cognitive revolution, those choices are sharply constrained by policies, permissions, regulations, organizational firewalls, personal experience, and institutional-level training and educational opportunities.

The second required revolution is cyber. Once complete, cyberspace coats all activity within the OE with an electronic membrane, until the OE pulses like a planetarium. The cyber revolution has four major objectives, or outputs: (1) the technical model of the situation, one that captures both the physical and mental shape of the OE, and adapts to the cognitive approach of the local leader; (2) the elemental combination, or task organized team, that acts under the influence and authority of the local leader; (3) the operational combination that assembles information, humans, and their proxies into the coherence of plans, orders, and intent; (4) problem-solving, or the ability to exploit Blue's collaborative brain to arrive at solutions in time to influence activity on terms favorable to Blue. While the cyber revolution can suggest elemental, even operational combinations that appear revolutionary, cyber depends entirely on human-provided instructions. Short of a cognitive revolution, those instructions reflect the doctrinal, operational, organizational, professional, political, and cultural

biases of its programmers. This is why cyber is preface to the cognitive revolution, which is greater.

Abstract

The chief *subject* of the OE is human activity organized around the security, toleration, and demise of nations (or groups). The *problem* at the center of the OE is the failure of the world's myriad nations (and groups) to accommodate one another's strategic goals and objectives. The *solution* is pervasive, synchronized local activity at every operational level that modifies strategic goals and objectives sufficient to accommodate national (and group) diversity.

The unified field theory (including its operational model and taxonomy) that solves the problem was constructed under four chief guidelines. First, the construct must be universal, otherwise our model is self-reflexive, revealing only our own biases. Although the unified field theory and its operational model are written from the perspective of Blue, that is only because all constituents, from their personal perspective, see themselves as Blue. If Red applies the model to its own circumstances, then the Red terrorist becomes the Blue martyr. Second, the model of the environment must proceed from a clear understanding of its chief subject. Environments, therefore, are constructed around a particular subject. Domains are used to further classify categories concerning the chief subject, while dimensions are used to describe the environment around which the subject finds itself. Third, the usefulness of the model depends on the extent to which it clarifies complexity; much of that clarity is derived from a clear understanding of its chief subject, from which all taxonomical terms proceed. Fourth, models must comprehend the totality of the circumstances that influence their subject, or else the subject inherits, with little warning, the effects launched from outside its model (and therefore the reach of its influence).

In the longer paper, I've more systematically distinguished between the current and proposed models for the OE. Here, I'll merely sum up the differences. Joint Publication 3-0 defines our current model of the OE as a "composite of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander."[9] The chief subject of the OE is only inferred: human decisionmaking with regard to employment of security-related capabilities (under myriad environmental influences and variables)? Less clear is the level and identity of the decisionmaker (commander implies military organizations); and at what level: tactical unit or strategic organization; and missing from the subject, considering the subject matter, is drama. So, within the field

theory, the chief subject of the OE is clear, dramatic, and comprehensive: human activity organized around the security, toleration, and demise of nations (or groups). That implies an additional difference between the two models. Where the current model describes multiple OEs that overlap, intersect, and integrate, we've used a single OE to stand as the highest level abstraction for the global situation, one that comprehends all security-related activity.

The unified field theory clarifies the confusion between the terms "domain" and "dimension." Domains constitute the chief categories of essential activities that must be performed by the chief subject. Domains do not imply that their particular activities are ever conducted in isolation from those of another domain; rather, domains are the means by which the nation or group establishes its priorities with regard to the study, development, resourcing, fielding, and adaptation of enabling capabilities. Dimensions, on the other hand, clarify or define the environment within which the chief subject acts. Without the "coordinates" of dimensions, the chief subject is buried in the individual acts that threaten to cocoon him in their overwhelming disconnected unreferenced diversity. In this sense, dimensions provide order to the chief subject's circumstances, and do so in three ways. First, dimensions provide the coordinates by which objects are identified and located; second, dimensions form the media that enables collective activity; and, third, dimensions serve as features over which humans collectively approach their objectives. To summarize, it is from the chief subject that we draw the domains to distinguish its chief categories of activities. Only then do we construct dimensions that provide shape to the environment from which the subject approaches his own survival, security, and prosperous future.

The unified field theory has collapsed part of the doctrinal domains of Air, Land, Sea, and Space into a single physical dimension that gives shape to physical objects; and has diverted the remaining aspects of those doctrinal domains into a physical domain that emphasizes four key critical activities: move, protect, force, sustain. The unified field theory has built a second domain, the cognitive domain, whose chief activities are lead/behave, form/shape, understand/decide, solve/adapt (all explained later). Finally, the unified field theory's three dimensions closely echo the three dimensions of the current theory (physical, cognitive, and information), but with two important caveats. The unified field theory replaces the cognitive dimension with "metaphysical" in order to create an image of the OE's collective mental terrain whose features are formed by the metaphysical organs of the human brain. The unified field theory replaces the information

dimension with an "information infrastructure," or II, in order to emphasize the self-constructed nature of this dimension. The most tailored form of the II is the network, defined by the leader at its center. This image is an evolution of the concept behind net-centric warfare, for it makes explicit the role of network in the service of a leader, whose activities are linked to both local outcomes and the achievement of political objectives.

The current model describes the strategic, operational, and tactical "levels of war." The unified field theory modifies the three level model so that it more explicitly acknowledges that every operational activity, whether campaign, battle, or engagement, has multiple levels to it, each of which shares a common core, or orders process, theoretically subject to a field order by which effects at the local and strategic levels are linked as part of the superior cognitive operation we call battle command. The current model describes the six phases of an operation in sequential and concurrent terms; we've modified the shape of the six operational phases so that it forms an ascending spiral, from which leaders at every phase share a common core. This is in order to acknowledge that the seeds of all phases are in each. Consider, as an example, that in practice, the move from dominate to stabilize to civil authority is often one and the same: the minute an enemy is defeated, the emergence of a future authority begins, usually imperceptibly, and under the watch of the same organization that supervised offensive operations. If one isn't structured for this almost simultaneous transition, or trained, or prepared, or equipped for its regulation, then the time/distance variable between liberated citizen and disillusioned Red recruit is too great to bridge.

The most significant change the unified field theory proposes is the role of battle command as the core cognitive operation from which the full spectrum of organized activity is derived. Within the unified field theory, battle command is the art and science of leveraging the full spectrum of elemental and operational combinations to resolve differences among Blue, Gray, and Red constituents via a series of forced and negotiated accommodations. It is the only operational activity within the unified field theory that is responsible for both tactical and political objectives. Battle command accomplishes that end via the integrated, synchronized adaptive achievement of a trio of continuously evolving cognitive effects: (1) Cognitive Capability, or the ability to reach collective understanding, apply collective solutions, regulate collective behavior, and adapt collectively; (2) Cognitive Vulnerability, or the ability to render Gray and Red constituents susceptible to Blue authority, plans, orders, and intent; and (3) Cognitive

Accommodation, or the willingness of constituents to modify their initial operational positions on terms favorable to Blue.

The end to which battle command aspires is the synchronization of Effects in order to achieve Operational Objectives, or *States of Accommodation*. The states of accommodation that presage a nation's return to relative harmony are four: (1) the long-term preservation of Blue; (2) the benign neutrality of Gray; (3) the surrender, conversion, assimilation, or neutralization of Red; and (4) suspension of hostile activity on terms favorable to Blue. These ideal states of accommodation effectively resolve the requirement for the most violent kind of operational activity, and set the conditions for the eventual satisfaction of a nation's (or group's) goals and objectives, and their return to a state of *tao*, or "cosmic harmony."[10]

For the achievement of its trio of cognitive effects, battle command depends on three derived, integrated, and fully continuous operational categories: physical, engagement, and regeneration operations. Although these categories are a point of departure from FM 3.0, it is actually an elevation of other operations explained, implied, or recognized as gaps within this excellent document. Battle command and its three derived operations must be entirely integrated within the operational concept and reflected in the paragraphs and annexes of plans and orders. Said another way, one cannot succeed physically without engagement, and one cannot execute engagement operations without significant support within physical operations, and one cannot outflank an adaptive, multi-generational enemy without continuously regenerating capability as part of the nation's adaptive strategy. That all three categories are part of virtually every operational plan is now a matter of presumed course by those engaged today.

Physical operations include the integrated, continuous categories of offensive, defensive, stability, and sustainment activities. Battle commanders employ physical operations for four chief uses: first, physical operations achieve sustained proximity to Gray and Red constituents. Second, physical operations produce imbalance, or the introduction of capability for which Gray and Red have no adequate response. Third, physical operations restore or reinforce stability in order to make Gray and Red vulnerable to Blue's arguments for cognitive accommodations. Fourth, physical operations sustain the life of Blue (Gray/Red as required) and their proxies during the span of an operation.

Engagement operations induce among populations: (1) the collective will and approach to war; (2) vulnerability in Gray and Red to the arguments of Blue; and (3) willingness across Blue, Gray, and Red constituencies to accommodate what were once mutually exclusive goals and objec-

tives. *Regeneration Operations* preserve the national capacity to evolve by (1) adapting to the current situation with the introduction of freshly trained and educated elements and tailored proxies; (2) by introducing international influences to security-related institutions via education, technology, commerce, cultural and other engagement venues; and (3) by conserving the sources of national power over the lifespan of a nation.

Mission Centers are the highest category of operations centers that observe, assess, direct, and modify operational activity. The mission centers in their sum provide the means by which leaders control the defense of their nation or group. Operations centers feed Missions centers, and are charged with building the OE's dimensional grid, so that all activity is identified and located by its three dimensional construct: physical, metaphysical, and information. The operations centers observe or direct activity throughout the OE, and are linked as part of a global constellation, so that no activity is ignorant of the other. The unified field theory, then, demands a corresponding theory of operations centers to determine an enabling architecture of operational control. The cognitive revolution ought to permit leaders to leverage the services of particular operations centers in the same way that cyber leverages the "footprint" of certain satellites.

Historical Precedents for Battle Command as the Core Operation From Which All Other Operational Activity Is Derived

The Problem

If the origins of war are psychological, rooted in human cognition, then so it its resolution. Within the unified field theory, operations are the means by which nations are moved from the will to war to the willingness to accommodate what were once mutually exclusive goals and objectives. That ought to be our core competency: the achievement of influence over Blue, Gray, and Red choice. We have no such superior operation, and no cognitive taxonomy with which to successfully address its absence.

We can learn from the way we as a community have approached the field of information operations. IO is the only major operational category whose explicit target is the human brain. No term in our doctrinal taxonomy has been so enhanced by its assigned mission set, or more diminished by the community approach toward its implementation. First, we used information in the title, suggesting that information is the decisive factor in influencing human choice (when compared, let's say, with financial,

emotional, physical, political, spiritual, artistic, and logical influences). Second, we limited IO's focus to Gray and Red minds, rather than including those minds that need cognitive attention just as much, Blue. Third, we assigned the function to an officer who was not also the battle commander (who, presumably, ought to be the cognitive exemplar across all constituencies). Finally, in execution, we understandably assigned "soft" missions to the IO teams, and "hard" missions to those skilled in creating physical effects. As a result, IO became euphemistic for soft operations as means to facilitate full spectrum operations, the chief categories of which remain implacably physical. In a brave and, I presume, controversial move, FM 3.0 drops the term altogether, an implied call to re-examine how the community approaches a category that tries to get at operations whose objective, theoretically, is preeminent.

Current efforts at rehabilitation fall short of what this paper proposes: that battle command, itself, moves to the cognitive operation at the core of full spectrum operations. Our solution will have to be at the expense of our considerable bias for physical operations and their effects. I'll frame our challenge and our opportunity via a vignette.

The author was tasked by the V Corps Commander and the Army G3 in 2003 to propose a near-term concept for mobile battle command, some of the author's observations are generally right; some are precisely wrong.

> The pivotal days of combat during Operation *Iraqi Freedom* were marked by classic, simultaneous, layered, synchronized engagement of Joint, Coalition, and Inter-Agency Forces. 3rd Infantry Division, under the C2 of V Corps, was the tactical Army ground maneuver unit poised for the ultimate conquest of Baghdad. Above the Corps' Area of Operations circled Air Force, Marine, and Naval Aircraft in Close Support of ground maneuver; on its flank was the 1st Division of the [1st] Marine Expeditionary Force, itself racing to attack Baghdad from the East; Special Operations Forces (SOF) and Other Governmental Agencies (OGA) maneuvered in, out, and through the Corps Area of Engagement. 82nd Airborne and 101st Airborne Divisions secured Lines of Communications South, Southeast, and West. National Intelligence Assets kept commanders aware of regional influences. On the battle's forward edge, the fight was raging at tactical TEMPO—every forward Command Post sought Situational Understanding of Blue and Red Forces as they converged on borders, boundaries, corridors, and zones. Time Sensitive Targets required Theater-wide clearance in a matter of minutes. Within a 150 square

> kilometer grid, the CENTCOM Commander's influence and interests were fully represented—Services, Agencies, Theater Operational Commands, Corps, Division, and small unit formations contributing to the dissolution of the Iraqi Armed Forces, and setting into motion the requirement for branch and sequel operations.[11]

Blame the late age at which the author experienced war; he was awed by the physical might of a nation (and its allies), by war's physical effects, and by war's geographical scope. This was, in his eyes, a glimpse of the future toward which AirLand Battle doctrine[12] had years ago pointed his generation: a networked environment in which leaders, regardless of level or location, their service or nationality, could treat space not as domains divided by proprietary proxies and procedures, but as continuous space—just as Newton conceived it. Physical objects and their effects, whether launched from ship, by air, on land, or monitored from space, could be traced, identified, synchronized, and sequenced to arrive as if part of a common plan or order, and their effects precisely measured. With an integrated, pervasive, fully interoperable information infrastructure, classical domains become a single physical dimension by which Blue marches relentlessly to meet and rout a thoroughly discouraged Red.

If battle command was merely the means by which leaders controlled physical operations and their effects, then I was generally right: an electronically sophisticated, pervasive network that could keep pace tactically would probably complete a revolution in battle command. And if operational success was defined by precision engagement, dominant maneuver, focused logistics, and full spectrum protection (the capabilities of the future OE as imagined by Joint Vision 2020),[13] then network-enabled battle command would be the revolution, and LandWarNet and all its like-minded, cyber-based information infrastructures (e.g. the GIG, or joint information environment, or the collaborative OE, and so forth) would mark the beginning of the end to the Army's transformational story. But the cyber technologies to which I referred, and for which I petitioned, would not have solved what we collectively as a nation had failed to account for operationally, which was the cognitive operation at the core of all wars. Said another way, today's cognitive revolution will require us to subordinate (or subsume) our growing interest in precise physical engagement in the same way that Einstein's theoretical revolution expanded Newton's cosmology.

The objectives of Operation *Iraqi Freedom* were the same as other wars: agreement among populations for the following states of accommo-

dation: Blue's long-term preservation; Gray's emergence as a benign, independent alternative to Red; and Red's surrender, conversion, assimilation, marginalization, neutralization, or destruction. Our objectives (largely left unstated) and the means by which to operationally approach each of those nuanced constituencies within and across the population groups were discontinuous. Lacking an effective institutional approach to cognitive operations, we had vocabulary only for the physical. After physical operations put Gray and Red on their heels, that's where they were largely left (despite extraordinary efforts to do otherwise): unmoored from their institutional support, some of their enabling infrastructure disabled by shaping operations, denied meaningful roles in emergent Iraq, and possessed of little financial, network, social, or political infrastructure with which to enable their own emergence. Both Gray and Red adapted by building new alliances within which fresh grievances fueled their psychological migration from humiliation or euphoria to common disillusionment to private understanding to personal decision to organized hostility and armed opposition. In this sense, some of liberated Gray emerged as Red and some Red remained Red. That situation, ironically, has been relieved only by the emergence of a superior cognitive operation (counter-insurgency) under the conduct of brigade, regimental, and special combat teams, the stirrings of which this paper strives to amplify.

So, with regard to the author's concept for a network-enabled battle command, the author was precisely wrong. What battle command needed—even more than a pervasive cyber network—was a superior cognitive operation and its trio of cognitive effects. First, we'll provide our extraordinary leaders and soldiers across Iraq and Afghanistan with good historical company.

Historical Precedent for Battle Command as the Cognitive Operation at The Core of the Operational Environment

The network is the offspring of the leader, provoked by his requirement to exercise influence over operations. That was true when the network and the operational formation were one and the same and primarily human (as will be argued in part V); and it is true today, when the network is increasingly electronic and provided to him. The network is like man's best friend: if battle command is focused on physical effects, the network is focused likewise. If battle command becomes our superior cognitive operations, the network will focus on the achievement of cognitive effects. What its architects, engineers (social and electrical) need is what the battle commanders must give them: a vocabulary, operational taxonomy, and a

unified field theory for an OE that is cognitive at the core, that in their integrated sum can guide the development of their technical, doctrinal, and organizational corollaries. We begin by turning to historical examples of operational commanders who, despite having won their fame by waging the most violent of physical battles, all considered their tactical fights in the service of a superior, cognitive operation.

The most compressed, complex, and violent category of operational events is Battle (whether on land, in air, on sea, from space). Where the objective of battle is an (often) unavoidable requirement to defeat (or survive) an opponent's physical activity, the objective of battle command is the achievement of a set of cognitive accommodations among local constituencies that set the conditions for states of accommodation across Blue, Gray, and Red populations. Cognitive accommodations set the conditions for the return (or emergence) of an international harmony, on terms favorable to the long-term preservation of Blue. Said another way, battle command is that root category sufficiently comprehensive to link the most violent form of operational activity to the political end from which justification for its horrific method is derived.

Sun Tzu wrote: "to gain a hundred victories in a hundred battles is not the highest excellence; to subjugate the enemy's army without doing battle is the highest of excellence."[14] For that, and other similar advice, Sun Tzu is occasionally reduced to a kind of anti-Battle guru. Sun Tzu is to whom we direct our Information Officers, even as our organic combat constituency labors over our core competency: physical operations and the achievement of their effects. Yet Sun Tzu was, if legend is history, also a great battle commander; and much of his treatise describes the cognitive nature of organized physical force. Battle represented failure to achieve operational ends by other means, but that didn't mean it was any less regulated or linked to the production of cognitive effects and objectives. The superior cognitive operation, from which battle is never discontinuous, is that which governs battle's violence, keeping it at sufficient pitch to gain ascendancy over one's adversaries; and at sufficient moderation to preclude irreparable bitterness between the sponsors of combatants.

John Keegan cites the example of primitive tribes who turned to battle to force accommodations among constituents whose minds remained unmoved by less physical arguments.[15] Young warriors led subsets of tribes into micro-battle. Within regulatory range, the tribes' elders stood poised to intervene if the sanctioned violence rose to the level that its physical damage overwhelmed the psychological benefit of conflict resolution (by spawning a bitter post-battle collective dispirit). Elders served to regulate

violence, linking its effects to the achievement of battle command's chief objective: cognitive accommodations among disputants for positions that were once mutually exclusive. Battle command is not restricted to a particular rank, or echelon, or profession, or location, or event (like battle); but it does depend on Sun Tzu's construction of a moral bloodline that unites the mandate of the ruler (or people or government), with the responsibility of leaders to secure the "national treasure," with the willingness of soldiers to act as "sons" and die for them.[16] Keegan's elders stood as a kind of surrogate orders process—a forward command post that synchronized the activities of all engaged constituencies: (1) the tribal leadership/community (nations or groups); (2) their battle commanders; and (3) their engaged soldiers; all linked to the political ends that underwrote their violence.

Although not in tactical command of their battles, those elders practiced battle command: a multi-level operation that leveraged the full spectrum of activity in order to achieve three distinct cognitive effects. First effect: *cognitive capability*, or the ability of Blue to act as if one, united by a common understanding of their situation, and able to act out their particular role in the proposed solution under the influence of plans, orders, and intent. Second effect: *cognitive vulnerability*, or the introduction of doubt, confusion, fear, or false understanding within the minds of Gray and/or Red. Getting routed in battle is one of many ways to achieve this effect. Third effect: *cognitive accommodation*, or the willingness of Blue, Gray, and Red to reconsider goals and objectives that once were mutually exclusive. The operational activity that provoked the trio of cognitive effects begins well before the outbreak of battle; continues throughout battle; and extends well into its aftermath. Otherwise, how to explain the willingness of warriors to recognize the authority of their elders; or the apparent ability by elders to assess battle damage sufficient to call it off; or the negotiations that, after the battle's conclusions, surely must take into account the heroic performance and sacrifice of engaged warriors? Although much of this taxonomical work is the author's own extrapolation, it conforms to observations of battle commanders across historical generations: there is a superior operational weave, within which the peculiar event we call Battle erupts and subsides, and the thrust of that weave is toward the production of cognitive effects, in line with political ends at one end and tactical objectives at the other.

No leader is more identified with physical battles than the Duke of Wellington, but he, like Sun Tzu and Keegan's elders, would have considered his Battle part of a superior cognitive operation meant to resolve the particular origins of the war by forcing new states of accommodations

among constituents. Despite being named after the town nearest Wellington's Headquarters, Waterloo was no "local" battle. The argument over which this particular battle erupted concerned the mutually exclusive nature of opposing political systems and the means by which European nations in general were governed (and by whom). That argument, in light of Napoleon's desire to rule Europe, would be resolved only via the removal of his army. Said another way, battle had become the only means by which to approach the collective brain of France.

Confiding to a journalist shortly after the battle's conclusion, Wellington confessed that the outcome at Waterloo was "the nearest run thing in your life,"[17] the success of which he attributed to his own personal presence and the "trouble"[18] he took about the battle. Riding into battle with his pistol holster containing no weapon but merely parchment, pen, and ink[19], the trouble Wellington took was largely devoted toward the achievement of that same trio of cognitive effects that would have long-term influence over the campaign's outcome. First, he made sure that his own precise commands, ubiquitous presence, and wise decisions united and regulated the moral spirit of his coalition sufficient to defeat France's physical argument. The discipline displayed by the British soldier in the face of French columns and their enthusiastic battle cries demonstrated to myriad French Waterloo veterans the moral superiority of the opposing force.[20] Wellington's social engagements and numerous letters were meant to calm a nervous Belgium. His decision to reward the Prussians for Blucher's late-day rescue by giving them the honor of pursuit went far in satisfying nationalistic pride.[21] His own narrative of the Battle was written within hours of its conclusions, meant not only to regulate the precise reaction of engaged publics to its results (part of a narrative operation I'll soon address), but to raise the morale of an Army whose casualties had exceeded those from any of Wellington's earlier battles. In short, the trouble Wellington took over Waterloo was to enable the superior operation and its cognitive objective: accommodations among nations for a Europe that resisted the urge to export the revolutions of its individual members.

While Wellington and Keegan's elders are examples of battles waged in the service of superior cognitive operations, Colonel MacFarland's experience in ANBAR province is an example of the superior cognitive operation that obviated the need for battle altogether. When Colonel MacFarland took his brigade combat team to ANBAR province in 2006, the region was already "liberated," by which I mean that its pre-war political infrastructure had been replaced with something else, although its identity was still emerging, and in ways that made providing it any assistance

problematic. Col MacFarland found himself sharing space with multiple groups sponsored by organizations across the levels of war. Each built their own model of the situation, sent it into cyberspace, where it hung in relative isolation from other judgments on ANBAR (most were dire). The consequence was a kind of operational paralysis. MacFarland reduced those views into a single situation with multiple caveats, and then applied his own command presence to serve as a kind of Wellington command post around which the multiple levels of constituents still interested in the fate of ANBAR rallied. Colonel MacFarland, like the battle commanders before him, embodied the shared orders process, and served as the common core of operational activity. And, not insignificantly, if ANBAR was to have a single situation with multiple caveats, it was going to be the battle commander's caveat that mattered most.

ANBAR, like Waterloo, was no "local" operation. When Col MacFarland made accommodations with the Sunnis, he had in practice (but not officially) negotiated on behalf of both the United States and the new Iraq. By striking a deal, trusting instincts, refusing to condescend, and approaching one another across the metaphysical dimension, MacFarland and his Sunni counterpart had at some level reconciled the psychological consequence from the earlier failure to assimilate what had been the ruling class within an emergent Iraq. Although he lost over 90 remarkable members of his joint force, no physical activity ever rose to the level of a classic battle. Instead, he had achieved what Sun Tzu considered the greatest good: the subjugation of an army without battle.

Within the context of this unified field theory, Col MacFarland had executed battle command as the superior cognitive operation. He used the full spectrum of operational activity not as distinct and phased events, but as operational combinations in the service of the trio of cognitive effects. First, he built a team, not all of which fell under him, that acted with uncommon character and uniform behavior; then leveraged physical force to put them in the heart of the population centers. Second, through direct engagement with constituents, discovered and exploited vulnerability within the seams of the Red alliance. Third, he used *narrative*, *emergent*, and *negotiation* operations (discussed below) to convert vulnerability into the willingness to accommodate Blue and Gray objectives. Word of his gains travelled across Iraq, went by cyberspace straight to the national command authority, and entered the public consciousness via *USA Today* and other media. Battle command, as the superior cognitive operation, had achieved its interim objectives: an agreement between the United States, Iraq, and McFarland's alliance to facilitate the emergence of a new kind of Gray (in

this case Sunnis who had been formerly Red), the marginalization of a subset of Red within the region (Al-Qaeda in Iraq), and the assimilation of those who would have otherwise joined their ranks.[22]

Battles are those rare events that usually earn start and end dates. On the other hand, battle command, as the examples of Wellington and MacFarland demonstrate, is the continuous "trouble" that leaders take to keep their activities aligned with the cognitive effects that power operational objectives. Part of that trouble begins well before the conditions for battles are ever met, and extend well beyond their conclusion. Said another way, there are operations that only under tortuous logic fall under the categories of offense, defense, stability, and support to civil authority, but are often so decisive that they demand equal status to the physical four. The unified field theory broadens full spectrum in two distinct directions. The first is by way of *engagement* operations, for which I will provide a few examples. The second is *regeneration* operations, which is developed in the fuller article to follow. We'll consider three examples of engagement operations: narrative, emergent, and negotiation. To do so, we need to face the political nature of our profession head on. And by way of introduction, a little obligatory Clausewitz to loosen whatever constraints readers remain under.

Full Spectrum Operations Reconsidered

> "The primary colors are only five in number but their combinations are so infinite that one cannot visualize them all."[23]

If war is, as Clausewitz states, "a continuation of politics by other means,"[24] then operations are perhaps the most comprehensive (or inclusive) political activity known to social man, for they are regulated, supervised, professional, voluntary, noble, vulgar, honorable, heroic, spiritual, hellish, violent, sanctioned, occasionally illegal, patriotic, legislated, and civilized—all at once. At various times during its phases, war's operations extend (essentially) the same services as the body politic: economic, political, cultural, informational, educational, services, and physical security. At other times, war exhibits what politics cannot: a willingness, quite often an impatience, to use force that leverages every element of national (or group) power. In all circumstances that I can think of, only war comprehends the full spectrum of organized human activity conducted by, among, and between psychologically disharmonic populations. And battle command is the highest level of organized activity that comprehends the full spectrum of operational activity permitted it by war.

Sun Tzu (and his Chinese contemporaries in general) took for granted that most engagements with an enemy would require "normal force"[25]: the kind that moved and fed an army, projected force to gain presence or create imbalance, protected the army to sustain its presence and preserve its authority.[26] But victories required the use of "extraordinary force,"[27] the basis for which was the leader's grasp of metaphysical terrain (the art of war): the emotional, physical, moral, political, professional, psychological, spiritual, and cultural identities of Blue, Gray, and Red and their proxies. Emerging from this landscape was the leader's understanding of his opponents' vulnerabilities or strengths, from which emerged a plan to organize his own elements into teams, activities into operations, and operations into plans. Those plans were tied to political intent, which in the case of Sun Tzu was the preservation of an intact nation. Said another way, Sun Tzu's ideal general required mastery of a broad spectrum of operational combinations that included not only "normal force," but "extraordinary force" that kept the nation under attack, *intact*. Applying that intent to our current circumstance in Iraq and Afghanistan, to what end is liberation, if the liberated don't emerge?

In theory, *full spectrum operations* is a term that conveys diversity and should provoke the kind of operational improvisation that permits Blue to rapidly exploit physical success by gaining access to the human brain. If AirLand Battle Doctrine expanded the kinds of elemental combinations theoretically available to the engaged ground commander to achieve physical effects, then battle command as the superior cognitive operation expands the kinds of operational combinations that will be required if we are to approach and shape mental effects within the metaphysical dimension.

If this is the case, then each single operational activity must have as part of its DNA an understanding of the broader effect for which its particular activity is in support. That broader effect has three chief currents, each of what operates at different speeds: (1) an engagement story that seeks accommodations, or relative harmony with all constituents on terms favorable to Blue; (2) a physical story that gets us "over there," sustains and protects our physical presence; and permits us to force agreements, if required; and (3) a story of regeneration that permits our continuous adaptation so that we aren't swallowed by another nation (or group) more "fit" than we to govern. Corresponding to these movements, the unified field theory has built three categories of enabling operations: engagement, physical, and regeneration. We've fitted each with a starter kit, or sampling of proposed doctrinal operations. Leavened effects depend on Blue's abil-

ity to combine operational activity across all three categories, as part of *each* activity (one of FM 3-0's important insights).

It is through elemental and operational re-combinations that Blue achieves its greatest advantage. Sun Tzu called it a kind of formlessness, or the ability to conform to a continuously evolving situation as "water shapes its flow in accordance with the ground."[28] The enemy acknowledges the effect of Blue activity, but cannot describe the form it took. Under this approach, our institutional formations that I'll sum up metaphorically as tables of organization and equipment (TOEs) and doctrine, dissolve into their elements so that leaders can rapidly recombine them into teams and operational combinations that conform to the dynamics of a situation defined by peril and opportunity. To succeed in this space, we must transcend the cognitive constraints that we have imposed on the shape of teams and the combinational diversity of operations. To what advantage is network connectivity within Blue, if Gray's internal connectivity is non-existent? To what advantage is Blue's combat superiority or ability to topple governments, if it doesn't presage political opportunity from Red's rubble? And to what advantage is our current success with our current threat, if we're not institutionally adapting to the situation that has not yet fully arrived? Stated differently, "full spectrum operations" has two interrelated meanings: first, it means that we combine at the elemental level activities across engagement, physical, and regeneration categories; second, it means that we do so in order to create the full spectrum of effect across populations: from cognitive capability, through vulnerability, to accommodation.

A few examples are introduced to expand the Army's notion of full spectrum operations so that it addresses directly the political nature and responsibilities of the profession. Within the unified field theory, battle command is the operation held responsible for both tactical outcomes and setting the conditions for the achievement of political objectives. We speak obliquely about our political responsibilities in our doctrine, because we've spent careers avoiding the subject. Certainly, the Soviet Union's cadre of political officers did nothing to rehabilitate the term within our operational tradition. And, finally, the role of nation-building is considered condescending by some, evidence of hubris by others. But I believe that such objections are voided by the nature of war itself; it demands that its military leaders, most especially its commanders, understand the nature of politics in the purest sense of that word. "I don't know what else to call them, but governors." That's the language I used in private correspondence to describe our Divisional commanders during OIF 1. Sun Tzu, Wellington, and Grant, as well as those many leaders who oversaw the post-World

War II emergence of Europe and Japan would have empathized. There are three operational categories for which I believe the senior mission commander is personally responsible. Each is essential to the success of tactical outcomes, each is decisive with regard to setting the conditions for the achievement of political objectives, and each requires that leaders throughout an organization exhibit the most acute of political sensibilities. Those operations are narrative, emergent, and negotiation.

Narrative Operations. Narrative operations have three chief ends. First, they justify operational activity and tell the story of on-going operations, in order to sustain Blue's will to war and retain authority for the war's strategic direction. Second, they build the rhetorical basis for the emergence of Gray constituencies. Third, they contribute to the rhetorical underpinnings of models designed to deceive, or influence, confuse, or discourage Red's cognitive processes. *Counter-Narrative Operations* perform two different, but related, and equally decisive roles. First, they translate Blue activity into Gray and Red narratives to make sure that Blue's plans, orders, and intent cannot be exploited by Gray or Red (a kind of Red team approach).[29] Second, counter narratives recommend changes to operational activity in order to reinforce, undercut, subvert, counter, and seize Gray and Red rhetorical operations. It is essential to the comprehension of the unified field theory that readers recognize that all operations, when written from the perspective of the constituent, are Blue.

Leaders must understand that all operational activities are acts of rhetoric, and form a narrative pattern that is leveraged and exploited by all constituents. Narrative operations amount to storytelling via art, literature, imagery, narratives, and patterns of operational activity that, over time, coalesces into story. Narrative operations tell the story of the bound fates of Blue, Gray, and Red as they seek accommodations within a competitive world. Most significantly, narratives are rooted in national or group myth, the short hand version of the story of national or group birth and emergence, survival and enlargement. The best narratives—especially the narratives that justify operations—force readers to see themselves and their acts as the newest chapter of their national or group myth, for better or for worse. But under no circumstances can narrative operations remain distinct from the plan that visualizes the means by which operations are eventually resolved. How will this story end? And that which links operational activity in general to narrative operations specifically is this: when the reason for fighting can no longer be related to a nation's (or group's) security, narrative operations will be perceived as propaganda.

Poorly designed narratives, therefore, can have huge strategic consequences. For example, Blue's invasion of Iraq was justified by a narrow national narrative that emphasized clear and present danger (weapons of mass destruction). That narrative, in turn, drove a force composition that emphasized physical effects and an urgent timeline that limited the amount of force structure available for the ground invasion. Shaping operations compensated by facilitating early physical success but at some cost to Blue enabling Gray's benign emergence. Finally, the decision to preclude the conversion or assimilation of former Baath officials was certainly influenced by the tone of a narrative that had so thoroughly demonized a party willing to launch WMD against its own.

But for those charged with enabling transition between decisive and stability operations, this was a war about understanding the mental states of multiple shades or Red and Gray (even Blue); it was about encouraging and facilitating the emergence of Gray from Red. The narrative that spoke to these nuanced constituencies was added only later, by engaged formations that had inherited the circumstances of their war, complete with a nearly-fleshed character. Cognitive revolution permits the narrative that justifies war to be broadened at its origin, shaped by narrators from combat teams destined to inherit operations in later phases.

Because the vast majority of operations take place outside the view of its key constituencies, narrative operations provide "witness" to the on-going war in the service of the superior cognitive operation. Wellington used his battle narratives as "instruments" by which he influenced the way constituents behaved. First, his narratives were meant to buoy the morale of a nation that had been at war almost continuously for six decades; secure resources for subsequent operations; and perpetuate his role as their strategic author. Second, his narratives judged military performances, and the consequent reward or punishment that came with those public judgments inspired emulation or provoked conformation across his formations. Third, his narratives were virtually devoid of literary effect, providing the Red reading public little emotional provocation for further resistance; providing the Blue public little with which to inflame their already aroused passion for achieving rapid, declamatory defeat of their cross-channel rivals; and providing the Gray public with an image of the kind of wise, restrained leader that would preside within a post-Napoleonic Europe.[30]

The expectation that one's participation in national or group operations becomes story remains powerful—if not the most powerful—incentive to fight in a particular way. Western minds recoil at the narrative compensa-

tion provided suicide bombers, but western narratives that publicize heroic activity can provoke similarly suicidal behavior. Wellington was so frustrated by ill-advised cavalry charges that provoked the premature commitment of his formations that he refused to give the charge any narrative space in his dispatch as means to discourage the practice.[31] Sun Tzu warns of generals whose operations are undertaken as means to earn glory and promotion, the outcomes of which were almost always disastrous. We all know the fate (and psychological origin) of the disastrous charge of the Light Brigade. As part of narrative operations, we must consider kinds of counter-narratives that are used to remind readers of the kinds of behavior that will win them roles to relish. Certainly, the act of taking photographs by those who abused prisoners at Abu Ghraib is an example of perverse heroic story-telling, for which we had little in the way of narrative art to counter.

On the other hand, battle commanders use their narrative operations to provide their adversaries with a deliberate look into the collective character of their formation (and, by extension, into the character of the nation or group that sponsors it). On the eve of the Battle of Guagamela, Alexander the Macedon faced Darius the Persian to determine the destiny of both kings and their armies. Alexander was advised by his chief strategist to take no chances, attack at night and rout the Persians in surprise. Alexander chose to attack in broad daylight, partly to preclude the emergence of apologists who might diminish the circumstances surrounding what would be a flood of witnesses to Alexander's almost super-human prowess.[32] While his advisers were focused on battle and its effects, Alexander was involved in battle command, linking the effects of battle to the superior operation: securing the loyalty of the Persian population for a Macedonian who was heretofore its arch rival and who from here on out would rule in absentia.

In a similar sense, Washington led his army on a bold crossing of the Delaware on what surely should have been a doomed attack against Great Britain's Hessian mercenaries garrisoned at Trenton, New Jersey. It was Washington's intent to have the story of that battle deliver what no physical blow could: evidence of the mental objects that occupied Washington's remarkable brain. The object that stood out most was the character of an emergent nation that would under no physical circumstances submit. If, as some historians suggest, Washington had a shaky command of battles, he certainly had a firm grasp on battle command, or the cognitive operation designed to make Great Britain reconsider its opposition to American independence. In summary, narrative operations are part of the continuous fabric of operational activity.

Emergent Operations. If we went to war to remove the threat of Iraqi's weapons of mass destruction, and that required the removal of Saddam Hussein, then the real story of Operation *Iraqi Freedom* was about the emergence of a post-Saddam Iraq. The removal of a corrupt Red political landlord necessarily gives way to groups who emerge from its shadow, and certainly the nation that provokes that dynamic must account for its consequences. We had no institutional or taxonomical vocabulary for this kind of operational responsibility, no means to quantify or qualify the force structure required to encourage its benign evolution, and therefore had no basis with which to mount a powerful argument to expand the composition of the invasion force. After all, even with a robust lexicon for physical operations, we had problems enough marshalling an argument to earn sufficient forces to *secure* a "liberated" Iraq.

Ultimately, *emergent* operations reduce the time, resources, and danger implied by Blue's long term operational occupation of nations whose political infrastructure has been removed but not yet replaced. It does so by encouraging the emergence of multiple shades of Gray as benignly neutral, and independent of a much diminished, marginalized Red authority. Emergent operations may be about the post-combat phase, but their effects are among the first achieved during any kind of operational activity. First, emerging operations establish among Blue leaders their pre-operational understanding of optimal mental end states for Gray and Red constituents (all shades of Gray and Red). Second, emerging operations filter all shaping activity to encourage those ends, from staged contracts, loans, cognitive experts, knowledge experts, to protection of key infrastructure (even at the expense of facilitating early physical activity). Third, emerging operations must reexamine from the wreckage of regime change, the emergent nature of the defeated army, liberated village, individual groups and alliances, and any surviving government to comprehend the nature of the new thing that is becoming. *Stability and advisory operations* are best seen in operational and concomitant combination with emerging operations. Stability operations restore those basic services that prevent constituents from considering the advantages of benign independence. In their absence, a group's devolution toward chaos is unconstrained. *Advisory* operations are distinct from emerging operations in that they take place after groups have found their political identities (in a relative sense). Advisory activities develop long term relationships between institutional counterparts of Blue and Gray (and Red, as part of Intelligence operations).

Emergent operations, then, have pure political ends: the ability of Gray to emerge from the shadows of an old Red political landlord. Emer-

gent operations require formations whose leaders have inculcated them with a psychological sensibility toward how liberated groups are shaped, formed, developed, destroyed, and recovered. So essential is its success to a war's timely resolution that it cannot be delegated: if the emergence of liberated groups is not under the gaze of a liberating Army, then it's performed under the pay of an insurgent. As the CG, 101st Airborne Division, General Petraeus employed his own combat formations as part of a broad emergent operation in and around Mosul. In every meeting I can recall, General Petraeus argued with exceptional passion and inescapable logic for the resources required to translate the momentum of our physical success into what he clearly viewed as the emergence of Mosul. He used the same tone and level of indignation I'd heard him apply to another kind of demand: sufficient network capability to enable him to fight his physical battles (our Divisional commanders were remarkably consistent in their expressed frustration with availability of resources for emergent operations).

Negotiation operations translate effects into early, temporary, provisional, incremental, or final accommodations. Just as narrative operations translate effects into stories that make mental impressions across multiple levels of constituents, negotiation operations seek from every operational activity the evidence of concession, or the evidence of opportunity to accommodate. Among some of the concessions that negotiation operations seek include meetings between constituencies; cease-fires; agreements with regard to services of any kind; public acknowledgements; truces; land exchange; terms of surrender; Blue's role in Gray's institutional construction; Red's role in Gray's emerging institutions. Negotiation operations produce gains that in their accumulated march lead to states of accommodation where populations agree to reconsider positions that were at the outset of hostilities considered mutually exclusive. They close the deal so to speak, even if they do so inch by inch, day by day.

We must avoid equating negotiation operations with the war's final movement. Negotiation is a persistent and pervasive operation by which leaders apply a range of concessions in order to achieve a more favorable position. Whatever McFarland did in ANBAR, part of it was negotiating concessions that weren't on any official gift list in exchange for the kind of metaphorical higher ground McFarland considered decisive. That way revolution—the right kind—leans. The Sunnis received a U.S.-trained, trusted Sunni security force that was returned to the neighborhoods from whence they came; and the Americans received a powerful ally in their war against what had become a common enemy. That cognitive accom-

modation soon gave way to an Iraqi-wide alliance between many Sunni tribes and the U.S.-led coalition.

Wellington negotiated with the French for the use of their markets, thus creating an ironic demand for the presence of an army that was, after all, intent on eliminating their head of state.[33] The cognitive accommodations between local French citizens and Wellington served the latter well in his role as de facto leader of post-war France. Finally, permitting a vulnerable opponent the right to negotiate how he wishes to cede, or surrender, or make a particular statement may be the most efficient means to save thousands of lives. For example, by preserving the dignity of Hirohito in the closing days of World War II, the Allies leveraged the authority the Emperor retained over his subjects: when he asked his armies to lay down their arms, divisions across China, who had never known defeat in battle, surrendered their swords to the tattered Nationalists who had never known victory (at least against the Japanese).[34]

Without a formal name for this decisive activity, how do we discover if there is a science to the art? What signs emerge when opponents who are vulnerable give way to a willingness to negotiate, and what kind of operational activity best seals the deal at least cost to the future? For negotiations take time, and while they are waged, the full spectrum of operations is also underway. In between the time the armistice that concluded the Great War was signed (approximately 0510 hours) and the time it took effect (1100 hours), military operations proceeded virtually unabated. On Armistice Day, 1918, all sides suffered 10,944 casualties, a loss that exceeded the war's daily average. Certainly much of that loss had to do with the attitudes of the prosecuting generals toward negotiation operations, heavily influenced by political views that had never been subjected to operational scrutiny—despite their potential consequences. When Pershing sent out the message that announced the "cease fire" that would take effect 1100 hours that morning, he did so without providing any orders that countermanded planned attacks or combat activity.[35] Certainly, those deaths changed or altered the personal histories of those affected.

The heartbreaking, almost absurd conclusion to Grant's pursuit of Lee is impossible to comprehend unless to presume that Lee had to demonstrate an absolute abhorrence for surrender, in order to surrender on the most favorable terms possible.[36] Was there some way to operationally account for that psychological insight short of virtual annihilation? What significant insights are to be learned by an examination of their exchange of messages, the precise terms over which they haggled, and the ceremony designed to establish optimal mental states for both victor and

vanquished. In the absence of a name for these decisive operations, we lack a corresponding science.

The Taxonomical Model of the Operational Environment, Its Two Domains, and Its Three Dimensions

> "[T]he primary purpose of any theory is to clarify concepts and ideas that have become, as it were, confused and entangled."[37]

Taxonomic models matter. The taxonomy of life classifies over five million living species, of which we are merely one, and permits scientists to clarify from the clutter of diversity those patterns that explain the origins, adaptive progress, and even likely fate of essential species. The alternative to taxonomical work is individual explanations for Earth's endless, present, and diminishing variety. And while we may exhibit empathy for life's diversity, that withers when some subset refuses in its evolutionary path to accommodate our own adaptive, evolutionary way. The taxonomical model is, in this sense, the dramatic story of accommodation: how its chief subject successfully competes for room within an environment that is characterized by the overwhelming biological urge to survive by any and all means available. Considering the stakes, taxonomies seek universal applicability in order to accelerate insights into the nature of their subject, thus the universal nature of this particular Unified field theory. And, from a security perspective, taxonomic models help focus the resources of a nation that are finite, on an essential subject whose potential capabilities, activities, and mysteries threaten to break our organizational and financial capacity. For example, the use of the taxonomic term, domain, to describe a particular capability is so tightly bound with fiscal permission and service sponsorship, that any recommendation to add a "new" domain excites an enervating, but necessary debate at the highest levels of the nation's security organizations.

Dimensions and the Problem of Operational Approach

If the origins of war are rooted in human psychology, then the only way to move populations from the will to war to the willingness to accommodate what were once mutually exclusive goals and objectives is to change minds (or annihilate or exterminate implacable constituents, an outcome that does not lend itself to long-term inter-group harmony). How does one approach such delicate mental organs, usually surrounded by significant physical protection, guarded by bias, under mysterious influences,

and often located at some remove, without putting themselves and their nations at risk, or planting the seeds of future conflict?

The overriding problem, then, that battle command must solve is one of approach. Consider Sun Tzu's advice, rendered as poetry and delivered as intent: "throw rocks at eggs."[38] This is no pitch for the use of overwhelming force, but an image that conveys the role of operational approach: first, one must get close enough physically to recognize Red's vulnerability (it is an egg,); second, one must engage with Red with sufficient delicacy to preserve Red's ability to negotiate, accommodate, convert, surrender (otherwise, the objective of operations is annihilation or extermination); third, one must do so without surrendering one's inherent physical advantage (Blue is still a rock). At some level, then, *The Art of War* is a meditation on the matter of operational approach, an examination of the means by which constituents approach one another in order to provoke three major effects: the collective will to war; the collective vulnerability of Gray and Red; and the collective accommodations among Blue, Gray, and Red that preserve the conditions necessary for a return to (or emergence of) international (or group) harmony.

Our own OE is self-cast and constructed around three dimensions in order to secure the collective survival of nations or groups. In our doctrinal approach toward dimensions, we've articulated only one, and ceded much of the description, development, and integration of the other two to an ad hoc chorus of diverse advocates. The three dimensions that extend our operational environment as means to approach our objectives are (1) the physical, within which constituents perform their physical acts (move, force, sustain, and protect); (2) the metaphysical, within which constituents perform their cognitive acts (lead/behave; shape/form; understand/decide; solve/adapt); and (3) the information infrastructure that unites the activities of the two, by providing form to thought, sufficient to enable collective understanding, behavior, regulation, and adaptation. Battle command supervises the construction of all three dimensions, and depends on all three to approach, pursue, and achieve their operational objectives.

We'll begin with a short examination of the dimension with which we are most familiar: the physical dimension. We currently refer to that dimension in terms of the four doctrinal domains of air, land, sea, and space. The unified field theory applies the term "dimension" to echo the approach science takes to explain natural phenomena. Physical dimensions (length, width, height, time, space) describe the nature and location of physical objects, thereby enabling a common picture of physical activity capable of being comprehended across broad and diverse populations.

Our current approach that emphasizes four distinct domains that fall under service sponsorships (and service common operational pictures) obscures the continuous nature of the physical activity that takes place across this dimension. Operational dimensions, as with their scientific counterparts, are human constructs overlaid on natural phenomenon. We overlay our maps, doctrine, coordinating instructions, proxies, and human organizations over earth, its geography, and its atmosphere in order to facilitate four primary physical acts: strategic movement and tactical maneuver; employment of force; protection of our physical objects; and their protracted sustainment. The end of such self-construction is a kind of Burma Road: the means by which we gather like-minded groups into tailored formations; move them to proximity with the enemy; then engage the enemy for effect.

If that were our sole objective, then dominance in this dimension would guarantee our nation's security. But we know that physical dominance doesn't guarantee national survival or security. If the origins of wars are psychological, then their resolution depends on changing minds; not merely the minds of our opponents, who may submit to our arguments from a variety of selfish motives, but the minds of Blue whose own resistance to adaptive change over multiple generations may have formed war's disharmonic root in the first place. The dimension by which we approach human brains is the metaphysical. For those who consider the term too philosophical, consider the alternative: the physical mass of human brain that serves as source to human identity. Even in casual conversation, we approach the subject using metaphors: from names we give each other (personal, professional, and role); to the names we give the organs of the brain: character, mind, soul, imagination, spirit, personality. We even measure these organs with words that qualify them: judgment and wisdom; charisma and spiritual; obstinate and intellectual. Even as science begins to map this mental landscape, and uncover how minds metabolize influences into mental objects that are in some sense visible, we have failed to direct cyber's attention to locating and identifying these mental objects as part of a cognitive common operational picture. And the object that matters the most is the decision to behave in a particular way, on behalf of a particular constituency, and in pursuit of a common objective. That decision is the ultimate cognitive act. That's the target of battle command. Leaders may need the physical dimension to get them physically close; but they'll need the metaphysical dimension and the cognitive activities it enables to close the deal.

Where sustained physical proximity, freedom of maneuver, and physical imbalance are the chief objectives of the physical domain and its

dimension, the objective of activity within the metaphysical dimension is the achievement and application of knowledge.

> "Know the enemy and know yourself; in a hundred battles you will never be in peril"[39]

This is the sine qua non for Sun Tzu devotees. Even FM 3.0 alludes to it by way of introducing the subject of information superiority.[40] But Sun Tzu's understanding of knowledge implied a range of cognitive activity that exceeds most of our current definitions, and encompasses what the unified field theory would call the core cognitive operation from which all other operational activity is derived, or battle command. His *Art of War* is an extended meditation on what precisely Sun Tzu meant by knowledge.

First, and above all, knowledge meant to lead as part of a political and spiritual mandate; from that comes an army that acts as one, with common character. Knowledge means to shape information into the cognitive model of the situation, one that tracks not only physical objects (weapons, organizations, log trains, transportation, environmental features), but the location and nature of mental objects, including the psychological, emotional, intellectual, and spiritual state of enemy and friendly minds. It is from this cognitive model that leaders draw an understanding of the peril they are in, as well as the opportunity that is within their grasp. Knowledge is to conform to the Janus-shape of situation like "water over earth," until threat is countered, and opportunity seized. Sun Tzu regularly objectified the mental states of his own generals, his opponents, and their formations, drawing from those insights the method for his approach: give the enemy no egress, Sun Tzu warned, and transform the human who is vulnerable and willing to accommodate into the animal that fights to its death.[41]

To know is to understand the situation so personally, that it becomes the leader's own conception—not that of the enemy, or staff, or public pundit. Leaders transform their understanding into metaphor or image, by which operations adopt the cognitive character of its leader. To know is to translate personal understanding into collective activity, as leaders and their staffs measure ground, estimate "quantities," calculate distance, compare plans, and project the "chances of victory."[42]

Finally, knowledge means using personal presence and intent to regulate the spirit of operations, so that its cognitive objectives are never compromised, "[f]or while an angered man may be happy, and a resentful man again be pleased, a state that has perished cannot be restored, nor can the dead be brought back to life."[43]

To know, then, is to operate wisely. It is how "the state is kept secure and the army preserved."[44] So, now that we've established the physical approach, articulated a metaphysical landscape by which leaders approach knowledge, all that's left is to approach the objective together as collective body and mind. It is here that the metaphysical and physical dimensions need the assistance of an information infrastructure.

The Third Dimension: The Information Infrastructure, the Network, and Cyberspace

The information infrastructure enables organized human activity, for it gives form to the thoughts inside human brains and their proxies. Without the Information dimension, there is no coordinated physical effort, no delivery of intent, no coherent, synchronized collective approach to the objective. This third environmental dimension is not new, but interest in it is fresh, thanks to the emergence of a revolutionary component: cyberspace, or man-made code imposed on electricity that travels at the speed of light.

The author was General William Wallace's Signal Officer when he commanded V Corps during the 2003 invasion of Iraq. Wallace's scoff was almost audible when in response to his query as to what the author's job was, the author answered, "C2." He said, "The hell it is. Your job is to enable it." This sharp distinction between the role of C2, which served as metaphor for the commander's cognitive authority over operations, and the role of an enabling information infrastructure is as profound and old as war itself. True to Wallace's word, the author was never consulted with regard to determining optimal avenues by which to approach V Corps' operational objectives (although the author would have been happy to oblige). The author's job was to surround the commander and his key leaders (above and below) with their network, a tailored type of information infrastructure from which they modeled their situation, and by which they formed teams, assigned them roles and responsibilities within the narrative of plans and orders, under the influence of intent, in order to counter threat and seize opportunity. That's a tall order, for which I was famously unsuccessful.

As with the physical and metaphysical dimensions, the information dimension is a self-constructed weave of enabling technologies (some human, some physical, some electrical, some mechanical, some pure animal), bent to a loose chain of command. I've added Infrastructure to the Information dimension in order to remind readers that this dimension is self constructed, self-directed, self-resourced, and requires the

same exceptional engineering, management, centralized planning, and significant resources that we devote toward enabling our transportation infrastructure. This Information Infrastructure (II) provides the means for leaders to collectively approach their operational goals and objectives. In the most fundamental sense, this information infrastructure gives form to operational thought, and is as personal as a voice in the ear, as intimate as shared understanding, and can carry a kind of spiritual authority when expressed as order or intent. The relationship, then, between the originator of thought, the information infrastructure, and the leader who tailors thought to local application is almost parental, certainly possessive. So entangled are the two that there are those who feel that the cyber and cognitive revolutions are one and the same. This is not the case. To continue to think so is to postpone the cognitive revolution that will make us more secure.

To disentangle the two, we'll ground our network discussion in history. First, we'll define the information infrastructure as the more global capability that serves the universal user, and use the word "network" to describe that portion of the II that is devoted to the needs of a particular leader, who is always at the center of his network. This network is not merely cyber, for how else to incorporate the non-electronic exchange and maturation of information? The network existed well before the birth and evolution of cyberspace. Our historical examples devoted significant personal effort to the design of their networks. Networks relied both on loose confederation of strategic assets (ships, trains, horses, wagons, messenger), and tightly controlled capabilities carved like an Adam's rib from their own formations (aides, dispatches, signals, sounds, meetings, and their own physical gestures). In many cases, the network that conveyed information was the same network that directly engaged a commander's opponents.

The ancient Chinese designed their chief combat formation around the central position and role of the leader, who was also the greatest warrior. That was done so that he could rapidly convey his personal example as a form of instructions to the members of his organization.[45] Wellington, likewise, interwove his experienced units from the Peninsular Campaign with inexperienced Belgian and Dutch formations in order to provoke consistent behavior.[46] Sun Tzu's describes the "drums, gongs, flags, and pennants" that conveyed his personal instructions in the most personal of terms, calling them the means by which "men's eyes and ears" are "unite[d]."[47] The Chinese staff included organizations whose job was to translate plans into feasible orders; another team was required to question

the wisdom of the General's provisional decisions, acting as an Army's strategic conscience.[48] Alexander collapsed his strategic network, bringing knowledge centers with him, augmenting his expeditionary staff with national-level experts so that their spiritual, historical, political, engineering, tactical, and rhetorical advice were within physical reach during the course of his campaigns.[49] Both Napoleon and Wellington were known to have brought with them personal libraries/databases that augmented their own private knowledge.[50]

No one understood the nature of the need for a global network at the center of which stood the battle commander better than Wellington. In fact, he was able to build a global information infrastructure over which he actually managed to enjoy loose configuration control. At the tactical level, Wellington's personal presence was ubiquitous; his exquisitely crafted dispatches to subordinate leaders were exchanged via an infrastructure of aides, and included words that were not meant to be altered by those who delivered them. They were sacred exchanges, and placed in hands that were trusted by commanders. These aides, who too often lost their lives in service to Wellington, were also the future commanders of regiments, brigades, and divisions (his personal aide, the future Lord Raglan, lost an arm at Waterloo, then earned command of the British Expeditionary Army during the ill-fated Crimean Campaign). Wellington was equally adept at what we might call the "operational level" of the information infrastructure, carving time to meet or exchange letters with allies, regional authorities, neutral population, even the deposed French family. His exchange with Blucher was particular decisive, for while it involved little in the way of written dispatch, it included a personal metaphysical connection that provoked a most improbable, almost inexplicable, Don Quixote-like performance and rescue by Blucher. At the strategic level, Wellington composed the Waterloo dispatch, from multiple locations, within hours of the battle's conclusion, conveyed over an infrastructure that included pen, ink, parchment, messenger, horse, ship, train, aide, editor, printing press, delivery boys, political forums, public and governmental authorities. The evidence that Wellington had established at least a loose hegemony over his global network is that, despite all those pieces and parts (as near many as our own!), when Wellington's strategically phrased account of the Waterloo Battle was published in *The Times* of London, it stood as the only published official word of its outcome.[51]

Building and defending a network, then, was part of a battle commander's job description. The network consisted of, for the most part, the personal skills of the individual commander: whether exchanging infor-

mation in person; or via the use of superior equestrian skills to convey orders and intent; or applying rudimentary code to messages interpreted by combatants themselves. The substructures that carried information beyond the engagement area were the same structures that conveyed soldiers and logistics (ships, rails); the dispatches that contained instructions and messages, orders and plans, were hand written, quite often by the senior leader themselves, whose selection of phrases were instrumental in conveying intent.

The historically underrated Albert Myer, the founder of the United States Army's Signal Corps, changed all that (or at least understood that all must change). His vision was that of Wellington's: a global network bent to the needs of the critical leader, regardless of location, level, or circumstance. The sticking point, of course, was that this Information Infrastructure would be under the relative command of the signal corps (and Myer as its leader), but with the promise that it would remain loyal to its local leader, whether it was the President and Secretary of War at their level, the Army Chief, the Army commander, or the engaged Corps Commander, Division, and Brigade Commanders at their levels. Soldiers and officers were detailed from the combat arms to form the bulk of what became a shadow formation, a corps of signalers whose description of Blue, Gray, and Red activity were conveyed by visual code. The codes were beyond the comprehension of the combat commanders, and the formations that transmitted them were independent of the engaged force. It was Myer's intent that the chief signal officer compose the intelligence conveyed (often observed personally) by the shadow network, assemble a model of the situation (Blue, Gray, and Red), along with a map that grounded their observations in a common picture, along with the atmospheric conditions that might influence the leader's decisions with regard to response.[52] The chief information officer must brave the mood of the mission commander, and hand the model of the situation—not his words, mine—to the man in the tent before the evening work was concluded. What he did with that model was a matter left to the metaphysical dimension (and the cognitive revolution).

This "Adam's rib," or signal service plucked from the combat corpus, had its triumphs, but at war's conclusion was considered by the Army's leadership a luxury enjoyed only at the expense of the indisputably indispensable combat formations from which most members of the Signal Corps came. Myer's vision, which included a single, common telegraph system that integrated all levels of war (a vision that was frustrated by Secretary of War Stanton's retention of direct control over the national

telegraph network),[53] was revolution. He recommended that manned signal capability form part of every expeditionary element; that it shadow Red, Gray, and Blue formations, and integrate their information within a common model tailored to the local leader's circumstances. Once in place, it was up to "[t]he Generals of our armies, and the officers commanding fleets" to discover "thousands of applications" for this network that "are not now thought of."[54]

He'd be glad to know that the joint network revolution he provoked is well on its transformational way—150 years later. The Army's contribution to Myer's explicitly joint vision is LandWarNet, but it is the network service center (NSC) construct that makes the vision practical. The NSC is the outgrowth of various white papers written in the wake of the Iraqi invasion, matured by a group of brilliant majors, chief warrants, and senior non-commissioned officers as an Army/Marine concept within the LandWarNet construct, provisionally approved by CG, TRADOC, the Chief of Staff of the Army, and the Secretary of the Army in October, 2006, recently reconfirmed by the current Chief of Staff, and now sits as the number one priority of the CIO/G6.

The NSC provides the same four basic services that Myer asked of his signal "servicemen:" (1) the technical model of the situation; (2) the means to connect tailored teams and control their operations; (3) the ability to simulate human problem-solving, by expanding the network of co-located minds; and (4) the ability to defend his enterprise, at considerable cost to his corps.[55] And, just as Myer envisioned, the NSC delivers the network by folding much of its enabling infrastructure, within a network chain of command (and accompanying TTPs and activities), itself nested within mission commands at every level and location. The network that results is segmented much in the same that a worm survives whether permitted to wiggle whole, or in sections that travel in opposing directions, under the influence of their local leaders. From global to regional centers that gird the earth, to tactical extensions that accompany expeditionary formations, it is a network that is at once universal and centralized, local and deeply personal. And that is because battle command must link every local activity and effect to the global operation and its political end.

There are six operations that permit an information infrastructure to perform as a network. *NetOps* keeps the leader at the center of his elemental combinations, aware of his situation, and capable of continuously reshaping formations to counter threat, seize opportunity, and solve problems. NetOps performs four functions: (1) NetOps builds and defends a

tailored network for leaders at every level and location; (2) NetOps enables leaders to shape their circumstances into the Model of the Situation that conveys peril and opportunity; (3) NetOps enables leaders to form tailored solutions to counter the former and seize the latter; (4) NetOps enables leaders to turn to the collective cognitive brain to solve problems. *ISR* keeps Blue connected to Gray and Red, and feeds the Network's model of the situation. *Intelligence* locates and identifies threat and opportunity (penetrates Gray and Red as required); feeds the network's model of the situation. *CyberOps* is subordinate to multiple superior operations, and never acts outside an operational combination, for the consequences of cyber operations will provoke, potentially, the enemy's own full spectrum response. First. In support of NetOps, CyberOps extends insights with regard to network threat and vulnerabilities as part of Blue network defense. As authorized, and as part of myriad operational combinations, CyberOps attacks Gray or Red threat at the source. Second. As part of ISR and Intel operations, CyberOps exploits access to Gray and Red networks to mature the Model of the Situation. Third. In combination with myriad operational activities, CyberOps helps to deceive, discourage, persuade, degrade, or destroy Gray and Red cyber and cognitive capability. *StaffOps* debates, measures, quantifies, publicizes, and translates private understanding and provisional decisionmaking into collective plans, orders, and broadly apprehended intent. *Knowledge* operations gather from historical, scientific, cultural, social, political, and spiritual sources the cognitive context for all decisions, projecting their consequences into the near, long, and multigenerational futures. Knowledge operations require significant skills in the fields of modeling and simulation. For optimal effect, all network-related operations are fully integrated within mission and operations centers (see abstract).

The Army's chief battle and battle command transformation programs, Future Combat Systems (FCS) and LandWarNet, integrate the Wellington approach and the Myer vision. In combination both programs return the network to the engaged combatants, and permit them to play roles at every level of war and during each operational phase, regardless of echelon, location, and time. In the manner of Myer, LandWarNet (and its family of like-minded information infrastructures) is an electronic echo of the physical formations of Blue, Gray, and Red. LandWarNet-enabled, FCS-equipped formations engage at a level of collaboration that treats all the objects across the physical dimension as subject to their authority, warning Blue of physical peril, or pivoting to exploit opportunity. This kind of networked force has reinvigorated our combat formations, sustain-

ing their viability as physical presence. There can be no question with regard to the necessity of this essential act of transformation: we must never cede physical strength to an enemy, for it means ceding our ability to get close enough to engage Gray and Red metaphysically.

But so far, the purpose for our cyber-enabled transformation is not to revolutionize operations, but to restore viability to traditional capability. We have transformed our powerful capabilities into cognitively agile capabilities, because the enemy is either less awed by our physical advantage, or because they are less vulnerable to our physical force—most likely because our opponents' objectives are psychological, and notoriously resistant to physical force. But has our physical advantage made us more secure? Does this extraordinary physical capability inform a cognitive activity whose consequences are always national and global; whose failures risk national prestige, exhaust the source of elemental power, and prevent the application of resources to resolve situations not yet underway? Without a cognitive revolution that provides it an operational and organizational context, will a LandWarNet-enabled, FCS-equipped Brigade Combat Team change the conditions that established OIF's peculiar character in the first place? Will it discover along with the facts and figures of its physical dimension, those mental objects that swim by undetected, shapes on their way toward making dangerous alliances? Can a LandWarNet-enabled, FCS-equipped BCT form elemental and operational combinations from across all sources of power at the *origins* of operational activity, within metaphorical moments of their engagement? Do our institutional doctrines—across the departments, agencies, and services—demand that leaders articulate the cognitive end states of their human targets before they apply their full spectrum solutions?

I'll use some short examples of the difference between network-enabled, FCS-equipped transformation and the need for cognitive revolution. When network-enabled, FCS-equipped combat teams squeeze triggers, those acts initiate an ammunition resupply; those acts do not demand a corresponding account for the fate of each individual round. We have always excused the soldier from such unconscionable accountability. A cognitive revolution, on the other hand, enables the staging of funds in the figurative hands of the triggerman within minutes following the liberation of Gray (or Grays). Cyber can't solve our inability to perform this mission. It is Blue's self-imposed cognitive constraint that currently demands an accounting for every dollar spent under the most god-awful circumstances, and fails to permit soldiers to extend such services to those whom they've physically dominated. Despite the evidence that we usually,

if not always, win physical "battles" and we usually, if not always, struggle with stability and transition operations, we still spend the preponderance of our training, doctrine, and organizational structure on reinforcing our physical success. My military education and training has focused on battles. And the story of battle, as I've argued, is always in the service of a superior operation.

We must do three things simultaneously. First, we must continue with cyber transformation, and complete the institutionalization of that technical revolution. Second, we must direct our technical efforts to establishing the conditions for the emergence of the cognitive revolution. Third, we must amplify by orders of magnitude the voice of this cognitive emergence that is stirring among engaged formations. This revolution has been only marginally reinforced by the application of our arts, sciences, technologies, and their associated laboratories. And, as a reminder of the scope of the unified field theory, those resources must be applied to the transformation of operational and strategic leaders, organizations, and doctrine in order to prevent the launching of a war whose early character resists the influence of a future tactical presence, regardless of how superior its cognitive advantages are.

Our failure to distinguish between the cyber and cognitive revolutions has left the cyber revolution stalled at the entry to the brain of the man in the tent. I believe that the conditions for victory have not historically changed: powerful nations will always need "normal force" that permits them to compete with their international (or inter-group) peers over space within a finite universe. Nations and groups who seek long-term preservation, though, seek "extraordinary force" to secure their prospects. It is increasingly clear that "extraordinary" force requires mastery of the metaphysical dimension, into which science and art and their technologies have begun to direct their considerable light as means to enhance man's natural insights. When the man in the tent or the leader on horseback demand a *cognitive* model of the situation, shaped to inform all organs of the human brain; when leaders demand a picture that captures the shapes of both mental and physical objects—past, current, and future; when leaders demand elemental combinations that modify more precisely the shape of mental objects; and when leaders demand operational combinations that respond to cognitive opportunities as rapidly as their proxies respond to physical danger, then the cognitive revolution will take off. When that happens, we'll appreciate LandWarNet-enabled, FCS-equipped formation for the extraordinary achievement it is, but one that serves as preface to one that is greater still.

Conclusion

Our doctrinal bias for physical operations is not shared by our current enemy, whose decisive operation is psychological, for which his physical activity is in support. A growing voice across those forces held accountable for land-based outcomes have arrived at similar conclusion: that their root operation is cognitive. Our brigade, regimental, and special operations combat teams are among history's finest examples of formations organized around the production of cognitive effects in pursuit of mental accommodations among and across constituencies.[56] They would agree that failure to gain early mastery of the cognitive domain and its essential activities unnecessarily initiates, extends, modifies, and resolves operations at an elevated cost in human life, and multi-generational diminution of international influence and national power. No other activity has that kind of catastrophic potential for mischief. Yet, we remain without a viable vocabulary with which to even approach the subject, certainly nothing sufficient to excite the kind of attention that, say, the tank did in the 1930s; or, for that matter, all things Cyber today.

The consequences of this failure are large. While we are understandably concerned about the implications of a cyber domain that captures the interest of Congress and potentially an ill-advised service sponsor, the land forces are justifiably in need of a strategic message that demands a revolution in the way we conceive operations. That won't happen unless we are willing to risk the prestige of our core competency, and lend the name battle command to our effort. It has been the central thesis of this paper that battle command must emerge as the evidence of a cognitive revolution, complete with a taxonomy of its own, if we are to enjoy the potential applications of our cyber revolution. As long as battle command remains primarily focused on closing with and destroying the enemy, cyber will continue on the path it has taken: transforming the way our grand formations network their physical effects.

Battle commanders will eventually revolt. Our formations in Iraq are examples of the future, but they dissolve upon return, and the forcing function for their reconstitution is precisely what we wish our cognitive revolution to obviate. The evidence of revolution will be in the composition of force structure, whether we continue to treat cognitive operations by adding staff officers, or whether we approach the kind of resource investment similar to that required to incorporate the capability of the tank. I also believe that even the mere acknowledgment that battle command

is our core cognitive operation will redirect some of cyber's attention, for wherever battle command goes, so goes its loyal greyhound, the network.

The goal of revolution is to make common that which was once rare. That's the promise of battle command once it assumes its role as the superior cognitive operation at the core of the operational environment: to make the wisdom, judgment, acumen, imagination, instincts, and mental courage that mark the professional lives of Sun Tzu and Wellington and Col McFarland (among many others) common across all levels of war. That kind of revolutionary transformation bodes well for the security of our nation.

Notes

[1] Timothy L. Thomas, *Dragon Bytes: Chinese Information-War Theory and Practice* (Foreign Military Studies Office, Fort Leavenworth, Kansas, 2004), 44.

[2] General Charles C. Campbell, USA, FORSCOM Commander, from his remarks with regard to the promise of LandWarNet at the LandWarNet Conference, August 2007, Fort Lauderdale, Florida.

[3] Bob Dylan, *Modern Times* (New York: Sony Music Entertainment, 2006).

[4] Martin Van Creveld, *The Art of War* (New York: Harper Collins Publisher, 2005), 37.

[5] United States. *Department of Army, Field Manual 3-0: Operations* (Washington, DC, 2001) 7-3, table 7-1.

[6] See, for example, The U.S. Army Concept for the Human Dimension in Full Spectrum Operations 2015–2024 (TRADOC, June 11, 2008), available at http://www.tradoc.army.mil/tpubs/pams/p525-3-7.pdf.

[7] Thucydides, *The History of the Peloponnesian War*, Trans. Richard Crawley. Project Gutenberg, December 2004. 14 June 2008. http.//Gutenberg.org/etext/7142.

[8] Sun Tzu, *The Art of War,* Trans. Samuel B. Griffith (New York: Oxford University Press, 1971), 84.

[9] 17 September 2006 Joint Publication 3-0 (all comparisons between the two models are based on this publication).

[10] Van Creveld, 29.

[11] COL Jeffrey G. Smith, Jr., V Corps White Paper, Battle Command Concept Derived from the Experiences of Operation Iraqi Freedom (Sep 2003), 9–10.

[12] United States. Department of the Army, Field Manual 100-5, Operations (Headquarters Department of the Army, 20 August 1982).

[13] United States. Joint Staff, Joint Vision 2020 (Washington, DC, 2006), 8–26.

[14] Tzu, III.3.

[15] John Keegan. *The Mask of Command* (New York: Penguin Books, 1987), 8.

[16] Tzu, I.4.

[17] Keegan, 103.

[18] Keegan, 92.

[19] Elizabeth Longford. *Wellington: The Years of the Sword* (New York: Konecky & Konecky, 1969), 424.

[20] Jeffrey G. Smith, Jr. The Literature of Disillusionment: Public War Correspondence from Waterloo to Khe Sanh (Dissertation, Princeton University, 1992), 87.

[21] Debate over whether Wellington sufficiently recognized Prussia's contribution to victory at Waterloo continues today.

[22] Jim Michaels. "An Army colonel's gamble pays off in Iraq," USA Today, April 30, 2007.

[23] Tzu, V.9.

[24] Carl Von Clausewitz, *On War*. Trans. and Ed. Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1989), 17.

[25] Tzu, V.3.

[26] Van Creveld, 35.

[27] Tzu, V.3.

[28] Tzu, VI.28.

[29] An approach institutionalized by the Army's recent change to TOE, authorizing such teams at Divisional and Corps HQs.

[30] Smith, Literature, 81–94.

[31] Smith, Literature, 61–62.

[32] Keegan, 44.

[33] Keegan, 134.

[34] LTG(R) Jeffrey G. Smith. One-on-one meeting. Eyewitness account of the surrender of Japanese forces in China at the conclusion of World War II.

[35] Joseph E. Persico. "World War I: Wasted Lives on Armistice Day." *Military History Quarterly* (Winter 2005). http://www.historynet.com.

[36] Jay Winik, *April 1865* (New York: Harper Perennial, 2001), 301–363. This final section describes the last few battles between Lee and Grant, their negotiations with regard for the terms of Lee's surrender, and the actual ceremony of surrender.

[37] Clausewitz, 7.

[38] Van Creveld, 37 .

[39] Sun Tzu, III.31.

[40] FM 3.0, 7–1.

[41] Tzu, VII.31.

[42] Tzu, IV.16–19.

[43] Tzu, XII.18.

[44] Tzu, XII.19.

[45] Van Creveld, 32.

[46] Keegan, 127.

[47] Tzu, http://www.sonshi.com/sun1.html. 1999–2004. Sun Tzu: The Principals of Warfare "The Art of War, VII.19.

[48] Van Creveld, 32.

[49] Keegan, 40.

[50] Keegan, 136.

[51] Longford, 485.

[52] Albert Myer, *A Manual of Signals: For The Use Of Signal Officers In The Field* (Washington, DC, 1864), Part VIII.

[53] Rebecca R. Raines, *Getting the Message Through* (Washington, DC: Center of Military History, 1996), 21.

[54] Myer, Part VIII.

[55] Raines, 29.

[56] Barry R. McCaffrey. "Visit Iraq and Kuwait 5–11 December 2007" (USMA: Department of Social Sciences), 7.

Chapter 3

Navy Operations to Achieve Military Power in Cyberspace: A Draft Concept for Navy Computer Network Operations

Michael A. Brown

The essential elements of national power have been characterized as diplomatic, information, military and economic in order to relate them to the primary means by which nations, groups, and people orient and order themselves in the real world. Governments have devoted substantial research and analysis to understanding if and how national power can be characterized in the ill-defined, complex, physical/virtual world of cyberspace. The United States Government and the Department of Defense have sought such understanding, and the National Military Strategy for Cyberspace Operations (NMS-CO) received the Secretary's approval in December 2006 as the basis for more substantive, operational work. Within DOD, the Services have been framing references and building concepts under which they can organize, train, and equip the forces to deliver military power in cyberspace. In the United States Navy, the doctrinal constructs of information operations (IO) and Computer Network Operations (CNO) have become the framework for empowering Sailors to achieve our nation's military objectives in cyberspace. The Navy has prepared a draft concept for CNO as an ordered, sustainable maritime means of realizing military power in cyberspace. That draft concept forms the remainder of this paper for the National Defense University.

The Navy has four years of success in organizing, training, and equipping forces for CNO. The ubiquitous expansion of globally distributed information networks now challenges us to accelerate the develop-

ment, deployment, and employment of full-spectrum CNO forces to fulfill Naval, Joint, and Commanders' requirements, as well as national requirements, for information dominance in all phases of conflict. The Navy's CNO forces work at the cutting edge of exploitation, attack, and defense of global information networks. With these forces, operating under a Maritime Headquarters/Maritime Operations Center (MHQ/MOC) or Joint Task Force (JTF), we will detect and defeat network threats; defend against them; find and attack adversaries throughout the information environment; and help shape and influence with traditional Naval forces. Navy CNO will be access-driven based on persistent 24x7x365 presence in the network and robust capabilities for exploitation, defense and attack.

Why Navy CNO Matters

The nature of military operations has radically changed since 1990. In a world of distributed information networks, built on proliferating information technologies, individuals, businesses, non-state entities, and governments now process and disseminate terabytes of information across the globe instantaneously. Traditional boundaries between military and civilian infrastructures are blurred. Point-to-point radio frequency (RF), terrestrial and satellite communications, RADAR, sensors, and control devices are networked together into a sophisticated global network of information providers and information users.

Never before has mankind enjoyed so much rapid access to data and knowledge via a single medium. This information explosion presents enormous challenges to operating forces charged with defending national interests and advancing U.S. policy. Conversely, because adversaries operate (or strive to operate) in the same environment, U.S. forces possess unprecedented opportunities to shape and control the battlespace to achieve national objectives. Thus, CNO is a core Naval mission.

Most U.S. kinetic weapons are fully integrated into networks and are accounted for in network-centric operations (NCO). Those that are not are scheduled for replacement or upgrades to enable such employment. The Tactical Tomahawk (TACTOM) AN/BGM-109E exemplifies an NCO-enabled weapon that receives pre-flight targeting data from national, operational, and tactical command centers and real-time in-flight updates from multiple sensors (aircraft, unmanned platforms, satellite, and personnel in the field, tanks, and ships). Equipped with onboard sensors, the TACTOM is also capable of sending sensor data and status information back to feed common operating pictures. If an adversary became

able to block or manipulate targeting, guidance, or command and control data to turn the TACTOM against U.S. forces or civilian populations, the enormous advantages of employing such NCO-enabled kinetic weapons in an information-dependent environment could become a severe liability. The need for information superiority to prepare, employ, and protect an NCO-enabled kinetic/non-kinetic campaign is real and immediate. As our potential adversaries apply the same technology and network-centric strategy to their command and control and weapons systems, information superiority provides real asymmetric advantages.

Successful IO is a vital foundation for joint and naval warfare when they contribute directly to information superiority to reduce risk in other lines of operation. CNO is one of five functional areas of IO and is a powerful contributor to information superiority. It is also a key element of modern warfare. The Navy has more than four years experience in planning and executing CNO during joint operations. From actions that contribute to finding, fixing, and capturing high-value targets, to those that help shape the battlespace during all phases of conflict, the Navy must remain well-prepared to lead DOD in establishing and maintaining information dominance.

Multiple elements are critical to the success of CNO, including: initial target intelligence, access, target development, weapon or tool development/certification, cyber counter intelligence, rules of engagement, and reporting processes. Historically, the most challenging element has been gaining access to target networks. The Navy aligns CNO forces in an access-based model, postured to engage threats at all levels of operation in any phase of conflict. Access is achievable through multiple means: the RF spectrum proximity, IP-based networks, and physical connections. When access and knowledge of an operational target are matched with certified weapons and operators, the commander may be confident that this precise targeting will achieve the desired effects. In addition to enabling offensive action, access increases our ability to recognize and identify adversary capabilities and methodologies and to counter attempts to limit or counteract U.S. presence in the information environment.

Computer Network Operations Processes

Well-planned, access-based CNO provides critical U.S. advantage across global networks. CNO actions are computer network exploitation (CNE) for permanent and scalable presence in global networks that provides the foundation for successful CNO; computer network defense (CND) for detecting and defeating threats; and computer network attack

(CNA) for denying adversaries any advantage in the network environment. CNO provides national decisionmakers and tactical commanders the information and freedom of action necessary to maintain strategic, operational, and tactical advantage in the information environment.

The Navy organizational construct enables synchronization of CNO activities, and requires Navy CNO forces to satisfy tactical, operational, and strategic objectives from sensor to weapon to effects assessment. MHQ/MOC will identify CNO requirements based on Combatant Commander tasks and plans and execute them in synchronization with national and joint warfare commanders.

Dependable CNO requires interactive, long-term contact with adversaries and full-time presence in the global network environment across physical domains. Creating and maintaining these accesses enable threat profiling, target development, adaptive weapon development (to react to changes in the target), and, when necessary, offensive operations. Forward-deployed naval forces provide unique target access. However, long-term deployed operations to maintain and expand these accesses may not be practical or sustainable. It is essential that tactical CNO capabilities (in aircraft, ships, submarines, expeditionary, and unmanned forces) be ready to enable, via CNO reach-back, fully-staffed Navy shore commands (such as our Navy Information Operations Commands NIOCs) to take over exploitation and execute CNO via access points achieved through tactical presence and action. This requirement reinforces the need for cross-platform, network-enabled CNO capabilities employed by the widest possible range of Navy forces and linked back to shore facilities.

Conversely, shore-based commands must also be able to push access forward to an operational or tactical unit that is equipped to expand such access for theater and national operations. This reciprocal access development capacity is critical for the synchronization of CNO with theater operational plans and bringing CNO in phase with the Combatant Commander's battle rhythm.

Given pervasive threats in the information environment, and our military's increasing dependence on networked operations, defense must often be the first consideration. Informed and warned by energetic CNE, Navy CND operators will actively defend U.S. networks against a wide array of threats by fusing all-source intelligence, network attack analysis. and known threat profiles to identify threat indicators and develop defense strategies to counter adversary attempts to degrade Naval operations. CND operators will apply the full range of CNO analytic methodologies in providing defense in depth.

CND operators analyze network anomalies through counter-intelligence operations, open-source information, and Red and Blue team vulnerability assessments (VA). Assessments orient results to intelligence products, including those from CNE, to identify threat patterns of operation, capabilities, intentions, and true points of origin. If these operators detect a compromise, they will employ in-depth diagnostics to identify "electronic fingerprints" and profile the threat and scope. Although passive collection at network management centers can determine some identifying information, cuing and engagement of CNO forces for precise and direct exploitation of adversary network activity will push U.S. network defense beyond the firewall. Such network activities may include CNA to enable CNE and CND, active defense techniques that require deconfliction with other activities and physical interdiction of adversary network operations. By synchronizing Navy CNE, CNA and CND capabilities, we will shift from a react/report/repair response to an active prove/predict/prepare defense. Success is possible only if CNE, CNA and CND are planned and executed as an integrated effort in a command and control structure that compliments National and Joint operations centers.

To achieve synchronization, the Navy will leverage the global access provided by our NIOCs, Naval Cyber Defense Operations Command (NCDOC), and forward forces to recognize and monitor adversaries, create new access points, profile threats. and plan and execute IO from the maritime domain. The Navy will coordinate with national and joint partners to operationalize network access for the execution of national, joint and naval CNO courses of action (COA). In this expanded, scalable, access-based environment, CNO is more demanding and dependent upon specialized forces, tailored access, and integrated command and control.

The sum of CNO processes is the end-to-end cycle of capability development, employment, and assessment. Each step in the cycle is described below.

Capability Development

Navy CNO research, development, test and evaluation (RDT&E) is centralized to respond to operational and tactical commanders' defensive and offensive requirements. The Navy will leverage internal and external partnerships to build widely applicable solutions. By centralizing RDT&E efforts, the Navy minimizes duplication of effort and applies a holistic perspective of technology across global regions (in response to commercial technology proliferation, among other trans-regional concerns). Vulnerability analysis on both technology and target network topologies

provides the foundation to build hardware and software (HW/SW) solutions to satisfy commanders' operational objectives. Although the core of capabilities development will be centralized, weaponization will occur at NIOCs as necessary to achieve specific operational objectives.

Capability Tailoring

NIOCs will have the lead, and NCDOC will provide iterative data regarding Navy network processes and technical configurations for fratricide review. Sailors will take the HW/SW solutions provided by the RDT&E effort and weaponize them for use within appropriate target domains. This weaponization process includes tailoring the HW/SW to the target network(s) and verifying that it is conformed to and interoperable with access method(s). The verification process validates that the capability is effective against the target network. The certification process ensures that the operator and the weapon can deliver the desired effect to support COA objectives.

Operations

The specific aspects of CNO will require specialized operations, but the dependence on global persistent access remains the same. Specific considerations follow:

CNE

Intelligence preparation of the environment (IPE) and access development are ongoing operations. We will invest people and resources against high-profile targets that provide the best opportunities for national, joint and maritime operations. CNE operations will be critical throughout the operational cycle to develop target expertise, measure effectiveness of operations, and conduct battle damage assessment (BDA). CNE sailors will be trained to conduct both CNA and active defense as operationally appropriate.

CNA

The Navy will task organize to meet the requirements of national, joint and maritime Commanders. For instance, Navy cyber attack teams (NCAT) are flexible and scaled to fulfill mission objectives and skill requirements. NCATs will be either virtually or physically aligned with the Maritime Component Commander to provide planning, capabilities expertise, access, and attack operations. The NCAT will create access and/or leverage access points already developed through CNE. The ultimate goal of the NCAT is to deliver capabilities via access points to achieve opera-

tional effects including: denial, degradation, disruption, and/or destruction of network/critical nodes; manipulation of information or information paths; injection or projection of information; and tracking and tracing of adversary operations. However, we must not simply rely on NCATs as the organizing principle, but look to regularize and operationalize wherever we have capability and capacity.

CND

The Navy must be able to detect, usurp, and counter all on-network threats. The fusion of network analysis, a clear understanding of adversary activity, and detailed forensics are required before covert activity against the U.S can be detected and countered. Threats to U.S. information systems are dynamic and rapidly evolving. Agile and flexible intelligence becomes critical for early warning and enables sailors to counter threats in advance. NCDOC is the Navy's primary command responsible for CND, but to evolve from reactive to predictive defense, the Navy must synchronize CNE and CND operations to characterize the threat while leveraging all-source intelligence for cues to adversary intent. Through the combined efforts of CND, CNE and CNA operations, the Navy will implement an active defense strategy that can counter both initial activity and retaliatory moves and continually improve the network defensive architecture.

Analysis

Although understanding the technical aspects of an adversary's networks and their capabilities are two primary objectives, understanding the human, cultural, and procedural factors that govern the adversary's command and control (C2) are equally important. Initial analysis, target development (TD) and post-operations analysis are interlinked. They must share the same regional and technical analysts. TD sailors will possess in-depth target knowledge critical for developing concepts to deliver IO effects through Navy CNO. This team will fuse information derived from open-source information and all-source intelligence to visualize adversary networks and determine their capability to impact U.S. military operations.

Planning

IO planners are directly responsible for achieving Commanders' effects by integrating network-targeting priorities into mission task orders (e.g., air tasking order, integrated tasking order), while simultaneously addressing counter-targeting strategies to defend network-centric weapons, C2 and intelligence, surveillance, and reconnaissance (ISR). Navy IO planners incorporate CNO courses of action into adaptive planning processes

(e.g., OPLANs and CONPLANs) and theater guidance, while providing specialized support to operational commanders whenever crisis planning is initiated. Planners synchronize CNO initiatives with air, land, sea, and special operations to attain naval, joint, national, and multi-national objectives. When an NCAT is activated, CNO planners provide expertise in the strike planning cell to ensure CNO plans are fully coordinated with all warfare commanders. Operational planners will leverage partnerships to enhance target development, indications and warning (I&W) and BDA.

Navy CNO Alignment

Navy CNO personnel will be integrated at all levels of command to provide unique expertise to the mission accomplishment of the assigned command. Whether they are at OPNAV conducting programming and developing policy and strategy or planning with national and joint warfighters, Navy CNO forces will be trained and ready to advise on the full range of IO options.

Strategic Support

National partners will have organic Navy assets assigned, augmented by the NIOC aligned to them. This partnership will allow for a mutually beneficial relationship to enhance naval CNO capabilities, while providing a ready force for the broad scope of tasks assigned to the national agencies. Through strategic partnerships, the Navy will leverage dual-use, national-tactical access points and capabilities to meet requirements. This strategy maximizes resources to engage in an ongoing, synchronized campaign for conducting CNO end-to-end.

Operational Support

Through the fleet information operations centers (FIOCs), Naval Network Warfare Command (NNWC) will deliver direct support (DIRSUP) CNO personnel to operational commanders tasked with CNO planning and execution. Navy CNO capabilities will be task-organized and scoped for the assigned mission. It may be a single CNO professional DIRSUP to a ship, airplane or submarine. It may be a full NCAT vulnerability assessment (VA) team, or regional target planning and capabilities experts.

MHQ/MOCs will also receive augmentation for planning and execution of IO, including CNO. NNWC will be responsible for building and managing Naval networks and CND through the NCDOC, which has special responsibility to the Navy for protecting naval networks and representing the health of those networks to joint commanders.

Tactical Support

Tactical assets will enable access to high-profile targets to meet Navy and national priorities. Similarly, Navy assets will weaponize national access points to meet JFMCC operational goals. CNO will be conducted where it makes the most sense operationally to maintain persistent access, maximize effect to target, and prevent disruption of U.S. sensor-to-shooter-to-sensor paths. CNO forces will also be embedded in tactical units, such as Naval Expeditionary Combat Command (NECC) and NSW teams, provided through a mix of organic assets and DIRSUP augmentation from the FIOCs. This investment will be a critical contribution to NSW's find, fix, and capture/kill strategy.

Implementation Actions

While a full implementation plan is not the focus of this vision paper, it is important to recognize the major actions that must be taken to realize this vision.

Policy and Doctrine: Implement CNO Policy and Doctrine to Enable CNO Alignment

OPNAV N3IO, NNWC and Naval Warfare Development Center (NWDC) will develop policy and direct doctrine development, to include tactics, techniques, and procedures (TTP) that integrate, synchronize, and deconflict CND, CNE, and CNA. This policy and doctrine must enable precise, repeatable CNO in an ever-changing information environment through rapid fielding of advanced capabilities. Policy and doctrine will also enhance training and mission effectiveness and improve resource allocation efficiency. Policy and doctrine enable effective command and control, mission synchronization, sailor training, and target development.

Operations: Execute Effective Computer Network Operations

Command and control (C2)

The NIOC structure enables Navy CNO forces to transition seamlessly between Navy joint and national missions. Maritime commanders can leverage co-located national and Navy CNO forces at NIOCs to achieve Navy objectives while also fulfilling national requirements. Benefits of this force partnership are:

- increased CNO access opportunities,
- shared national and tactical CNO target development,
- improved Battle Damage Assessment,

- shared CNA/CND/CNE physical infrastructures, tools, and techniques,
- improved CNA/CND/CNE planning and operations deconfliction,
- improved training and certification of personnel.

OPNAV N3IO and NNWC will collaborate to develop a C2 architecture to ensure that CNO forces have the authority to conduct time-sensitive operations and deconflict those operations with national and joint missions focused at the NIOCs. NNWC will pursue clear alignment of CNO authorities and clear rules of engagement that enable mutual satisfaction of Navy, joint, and national objectives.

Alignment of C2 must enable NIOCs to conduct CNO in support of Navy, joint and national objectives as forces TACON to their associated JFMCC; as a force provider conducting CNE or target development under national authorities; or as the execution element for USSTRATCOM Joint Force Maritime Component Commander JFMCC (that is, NNWC) CNO tasking.

Planning

United States Fleet Forces Command (USFFC) and NNWC will train Navy IO planners in CNO capabilities and TTP so they can coordinate Navy CNO efforts as an integral part of the adaptive operational planning cycle.

Networks

NNWC will plan, deliver, and operate networks with security as a primary design factor. NNWC will coordinate with RDT&E centers to use the latest technology to develop automated mapping tools. They will have the availability, confidentiality, and integrity suitable for a weapons system.

Access

NNWC will develop persistent logical or physical access to targeted networks.

Network Awareness

NNWC will train IO forces to conduct network mapping and target development as part of CNO. These operations will facilitate understanding of potential adversarial networks, lay the groundwork for future missions, and provide sailors with opportunities to build their technical skills and cultural awareness. NNWC should coordinate with ONI to identify all-source intelligence products that refine and complement these on-network efforts.

Tool and Weapons Building

NNWC will build the process to efficiently move tools from the RDT&E centers to the NIOCs for weaponization and use. This process will ensure partnering with national agencies through the NIOC structure to leverage unique capabilities to meet Navy, Joint and national objectives. It is imperative that CNO Sailors be collocated with national forces at the NIOCs to speed weaponization and use based on tailored access and deep technical and cultural understanding of targets.

People: Deliver Cyber Forces with the Right Skills and Target Knowledge to Execute CNO Mission Objectives

CNO Workforce

USFFC and NNWC will ensure that Sailors remain the premier CNO force in DOD. information warfare (IW) officers (1610/6440/7440) and cryptologic technicians (CT) must have the skills to analyze threats, write and evaluate requirements, gain access, develop targets, design weapons, plan strikes/counter strikes, and execute courses of action (COA). IW Officers and CTs must also understand how to employ CNO capabilities through RF and physical access.

Information warfare officers must be trained in both planning and execution and have the technical expertise necessary for access, target, and weapon development. They also must be able to lead sailors with in-depth target expertise to develop CNO COAs.

Cryptologic technicians (networks) (CTNs) must be the Navy's CNO professionals and be able to work closely with information technicians at network management centers. CTNs' specialized skills must be applicable to CNA, CNE, and CND. NNWC will move quickly to provide these specialized, highly technical sailors with an innovative and rewarding career path.

Cryptologic technicians (collection) (CTRs) and cryptologic technicians (technical) (CTTs) are critical members of the target development team who will analyze how CNO can affect the performance of adversary C2 networks. NNWC will train these sailors in CNO fundamentals so that they can best apply their technical abilities to enable integrated IO.

Cryptologic technicians (interpretive) (CTI) are critical for content analysis required before, during, and after CNO. NNWC must train these sailors in CNO fundamentals so they can best apply their language skills, regional expertise, and cultural awareness to enable integrated IO.

Training, Education, and Certification

NNWC and Center for Information Dominance (CID) will enable education, training, and certification across all aspects of CNO, emphasizing the cooperative and integrated nature of CND, CNE, and CNA. Training will ensure that operational experiences reinforce technical skills against specific target sets throughout each sailor's career. Training and certification should include cultural awareness, employment of technology, best practices, and adversary TTPs and mindsets.

OPNAV N3IO will lead work with the Office of the Secretary of Defense (OSD), the other Services, and strategic partners to centralize CNO standard development and decentralize certification authorities. NNWC will work with other operational commanders to enable distributed training and certification at CNO-capable NIOCs, using all appropriate service, joint, and national education and training.

Technology: Develop Capabilities to Plan and Execute CNO Courses of Action

Navy RDT&E organizations will continue to aggressively exploit current and future technologies and techniques to develop innovative capabilities and accesses to provide full-spectrum CNO effects at the lowest possible classification. This is accomplished through a centralized effort that leverages strategic partnerships, acquisition authorities, and organic development efforts to reduce duplication of effort and provide a variety of effects-based capabilities across targets and technologies.

To maximize the return on investment for personnel and resources, the Navy's CNO capability and access development occurs on three parallel axes:

- Leverage existing and future partnerships to apply National, Joint, and Service developed capabilities and accesses to address warfighter requirements in the Navy mission areas;
- Contract with industry experts to develop new capabilities and accesses to meet National, Joint, and Navy requirements;
- Indigenously develop CNO capabilities and access methods to meet maritime requirements.

NNWC will fill key development and influence billets in national agencies and joint organizations and will partner with other services to share capabilities at the earliest stage of development. NNWC will leverage streamlined acquisition authorities and rapid prototyping to develop new and innovative network capabilities and access methods.

Summary

As the Navy operates in a network-centric environment, we must rapidly organize, train and equip for CNO. The global landscape is filled with rapidly evolving networks. Navy CNO must evolve as fast or faster. The Navy must capitalize on its experience and talents and prepare sailors and capabilities for daily, sustained CNO.

Navy CNO sailors will be a new class of warrior, fully equipped with CNO weapons to serve alongside those who conduct surface, air, subsurface, and expeditionary warfare, from a vantage unique in the maritime domain and with combat skills commensurate with the risks they will overcome.

Through CNO the Navy will detect, defend against, and defeat adversaries in the information environment. As technology advances, this vision must evolve. As we implement this vision and capitalize on our past successes, we will depend upon our information warfare component to lead full-spectrum CNO, fully aligned with naval, joint, and national priorities, requirements, policy and doctrine to achieve information dominance.

Chapter 4

The Air Force in Cyberspace: Five Myths of Cyberspace Superiority

Forrest B. Hare and Glenn Zimmerman

In 2005, the Secretary of the Air Force revised the U.S. Air Force mission statement to recognize that cyberspace is a key domain for the warfighter today, along with air and space.[1] The mission statement now reflects Air Force recognition of cross-domain interdependence and emphasizes a commitment to deliver dominant options for the United States not only through air and space, but also through the domain created from the electro-magnetic environment: cyberspace.

To help frame the Air Force way ahead in this domain, the Secretary and Chief of Staff of the Air Force established a Cyberspace Task Force. The next step is to communicate that the way to achieve cyberspace superiority is by holding our adversaries at risk in the domain, ensuring freedom of action for friendly forces, and exploiting the resulting advantage to its fullest potential for cross-domain dominance.

It is helpful, first, to identify what cyberpower and superiority are not. therefore, this chapter describes five common myths encountered by the Cyberspace Task Force. Some myths arise from a simple lack of understanding of our capabilities and vision; some represent rationalizations to justify misallocation of scarce resources; and some are red herrings presented to promote agendas and protect resources. In all cases, myths hinder efforts to build a robust warfighting capability in the cyberspace domain. The chapter then explains why achieving cyberspace superiority is a prerequisite to cross-domain dominance.

Five Myths: What Cyberspace Superiority Is *Not*

The Cyberspace Task Force has encountered five myths repeatedly. This section explains why each of these myths is false.

Myth No. 1: "Dual-Hatting"

Myth No. 1 is that, because the technical skills are the same, it is advantageous to "dual-hat" the intelligence collector or information service provider as the lead cyber warrior. This myth is false for two reasons. First, dual-hatting is not effective when the tasks may compete for priority and advocacy. In the case of dual-hatting the intelligence collector, the competition is the traditional one of intelligence gain/loss. In all operational scenarios, the final authority on intelligence gain/loss is the operational commander, who alone must accept the potential risks. However, if the authority also has the role of intelligence collector, the tendency will be to avoid any operations jeopardizing collection activities. This conflict will be exacerbated in a large organization. Even if the leader accepts the dual-hatted responsibility, the staff, which is devoted to collection, will tend to impede all other effects-producing operations.

There is also inherent conflict between the role of cyber-warrior and that of information service provider. Service provision implies the imperative to counter threats to the network. Since the responsibility for protecting the network normally lies with the information service provider, the latter will most often emphasize ensuring service availability, while downplaying threats, due to a lack of tangible impacts. This imbalance is reinforced when the operational commander lacks an understanding of the potential operational impact of threats, but pressures the information service provider to ensure information availability at all costs. Though the threats and their operational impact on mission accomplishment may be difficult to quantify, the service provision decision should still be subject to an "information service gain/loss" evaluation. There may actually be times when incomplete or suspect information is preferable to no information, but the final "service gain/loss" decision must be made by the operational commander, who is ultimately responsible for the success of the operation. He or she must understand the trade-offs, and must accept the risks.

Second, possession of technical skills is an important foundation, but not automatically equivalent to possession of warfighting skills. Just as we would not send an aeronautical engineer straight from the lab bench to lead a four-ship of bomber aircraft over Baghdad, we should not expect the computer-science engineer to be prepared for the cyber fight, just because he or she understands networks. The abilities required to be a warfighter are not the same as the engineering skills obtained in school or the lab. Computer network exploitation experts may be excellent analysts and engineers who understand ways to defeat the adversary, but they must

also grasp issues such as integration with other operations, translating effects to tasks, collateral damage estimation, weaponization, standardization, combat assessment, and laws of armed conflict. Cyber attack is not a mouse click away from computer network exploitation, and characterizing it as such is dangerous and reduces the commander's confidence it will be done right. It requires specific training for the actual task.

Myth No. 2: "Nature of the Domain"

Myth No. 2 is that the domain is a "virtual" one characterized by the Internet. This might be a convenient label for teenagers, but it has proven costly to the Department of Defense. General Ronald Keys, USAF, commander of the Air Combat Command (COMACC), discussed issues arising in operations in Iraq and Afghanistan:

> We have to have more visibility of what's going on and where. Right now we don't. We didn't anticipate there was going to be this level of jamming.... At the same time, we've got people trying to listen [to insurgent conversations], a lot of it on the same or overlapping frequencies.[2]

The cyberspace domain encompasses far more than the Internet and is anything but virtual. It is not a mere "cognitive concept," although it transcends and often links the other physical domains to our perception of what occurs around us. In the cyberspace domain, the electromagnetic environment is the maneuver space. The domain is a physically manifested space with closed or wired segments as well as free space segments. Just as the boundaries between air and space may sometimes be blurred, cyberspace can occur within the other physical domains. If we do not recognize cyberspace as a physical domain—occurring wherever we interlink the electro-magnetic spectrum (EMS) and electronic systems—we allow for seams and access points where the adversary can hold us at risk. As described by General Keys above, we also risk committing fratricide as we try to conduct operations in the domain without understanding it correctly.

Recognizing cyberspace as a physical domain can improve our ability to develop and field capabilities that operate in and through the domain, expanding the opportunities to execute influence operations. However, influence operations—that is, the planning and execution of operations with the intent to affect cognition—can be executed across all the physical domains and should be effectively integrated with all operations in all the physical domains. Thus, they should not be linked with the cyberspace domain any more closely than with the others. Such an unnecessary linkage

confuses operational planners and leads to a sub-optimal organization of capabilities at the operational and tactical level. For example, when there are limited seats at the strategy table, the cyberwarrior may be tagged to be the "deception rep." However, there is no reason to believe that a person trained in cyberspace operations is any more capable of being a deception planner than a tank driver or logistician would be.

Myth No. 3: "Fight from One Location"

Myth No. 3 is that the battle to achieve cyber superiority in any conflict can be fought from one location having independent, full situational awareness. Cyberspace is an extremely dynamic domain. Critical vulnerabilities and centers of gravity (COGs) can shift at the speed of light. Points of access into adversary systems can open and close in seconds. Although the United States is linked extensively through the inter-connected portion of the domain, operations in this segment may comprise only a fraction of the fight against many potential enemies to dominate cyberspace.

For example, much of the adversaries' use of cyberspace can only be held at risk by capabilities operating in the line-of-sight of radio networks and closed battlefield command networks, in the footprint of satellites, with human-enabled access, or within the range of future, high-powered, energy wave devices. Capabilities must not only be expeditionary, they must be flexible, adaptable, and integrated with the rest of the operational fight. The necessary level of situational awareness cannot be achieved independent of regional operations. Although a cyberwarfare commander may have command and control (C2) capabilities that can create effects globally from a single location, the C2 mechanism must be linked with other operations globally to achieve the necessary situational awareness.

It is true that the global nature of the fight in cyberspace may sometimes require a central coordinating element to integrate global operations and ensure proper allocation of low-density, high-demand assets to tactical operations. The nature of many attacks in cyberspace, and the ability for the adversary to conduct those attacks at many locations simultaneously, make it imperative to improve global situational awareness and to be able to respond to those attacks globally via the most effective means.

Myth No. 4: "Control of Cyber Weapons"

Myth No. 4 is that effects of cyber weapons are difficult to control. This is not nuclear warfare; we have in fact been conducting cyberwarfare with cyber weapons for many decades. Cyberwarfare with decidedly non-cyber weapons (e.g., a pair of scissors cutting telegraph lines) goes back

much farther. Even with the development of computer network attack capabilities, the targeting and collateral damage issues are analytically no different than issues of explosive or kinetically destructive means.

All combat operations have potentially cascading effects. If we drop a bomb on a hydro-electric power facility, or destroy an electrical transformer yard, the impact can cascade to many different systems. In some instances, this is the exact intent of the attack. It is even possible that an activity that we do not intend to affect, such as telephone service to a hospital, may be degraded by shutting down power to a military target or destroying a communications link that serves the facility. In all instances, the potential unintended consequences must be considered with respect to proportionality and other laws of armed conflict considerations. The United States would never conduct a cyber attack without first exercising and developing the proper understanding of the effects, so that an informed operational decision could be made with the proper legal reviews. In other words, cyber weapons should be used in the same professional manner and with the same operational rigor with which we employ with all other conventional weapons.

Myth No. 5: "Defense of the Domain"

Myth No. 5 is that increasing security at every node will allow for effective defense of the domain. While it is imperative that we improve the security of our networks and systems, this alone will not ensure friendly freedom of maneuver. If the adversary were intent on conducting multi-pronged attacks throughout the domain, we could be quickly overwhelmed. Physical security is dependent on cybersecurity, while cybersecurity is dependent on the systems that control our use of the domain. All of the networks are interdependent. We currently have problems ensuring that we do not inadvertently degrade or otherwise damage our own operations, even in the absence of concerted adversary attacks. We must begin to conduct real maneuver in the domain and be prepared to operate with degraded capabilities. There must be a coordinated effort across the entire joint team.

Considering the multitude of connections created by each service operating in cyberspace, multiplied by several service or functional components, a well-secured segment might still be rendered ineffective if a weaker link in the joint chain is attacked. History is instructive here. After World War I, the French vowed to defend their shared border with Germany at all costs; unfortunately for them, the 1939 attack occurred through Belgium. The Air Force's Constellation Net may be the securest section of the global information grid, but if the rest of cyberspace is left under-defended, we

will only be able to communicate with ourselves. Even worse, we will only be inter-connected with a sub-set of ourselves. All of the non–Internet Protocol (IP) Air Force segments of the domain may still be "outside the Maginot Line," or may provide a tunnel to get under the line. Assuming that the line will be breached and the adversary will be operating behind our defenses, we must be prepared to fight in a contested domain. Rapid reconstitution, redundancy, and maneuver will provide the means to remain effective. Taking lessons from the spring 2007 cyber attack in Estonia, we must plan to continue operations even when cyberspace is contested.[3] We must be prepared to counter an attack in cyberspace, just as we do in the other domains. For example, we do not rely just on Patriot batteries to defend the airspace; the Air Force also must hunt down and neutralize the adversaries' offensive air and missile capabilities. With this in mind, a robust ability to conduct maneuver and counter-attacks in cyberspace may become an effective deterrent in and of itself.

Finally, it is important to realize that we would not necessarily counter-attack on American soil, just as we would not bomb the flight school in Florida that trained the 9/11 terrorists. We will take the fight to cyber attackers at a time and place of our choosing. Trying to respond on the same vector as that of the attack would be pointless. By the time the response occurred, the adversary would already have relocated to a different firing position in anticipation of the counter-battery fire.

Cyberspace Superiority

Based on this understanding of what cyberspace is and is not, we now turn to the imperative of cyberspace superiority. Cyberspace operations and its roles, purposes, and relationships to other aspects of the Air Force mission, reflect two fundamental propositions. First, cyberspace is a COG for all aspects of national power spanning economic, financial, technological, diplomatic, and military capabilities of the United States. Second, cyberspace superiority is the prerequisite to effective U.S. military operations in all other warfighting domains. We explain these propositions in this section.

Proposition 1: Cyberspace is a Center of Gravity

Cyberspace is a COG for all aspects of national power spanning economic, financial, technological, diplomatic, and military capabilities. According to Clausewitz, a COG is "the hub of all power and movement on which everything depends."[4] We have evolved from reliance on physical activities to convey information or conduct transactions, using pen and

paper, hard currency, and the like; now we can move digital representations through cyberspace of both information and wealth. Thus, the importance of this domain has increased exponentially. Fifty years ago, the loss of access to cyberspace would have been an inconvenience to a few. Today, it could cause communication systems, financial markets, transportation, and power generation facilities to fail as they became isolated or corrupted. One might argue such systems are not fully automated, that they retain a human in the loop, but the great blackout on the East Coast in 2003 indicated just how little this might help. The human operators ignored the alarms and activated shutdowns that worsened the blackout and extended it far beyond where it would have occurred without human intervention. Thus, humans may be just as vulnerable as the automated system. There is no doubt, then, that cyberspace is a COG.

Proposition 2: Cyberspace Superiority is Crucial

It follows, then, that cyberspace superiority is a prerequisite to effective operations in all other warfighting domains. Without cyberspace superiority, hence, with loss of access to the Global Positioning System (GPS), precision munitions become mere dumb bombs, and command and control are crippled as communications become unreliable and unavailable. Without cyberspace superiority, military operations in all domains are at risk. Operations are degraded, with potentially severe consequences to the warfighter.

Regardless of whether one is prepared to acknowledge that cyberspace is truly a warfighting domain, our adversaries have been operating there uncontested. They have successfully exploited the cyberspace domain repeatedly in a variety of contexts. For example, in the attack at Khobar Towers in June 1998, the attackers employed radio communications for coordination and radio frequency (RF) detonators for remote detonation of the explosives. On September 11, 2001, the attackers utilized a variety of online coordination including e-mail, Web sites, and file transfers. They had also trained virtually, through the use of commercial flight simulators.

Current areas of emphasis in the ongoing cyberspace conflict include data collection, reconnaissance, and the online recruiting of potential terrorists. The cyber Jihad is growing in both influence and capability. Recent operations in Iraq exemplify this trend: insurgents employ RF systems to trigger improvised explosive devices (IEDs), while displaying the resulting mayhem in digital video across the airwaves and the web. Just as in air and space, it is imperative that we dominate the cyberspace domain. Due to the all-pervasive nature of this particular domain, mastering it presents new challenges. The emphasis placed by both traditional state actors and

non-state entities on operations in cyberspace is a strong call to action for the United States to assert itself.

Without cyberspace primacy, operations in all of the warfighting domains run risks. An example would be employing kinetic assets when non-kinetic cyber alternatives might have the same effect faster and with reduced risk of collateral damage.

Cyberspace permits easy entry at low cost and can provide tremendous return with relatively little investment or resources, hence, offers unequaled ability to prosecute asymmetric warfare. Even a relatively poor nation or non-state actor can readily obtain the tools and access necessary to become a threat to the United States. By contrast, both air and space require substantial infrastructure and resource capabilities for even a marginal level of participation.

The very capabilities that allow the United States to dominate in air and space are those most at risk in the cyber realm. As a nation and as a military, we are heavily reliant on advanced technology to leverage a strategic and tactical advantage against our adversaries. The fundamental capability that brings us these advantages also makes us more vulnerable to cyber attack. Conversely, we have the opportunity to leverage our technological advantage not only to protect our own capabilities in the other domains, but also to expand our ability to attain superiority and dominance in cyberspace, if we can effectively counter an adversary's cyber attacks. The nation must become capable of holding enemy COGs at risk through cyberspace, if necessary. These COGs will vary widely depending on the adversary's level of development and extent of operations in the domain. For the more advanced adversary, areas of vulnerability will be much like our own—a significant infrastructure with electronic tendrils extending into many or all aspects of the society and the economy. Less developed and more erratic opponents will also be vulnerable, but typically tied more to a mobile ad hoc communications system, such as wireless local loop telephones or cellular communications, and little, if any, fixed cyberspace assets.

Based on its importance to all our operations, achieving superiority in the cyberspace domain is a prerequisite for U.S. dominance across all the warfighting domains. While each of the warfighting domains represents a significant component of the overall battlespace, we cannot achieve victory without dominating across all three domains: air, space, and cyberspace. Air superiority, for example, cannot be achieved purely by air-based operations, but depends on intelligence and surveillance data obtained from space-based and air-breathing platforms, as well as targeting provided by GPS for both aircraft and precision-guided munitions.

Similarly, future conflicts will depend on the cyberspace domain, as more and more of our combat capability operates within or from this domain. This transformational trend will be driven by a variety of factors, including technological development, the ever increasing costs, both direct and indirect, of air-breathing manned platforms, and public opinion regarding the consequences of kinetic attack with respect to collateral damage and noncombatant casualties. As cyberspace becomes ever more intrinsic to combat operations, it takes on increasing visibility and criticality to the overall cross-domain fight as well.

Conclusion

To fully integrate and implement this transition to cyberspace superiority, we need to transcend paradigms entrenched in the purely kinetic traditions of warfare, and transform the force to achieve cross-domain dominance of air, space, and cyberspace. This is a transformational event in modern warfare no less dramatic than the leap from the concept of cross-domain attacks espoused by Billy Mitchell in Winged Defense to the combat reality of land and air in the Blitzkrieg a mere 14 years later.[5] Cyberspace is a complex domain where the Air Force has recently begun to acknowledge its roles to contribute to the national defense. Other Services, the Joint community and the larger national security field have also joined forces to chart the way ahead in cyberspace. Our nation's leadership role in cyberspace is not assured. While some academic debates are important to ensure rigor in our analysis, we must swiftly move our Services, and the Nation, forward to maintain our leadership in the domain. We must separate the real issues from political agendas and overcome genuine misunderstanding of the task at hand. The next few years and our actions during that time will determine if we prove to be the masters in this new realm or merely an also-ran.

Notes

[1] Master Sergeant Mitch Gettle, "Air Force Releases New Mission Statement," *Air Force Link,* available at http://www.af.mil/news/story-asp?id=123013440.

[2] Amy Butler, "Holistic Approach," *Aviation Week and Space Technology,* January 22, 2007, 46–47.

[3] "A Cyber Riot," *The Economist,* May 10, 2007, available at http://www.economist.com/world/europe/displaystory.cfm?story_id=9163598.

[4] Carl von Clausewitz, *On War* (London: N. Trubner, 1873), 577–627.

[5] Billy Mitchell, *Winged Defense* (New York: G.P. Putnam's Sons, 1925).

Chapter 5

Marine Corps Cyberspace in Support of MAGTF C2: By Many a Marine, With a Single Vision

John L. Cloninger

> "The Marine Corps' path to fully leverage Cyberspace's potential will require continued diligence to ensure Net-Centric Enterprise Services interoperability, detailed data strategy development, and vigilance in maintaining a secure and trusted network environment. Realizing the full capabilities of such a Cyberforce requires an appropriately resourced plan embodying an appropriate spirit of transformation. My commitment: to leveraging joint capabilities in Cyberspace, to partnering fully in joint Cyberpower solutions, and to adopting effective information technology efficiencies in support of our Cyberstrategy and warfighting domains."
>
> *Brigadier General George J. Allen, Director, Command, Control, Communications and Computer—C4 Headquarters, United States Marine Corps*

September 11, 2001, soon after the initial horror, we knew who was behind it. To get the attackers, and ensure they did no more, we insisted the Taliban grant us access into Afghanistan to root out al Qaeda. They refused.

In November 2001, we sent a massive Naval Task Force off the coast of Pakistan, implementing a mission capability only envisioned a decade before. From carrier decks and amphibious assault ships, the Marines flew over Pakistan into Afghanistan onto a long-ago dried lake bed. Upon landing, the Marines secured the area, reinforced, and spread throughout the country. From 6,000 miles away, Brigadier General Robert Shea, USMC,

watched the scene unfold on SIPRNET Cyber Screens. BGen Shea, Senior C4 Marine, at the time Director, C4 Headquarters Marine Corps, was eventually to become Lieutenant General Shea, Joint Chiefs of Staff J-6. In his words, "10 years before [i.e., during Desert Storm] we could not have done this."

He went on to explain (translated into 2007 cyber terminology for this summation) that though the leveraging of cyberspace always existed, leveraging cyberpower with 21st century technology on a grand integration of air, land, and sea operational, medical, logistical (fuel, food, munitions), intelligence, and administrative forces, all under a high-bandwidth network secure umbrella just had not been possible any earlier. Only technological advances in communication systems made this possible. "We could not have leaped thousands of Marines 800 miles across one country into an adjacent landlocked hostile one."

Not until then did we have, on a large scale, our command and control land, air, and sea operational and logistic capabilities so thoroughly integrated to allow continuous awareness, interface and interaction. This incredible event is easily arguable as the first major adaptation of what we now call cyber power to a core doctrine known as Marine Air-Ground Task Force Command and Control: MAGTF C2.

For the Marine Corps, cyberpower is primarily focused on supporting the needs of the Warfighting, Intelligence, Business, and Enterprise Management areas. Many organizations within the Marine Corps are working together to develop an integrated concept of cyberpower that includes many other elements, such as computer network attack (CNA), computer network defense (CND) and C4 net operations (NetOps) (which in itself could have a book dedicated to its cyberpower implementation: GIG enterprise management (GEM), GIG network defense (GND), and GIG content management (GCM)), but these efforts are beyond the scope of this discussion. In these areas, the Marine Corps seeks to leverage best practices from other organizations to seamlessly interoperate with other organizations. Where practical, it shapes its people, processes, and technology to imbue its warrior ethos and warfighting capabilities into traditional information technology, mission assurance, information assurance, and business management approaches. An example is beginning work to evolve Lean Six Sigma into Security Six Sigma.

While the term may change in the future, the Marine Corps uses the term C4 (command, control, communications, and computers) for the cyberpower infrastructure that supports MAGTF C2.

MAGTF C2 is a core Marine Corps vision and concept that shapes its application of cyberpower. Understanding MAGTF C2 will bring the reader much closer to understanding where the Marine Corps is moving in the area of cyberpower.

MAGTF C2: The Vision

> "This Vision is intended to initiate the process of discussion, research, experimentation and development necessary to help us find new solutions to the Command and Control challenges of the 21st Century."[1]

The commander's ability to exercise his authority over assigned and attached forces to accomplish the mission is the primary objective of MAGTF C2.

The United States is currently engaged in a long-term, global conflict of competing wills and ideologies. As the premier expeditionary "Total Force in Readiness," the Marine Corps requires a robust and secure command and control (C2) capability to leverage cyberpower across the cyberspace spectrum of joint and coalition military operations and to maximize the kinetic capabilities of Marine forces, thereby increasing strategic agility, operational reach, and tactical flexibility of the MAGTF and our coalition partners.

Command and Control

Joint Publication 1-02, "DOD Dictionary of Military and Associated Terms," defines C2 as "the exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission."

From a Marine Corps cyberpower perspective, C2 consists of the means and methods by which a commander recognizes what needs to be done in any given situation, and then sees to it that appropriate actions are taken (MCDP 6). Further, the foundations of Marine Corps C2 are rooted in their warrior ethos and their warfighting philosophy of maneuver warfare.

As the creation of MAGTF C2 evolves, the term "Command" will refer to all of the functionality that supports the commander's contribution to the planning phase and the decision-making processes from pre-deployment planning to execution and redeployment. Regarding "Control," MAGTF C2 envisions a process incorporating multiple technologies leveraging the vastness of cyberspace that captures feedback—the continuous flow of information about the unfolding situation returning to the commander—in all planning, execution and specified/implied re-

porting functionality and imbeds it within the philosophy of command. Marine leaders will use MAGTF C2 systems to issue mission-type orders and commander's intent, then exert control through improved situational awareness and shared understanding, enabling rapid collaborative maneuver, engagement and support. Marines acknowledge that the fog of war can never be eliminated, nor will any of us ever achieve perfect clarity or total knowledge superiority. Therefore, the intended effect of MAGTF C2 is decentralized execution that provides subordinates the latitude to accomplish assigned tasks in accordance with the commander's intent.

The commander's ability to exercise authority over assigned and attached forces to accomplish the mission is the primary objective of MAGTF C2. MAGTF structure assures unity of command and facilitates the full integration of air, ground, and logistics operations in support of the commander's overall mission. The challenge at this stage is that there is no single C2 cyberpower capability in place to facilitate the full potential of the MAGTF command structure. In the past, Marines have adopted individual stove-piped pieces to address individual functional areas, which then left to the commander the responsibility to splice them together. In the future, Marines will incorporate new technologies in a manner that will promote enhanced informed decisionmaking at appropriate echelons. The future command and control capability must evolve to a comprehensive approach to C2 that will enable any commander across the globe to leverage and focus not only MAGTF capabilities, but all elements of Marine Corps, naval, joint, national and multinational power. The future MAGTF C2 must enable decentralized decisionmaking that promotes taking advantage of fleeting battlefield opportunities. The Marine approach to C2 must enhance understanding of the commander's intent, emphasize initiative of small units, and provide relevant displays that promote understanding throughout the MAGTF.

MAGTF C2: Strategy and Cyberstrategy, Process and System

MAGTF C2 is a strategy and a cyberstrategy, a process, and ultimately a system-of-systems by which the Marine Corps will develop current and future capabilities and programs in order to achieve net-centric operations and warfare (NCOW), and implement the FORCEnet Functional Concept of providing robust information sharing and collaboration capabilities.

MAGTF C2 will support and enable joint, multinational, and interagency interoperability.

Strategy and Cyberstrategy

MAGTF C2 is the strategy, with an associated C4 cyberstrategy, by which the Marine Corps will implement the Naval FORCEnet Functional Concept and is the functional and conceptual equivalent to the other Service net-centric concepts of LandWarNet (Army) and C2 Constellation (Air Force). The Marine Corps will be fully engaged with the development of the net-enabled command capability (NECC) effort to ensure that Marine Corps requirements are fully considered and to also ensure that Marine Corps programs align to this concept. The Marine Corps will engage in the development of command and control concepts with the other Services, on a service-to-service basis, to ensure interoperability between Services below the level that will be accomplished by NECC. Key will be the ability to engage in the joint arena, and to function effectively within the labyrinth of interdependencies that will exist. MAGTF C2 systems and the associated C4 cyberstrategies will also integrate with formal alliances, like NATO, and be able to facilitate "coalitions of the willing" as needed.

MAGTF C2 entails a truly interoperable Marine Corps C2 capability that is seamless, scalable, modular, and relevant across the full spectrum of military operations, from major theater war, to irregular operations, to humanitarian assistance operations. It is oriented around the Marine Corps C2 philosophy, is derived from the Naval FORCEnet Functional Concept, and is agnostic of the limited perspectives imposed by ground, air or logistics "formations." It is a capabilities-based approach for the development of Marine Corps C2 that will be expeditionary in nature; will be fully capable in an austere forcible entry environment; and will enable joint task force capabilities from the seabase while being essentially transparent to the commander. Overall, MAGTF C2 provides the strategy needed to synchronize C2 requirements generation and acquisition in the force development process. Marine Corps cyberstratergy provides the needed infrastructure and capabilities to support these C2 requirements.

Process

As a process, MAGTF C2 constitutes an approach to commanding and controlling Marine forces that drives the creation of networked capabilities. Every node in the network—commander, staff, unit, riflemen, supporting organization, platform, piece of equipment or item—can be a producer, processor, and user of information, and all information must be readily available to any node without overloading or paralyzing any node with irrelevant information. Many of the nodes in the network will be required to perform multiple functions. Thus, the essence of MAGTF C2 is a

decentralized and highly adaptive form of command and control that uses the digital, global network to foster and exploit the human capacity for mutual understanding, implicit communication, and intuitive decision-making. The cumulative network effect achieved by organizing all nodes into an information-rich, collaborative, global network is expected to enhance these inherently human qualities.

MAGTF C2 enhances the ability of commanders at all levels to gain and maintain situational awareness, make decisions at an increased tempo, and exercise authority through commander's intent and mission-type orders. It will facilitate planning and execution by providing the warfighter with distributive and collaborative planning tools, an accurate user-defined, fused common operational picture of the operational environment to facilitate more rapid decisionmaking through increased situational awareness, and shared understanding. The intent is to increase freedom of action and small unit initiative through decentralized C2, while minimizing the requirement for specified and implied linear control measures that limit the initiative of subordinates in a complex and increasingly ambiguous operational environment.

In seeking to exploit the power of cyberspace, the Marines Corps is considering the potential needs levied by operations in an austere environment, or when temporarily disconnected from the network. All Marine operations must be equally capable of operating either within the global information grid (GIG), or without the benefit of its full range of services. As a result, it is critical in leveraging cyberspace to ascertain the proper balance between GIG services and organically deployable networking capabilities. The expansion of MAGTF C2, to include the non-warfighting or business operations of the Marine Corps, will likewise require greater exploitation of cyberspace: network, integration of additional processes, and vastly improved interoperability. The goal of the expanded C4 net operations (NetOps) processes that support MAGTF C2 will be to ensure that the entire Marine Corps and all of its supporting elements become nodes in the network that can share information seamlessly, thereby attaining the true, end-to-end capability fundamental to the future net-centric environment.

System-of-Systems

As a system, MAGTF C2 must constitute the adaptive, distributed network of commanders, staffs, operating units, supporting organizations, sensors, weapons and other C2 nodes interacting with one another over an underlying supporting information infrastructure, as well as the asso-

ciated equipment communications, facilities, and personnel necessary to allow them to interact. The most important function of MAGTF C2 is to enhance the strategic agility, operational reach, and tactical flexibility of Marine Corps forces across the warfighting functions and cyberspace in support of naval and joint operations. To achieve this agility, and to lessen the doctrine, organization, training, material, leadership, personnel, and facilities (DOTMLPF) impacts of migrating to MAGTF C2, Marines will align where appropriate with the NECC program.

C2 and Communication Systems

MAGTF C2's vision is, unquestionably, locked into encompassing the cyber elements of communications and information technology, without which the vision of C2 cannot be achieved. A significant element of MAGTF C2 will track the cyberspace communications and network requirements needed to support C2 functions. Constant attention to current and emerging technologies will be required to ensure that commanders have the best possible cyberspace infrastructure within which to work. Marines envision the use of a cyberpower architecture and hardware that integrates software solutions that permit timely upgrades at reduced costs. The capabilities, requirements, architecture, process and material solutions will be developed with the complete integration of C2, communication systems, and information technology in mind. Agility is key—jokingly referred to as "Semper Gumby," which translates to "Always Flexible."

MAGTF C2 Implementation

In The Near-Term

MAGTF C2 will migrate to a fully integrated, cross-functional set of C2 capabilities that include forward-deployed as well as reachback capabilities, and the C4 infrastructure will grow and adapt to support these capabilities. As Marines pursue this goal, they will also examine other options, such as enhanced forward data storage that could free up significant portions of reachback-related bandwidth that could be better used for other aspects of warfighting.

In The Mid-Term

MAGTF C2 will become an integrated C2 solution that will migrate the current multiplicity of stove-piped, disparate systems into an integrated system-of-systems that will support deployed aspects of Marine Corps C2 requirements from pre-deployment planning to execution and redeployment via multi-functional C2 nodes. Marines will accomplish this

in great measure through an increased reliance upon common hardware and software to reduce costs and minimize operations and training impact on the warfighter as updates are fielded.

In The Far-Term

Marines envision that MAGTF C2 will be expanded and extended to include all elements of the Marine Corps global enterprise, to include business, garrison, and administrative C2 processes.

Timeframe For Implementation

Timeframe for MAGTF C2 implementation is from the present to 2015. The approach, though, must comprise a full DOTMLPF solution set, to include the migration of MAGTF C2 systems in the near-term (FYDP), mid-term (FYDP plus five), and far-term (FYDP plus ten). The goal is to achieve a full, integrated MAGTF C2 capability by 2015, within the constraints of technology and funding. But, in contrast, *a focused sense of urgency must pervade all aspects of the Marines* "C2 Harmonization" *effort to achieve maximum MAGTF C2 integration as rapidly as possible.*

MAGTF C2: The Harmonization

The Marine Corps C2 Harmonization, which could be considered by some as the 30,000-foot view of the MAGTF C2 cyberstrategy, received requests for Congressional testimony in 2007 and Secretary of Defense briefing in 2006. Additionally, the MAGTF C2 harmonization effort is one (of only seven) Marine Corps C4 formal priorities established by the Director, C4 Headquarters. The following is a summary of the C2 harmonization being implemented to make MAGTF C2 a reality:

Bottom-Line

The C2 harmonization strategy incorporates joint integrating concepts and C2 mandates, and is a holistic approach that integrates warfighter requirements into a common capability to deliver an end-to-end, fully integrated, cross-functional set of capabilities, including forward-deployed and reach-back functions. The strategy's end state is a seamless capability that crosses warfighting functions and supports Marines from the supporting establishment to Marines in contact with the enemy, taking the best of emerging capabilities and joint requirements to build a single solution. With Common Aviation C2 System, CAC2S, and C2 Harmonization, a joint task force commander will discover that his MAGTF battlespace offers maximum flexibility due to seamless integration with joint and coalition partners.

Key Points

The C2 harmonization strategy synchronizes top down direction and bottom up requirements to create a joint integrated and resource informed vision for MAGTF command and control.

It is the Marine Corps' application of naval FORCEnet capabilities and the service "plug-in" to the NECC.

The holistic approach represented by the C2 harmonization capabilities framework is used to inform and guide C2 requirements development and integration. The C4 infrastructure and NetOps support MAGTF C2 with the needed cyberpower and:

1. Is composed of four fundamental service layers:
   a. Applications/Systems,
   b. Enterprise Services,
   c. Network Services, and
   d. Transmission Tactical/Transmission Operational.
2. Includes cross-functional integration across warfighting functions.
3. Spans strategic, operational, and tactical C2 requirements.
4. Uses proven capability identification and synchronization tools to support C2 portfolio management linking requirements and directives to program of record development. Specifically, the tools link complex, and sometimes divergent, C2 requirements developed independently by JROCM 161-03 (Joint Blue Force Situational Awareness), the joint battlespace management roadmap, and the NECC linked with service C2 requirements.

The C2 harmonization strategy takes the best of emerging service capabilities and joint requirements to build a single end-to-end C2 solution.

1. CAC2S fuses data from sensors, weapon systems, and C2 systems into an integrated display. It allows rapid, flexible operations in a common, modular, and scalable design by reducing the current five stove-pipe systems into one hardware solution with streamlined equipment training. CAC2S will enable MAGTF commanders to control timing of organic, joint, and coalition effects, assault support, and ISR in their battlespace while operating within a joint task force.
2. Unit Operations Center (UOC), the material solution for O5 and O6 commands, is already fielding across the MAGTF.
3. Marine Expeditionary Force (MEF) Combat Operations Center (COC) is being fielded.
4. Major Subordinate Command (MSC) COC is still being developed.

5. Marine Corps Systems Command (MCSC) is in the process of deploying initial Marine corps enterprise information technology services MCEITS (SharePoint) capabilities to all MEFs.
6. Numerous operational and tactical bandwidth solutions are being fielded.
7. DC DC&I has directed the stand-up of the MAGTF C2 Transition Task Force to ensure that all aspects of DOTMLPF are duly considered and planned for prior to the fielding of new MAGTF C2 capabilities.

MAGTF C2: Concept of Operations

> "The MAGTF C2 CONOPS describes steps on the path to achieving the MAGTF C2 Vision. It lays the foundation for developing and fielding the C2 capabilities...."[2]

The MAGTF C2 concept of operations (CONOPS) contains the details of the cyberstrategy behind C2 harmonization: required USMC future MAGTF C2 capabilities, programmatic information, 500-day plan, service layer taxonomy, approach and methodology … in short, this is the MAGTF C2 cyberstrategy playbook to leverage the capabilities of the technology and Marine Corps support cyber-infrastructures.

The framework for developing the MAGTF C2 capability is the "MAGTF C2 Capability Model," which addresses the fundamental need to integrate Marine Corps C2 and communications systems capabilities with each other and with existing and future Joint and multi-national capabilities. It is the primary component of the MAGTF C2 strategy that will migrate today's stove-piped C2, communications, and networking capabilities to a future integrated system-of-systems across all echelons of the Marine Corps and across all warfighting functions. The model provides a foundation to create the verifiable, repeatable processes that are necessary to enable spiral development of end-to-end, holistic C2 capabilities.

The MAGTF C2 Capability Model is based on the principle that C2 systems are underpinned by a support structure of capabilities and services. By grouping together services of similar function, it becomes easier to identify redundancies. This enables re-use of existing services and reduces development of redundant or stove-piped capabilities. The services that embody MAGTF C2 are organized by the MAGTF C2 Capability Model into those that directly support C2 and communications processes. The underlying C2 support structure enables critical information exchange and shared services that create an information-rich environment. The communication system support structure is further divided

into three components consisting of those services that support the requisite information transport services, those that connect distributed nodes and services into an integrated network, and those that provide necessary bandwidth for communication. The support structure supports all of the warfighting functions and the business mission area, and is critical to coordinating and integrating to achieve the mission.

The following contain summary descriptions of each system and layer in the capability model:

System-of-Systems (SoS): A set or arrangement of interdependent systems that are related or connected to provide a given capability. The loss of any part of the system will significantly degrade the performance or capabilities of the whole. An example of an SoS would be a combat aircraft. While the aircraft may be developed as a single system, it could incorporate subsystems developed for other aircraft (e.g., the radar from an existing aircraft may be incorporated into the aircraft being developed rather than developing a new radar. The system of systems in this case would be the airframe, engines, radar, avionics, etc. that make up the entire combat aircraft capability).

Family of Systems (FoS): A set of systems that provide similar capabilities through different approaches to achieve similar or complementary effects. For instance, the warfighter may need the capability to track moving targets. The FoS that provides this capability could include unmanned or manned aerial vehicles with appropriate sensors, a space-based sensor platform, or a special operations capability. Each can provide the ability to track moving targets, but with differing characteristics of persistence, accuracy, timeliness, etc.

Applications (applications and end-user equipment): End-user information technology programs (software) and equipment (hardware) that enhance the ability to perform C2:

Enterprise Services: Provides the operating environment and other supporting applications, services and interfaces (i.e., Shared Data Environment, storage, collaboration, messaging, etc.) to users throughout the network.

Network: Provides basic DISN services pulled from the GIG; DSN, the IP backbone (NIPRnet and SIPRnet) connectivity to the GIG.

> Bandwidth, Tactical: The bandwidth communications essential for the planning, directing, and controlling of fires, movements or maneuver within the operational area to accomplish missions and tasks.
>
> Bandwidth, Operational: Provides mobile, robust bandwidth communications essential for the employment of military forces to attain strategic and/or operational objectives through the design, organization, integration and conduct of strategies, campaigns, major operations and battles between specified nodes.

The MAGTF C2 Capability Model expands upon the joint expertise of the Marine Corps to integrate and be interoperable with joint and other Service concepts for C2 and communications systems. It is the Marine Corps equivalent of the system framework that guides C2 for all services put forth by the DOD in the *Net-centric Operational Environment Joint Integrating Concept* (NCOE JIC)[3] and is consistent with current and evolving DOD policies for the management of information technology (IT).

MAGTF C2: Foundation Building-Blocks for the Marine Corps Cyberspace Vision

To get where you want to go, you must know where you are. So, where are we? As illustrated, MAGTF C2's vision is not starting from a cyber Big Bang. It is starting from a foundation steadily evolved. The most potent foundation building-block being in the lever-of-power IT advantage held by U.S. forces and our ability to collect, process, and share data within a trusted environment. Well known is that the keys to the maintenance and future growth of this advantage are the extension of enterprise services to the tactical edge, a data cyberstrategy that facilitates data exposure and transparency across functional domains, and fully joint operation and defense of our networks. Where the Marine Corps currently stands in the cyber world is summarized in a synopsis of the statement of Brigadier General George Allen, Director, C4 Headquarters Marine Corps, to the House Armed Services Committee on 6 April 2006:

> USMC computing and communications environments have evolved over the past 20–30 years to meet specific Marine Corps requirements. As with the rest of DoD and Department of the Navy, this initially occurred in a highly stove-piped manner leading to a proliferation of systems, applications, and data. As a result, the USMC IT

infrastructure became difficult and expensive to maintain and support. However, early in the 90's the Marine Corps began managing its own enterprise network and in the years prior to the Navy Marine Corps Intranet (NMCI) embarked upon a series of programs designed to standardize policies, funding, acquisition, technical specifications, security, and life cycle management of systems. In 2003, with a basic foundation in enterprise-level IT management and operations established, the Marine Corps began transitioning to the Navy Marine Corps Intranet (NMCI). Today the USMC IT environment is supported by continuously evolving Service-wide IT management processes focused on integrated IT support for the warfighter from the business operations of the USMC Supporting Establishment to MAGTF operations in the deployed tactical environment. While the Marine Corps has experienced progress in enterprise-wide IT management, much additional work is needed. Improvements in the areas of NMCI provided capabilities and management, enterprise-wide application and data management, and a complete suite of mature ITIL processes remain if the Marine Corps is to successfully adopt technologies and concepts needed for Network Centric Operations and Warfare (NCOW).

The Marine Corps Enterprise Network (MCEN) is the backbone of Marine Corps' cyberpower. The Marine Corps defines the MCEN as the totality of the Marine Corps' general service (collateral) network and voice, video and data services environment from wide area network circuits to the desktop. The MCEN is a global network environment that includes all capabilities necessary to execute Joint NetOps including GIG Enterprise Management, GIG Network Defense, and GIG Content Management. The MCEN is comprised of Supporting Establishment networks (both NIPRNET and SIPRNET; NMCI and non-NMCI), deployed/tactical networks (both NIPRNET and SIPRNET) and infrastructure that provides access to DoD/DISA services (mainframe, Defense-On-Line, etc.) and coalition networks. The USMC Community of Interest (COI) within NMCI provides the Marine Corps the ability to independently provide operational direction to the NMCI vendor to control the Marine Corps portion of NMCI and ensure network operations and defense are tightly integrated with and directly supportive of USMC operations around the world. *The USMC NMCI COI is a subset of the MCEN.* The Marine Corps Enterprise Information Technology Services (MCEITS) program rep-

> resents a maturing set of capabilities designed to address enterprise application and data services that will meet the requirements for GIG Content Management and NCOW. Net-Centric Enterprise Services (NCES) provides the Department-level capability to provision a common suite of services and tools to the Services.

Capitalization on NCES and adherence to NCES standards are keys to the architecture and design of MCEITS and will that ensure joint information technology services are extended to the warfighter. MCEITS capabilities reside within and are a part of the MCEN. The bottom-line is that the MCEN is the Marine Corps area of operations within the GIG and includes all IT systems, data, people, and processes governed and controlled by the Marine Corps in support of the Marine Corps mission of making Marines and winning battles.

The future extension of cyber infrastructure and services across the battlefield will be facilitated by the Joint Tactical Radio System (JTRS), the Advanced Extremely High Frequency (AEHF) program, the Mobile User Object System (MUOS) and the Transformation Communication Satellite (TSAT), as part of the joint Transformation Communication Architecture (TCA). As evidenced by the ongoing war on terrorism, wideband, on-the-move, over-the-horizon communications enhance the mobility, flexibility, accuracy, and lethality of our forces, but place greater information demands on the cyberspace network. TSAT will provide on-the-move, satellite-based C2 access within a theater of operations, allowing Marine commanders to maintain battlefield tempo and exploit initiatives gained through mobility. The Marine Corps will leverage JTRS-like assets to transform our battlefield radio capability from a loosely integrated collection of legacy systems into an integrated, end-to-end networked system of systems. The combination of TSAT, AEHF, MUOS, and JTRS-like capabilities will create and extend secure mobile, ad hoc, battlefield networks to last-tactical-mile, including extension of net-centric services and data.

The added value of extending joint tools and services to the cyber and operational battlefield is enhanced through the deliberate and logical creation, storage, discovery, and processing of data. The DOD and Marine Corps data strategies require tremendous coordination among numerous domains. Subject matter experts within each domain at the DOD and service level define the relevant data, structure of the data, and data-tagging standards, thus enabling cataloging and discrete discovery of data. Accurate, timely, and consistent access to data on the battlefield by joint forces depends on a measured enterprise data strategy effort. The Marine Corps

has adopted the Joint Consultation Command and Control Information Exchange Data Model (JC3IEDM). JC3IEDM is an information model that is being used by several DOD components, coalition forces, and commercial organizations. Regarded as an information exchange model, JC3IEDM is being used as the Marine Corps' primary tool for integrating DOD and Marine Corps data strategies into requirements definition, acquisition, and Clinger-Cohen Act compliance.

The net-centric approach to network operations and network defense underpins and protects our network services and data. Under the auspices of United States Strategic Command, the operational control of Joint Task Force Global Network Operations (JTF-GNO), and administratively controlled by the Marine Corps Director of C4, the Marine Corps Network Operations and Security Command (MCNOSC) ensures all Marine Corps portions of the Global Information Grid are operated and defended in a joint manner. The malicious cyber forces arrayed against our networks are adaptive and continually upgrade their capabilities and methods of attack. A wide range and variety of skill sets exist within these forces, from the use of pre-packaged tools to highly customized vectors, employed by rogue individuals, crime syndicates, and nation-states. The Marine Corps has robust means to defend, but currently lacks the ability to clearly identify the individual conducting the network attack. Further enhancements to information assurance and network defense, to include increasing network vulnerability assessments, establishing blue/red training teams, and provisioning improved tactical and coalition network security tools are being worked. A standardized cross-domain solution (CDS) implementation, with a robust and consistent configuration, and an increased level of assurance is eagerly anticipated and needed by the Marine Corps. This latter is an area where the Marine Corps leverages the work of outside expertise, including that of the National Security Agency, as it aggressively identifies solutions meeting these standards, and will draw from a short list to build out the Marine Corps portion of the Global Information Grid.

Closing Thoughts: "Pointy-End-of-the-Cyber-Power-Spear"

Over the next 7–10 years, the Marine Corps will begin employing the MAGTF C2 strategy to transform existing C2 systems and supporting communications capabilities to the integrated system of systems depicted by the MAGTF C2 vision. The migration will begin by building from an established cyberspace foundation using the MAGTF C2 Capability Model to consolidate redundant capabilities across all existing programs into a

single set of services. It will include initiatives to standardize non-materiel C2 and communications systems across the Marine Corps enterprise, as necessary. As successes supporting the MAGTF C2 Capability Model are reached, the process will add operational perspective to enable spiral development of enhanced C2 cyberpower and leverage the full potential cyberspace offers.

"We are what we do everyday."[4]

Notes

[1] Lieutenant General James N. Mattis, Commanding General, I Marine Expeditionary Force; and Commander, U.S. Marine Corp Forces Central Command.

[2] Lieutenant General James F. Amos, Commanding General, Marine Corps Combat Development Command.

[3] Available at http://www.defenselink.mil/cio-nii/docs/netcentric_jic.pdf.

[4] Colonel Eric Rolaf, Commanding Officer, Marine Corps Network and Operations Security Command.

About the Authors

Charles L. Barry is a Senior Research Fellow at CTNSP and President of Barry Consulting, Inc. He is a retired Army officer with extensive experience in joint and multinational operations. His areas of specialization include international relations, U.S. military strategy, joint command and control, land warfare, and information networks related to command and control. Barry received his doctorate in public administration with a concentration in information resource management from the University of Baltimore. He holds a BA in political science from Loyola University, Chicago.

Michael A. Brown graduated from the United States Naval Academy in 1980 with a bachelor of science degree in mathematics. His first three years as a commissioned officer were in the Surface Line Community, where he served on board USS Vogelsang (DD 862) and USS Connole (FF 1056). After a lateral transfer to Cryptology, he attended the Naval Postgraduate School graduating with his Masters of Science, Systems Engineering (Electronic Warfare) in 1985. Following Naval Postgraduate School, he was assigned to the National Security Agency/Central Security Service (NSA/CSS) in the Electronic Warfare and Technology Directorate. In August 2005, he reported to the staff of the Chief of Naval Operations as Director, Information Operations Division (OPNAV N3IO) and Deputy Director for Cryptology Division (OPNAV N2C). Rear Adm. Brown also serves as the Senior Advisor for Information Operations and Signals Intelligence to the Commander Naval Network Warfare Command.

John L. Cloninger, Col USMCR, entered the Marine Corps through the U.S. Naval Academy, Class of 1980. Upon graduation, he entered the Marine Corps Basic School followed by graduating with honors from Naval Flight School. From 1981 through 1985 he served as a Marine Corps Naval Aviator in Marine Fighter/Attack Aircraft F/A-4 Phantoms. From 1985 through 1989, after completing Marine Corps Computer Sciences School, he was assigned as Head of Automatic Data Processing Liaison Officers (ADPLO), staffs and supporting computer sections to the Joint Chiefs of Staff. From 1989 through 1992, he fulfilled duties as Marine Corps Computer Sciences School Dean for USMC Data Systems Officers studying toward the Data Systems Officer MOS.

From 1992 through 2001, he transitioned and fulfilled multiple leadership roles as Federal Government Computer Scientist/Defense Information

Systems Agency (DISA) while preserving USMC Reserve Commission. His IT Program and Project Manager (PM) positions included Global Command and Control System (GCCS) Information Security PM, GCCS Y2K Command Center PM, Data Standards Tools PM, Software Reuse Initiative PM, HQMC C4 Information Assurance (IA) Awareness PM, and Global Network Operations Systems Center (GNOSC)–Computer Network Defense (CND) USMC Team PM. During evening hours, he served as Information Systems Adjunct Professor, University of Southern California.

On September 12, 2001, Col Cloninger returned to active duty as USMC Head C4 Continuity of Operations/Homeland Defense, followed by assignment as Joint Matters/Spectrum/Science and Technology IT Head. In Col Cloninger's final tour until his active duty retirement in January 2009, he serves as the C4 Headquarters Marine Corps' Liaison Officer to the Department of the Navy Chief Information Officer.

Col Cloninger holds a Master of Science in Systems Management, University of Southern California; BS in mechanical engineering, U.S. Naval Academy; Marine Corps Command and Staff College, Marine Corps Amphibious Warfare School, Marine Corps Data Systems Officer Computer Sciences School, Naval Flight School.

Forrest B. Hare, LtCol, USAF, is an intelligence officer assigned to Headquarters U.S. Air Force Deputy Chief of Staff for Operations, Plans and Requirements Cyberspace Operations Directorate. Lt Col Hare recently served for one and a half years on the AF Cyberspace Task Force. He has also served as the commander of the AF Information Operations detachment in the European Air Operations Center and Chief of Targeting Intelligence for the Korean Theater.

Jeffrey G. Smith, Jr., BG USA, is Deputy Commander, United States Army Network Enterprise Technology Command/9th Army Signal Command, Arlington, Virginia. Previously, he has serves as Director, United States Training and Doctrine Command Program Integration Office-Networks, United States Army Signal Center and Fort Gordon, Fort Gordon, Georgia. Brigadier General Smith holds a BA from the Virginia Military Institute and an MA and PhD from Princeton University. He has also attended the United States Army Command and General Staff College and the National War College.

Stuart H. Starr is a Distinguished Research Fellow at the Center for Technology and National Security Policy, National Defense University, Fort McNair, Washington, DC. Concurrently, he serves as President, Barcroft Research Institute (BRI), where he consults on Command and Control (C2) issues, serves on senior advisory boards to defense industry (e.g., Northrop Grumman, Titan), lectures to audiences world-wide on C2 issues, and participates on blue ribbon panels (e.g., the Army Science Board and the National Research Council Task Force on Modeling and Simulation to support the Transformation of DoD).

Elihu Zimet is a Distinguished Research Fellow at CTNSP, The National Defense University. Prior to this he headed the Expeditionary Warfare Science and Technology Department at the Office of Naval Research. In this position he directed science and technology (S&T) programs in missiles, and directed energy, aircraft, and stealth as well as S&T support to the Marine Corps. Dr. Zimet holds a BS (ME) from the Polytechnic Institute of Brooklyn and a PhD from Yale University.

Glenn Zimmerman is the Chief of Strategic Outreach, Chief of Staff Strategic Studies Group, CHECKMATE, Headquarters, United States Air Force. Colonel Zimmerman graduated from the University of Colorado, Boulder Colorado, in 1985, with a BS in electrical engineering and computer science and was commissioned through AFROTC that same year. He completed his MBA in 1991 with specialization in statistics and finance. He holds 15 current national and international Information Technology certifications. Colonel Zimmerman has commanded at the detachment and squadron level and held staff positions at the wing, intermediate headquarters, and Air Staff levels including a tour as the Director, Air National Guard NOSC. Preceding his current assignment, he was handpicked to serve as a senior cyber strategist with the CSAF Cyberspace Task Force in 2006–2007. In this role, he helped craft the foundational framework that led to the stand-up of the AFCYBER major command scheduled for October 2008.

Note: Authors' positions and assignments were current as of the time of writing in 2008.