REPORT DOCUMENTATION PAGE	*Form Approved* *OMB No. 0704-0188*

1. REPORT DATE *(DD-MM-YYYY)* 26-03-2014	**2. REPORT TYPE** JAWS Master's Thesis	**3. DATES COVERED** *(From - To)* 22-07-2013 to 13-06-2014

4. TITLE AND SUBTITLE
Cyber Power for the Joint Force Commander: An Operational Design Framework

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
William S. Angerman, Lt Col, USAF

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Joint Forces Staff College
Joint Advanced Warfighting School
7800 Hampton Blvd
Norfolk, VA 23511-1702

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 is unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

In modern and future warfare, the Joint Force Commander (JFC) must skillfully and effectively leverage cyber power. Anecdotal evidence suggests, however, that the JFC is unable to assemble, coordinate, and integrate elements of cyber power within an operational design to employ a dominant, full spectrum capability. Significant but not insurmountable barriers to accomplishing this outcome exist in current doctrine, policy, and organizational relationships. JFCs do not have a conceptual and pragmatic mission-focused construct for planning, employing and leveraging available cyber power in concert with other existing capabilities to develop a modern operational warfare approach. At this point, the JFC lacks the integration means to think about and apply cyber power. Cyber capabilities need to be planned for, coordinated, and employed from Phase I to Phase V as part of an integrated operational plan. To do this, a cyber operationalization framework is needed with which to shape JFC operational art and operational design to meet the requirements of modern warfare. To address this deficit, a JFC cyber operationalization framework incorporated within operational design is proposed to empower the JFC to fully leverage cyber power in campaign conception, planning, and employment. The framework provides an integrated cyber operational approach and attempts to improve and rebalance the JFC and USCYBERCOM working dynamic while meeting requirements for a JFC's operationally phased campaigns.

15. SUBJECT TERMS

Cyber; Joint Force Commander (JFC); operational design; cyber power; operationalization; operational campaign; joint operations; framework; USCYBERCOM; spectrum penetration & control; cyber protection & fires; virtual coalition; strategic cyber messaging

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	Unclassified Unlimited	64	**19b. TELEPHONE NUMBER** *(include area code)* 757-443-6301

NATIONAL DEFENSE UNIVERSITY

JOINT FORCES STAFF COLLEGE

JOINT ADVANCED WARFIGHTING SCHOOL

CYBER POWER FOR THE JOINT FORCE COMMANDER: AN OPERATIONAL DESIGN FRAMEWORK

by

William S. Angerman

Lieutenant Colonel, United States Air Force

CYBER POWER FOR THE JOINT FORCE COMMANDER: AN OPERATIONAL DESIGN FRAMEWORK

by

William S. Angerman

Lieutenant Colonel, USAF

A paper submitted to the Faculty of the Joint Advanced Warfighting School in partial satisfaction of the requirements of a Master of Science Degree in Joint Campaign Planning and Strategy. The contents of this paper reflect my own personal views and are not necessarily endorsed by the Joint Forces Staff College or the Department of Defense.

This paper is entirely my own work except as documented in footnotes.

Signature: ______________________

26 March 2014

Thesis Adviser:
Name

Signature: ______________________

Keith Dickson, PhD
Thesis Advisor

Approved by:

Signature: ______________________

Denis Doty, Colonel, USAF
Committee Member

Signature: ______________________

Charles Cunningham, Lt Gen, USAF retired
Committee Member

Signature: ______________________

Richard E. Wiersema, Colonel, USA
Director, Joint Advanced Warfighting School

ABSTRACT

In modern and future warfare, the Joint Force Commander (JFC) must skillfully and effectively leverage cyber power. Anecdotal evidence suggests, however, that the JFC is unable to assemble, coordinate, and integrate elements of cyber power within an operational design to employ a dominant, full spectrum capability. Significant but not insurmountable barriers to accomplishing this outcome exist in current doctrine, policy, and organizational relationships. JFCs do not have a conceptual and pragmatic mission-focused construct for planning, employing and leveraging available cyber power in concert with other existing capabilities to develop a modern operational warfare approach. At this point, the JFC lacks the integration means to think about and apply cyber power. Cyber capabilities need to be planned for, coordinated, and employed from Phase I to Phase V as part of an integrated operational plan. To do this, a cyber operationalization framework is needed with which to shape JFC operational art and operational design to meet the requirements of modern warfare. To address this deficit, a JFC cyber operationalization framework incorporated within operational design is proposed to empower the JFC to fully leverage cyber power in campaign conception, planning, and employment. The framework provides an integrated cyber operational approach and attempts to improve and rebalance the JFC and USCYBERCOM working dynamic while meeting requirements for a JFC's operationally phased campaigns.

ACKNOWLEDGEMENT

This thesis draws from the work and ideas from many joint cyber pioneers who are bravely exploring and creating a whole new world. I am grateful for their daily contributions to national security and am proud to be one of their tribe.

To Seminar 2, you guys rock! Thanks for helping even the most difficult material at JAWS seem fun and engaging. I tremendously enjoyed learning from each and every one of you and look forward to working together in the future.   Good luck on the staff.

Finally, this thesis would not be near as good as it is without the wise and tireless efforts of my thesis advisor, Dr. Keith Dickson. In record time he plowed through my most dense writing and came out motivated on the other side with helpful organization and powerful insights. Doc, your work at JAWS is critical to the school’s success and our nation’s planning cadre. Thank you for what you do.

DEDICATION

This thesis is dedicated to my wonderful wife, Tana, and my boys, Jacob and Zachary. Your love and support keep me going every day in good times and bad. Tana, I love you now more than ever…thank you for putting up with another thesis. This military adventure is a wild ride with all the moves and transitions, but it’s pretty exciting with you by my side. Boys, I’m so proud of the young men you are becoming. You know I love you unconditionally…keep up the good work anyway.

TABLE OF CONTENTS

CHAPTER 1

Introduction

"Victory smiles upon those who anticipate the changes in the character of war,
not upon those who wait to adapt themselves after the changes occur."[1]

Italian Air Marshall, Giulio Douhet

Current Cyber Environment

It is a brave new world (again). The information age has changed the world with the rapid expansion of computing technology, networks, communications, and dynamic cyber capabilities.[2] Modern cabled and wireless networks allow ubiquitous system-to-system connections. Faster and smaller computing power fuels information processing and virtualization. The Internet and largely unmanaged online environments globally connect a wide spectrum of data communications and information applications that enhance situational awareness. People today have more access to information and connectivity than ever before.

Today's cyber capabilities underwrite modern civilization; this connected, online environment serves government, business, and individual activities. Information systems and computer networks present a powerful environment for discovery, computing analysis, command and control, data sharing, and creating online communities. Globalization fed through Internet connectivity has decreased the relevance of geographic boundaries, increased people's

[1] Douhet, Giulio, *The Command of the Air*, translated by Dino Ferrari (Washington, DC: Office of the Air Force History, 1983, originally published 1942).

[2] *Brave New World* is a futuristic novel written by Aldous Huxley in 1932 that dealt with contemporary issues of the 20th century stemming from the industrial revolution. The term *information age* has been defined as "The period beginning around 1970 and noted for the abundant publication, consumption, and manipulation of information, especially by computers and computer networks."; Norbert Weiner, *Cybernetics, or Control and Communication in the Animal and the Machine* (Cambridge, MA: MIT Press, 1948) "Cyber" is a prefix used to describe a person, thing, or idea as part of the computer and information age and/or related to the culture of computers, information technology, and virtual reality. The term stems from the word "cybernetics" used by Norbert Weiner derived from the Greek *kybernetes*, meaning "steersman" or "governor."

information reach and influence, and facilitated international interdependence. The ever-changing cyber domain continues to shape the modern world.

Cyber capabilities also underwrite modern warfare.[3] The cyber domain has become a recognized operational battlespace. Most modern weapon platforms (air, land, sea, and space systems) are cyber dependent. Modern fighting organizations assume the operational capability to function in cyberspace. Cyber influence and/or denial are evolving considerations in warfare, but cyber is not well understood in an operational context.[4] Currently, the United States, like all nations, is struggling to deal with cyber capabilities and vulnerabilities. The 21st century will likely continue to be a period of rapid change and contest where friendly, neutral, and enemy actors vie for cyber power, influence, and security. These realities require the United States to understand and develop effective cyber power employment as a means of modern and future warfare.

Nature of the Problem: Sub-optimal JFC Cyber Operationalization

In modern and future warfare, the Joint Force Commander (JFC) must skillfully and effectively leverage cyber power.[5] A JFC needs maximum integration and unity of effort in all domains (air, land, sea, space, and cyber) during operational planning and execution. Operations

[3] U.S. Department of Defense, *Department of Defense Strategy for Operating in Cyberspace* (Washington, DC: U.S. Department of Defense, July 2011), 1. This DoD strategy acknowledges, “DoD uses cyberspace to enable its military, intelligence, and business operations, including the movement of personnel and material and the command and control of the full spectrum of military operations.”

[4] Peter Finn, "Cyber Assaults on Estonia Typify a New Battle Tactic," *Washington Post*, May 18, 2007. This Washington Post article attributes a Russian concerted denial of service cyber-attack against Estonia; the author posits, “In the 21st century, the understanding of a state is no longer only its territory and its airspace, but it’s also its electronic infrastructure”; Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (New York, NY: Ecco, 2010) 1-8. Authors theorize that Israel cyber efforts mitigated air defense systems during raid on Syrian nuclear complex in 2007; James P. Farwell and Rafal Rohozinski, "Stuxnet and the Future of Cyber War," *Survival: Global Politics and Strategy* 53, no. 1 (2011): 23-40. Authors use the 2010 Stuxnet worm attack on Iranian nuclear facility to discuss cyber operational issues of attribution, risk of collateral damage, and strategic risks from potential escalatory responses.

[5] U.S. Joint Chiefs of Staff, *Doctrine for the Armed Forces of the United States.* Joint Publication 1 (Washington, DC: U.S. Joint Chiefs of Staff, March 25, 2013), I-7. A JFC is defined as “a general term applied to a combatant commander, subunified commander, or joint task force commander authorized to exercise combatant command (command authority) or operational control over a joint force.”

in the cyber domain must be integrated with other joint functions for mission assurance of combined and joint forces.[6] Cyber operations are a critical warfighting function; cyber capabilities and integrity are inherently required for modern military operations and have to be interdependent with all other joint functions.[7] Operations in cyberspace, by their very nature, can be overt (in clear view), clandestine (secret, but attributed eventually to operator after the operation), or covert (secret and not acknowledged). A JFC requires cyber power integration to ensure freedom of action, while denying the same advantages to an adversary during conflict. The JFC must engage cyber vulnerabilities and opportunities as responsively and effectively as engagements in other domains. Anecdotal evidence suggests, however, that the JFC is unable to assemble, coordinate, and integrate elements of cyber power within an operational design to employ a dominant, full spectrum capability. Significant but not insurmountable barriers to accomplishing this outcome exist in current doctrine, policy, and organizational relationships.

Current doctrine for cyber operations lacks cohesion and is descriptive rather than prescriptive. This limits its usefulness for JFC operational cyber power employment. Doctrinal publications, as well as concepts and processes on information, cyber, and spectrum operations,

[6] Air Force Research Laboratory, Dr. Sarah Muccio, "Cyber Mission Assurance," web page memo, http://www.wpafb.af.mil/shared/media/document/AFD-110516-046.pdf (accessed December 4, 2013). Mission assurance is attributed as “the number one goal in current cyber operations, versus the old paradigm of information assurance.” Assuming a contested cyber environment, mission assurance is described as correlating mission essential functions onto their cyber assets to identify mission dependence and protect potential vulnerabilities in cyberspace capabilities.; This thesis views *operationalization* as resulting in integrated cyber power as distinguished from *operations* that results in cyber capability production; this is viewed as the difference in focus on cyber outcomes and outputs.

[7] U.S. Joint Chiefs of Staff, *Joint Operations*, Joint Publication 3-0 (Washington, DC: U.S. Joint Chiefs of Staff, August 11, 2011), xiv. JP 3-0 states “Joint Functions are related capabilities and activities grouped together to help JFC’s integrate, synchronize, and direct joint operations.” The six joint functions—command and control (C2), intelligence, fires, movement and maneuver, protection, and sustainment—are interdependent with fully integrated cyber capabilities for mission success. Cyber confidentiality, integrity, and availability enables the other joint functions through their system capabilities and networks, but appears to be taken for granted in JP 3-0, Chapter III descriptions.

are splintered.[8] Significantly, cyber is not identified in joint doctrine as a joint function. These factors segment and constrain operational perspectives and prevent a JFC from planning and effectively employing cyber capabilities. The JFC is less interested in the arcane differences and distinctions that exist within the information-cyber-spectrum operational construct or their complex inter-relationships; instead, the JFC requires understanding of cyber power to gain an advantage from their integration and employment with other functions.[9] In short, the JFC is interested in the *operational possibilities of what can be done* with cyber power (from, within, and through the cyberspace mediums). From the JFC perspective, how cyber operations are employed and controlled is essential to their effective integration and success in operational warfare.[10]

Cyber policy, especially for operational warfighting, is still in early development. Law and policy for cyber operations is still evolving via dictate, precedence, or standards of practice. Authorization for cyber operations usually stems from either Title 10 or Title 50.[11] Policy and legal constraints for approving, synchronizing, and de-conflicting global and regional cyber operations are understood by only a few.[12] For the JFC, there are more questions than answers.

[8] Amongst Joint Publication (JP) 3-12 (Cyberspace Operations), 3-13 (Information Operations), JP 3-13.1 (Electronic Warfare), JP 3-13.2 (Military Information Support Ops), JP 3-60 (Joint Targeting), JP 6-0 (Joint Communications System), JP 6-01 (Electro-magnetic Spectrum Ops).

[9] Information/cyber/spectrum operational inter-relationships can be very convoluted. Information manipulation (ends) can come from cyber operations (ways) over the electromagnetic spectrum (means).

[10] Brett T. Williams, "Ten Propositions Regarding Cyberspace Operations," *Joint Forces Quarterly* 61 (2d quarter 2011): 11-17. The JFC's operational requirements have been recognized: "As I consider the ever-increasing scale, scope, and tempo of cyber activity compared to the warfighting needs of the joint force commander (JFC), it is obvious that treating cyber like space is a mistake. This thinking produces a global command and control model that is acceptable for peacetime 'enterprise' efficiency but is suboptimal for wartime. Global control does not provide the integration, responsiveness, and agility necessary for cyberspace at the theater level."

[11] From a legal perspective, intent of cyber operations (intelligence or military operations) may make a difference in authority required.

[12] Kyle G. Phillips, "Unpacking Cyberwar: The Sufficiency of the Law of Armed Conflict in the Cyber Domain," *Joint Forces Quarterly* 90 (3rd quarter 2013): 70-75. While the current legal framework is assessed as adequate to navigate operational cyber issues, many factors exist that complicate cyber ops decisionmaking: the state of conflict from a legal perspective, targeting and collateral damage considerations, dual-use military-civilian infrastructure, attribution of adversary cyber activity, and speed of action in the cyber domain to name a few.

The following excerpt from T*echnology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities* illustrates just one issue regarding the employment of a cyber capability:

> When to execute a cyberattack--what are the circumstances under which cyberattack might be authorized? Scope of a cyberattack--what are the entities that may be targeted? Duration of the cyberattack--how long should a cyberattack last? Notifications--who must be informed if a cyberattack is conducted? Authority for exceptions--what level of authority is needed to grant an exception for standing [Rules of Engagement] ROEs?[13]

These questions go to the heart of employing any cyber capability. These capabilities are not well known or understood outside a small group of experts.[14] Certainly, many commanders lack this understanding.[15] Further, these questions paralyze any attempt to integrate and synchronize cyber into a JFC's operational design.

Another significant condition limiting the JFC's integration of cyber is that the organization of U.S. cyber power is optimized for the strategic level under U.S. Cyber Command (USCYBERCOM), not the operational level. One analyst notes that, "U.S. STRATCOM's monopoly over planning and execution of cyberspace operations, as well as the structure and composition of the geographic command that must integrate cyberspace operations at the operational level, [is] suboptimal to creative operational design and integrated force

[13] William A. Owens, Kenneth W. Dam, and Herbert S. Lin, eds, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities* (Washington, DC: National Acadamies Press, 2009), 169. Used as formatted in Harry M. Friberg, *U.S. Cyber Command Support to Geographic Combatant Commands* (Carlisle Barracks: U.S. Army War College, March 2, 2011), 6.

[14] Martin Stallone, *Don't Forget the Cyber! Why the Joint Force Commander must integrate cyber operations across other war fighting domains, and how a Joint Force Cyberspace Component Commander will help* (Newport, RI: Naval War College, May 4, 2009), 12. Stallone notes, "Unlike land or maritime forces, cyberspace forces often come from outside the GCC in a manner that is secretive, poorly integrated, and confusing to those at the operational level."

[15] Brett T. Williams, *Cyberspace Operations*, USCYBERCOM/J3 presentation at the Joint Advanced Cyber Warfare Course in Linthicum, MD, June 25, 2013. USAF Major General Williams, USCYBERCOM J3 Director of Operations, noted, "…[for the most part] commanders don't understand cyber. This leads to either too-tactical guidance…or abrogation to the signal and [intelligence planners] who [many times] have no idea regarding planning, or haven't been involved in the planning process from the beginning. Apart from the [operators and] planning community, signal and [intelligence planners] weren't developed for it." Quote found in Jason M. Bender, "The Cyberspace Operations Planner: Challenges to Education and Understanding of Offensive Cyberspace Operations," *Small Wars Journal* 9, no. 11 (November 2013). http://smallwarsjournal.com/jrnl/art/the-cyberspace-operations-planner (accessed 14 November, 2013).

employment."[16] Another study that elicited opinions from the Geographic Combatant Commands (GCC) found other integration concerns:

> Many GCCs contend, a cyberspace operator at a cyber headquarters thousands of miles away will likely not understand the operational requirements necessary for integrated success in a particular [Joint Operational Area] JOA, let alone understand the local or regional commander's intent. There must be established, coordinated relationships to allow flexibility at the Joint Force Commander level while simultaneously protecting strategic/global interests.[17]

These concerns are not based on recent dysfunctionalities, but long-standing results of disparate cyber planning and execution processes. In 2007, a former USSTRATCOM commander discussed problems with coordinating cyber operations:

> Cyber operations [are] often cloaked behind a lot of green doors and 'I can't tell you this' and 'I'd like to tell you that'…[We] set expectations that are probably unrealistic…We launch "recce teams" out to see what's going on…we build a couple of attack teams over here, we make sure the "recce teams" don't tell the defenders what they found, or the attackers, and the attackers go out and attack and don't tell anybody that they did. It's a complete secret to everybody in the loop and it's dysfunctional. It's really got to change.[18]

USCYBERCOM established a goal to work with the combatant commands and the Services to synchronize plans and processing efforts to provide required joint cyber effects.[19] Associated efforts were made to improve coordination with geographic combatant commands (CCMDs) after specific command and control (C2) relationships had been identified as shortfalls.[20] Although specific C2 mechanisms and liaison personnel between USCYBERCOM

[16] Ibid., abstract.

[17] Brett Reister, *Cyberspace: Regional and Global Perspectives* (Carlisle Barracks, PA: U.S. Army War College, February 22, 2012), 20; Joint Chiefs of Staff, *Joint Operations*, JP 3-0, GL-12. A Joint Operational Area (JOA) is defined as "An area of land, sea, and airspace defined by a geographic combatant commander or subordinate unified commander, in which a joint commander (normally a joint task force commander) conducts military operations to accomplish a specific mission."

[18] James Cartwright, *Striking the Balance - Today's War, Tomorrow's Threats , Future Technology*, USSTRATCOM commander speech to Air Force Association in Orlando, FL, February 8, 2007. http://www.stratcom.mil/speeches/2007/4/AFA_Symposium/printable (accessed March 16, 2014).

[19] Keith B. Alexander, "Building a New Command in Cyberspace," *Strategic Studies Quarterly* 5 , no. 2 (2011): 3-4.

[20] U.S. Government Accountability Office, *Defense Department Cyber Efforts: More Detailed Guidance Needed to Ensure Military Services Develop Appropriate Cyberspace Capabilities*, by Davi M. D'Agostino, report GAO-11-421, 2011, http://www.gao.gov/assets/320/318604.pdf (accessed October 7, 2013), 14-15. This GAO

and the JFC have been initially established, none have been fully implemented.[21] In any case, while the relationship between USCYBERCOM, the GCC, and the JFC is not ideal, it is recognized that a "balance must be struck to allow measured GCC prioritized effects to be achieved supporting the [Unified Campaign Plan] UCP directed [Area of Responsibility] AOR specific mission; along with similarly measured, consolidated, globally focused prioritized effects to be achieved in support of CYBERCOM's worldwide offensive and defensive mission as well."[22] It is clear that the essential problem of the difficulty integrating JFC cyber warfighting is recognized, but not understood or appreciated; no solutions are forthcoming. This impasse threatens the employment of cyber power and limits the effectiveness of the operational commander at both the theater and JFC levels. No standard cyber vision or conceptual structure exists to help shape JFC operational art and design activities or functional relationships in executing combat operations.

Under USCYBERCOM operational control, the cyber joint force is currently too small to support operational commands. It is split between service specialties, suffers from shortfalls in

report states that "more detailed guidance" is needed to clarify C2 support relationships between USCYBERCOM and the geographic CCMDs; U.S. GAO, *Defense Department Cyber Efforts: DOD Faces Challenges In Its Cyber Activities*, by Davi M. D'Agostino and Gregory C. Wilshusen, report GAO-11-75, 2011, http://www.gao.gov/new.items/d1175.pdf (accessed October 7, 2013), 8. This GAO report finds, "Without complete and clearly articulated guidance on command and control responsibilities that is well-communicated and practiced with key stakeholders, DoD will have difficulties in achieving command and control of its cyber forces globally and in building unity of effort for carrying out cyber operations."

[21] U.S. Joint Chiefs of Staff, *Joint Cyberspace Operations*, Joint Publication 3-12 (Washington, DC: U.S. Joint Chiefs of Staff, February 5, 2013), III-6. Cyberspace Support Elements are currently provided to CCMDs from USCYBERCOM to facilitate development of cyberspace requirements and coordinate, integrate, and deconflict cyberspace operations into the command's planning process; U.S. GAO, *Defense Department Cyber Efforts*, 15. Cyber C2 relationships are presented and explained based on Joint Task Force, USSOCOM, and USTRANSCOM models; Michael Hudson, "Cyber Workforce Development: Trained and Ready Cyber Teams," USCYBERCOM/J72 Training & Readiness Division briefing to Armed Forces Communications and Electronics Association (AFCEA), June 27, 2013. From Google search (accessed February 6, 2014). A note from slide 4 of the USCYBERCOM brief describes how Cyber Combat Mission Forces (CCMFs) are being deployed to CCMDs to replace Cyber Support Elements and liaison officers. CCMFs are to strengthen C2 by "conducting cyber target development in support of CCMD operations plans and, when authorized, assisting in the delivery of cyber effects against CCMD prioritized targets. The teams will also assess cyber tool delivery and effectiveness."

[22] Reister, *Cyberspace: Regional and Global Perspectives*, 22-23.

standardized training, and lacks experience.[23] Military leaders and CYBERCOM recognize the need for improved readiness for cyber capabilities and have allocated resources to improve the cyber joint force.[24] Nevertheless, the organizational, systemic, functional specialty, and authority barriers are significant. In addition, current cyber employment theory and experimentation is nascent, especially for employment at the operational level.[25]

Targeting the Problem: Structuring Cyber for JFC's Operational Effectiveness

JFCs do not have a conceptual and pragmatic mission-focused construct for planning, employing, and leveraging available cyber power in concert with other existing capabilities to develop a modern operational warfare approach. At this point, the JFC lacks the integration means to think about and apply cyber power. Cyber capabilities need to be planned for, coordinated, and employed from Phase I to Phase V as part of an integrated operational plan. To do this, a cyber operationalization framework is needed with which to shape JFC operational art and operational design to meet the requirements of modern warfare.

A cyber operationalization framework could help the JFC conceive the effective employment of cyber (through the operational art) and structure cyber operations (within the

[23] U.S. GAO, *Defense Department Cyber Efforts*, 18. As of 2011, a GAO report notes, "In the absence of requirements from U.S. Cyber Command, the services have started to develop their own cyber training programs geared toward service-specific cyberspace requirements and attempts to anticipate the future needs of U.S. Cyber Command."

[24] Stimson, *Strategic Agility: Strong National Defense for Today's Global and Fiscal Realities* (Washington, DC: The Stimson Center, September 2013), http://www.stimson.org/images/uploads/research-pdfs/Strategic_Agility_Report.pdf (accessed November 12, 2013). A Defense Advisory Committee from retired joint leaders petitioned for a $50B reduction in cuts and saving in FY15 to respond to fiscal realities, while at the same time advocating a $1.2B increase to the $4.7B requested in FY14 in order to "Increase Resources for Offensive and Defensive Cyberwarfare by 25 percent"; Christina Ortiz, "U.S. Cyber Command to Recruit 4,000 new Cyber Soldiers," *ReadWrite.com*, January 31, 2013. http://readwrite.com/2013/01/31/us-cyber-command-to-recruit-4-000-cyber-soldiers#awesm=~oxGPQt9EGW4KyK (accessed February 15, 2014). Web site notes Pentagon announcement to increase U.S. Cyber Command from 900 military and civilians by 4,000 "cyber soldiers."

[25] Stuart H. Starr, "Toward an Evolving Theory of Cyberspace," *Cryptology and Information Security Series (The Virtual Battlefield: Perspectives on Cyber Warfare),* 2009: 18-52; Colin Gray, *Making Strategic Sense of Cyber Power: Why the Sky is Not Falling* (Carlisle Barracks: U.S. Army War College (Strategic Studies Institute), April 2013), iii. The Foreword notes, "Cyber is now recognized as an operational domain, but the theory that should explain it strategically is very largely missing"; Modelling & Simulation Journal, "Cyber Warfare is No Computer Game," *M & S Journal,* 2013: 1-48. Need for more cyber experimentation is a recurring theme in multiple articles.

operational design). Like any other capability, cyber operations need to be aligned with the commander's operational concept and intent. Like other capabilities, cyber operations and activity lanes will have to be de-conflicted and pre-coordinated to ensure unity of effort and unified action. Like other capabilities, specific cyber operations need to be optimized across all campaign phases with a common understanding of how these actions leverage decisive point advantage, influence the operational or strategic centers of gravity, and how they support achieving the operational objectives. Cyber operations must also be clearly understood in terms of their role in the transition to each phase in the operation. Finally, like other capabilities, cyber operations must be resourced with the proper technology (systems), expertise (manning), and rules of engagement (integration) to enable effective employment. This thesis intends to propose a framework for operationalizing cyber planning and executing joint cyber activities at the operational level. The exploration of cyber operationalization targets JFCs and their staffs for the purpose of considering the best way to integrate cyber power as an additional capability available to the joint force to support operational level mission planning and execution.

Approach to Research Cyber Operationalization

What is an operational cyber framework? How would such a framework support JFC missions? Figure 1 presents a model to illustrate the concept of cyber operationalization. The model depicts cyber operationalization as drawing from four cyber elements (environment, command and control, weapon systems, and operator).

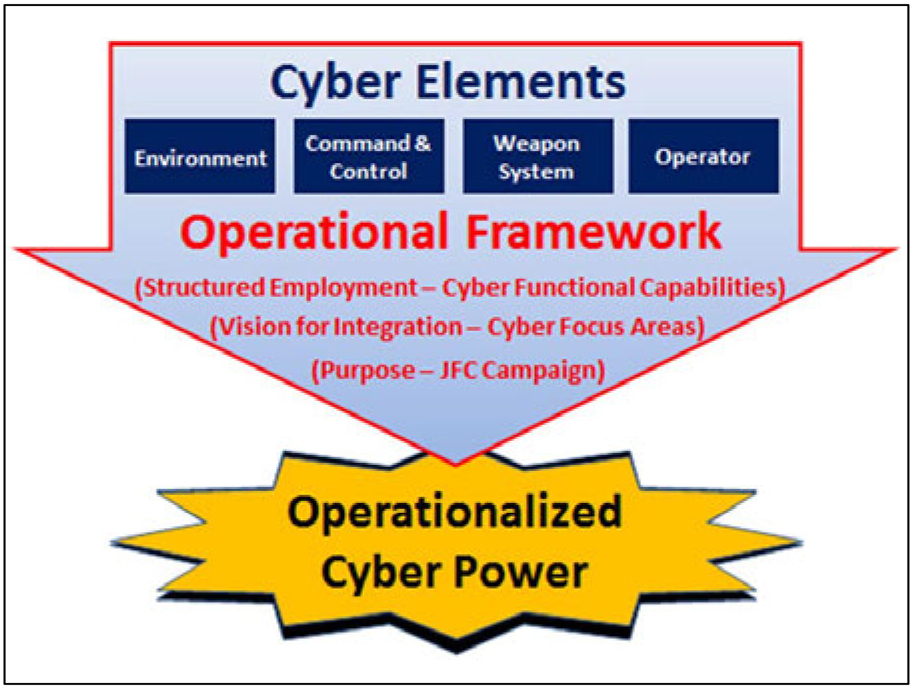

Cyber Elements
Environment
Command & Control
Weapon System
Operator
Operational Framework
(Structured Employment – Cyber Functional Capabilities)
(Vision for Integration – Cyber Focus Areas)
(Purpose – JFC Campaign)
Operationalized Cyber Power

Figure 1. Model for Cyber Operationalization

For the purpose of this thesis, the *environment* is the cyberspace domain (to include the infosphere), the physical area of operations or AOR, and the associated information available to the JFC.[26] The cyberspace domain should be considered as part of the JFC's battlespace.[27] *Command and control* involves the authority to use cyber power, as well as the organizational processes associated with conducting cyber operations. The *weapon system* refers to cyber systems, hardware, and software used to influence the cyber environment. The *operator* is the cyber joint force representative who employs the systems within the environment under a C2 structure to achieve a decisive influence on the enemy as part of the JFC's operational design and

[26] Shmuel Even and David Siman-Tov, *Cyber Warfare: Concepts and Strategic Trends*, white paper (Memorandum 117), (Tel Aviv: Institute for National Security Studies, May 2012), 10. http://mercury.ethz.ch/serviceengine/Files/ISN/152953/ipublicationdocument_singledocument/f3e19de1-bcf7-4d07-b088-f3d477b4329c/en/INSS+Memorandum_MAY2012_Nr117.pdf (accessed November 5, 2013). Cyberspace is described as three (human, logical, and physical) interdependent layers; *infosphere* is defined by www.dictionary.com as "The global network of military and commercial command, control, communications, and computer systems used in carrying out a mission."

[27] George J. Franz III, "Effective Synchronization and Integration of Effects Through Cyberspace for the Joint Warfighter," USCYBERCOM Director of Current Operations briefing to AFCEA, on August 14, 2012. Slide 6 of USCYBERCOM brief shows the joint cyberspace domain as interlinked people, cyber identities, information, physical infrastructure, and geography associated with cyber operations.

intent. Within an operational design, cyber effectively integrates the four elements with other joint functions providing a full-spectrum, synchronized operational schema that supports the JFC's mission in each phase.

Thesis and Paper Structure

This paper's thesis is that the JFC needs a unifying cyber framework with which to shape operational art and operational design to support mission planning and execution. The cyber operationalization model in Figure 1 can provide the JFC with an approach to facilitate planning for cyber power to integrate a cohesive and responsive cyber campaign into the overall operational approach. For purposes of this paper and to ease illustration, the JFC cyber operationalization model will focus only on overt cyber activities and capabilities that are addressed later in Chapter 4. While official joint cyberspace doctrine is classified, integration and synchronization of cyberspace effects requires bringing together planning, warfighting, and cyber execution capabilities elements in the cyber domain.[28]

Chapter two provides foundations for a JFC cyber framework and outlines requirements for framing, planning, and executing cyberspace operations. Chapter three provides the framework for JFC cyber operations to answer the question: What does a cyber-integrated campaign look like? This thesis proposes JFC cyber operations structured around four concepts: spectrum penetration and control, cyber protection and fires, virtual coalition, and strategic cyber messaging. Chapter four analyzes the JFC cyber framework considering the cyberspace environment, command and control, weapon systems, and the operators who plan and perform in the campaign environment to answer the question: How does a JFC integrate cyber as part of operational design? Integration of technology, experience, and resources for JFC cyber

[28] Joint Publication 3-12, Cyberspace Operations; Franz, "Effective Synchronization and Integration of Effects Through Cyberspace for the Joint Warfighter," slide 5.

operationalization are assessed. Chapter five provides thesis conclusions, assessment of operational relevance, and recommendations pursuant to applying cyber power to JFC campaigns. A notional phased JFC cyber campaign based around the thesis framework is described in the subsequent appendix.

Applying cyber power within a cyber domain understood as fully as other domains is essential to current and future operational level warfare. *Operationalization* of domains is essential to successful military campaigns.[29] For such operationalization, a commander-centric operational approach is essential to mission effectiveness. The JFC must be able to fully shape and employ cyber power; today's modern warfare requirements demand prepared and equipped cyber offenses, defenses, and support. The JFC and his staff must be as comfortable with employing cyber power as with employing any other capability.[30] Moreover, the JFC must appreciate the new dimensions that cyber opens to support operational design. Cyber has been too dark for too long.

[29] The German Blitzkrieg lightning war operationalization unleashed in World War II to overwhelm European defenders is one such example. Taken separately, tanks, dive bombers, radio communications and internal organic command and control were developed individually. What was original, innovative, and revolutionary to land domain manuever warfare was ***operationalization***—how the technology, expertise, and rules of engagement were fully integrated in Blitzkrieg for optimized operations and maximum effectiveness.

[30] Rosemary Carter, "Offensive Cyber for the Joint Force Commander: It's Not That Different," *Joint Forces Quarterly* 66 (3rd quarter 2012): 25. The author makes a similar case: "The commander and his staff must fully understand both the friendly and adversary cyber domains to the same degree they understand the other domains."

CHAPTER 2

Joint Force Commander Cyber Foundations

"There is no type of human endeavor where it is so important that the leader understands all phases of his job as that of the profession of arms."

Major General James C. Fry, United States Army

"There is no exaggerating our dependence on DoD's information networks for command and control of our forces, the intelligence and logistics on which they depend, and the weapons technologies we develop and field. In the 21st century, modern armed forces simply cannot conduct high-tempo, effective operations without resilient, reliable information and communications networks and assured access to cyberspace."[1]

2010 Quadrennial Defense Review

How a JFC Conducts an Operational Campaign

The JFC's assigned missions may vary widely across the possible range of military operations. The scale and purpose of the joint forces employed may vary as well. These missions may involve military engagement, security cooperation, and deterrence activities that establish, shape, maintain and refine relations with other nations.[2] A JFC might be tasked with crisis response missions, or performing limited contingency operations, or the JFC may be responsible for planning and executing major operations and campaigns.[3] In all of these roles, the JFC's focus is determining best use of assigned forces at the operational level of warfare to

[1] Robert M. Gates, *Quadrennial Defense Review* (Washington, DC: U.S. Department of Defense, February 2010), 37. Quote from under heading "Operate Effectively in Cyberspace."

[2] U.S. Joint Chiefs of Staff, *Doctrine for the Armed Forces of the United States,* JP 1, I-15.

[3] Ibid., I-15-16. JP 1 states, "A crisis reponse or limited contingency operations can be a single small-scale, limited-duration operation or a significant part of a major operation of extended duration involving combat." JFC roles are detailed, "When required to achieve national strategic objectives or protect national interests, the US national leadership may decide to conduct a major operation or campaign involving large-scale combat. In such cases the general goal is to prevail against an enemy as quickly as possible, conclude hostilities, and establish conditions favorably to the US and its interorganizational partners. Major operations and campaigns feature a balance among offensive, defensive, and stability operations through six phases: shape, deter, seize initiative, dominate, stabilize, and enable civil authority."

achieve mission objectives. Ultimately, the JFC is responsible for effectively integrating joint force ends, ways, and means.[4] The JFC's focus at the strategic-operational level is further described in JP 1:

> The operational level links strategy and tactics by establishing operational objectives needed to achieve the military end states and strategic objectives. It sequences tactical actions to achieve objectives. The focus at this level is on the planning and execution of operations using operational art: the cognitive approach by commanders and staffs—supported by their skill, knowledge, experience, creativity, and judgment—to develop strategies, campaigns, and operations to organize and employ military forces by integrating ends, ways, and means. JFCs and component commanders use operational art to determine when, where, and for what purpose major forces will be employed and to influence the adversary's disposition before combat. Operational art governs the deployment of those forces and the arrangement of battles and major operations to achieve operational and strategic objectives.[5]

Ultimately, the JFC is the central figure for operational art and design that structures vision into plans and execution to accomplish assigned missions.[6]

A JFC may design and focus operations within campaigns to achieve unified action and unity of effort in defeating adversary forces, functions, or a combination of both.[7] The JFC accomplishes this result through a phasing construct, which "helps the JFC organize large operations by integrating and synchronizing subordinate operations. Phasing helps JFCs and staffs visualize, design, and plan the entire operation or campaign and define requirements in terms of forces, resources, time, space and purpose."[8]

[4] Arthur F. Lykke, "Toward an Understanding of Military Strategy," in *Military Strategy: Theory and Application* (Carlisle Barracks, PA: U.S. Army War College, 1993), 3-8. Lykke's strategic framework might be expressed Strategy = Ends + Ways + Means. Lykke advocated for balancing of ends (i.e. end states of operations or strategy), ways (i.e. methods and processes executed to achieve the ends), and means (i.e. resources needed to execute the ways).

[5] U.S. Joint Chiefs of Staff, *Doctrine for the Armed Forces of the United States*, JP 1, I-8.

[6] U.S. Joint Chiefs of Staff, *Joint Operations*, JP 3-0, xiii.

[7] U.S. Joint Chiefs of Staff, *Joint Operation Planning*, Joint Publication 5-0 (Washington, DC: U.S. Joint Chiefs of Staff, August 11, 2011), III-38.

[8] U.S. Joint Chiefs of Staff, *Joint Operations*, JP 3-0, V-5; U.S. Joint Chiefs of Staff, *Joint Operation Planning*, JP 5-0, III-36 adds, "Phasing is a way to view and conduct a complex joint operation in manageable parts. The main purpose in phasing is to integrate and synchronize related activities, thereby enhancing flexibility and unity of effort during execution."

The current common construct for phasing is Phase 0 through V: Phase 0 – Shape; Phase 1 – Deter; Phase II – Seize Initiative; Phase III – Dominate; Phase IV – Stabilize; Phase V – Enable Civil Authority.[9] The phasing model for current U.S. doctrine is designed to provide flexibility to arrange combat and stability operations as scenarios change.[10] Each of these phases is separate and distinct from each other in time, space, and purpose, but they must be conceived and planned collectively to align resources and activities to achieve a decisive result. Phases are linked in order to achieve larger JFC operational and strategic objectives. The JFC will coordinate and synchronize activities in all domains (land, sea, air, space, and cyberspace) in order to maximize goals in each phase and progress to the next phase. Both Joint Publication 3-0 and 5-0 describe phasing and transition that would be part of a JFC's campaign.[11]

How Cyber Capabilities are Currently Envisioned to Support a JFC

Currently, the responsibilities and authorities for warfighting within cyberspace are shared between United States Cyber Command (USCYBERCOM), a functional sub-unified combatant command under United States Strategic Command (USSTRATCOM), and geographic combatant commands.[12] USSTRATCOM via USCYBERCOM directs defense of specified DoD network and supports cyber operations for the geographic combatant commanders (CCDRs) and JFCs.[13] In addition, Combat Support Agencies (CSAs), like the National Security Agency and

[9] See Appendix for details regarding campaign phasing.

[10] U.S. Joint Chiefs of Staff, *Joint Operation Planning*, JP 5-0, III-39. Phasing model is shown.

[11] U.S. Joint Chiefs of Staff, *Joint Operations*, JP 3-0, V-5 throughV-9; U.S. Joint Chiefs of Staff, *Joint Operation Planning*, JP 5-0, III-41.

[12] Although, currently, there is much high-level discussion about making USCYBERCOM a functional combatant command in its own right.

[13] U.S. Joint Chiefs of Staff, *Doctrine for the Armed Forces of the United States*, JP 1, III-10. U.S. Strategic Command is the functional component command for synchronizing planning for cyberspace operations; U.S. Department of Defense Office of Public Affairs, *U.S. Cyber Command Fact Sheet* (Washington, DC: U.S. Department of Defense, May 25, 2010). USCYBERCOM mission statement: "USCYBERCOM plans, coordinates, integrates, synchronizes, and conducts activities to: direct the operations and defense of specified Department of Defense information networks and; prepare to, and when directed, conduct full-spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries."

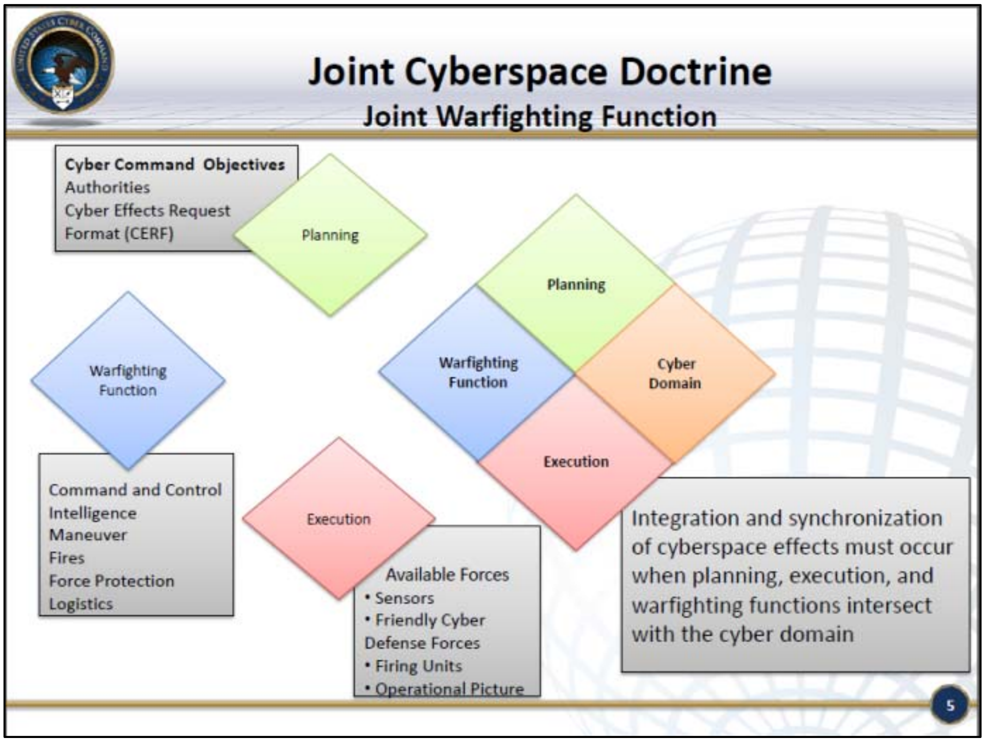
Defense Information Systems Agency, are directed to support CCDRs.[14] CCDRs have COCOM authority to organize, employ, and assign commanders and forces to carry out command missions.[15] As such, the CCDR should be able to assign cyber capabilities and delegate authority (including the ability to reorganize and employ them in an AOR) to a subordinate commander, such as a JFC.[16] The JFC, in turn, has considerable influence and control in determining how joint cyber forces are organized, presented, and employed within their theater and JOA in order to accomplish assigned missions depending on the C2 relationships.

By these descriptions, USCYBERCOM is a force provider for cyber capabilities and effects to the JFC within the cyber domain. The JFC as the supported commander in a campaign should receive all assistance required in order to execute assigned missions or campaign objectives. Figures 2 and 3 below show how USCYBERCOM envisions integration and synchronization of cyber operations. Figure 2 shows a responsibility view on cyber operations from USCYBERCOM's perspective. Figure 3 depicts a USCYBERCOM targeting cycle "in support of a Joint Force Commander."

[14] Ashton B. Carter, "Department of Defense Directive 3000.06, Combat Support Agencies (CSAs)," Deputy Secretary of Defense Policy Directive (Washington, DC, June 27, 2013). http://www.dtic.mil/whs/directives/corres/pdf/300006p.pdf (accessed October 10, 2013). Para 3.d. states that "The relationship between a CSA and a CCMD is support…with the CSA typically operating in a supporting-to-supported relationship relative to the CCDRs…A CCDR may modify the support relationship to that of direct support to a subordinate unit within the CCMD. The CCDR may also give authoritative direction regarding the CCDR's requirements to CSAs supporting the CCDR's military operations. CSAs typically operate in a supporting-to-supported relationship relative to the CCDRs."

[15] U.S. Joint Chiefs of Staff, *Doctrine for the Armed Forces of the United States*, JP 1, III-7. Authority, direction, and control of the commander of CCMD, with respect to the commands and forces assigned to that command are specified in Title 10, USC, Section 164.

[16] Ibid.



Joint Cyberspace Doctrine

Joint Warfighting Function

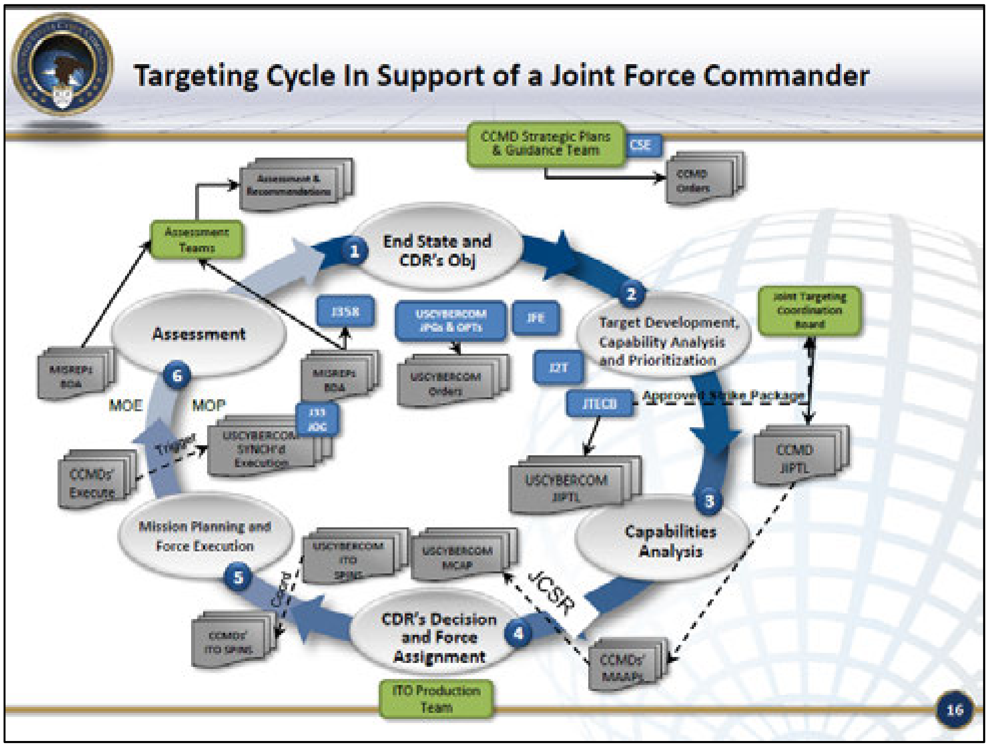
Cyber Command Objectives
Authorities
Cyber Effects Request Format (CERF)

Command and Control
Intelligence
Maneuver
Fires
Force Protection
Logistics

Available Forces
- Sensors
- Friendly Cyber Defense Forces
- Firing Units
- Operational Picture

Integration and synchronization of cyberspace effects must occur when planning, execution, and warfighting functions intersect with the cyber domain

Figure 2. Integration and Synchronization of Cyber as Warfighting Function[17]



Targeting Cycle In Support of a Joint Force Commander

Figure 3. USCYBERCOM Targeting Cycle[18]

[17] Franz, "Effective Synchronization and Integration of Effects Through Cyberspace for the Joint Warfighter," slide 5.

[18] Ibid., slide 16.

Disconnects in Understanding Employment of Cyber Capabilities

In Figure 2, the distribution of cyber operational planning seems to be heavily skewed toward USCYBERCOM, leaving the JFC not as the employer of forces, but as a cyber subscriber or requester. Notice also in Figure 2 how "Planning" is couched in strictly production or output terms where cyber effects are requested (using Cyber Effects Request Format) and approved.[19] USCYBERCOM clearly plans for cyber capabilities when requested; it does not function as a force provider, planning for deployment of capabilities to the JFC. Figure 3 shows a highly involved USCYBERCOM targeting cycle supporting a JFC (e.g. a combatant command, CCMD) based on orders. The highly controlled process within USCYBERCOM provides discreet targeting on an on-call basis. However, this cycle assumes that the JFC will be knowledgeable enough to be able to make ad hoc targeting decisions, relay a timely request to USCYBERCOM, and the JFC reacts based on the results. If such a concept was applied to any other capability, such as special operations, the defects in this approach would be obvious. Yet, because cyber is still an underappreciated element of warfare, the constraints this model places on the JFC are not immediately obvious. This USCYBERCOM model of operations prevents the JFC from including cyber capabilities in the operational design, limiting its use and effectiveness. It forces the JFC to be dependent upon a separate independent headquarters to provide capabilities that have indeterminate effects that may or may not be related to the commander's operational approach. It assumes expertise and knowledge where there is none. Operationalizing cyber power is more than effective targeting.

A JFC needs a mission-focused construct for planning and leveraging available cyber power at the operational level. This includes conceiving (cyber included in operational art and

[19] Ibid., slide 4 justifies this approach as USCYBERCOM needing to "maintain strategic and tactical understanding of the military cyberspace domain that informs operational risk decision, support current action, and does not interfere with ongoing operations."

design), organizing and employing cyber forces in the JOA, and integrating cyber capabilities throughout all campaign phases.

Guiding Concepts for JFC Employment of Cyber Capability

If the JFC is to be able to employ cyber capabilities effectively, there must be doctrinally sound governing principles established to guide understanding, planning, and employment of cyber within the operational approach.[20] Doctrine, technology, people and processes should be integrated to achieve synergy and decisive results. Thus, the JFC's operational cyber campaign should be guided by the following concepts:

1.) Use cyber and information focus areas to achieve the JFC's operational-strategic objectives. The cyber capabilities should help achieve the JFC's objectives within a coherent, integrated, phased, and synchronized operational plan. The operational tempo and scale of cyber operations should be driven by the conditions the JFC faces, not by USCYBERCOM.

2.) Align cyber activities with the theater strategy and with other JOAs and domains. The responsiveness and effectiveness of cyber operations should contribute to unity of effort and synergy with other operational activities in air, sea, land, and space supporting, where possible, theater as well as JFC outcomes. JFC cyber operations should be consistent with tenets of interagency, coalition, and U.S. cyber strategy.

[20] Brett T. Williams, "Ten Propositions Regarding Cyberspace Operations," *Joint Forces Quarterly* 61 (2^{d} quarter 2011): 11-17. Many of the proposed concepts incorporate ideas based on USAF Major General William's 10 cyber propositions: 1. Cyberspace is a warfighting domain. At the operational level of war, cyberspace operations are most similar to those in land, maritime, and air; 2. The JFC must have C^2 of cyberspace, just as he does of the terrestrial domains; 3. C^2 of cyberspace is the key enabler for exercising operational command and control; 4. Defense is the main effort in cyber at the operational level of war; 5. Cyber is the only manmade domain. We built it; we can change it. Creating a cyber JOA is the first requirement; 6. Cyberspace operations must be fully integrated with missions in the physical domains; 7. The JFC must see and understand cyberspace to defend it—and he cannot defend it at all; 8. Networks are critical and will always be vulnerable—disconnecting is not an option. We must fight through the attack; 9. Our understanding of nonkinetic effects in cyberspace is immature; 10. Understanding operational impact is the critical measure of cyberspace engagments.

3.) Incorporate regional theater expertise and integrate intelligence, information technology, and operations expertise. Human capital interactions are critical to planning and operations. A wide range of campaign planning and subject matter experts local to JFC and from USCYBERCOM must collaborate to fully exploit cyber operational benefits.

Cyber operations and effects may be geographically independent, but local knowledge is very important to cyber operational employment and approach. Embedded geographic theater experience regarding networks (both human threat networks and technical networks), local intelligence (to include coalition partner information sharing), and culture is critical to the success of cyber operations. Without regionally focused expertise, cyber operations could suffer from lack of understanding of the local operational environment, the consequences (first and second order effects of cyber actions), the behavior of neutral and adversary parties, and the influence on the JFC's mission. Incorporation of theater expertise into a JFC's cyber campaign will also bolster trust in its goals and employment. These contributions from the JFC's local staff will inform and vector integrations of direct support from USCYBERCOM.

4.) USCYBERCOM provides tools and coordination in direct support. JFC cyber operational campaigns must be de-conflicted with other cyber operations. And, if proper authority has been granted at the operational level, cyber activities should be shared with friendly forces. Cyber planning and employment should be shaped by the CCDR and JFC to support theater objectives. USCYBERCOM provides direct support with cyber operations to integrate with JFC intent and Combat Support Agency (CSA) contributions.

5.) Cyber is a weapon system. Hardware and/or software designed for cyber operations that is capable, sustainable, defensible, and upgradeable is valuable for system standardization. Also, a defined weapon system usually has a planned logistics support structure and training requirement. Personnel make the weapon system work. Personnel who are assigned to the JFC's cyber campaign should have specialized knowledge on cyber systems, the operational environment, the planning and execution processes, and interactions required by the CCMD and JFC. Personnel must be developed and assigned to allow shared cyber expertise between Service requirements and JFC operations.

6.) Perform cyber activities at the operational level under both Title 10 (military action) and Title 50 (intelligence). Cyber activities will be just one facet of JFC decision making and must integrate other operations and plans. The JFC's cyber capabilities must have the authority for operations. Cyber campaign operations will be fluid. Exploitation windows may be fleeting. The dynamic security imperatives of the modern battlespace demand the authority to make decisions and responsively execute plans.

7.) Ensure affordability (in terms of money and personnel). One of the advantages of cyber operations is that associated technology is relatively inexpensive. System requirements of hardware, software, network interfaces and associated development must be kept at financially sustainable levels.

Each of these cyber parameters is important either in terms of ensuring operational effectiveness or long term viability. These guiding concepts can serve as solution set boundaries for a cyber framework focused on the JFC.

CHAPTER 3

Categorizing and Applying Cyber Operations to the JFC Campaign

"[C]yberpower…is the ability to use cyberspace to create advantage and influence events in all operational environments and across the instruments of power."[1]

Dr. Daniel T. Kuehl

"[C]yber power is the ability to do something strategically useful in cyberspace"[2]

Colin Gray

Proposing a JFC Cyber Operationalization Framework

For cyber power to be focused properly, an operationalized cyber framework must exist to provide an actionable vision for integrating cyber capabilities for the JFC.[3] To do so, it must be inclusive enough so that the JFC can apply the cyber domain effectively. It must also ensure that structured activity can reasonably tie resources to purpose in processes that are repeatable and sustainable. JFC cyber operationalization must link operational and strategic plans and must allow for national, COCOM, interagency, and coalition cyber activity interfaces. To be advantageous, an operationalized cyber framework should provide a lasting benefit in a fluid, ever-changing technical backdrop, while supporting purposeful actions and effects at the JFC level.

The cyber framework categorizes capabilities into JFC focus areas in order to help a JFC think about what, when, and why cyber operational activities should be employed. Cyber focus

[1] Daniel F. Kuehl, "From Cyberspace to Cyberpower: Defining the Problem." In *Cyberpower and National Security* (Washington, DC: National Defense University Press, 2009), 38.

[2] Gray, *Making Strategic Sense of Cyber Power*, 9.

[3] Cyber capabilities should be considered as ability to project *end* effects via cyber system, personnel, and process *means*.

areas are conceived to target JFC objectives directly and improve the operating environment in favor of the JFC. The proposed JFC cyber operationalization framework provides four focus areas: *Spectrum penetration & control*, *cyber fires and protection*, *virtual coalition*, *and strategic cyber messaging*. JFC cyber focus areas seek to leverage cyber power in terms of purpose, structured activity, and best JFC effect. And, all are specific enough to derive intent, organize improvements, and measure progress toward JFC goals. Each of these focus areas relates to an area of interest to the JFC tied to inherent portions of the cyberspace domain (whether physical, logical, or human). While cyber-related, none of these JFC focus areas dictate a particular technology or advocate template solutions. The technology, organizational experience, and techniques/tactics/procedures (TTPs) are to be applied as needed within the framework to meet the JFC's requirements.

JFC Cyber Focus Area: Spectrum Penetration and Control

The idea for this focus area is to *dominate the spectrum at a time and place of the JFC's choosing in line with the commander's operational approach and intent*. Operations in the electromagnetic spectrum (EMS) are not new.[4] However, spectrum operations can be a challenge; the U.S. has not yet perfected spectrum operations or management of the spectrum.[5] The electromagnetic spectrum should be understood in operational terms as a contested medium for both information collection capabilities and information-dependent capabilities. The JFC must use the physical spectrum as cyber maneuver space for friendly protection and facilitation, as well as to deny the space to adversaries. (See Figure 4 for a depiction of the JFC's

[4] U.S. Joint Chiefs of Staff, *Joint Electromagnetic Spectrum Management Operations*, Joint Publication 6-01 (Washington, DC: U.S. Joint Chiefs of Staff, March 20, 2012), vii. JP 6-01 states, "All modern forces depend on the EMS. The EMS is a physical medium through which joint forces conduct operations."

[5] Ibid., V-1 highlights, "Based on lessons learned in Iraq and Afghanistan, a lack of adherence to SM [spectrum management] integration coupled with a lack of real-time SM, had an adverse effect on friendly communications."

electromagnetic spectrum environment). The JFC needs a complete understanding of this environment to operate effectively on the modern and future battlespace. Operationally, the JFC must be able leverage frequencies, electromagnetic energy, and system signals in a contested environment to enable forces and capabilities. The JFC's forces and systems must be able to penetrate and control this spectrum to succeed.

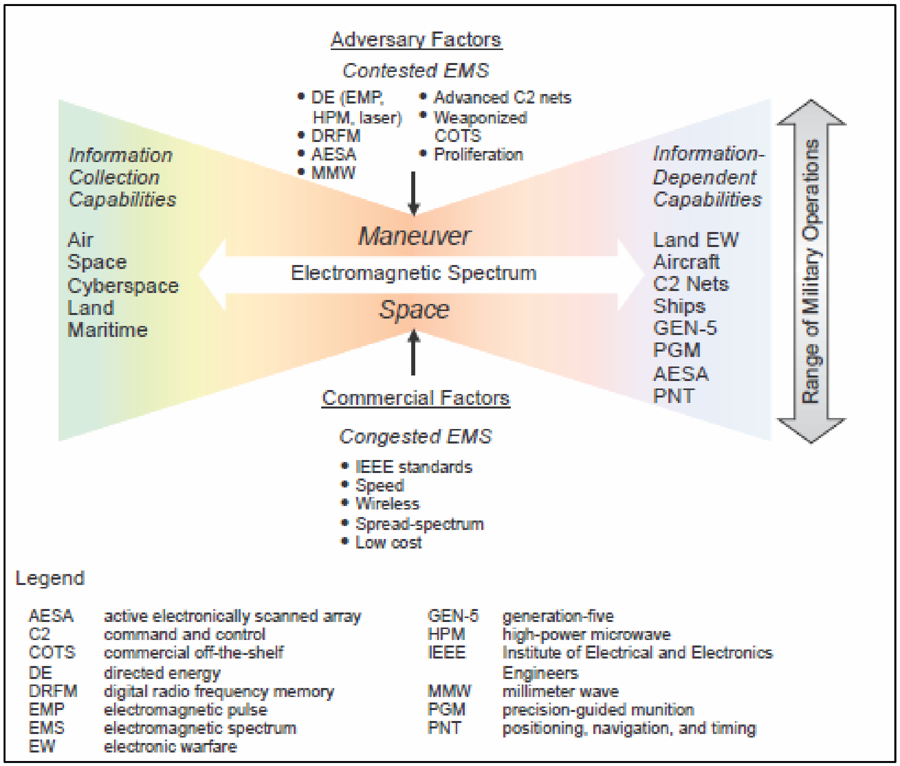


Figure 4: The JFC's Electromagnetic Spectrum Environment[6]

Both ***spectrum penetration and control*** are necessary for wireless cyber activities and terrestrial, aerial, and space networks. Spectrum penetration and control has two inter-related elements within the time and space considerations of JFC operations. Penetration refers to the JFC's capability to operate forces and cyber activities effectively within the spectrum of a physical AOR. Control refers to the JFC's need to dominate, manage or influence the spectrum in support of a specific action.

[6] Ibid., I-2. Figure 4 title was adapted to show JFC's perspective. It was originally titled, "Electromagnetic Spectrum Constraints on Military Operations."

Specifically, spectrum penetration and control would be necessary for, and underwrite, Air Force proposed strategic vision for a Single Integrated Network Environment (SINE).[7] The SINE stated objective is to "seek a single integrated network [environment] encompassing air, terrestrial, and space layers that is managed and commanded/controlled…and that is fully compatible with a seamless DoD network."[8] The AFNet 2025 Operational View (OV-1) shown in Figure 5 is provided as an example of a warfighting environment for the JFC:

> Today's warfighter requires a dynamically configurable, defendable environment to protect mission critical systems that support operational plans and strategies. Systems within cyberspace must be operated and maintained with the rigors of a warfighting system to satisfy critical mission needs. Likewise the SINE architecture must be based on operational requirements of the Joint Force Commander. This includes providing the warfighter with robust network operations and network defense capabilities based on seamless and secure connectivity and information system access across terrestrial, aerial, and space network.[9]

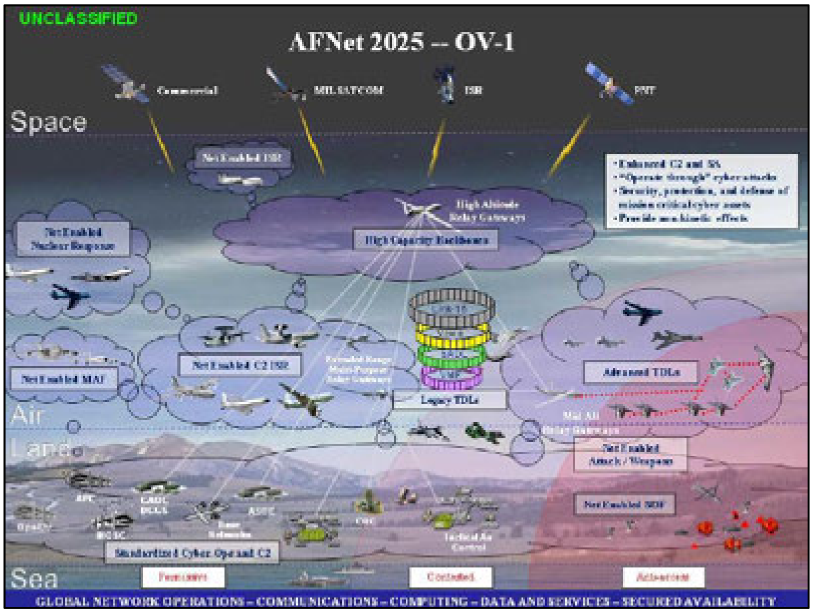

UNCLASSIFIED
AFNet 2025 – OV-1
Commercial
MILSATCOM
ISR
PNT
Space
Net Enabled ISR
High Altitude Relay Gateways
High Capacity Backbone
•Enhanced C2 and SA
•"Operate through" cyber attacks
•Security, protection, and defense of mission critical cyber assets
•Provide non-kinetic effects
Net Enabled Nuclear Response
Net Enabled MAF
Net Enabled C2 ISR
Extended Range Multi-Purpose Relay Gateways
Legacy TDLs
Advanced TDLs
Mid Alt Relay Gateways
Net Enabled Attack / Weapons
Net Enabled SOF
Air
Land
APF
CAOC DCGS
ASOC
Base Networks
Tactical Air Control
Standardized Cyber Ops and C2
Sea
Permissive
Contested
GLOBAL NETWORK OPERATIONS – COMMUNICATIONS – COMPUTING – DATA AND SERVICES – SECURED AVAILABILITY

Figure 5: AFNet 2025 Operational View as JFC Warfighting Environment[10]

[7] U.S. Air Force Space Command, *Strategic Vision for an Air Force Single Integrated Network Environment* (Peterson Air Force Base, CO: Headquarters, U.S. Air Force Space Command, 2011).

[8] U.S. Air Force Space Command, *The United States Air Force Blueprint for Cyberspace* (Peterson Air Force Base, CO: Headquarters, U.S. Air Force Space Command, 2009), quoted within U.S. Air Force Space Command, *Strategic Vision for an Air Force Single Integrated Network Environment*, 3.

[9] Ibid., 4.

[10] Ibid. Figure retitled to show JFC's perspective.

The warfighting environment described is a *physical* one that will support operations in all spectrum conditions (permissive, contested, and anti-access) for systems in all other domains (air, land, sea, space, and cyberspace). The JFC must envision, as well as manage, spectrum penetration and control to assure cyber access (for modern communication, command and control, situational awareness, enterprise services and other system capabilities). Spectrum penetration and control seeks the mission assurance (or at least the temporary dominance) of the physical medium. Activities related to spectrum access and operations would involve expanding coverage and improving resilience of JFC wireless networks in the JOA, boosting signal strength, jamming and anti-jamming, pushing an adversary to a hard-wired environment, frequency allocation, coordination and system interoperability, contingency planning for spectrum denial, and broadcasting and/or relaying signals for radio and other systems communications.[11] It is important to realize, however, the JFC will be focused on spectrum penetration and control operational capabilities and how to leverage them, rather than tactical technology management. So, while the previously described warfighting environment emphasized network connectivity, interoperability, and system access, the JFC will be more interested in delivering the resulting mission improvements to power projection, flexibility, freedom of action, and operational reach – in other words, operationalization of cyber capabilities.

JFC Cyber Focus Area: Cyber Protection and Fires

The idea for this focus area is to *promote integrity of JFC systems while influencing adversary systems for strategic gain*. Cyber protection (defensive cyber operations) and fires

[11] Via fixed transmitters, aerial networks, near space platforms, and drones.

(outwardly-focused cyber operations) are two sides of the same coin.[12] A JFC will want cyber protection capability for friendly forces, with an offensive capability to degrade enemy cyber capabilities.

Cyber protection is focused on maintaining integrity and mission assurance of friendly systems and information. Protection extends beyond creating in-depth cyber defenses from adversary manipulation, degradation or denial of service of friendly capabilities. Protection also includes development of systems, networks and processes that are resilient to failure. The JFC desires operational capabilities that are monitored, robust, resilient, fault-tolerant, and contingency-ready.[13] Moreover, the JFC must have the capability to overcome contested or otherwise negative conditions in friendly cyberspace.

Cyber fires have many advantages that lend themselves to the JFC's execution of the operational plan. Cyber effects can be extended from relative safety beyond traditional geographic boundaries. Cyber fires can create strategic or operational effects of a temporary nature without lasting kinetic destruction. Cyber fires are flexible in that actions taken can be clandestine or covert (e.g. data manipulation) as well as overt (e.g. denial of service attack). Cyber fires can be employed across the range of conflict and scaled to the micro or macro level. JFC-directed cyber fires will have to be linked to national and COCOM authorizations for operational approval in accordance with the Law of Armed Conflict and cyber policy Rules of Engagement (ROE).[14] In addition, JFC cyber fires and effects will have to be coordinated with

[12] The term "cyber fires" is used to stay consistent with joint functional terminology. The term "outward-focused" is used instead of "offensive" in this description as a JFC-coordinated cyber operation might involve surveillance or other cyber access preparations that are not necessarily offensive or destructive.

[13] Fault tolerance should protect from adversary, accident, internal threat, or act of God.

[14] Under Title 10 or Title 50 depending on circumstances and intent.

USCYBERCOM in order to ensure de-confliction of regional and global intent and proper prioritization of constrained cyber development resources.[15]

In considering cyber protection and fires, the JFC must consider a number of issues. The JFC should seek synergy in employing offensive and defense cyber operations. The JFC must be cognizant that the interdependent human, logical, and physical layers of cyberspace are involved in cyber effects, reactions, and unanticipated consequences. Given the often hidden nature of actions in the cyber domain, the JFC must measure the instability caused to an adversary in the short term with loss of surprise, loss of trust, retaliatory response, or long term consequences.[16]

JFC Cyber Focus Area: Virtual Coalition

This focus area addresses *secure, flexible, and manageable information sharing for JFC coalition*. The term *virtual coalition* is meant to describe the JFC's intent to facilitate information sharing and knowledge management to maximize unity of effort toward objectives. The JFC desires information (command and control, situational awareness, decision support, etc.) to be widely and easily available to coalition partners. Systems interoperability has long posed a challenge to the JFC's operational environment.[17] The virtual coalition seeks a data-centric approach to serve as a basis for coalition shared understanding, cooperation and collaboration.[18] Campaign command and control should be seamless and well understood. Situational awareness should be continuously provided (both through digital real-time "pushes" and inquiry "pulls"). Distributed operations would be integrated with built in feedback channels.

[15] "…constrained development resources" is meant to confer limited time and system access of finite highly-skilled cyber cadre as well as cyber operational tools and techniques that may only be able to be used once before becoming ineffective. So, a cyber fire decision may involve both resource allocation and gain/loss considerations.

[16] Like a cyber warfare arms race.

[17] System and classification interoperability are long-standing challenges; an example of interoperatbility challenges is needing two different Air Tasking Orders (U.S. and NATO SECRET) with separate C2 systems during the NATO air war over Serbia in 1999.

[18] "Data-centric" refers to a focus on data standards and meta-data to facilitate information sharing interoperability as opposed to "system-centric" kluging together stovepiped system interfaces.

The JFC would organize information, tools, and management to oversee a theater's privilege-based information enterprise. Access would be granted according to system security, information classification, and need to know. It is envisioned that information would be extended out to the friendly operator level and not just command elements. Information dominance only extends as far as the JFC's ability to act collectively on it. Because JFC operations using coalition and interagency partnerships are the modern standard, a properly operationalized and managed virtual coalition will be better equipped for unity of effort and unified action toward JFC objectives.[19]

For the JFC, the virtual coalition will not just allow technical information sharing and interoperability. It will also facilitate integration of joint functions (including cyber) and synchronization of joint force operations. The JFC will leverage this virtual coalition integration to improve planning, coordination, and mission execution towards a full-spectrum campaign.

JFC Cyber Focus Area: Strategic Cyber Messaging

The JFC must understand and influence friendly, neutral, and adversary perceptions via *proactive access and engagement of digital media*. Strategic cyber messaging is not about data manipulation, but being aware of online communities and effectively leveraging the power of responsive and resonant messages toward JFC objectives. Winning the perception war is critical to the JFC's success at home and abroad. While information operations and strategic communications have well established concepts and processes, strategic cyber messaging seeks to facilitate speed, coverage, and impact of JFC messages in the digital world. Desired digital media outlets of influence should be broad: cable television news (e.g. CNN effect), the internet

[19] Virtual coalition management includes data management, information management, and knowledge management.

(e.g. blogs, You Tube, online communities), social media (e.g. Twitter), and perhaps even personal (e.g. text messages to selected phones).

The JFC should be capable of observing and engaging communities of interest (regional and global). Intelligence should be leveraged to understand perceptions and intentions of friendly forces, neutral parties, and adversary actors. JFC messages should be crafted to be persuasive and informative to the minds of the intended audience. JFC messages should use the strengths of digital media (visual imagery, reach, access, and responsiveness) to push JFC positions and agenda. JFC messages should resonate to leave lasting imprint as well as dominate coverage and discussion.[20] Strategic cyber messaging addresses pivotal issues by promulgating messages that demonstrate commitment, reinforce positive behavior, win the battle for public opinion, manage expectations and influence morale. Positive reactions, real and perceived, in the digital media are critical to JFC success.

In strategic cyber messaging, the JFC has to be mindful of the (cyber) medium and the message. Overexposure in the media can lead to desensitized audiences. The JFC must be mindful of the credibility of messages in immediate terms as well as long-term commitments. Multiple audiences (friendly, neutral, and adversary) will perceive the same message in different ways. Messaging must be consistent and balanced; overly demonizing an adversary could be negatively polarizing in people's perceptions and counterproductive in the long term. Finally, the JFC must accept the limitations of pushing strategic messages through cyber medium for an unpredictable audience. While powerful and necessary, strategic cyber messaging cannot fully assess influence because human perception and behaviors are not perfectly predictable. However, JFC messaging at this audience through this medium is an essential part of the operational design.

[20] The JFC should attempt to use up all the oxygen, so to speak, depriving the adversary of an equal voice.

A Simplified Model for JFC Cyber Operationalization

Seen collectively, a simplified conception of the continuous JFC cyber operationalization process is depicted in Figure 6 below. It uses a classic Observation-Orientation-Decision-Action cycle as a meta-model for data collection, information analysis, decision making, and cyber engagement in the JFC operational environment.[21] Within this construct, cyber ops process teams are organized around JFC focus areas to achieve operational approach and intent. This meta-model is useful in that it reflects both the systemic learning and adaptation going on within both the JFC's staff and cyber ops process teams during an operation, as well as the systematic processing and continuous responses as data and information are cycled and leveraged. This OODA based meta-model is conceived to reflect both the qualitative refinement of data to information to JFC knowledge as well as operations tempo of cyber ops process teams.

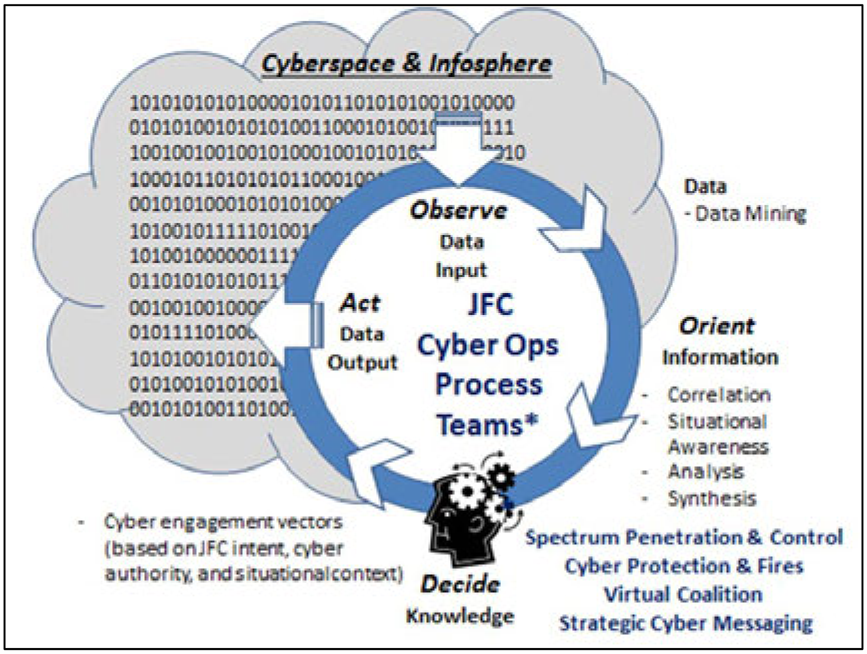


Figure 6: Simplified Conception of JFC Cyber Operationalization Process

[21] Derived from USAF Colonel John Boyd's Observation-Orientation-Decision-Action (OODA) Loop. For additional information, see William S. Angerman, *Coming Full Circle on Boyd's OODA Loop Ideas: An Analysis of Innovation Diffusion and Evolution* (Wright Patterson Air Force Base, OH: U.S. Air Force Institute of Technology, March 2004). The figure depicts the cyber operationalization integration process for the JFC.

Applying Cyber Operationalization Framework to the JFC's campaign

Cyber focus areas should be part of operational planning in line with operational design and integration of joint functions. As part of operational art, the JFC uses these cyber focus areas with understanding (e.g. experience, intellect, creativity, intuition, education, and judgment) of joint functions to develop an operational approach addressing the existing ends-ways-means-risk situation.[22] Stated differently, "[t]he operational approach is based largely on an understanding of the operational environment and the problem facing the JFC."[23] Joint functions (including cyber) must be incorporated into JFC plans as part of operational design elements.[24] Operational design elements are critical to the JFC and planners as they serve as conceptual structural building blocks for creative/critical thinking, analysis, systematic methodology for plans, and systemic engagement with the operational environment. In short, joint functions are crucial design elements used to guide and shape a JFC's concept and conduct of operations. JFC cyber focus areas provide scope and purpose parameters for a cyber joint function. Proposed cyber focus areas shape the JFC's conceptualization process of the operational art to facilitate understanding and successfully engagement of the environment, friendly force activity, and the adversary for desired operational end states.

Readying for the Cyber-Integrated Campaign

JFC cyber focus areas (spectrum penetration and control, cyber protection and fires, strategic cyber messaging, and virtual coalition) are only part of a cyber-operational framework. They provide a purpose and operational approach for cyber mission accomplishment in

[22] U.S. Joint Chiefs of Staff, *Joint Operation Planning*, JP 5-0, III-2.

[23] Ibid., III-6.

[24] Ibid., III-18. Operational design elements include termination, end states, objectives, effects, center of gravity, decisive points, lines of operation and lines of effort, direct and indirect approach, anticipation, operational reach, culmination, arranging operations, and forces and functions.

cyberspace and supporting other military efforts. What remains is to integrate these cyber focus areas within the JFC's operational design. The next chapter will propose and assess cyber operational design to meet JFC operational planning and execution.

CHAPTER 4

Integrating Cyber into JFC Operational Design

"While cyber may be our nation's greatest vulnerability, it also presents our military with a tremendous asymmetric advantage; the military that maintains the most agile and resilient networks will be the most effective in future war."[1]

General Martin E. Dempsey, Chairman of the Joint Chiefs of Staff

"**The commander is the central figure in operational design.**"[2] (bold font retained)

Joint Publication 3-0, Joint Operations

Cyber Operational Design

Cyber considerations are essential in describing how the JFC employs joint force capabilities to promote unified action to achieve operational strategic objectives. The JFC must have the greatest ability possible to leverage cyber power along with all other capabilities to meet the requirements of modern and future warfare. Operational design is the commander's vehicle to tie strategic imperatives to tactical actions.[3] A cyber operationalization framework incorporated within operational design is thus intended to use design elements to integrate cyber operations into an overall operational approach. An effective operational design framework will help translate the JFC's intent for employing cyber design elements as a joint function to support effective planning and execution.[4] A framework using the design elements will facilitate defining clear cyber decisive points and support an analysis of center(s) of gravity by exploring

[1] Claudette Roulo, "DOD Must Stay Ahead of Cyber Threat, Dempsey Says," *American Forces Press Service*, June 27, 2013. From the Chairman's remarks given to the Brookings Institute.

[2] U.S. Joint Chiefs of Staff, *Joint Operations*, JP 3-0, xiii.

[3] To achieve reach, simultaneity, depth, timing, tempo, leverage, balance, anticipation, and/or synergy in arranging operations.

[4] Universal joint functions are command and control (C2), intelligence, fires, force protection, logistics, and movement and manuever.

critical capabilities and critical vulnerabilities from a cyber perspective for both protection and exploitation.[5] So enabled, the JFC can articulate to planners how cyber contributes to every phase of the operation, timing of phases, as well as how cyber objectives and effects support achievement of the desired end state.

Incorporating the Cyberspace Domain

It is important the cyberspace domain be incorporated into the JFC's operational design. Figure 7 illustrates portions of cyberspace domain directly involved and influenced using the JFC cyber focus areas of spectrum penetration and control, cyber protection and fires, virtual coalition, and strategic cyber messaging. Cyber focus areas are the means for the JFC to integrate cyber into the operational design. The figure shows the comprehensive way the JFC shapes the human, logical, and physical portions of cyberspace using focus areas.

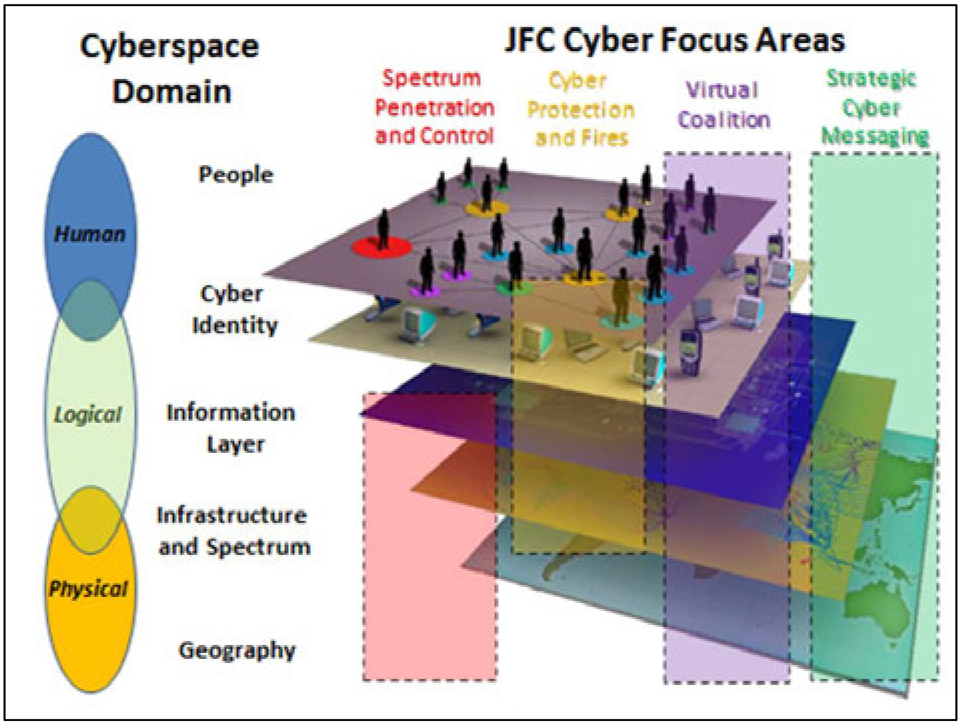


Figure 7: Depiction of Cyberspace Domain with JFC Cyber Focus Areas[6]

[5] Balancing offensive and defensive cyber capabilities for the JFC.

[6] Franz, "Effective Synchronization and Integration of Effects Through Cyberspace for the Joint Warfighter," slide 6. Figure adapted to show JFC's cyber focus areas within depiction of cyberspace domain.

Spectrum penetration and control involves the logical and physical portions of cyberspace to dominate the spectrum at a time and place of the JFC's choice.   Cyber protection and fires is performed at the logical level to promote integrity of JFC systems, while influencing adversary systems for strategic gain in support of unique decisive points or supporting decisive points. A JFC's virtual coalition uses all layers of cyberspace (e.g. integrating members across the JOA geography) for secure, flexible, and manageable information sharing. Strategic cyber messaging involves all layers of cyberspace as the JFC influences friendly, neutral and adversary perceptions via proactive access and engagement of digital media. Strategic messages may be precisely targeted or broadly promulgated to either people or geographic regions in the JOA. As shown, all elements and inter-related layers of the cyberspace domain are incorporated.

The JFC must work and be effective in the cyberspace environment. It must be understood as the battlespace, both physically and logically. The JFC cyber framework is designed to address the entire cyberspace environment (human, logical, and physical layers). As lead for assigned missions in the JOA, the JFC should have operational knowledge of, and feel for, the potential battlespace in all domains: physical conditions, complementary joint functions, cyber limitations, critical cyber infrastructure (friendly, neutral, adversary), relevant history, adversary decision making, organizational behavior, and regional culture. This inherent JFC mission knowledge must be infused into cyber operations, cyber operational approach in all domains, and contingency planning. The framework achieves progress in rationalizing and specifying JFC objectives with associated aspects of the cyber environment that are of interest to joint planners.[7] Moreover, the framework can help provide a unifying operational view of, and

[7] See Table 1 for specified campaign objective aligned to JFC cyber focus areas.

focus within, the cyberspace environment between JFC and USCYBERCOM command and control organizations.

Incorporating Cyber as a Joint Function

According to Joint Pub 3-0, "Joint functions are related capabilities and activities grouped together to help JFCs integrate, synchronize, and direct joint operations."[8] The current ascribed joint functions are: C2, intelligence, fires, movement and maneuver, protection, and sustainment. A JFC needs to use and integrate these joint functions effectively in time, space, and purpose to achieve success. Joint Pub 1-0 warns,

> The commander must exercise all the joint functions to effectively operate the force and generate combat power. Inadequate integration and balancing of these functions can undermine the cohesion, effectiveness, and adaptability of the force.[9]

Cyber capabilities and activities relating to the cyberspace domain support the six current joint functions, and vice versa. For instance, command and control might be supported via cyber means (i.e. a C2 system), but in a complementary fashion, a JFC will want to command and control cyber forces in the JOA. However, current joint functions insufficiently capture the essence of cyber actions and dependencies required for modern warfare. *Leveraging cyber power as a cyber joint function will be a distinct, unique necessity for the future*. As one author posits,

> Warfare of the 21st Century involving opponents possessing even a modicum of modern technology is not possible without access to cyberspace, and entire new operational concepts such as "Network Centric Warfare" or fighting in an "informationized battlespace" would be impossible without cyber-based systems and capabilities.[10]

Just as other joint functions represent capability (noun) and activity (verb), so would a cyber joint function. As this thesis has demonstrated, cyber can no longer be considered ancillary to

[8] U.S. Joint Chiefs of Staff, *Joint Operations*, JP 3-0, III-1.
[9] U.S. Joint Chiefs of Staff, *Doctrine for the Armed Forces of the United States*, JP 1, I-18.
[10] Kuehl, "From Cyberspace to Cyberpower," 29.

the JFC's operational approach and operational design. It must be fully integrated—this is accomplished by connoting cyber as joint function as applying it as such. A cyber joint function can be defined as, *"**Use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies.**"*[11] This cyber joint function definition should be sufficient to address the unique nature of cyber (e.g. noun) and its applied effects (e.g. verb) on the global information environment:

- the physical platforms, systems and infrastructures that provide global connectivity to interconnect information systems, networks, and human users;
- the massive amounts of informational content that can be digitally and electronically sent anywhere anytime to virtually anyone, a condition which has been enormously affected and augmented by the convergence of numerous informational technologies;
- the human cognition that results from greatly increased access to content and can dramatically impact human behavior and decision making[12]

Actions, effects, and consequences within the cyber domain are highly interdependent. A JFC that has outsourced all cyber operational responsibility is marginalized in thought and effectiveness. The JFC must incorporate cyber domain characteristics and cyber operational processes into their operational planning. Ultimately, the JFC, as the commander charged with mission responsibilities in their JOA, must conceive of cyber, not just in terms of technology, but as a joint function. A JFC, as part of exercising operational art, should consider cyber operations ends (e.g. effects and second-order consequences of cyber actions), ways (e.g. cyber actions taken; cyber mission planning and execution processes), means (tools, forces and time required to achieve cyber effects; the use of the cyberspace domain as an medium for decisive effects; the protection of friendly cyberspace resources to ensure operational force mission assurance) and

[11] Ibid., 28. Proposed cyber function adapted from Dr. Kuehl's proposed cyberspace definition.
[12] Ibid.

risk (probability and consequential impact of cyber failure to mission plans). The means to do this is understanding the cyberspace domain from an operational perspective and considering how the JFC cyber focus areas are integrated into the operational design.

Synthesis of JFC Cyber Operationalization Framework

Just like other joint functions, a cyber function for the JFC would consist of cyber activities (e.g. JFC cyber focus areas) structured in operational design for a viable operational approach toward achieving assigned missions. Table 1 proposes a JFC cyber operationalization framework. This framework was devised by considering a notional JFC operation fully integrating cyber capabilities; the JFC campaign is further described in the Appendix. The cyber focus areas serve to identify specific capabilities that can be applied by the JFC throughout the operation. Decisive points (e.g. spectrum superiority in the JOA; cyber integrity of friendly forces and systems; cyber influence in the JOA; JFC force synergy; winning the information war; winning hearts and minds) should support the JFC's operational design. Each cyber focus area is broken down into discrete cyber functional capabilities that are performed in a specific phase, or in concert with another joint function. A JFC can use this organizing framework to conceive within his operational art how cyber capabilities can be fully incorporated to achieve objectives. The JFC can achieve campaign objectives with the appropriate integration and employment of cyber elements: environment, command and control, weapon system(s), and operator(s). This framework is organized using traditional operational design elements for a JFC to structure cyber within an overall campaign. The framework's break out by campaign phase and related joint functions provides integration insights for arranging operations, capability development, and needed planning coordination.

JFC Cyber Focus Areas	**Spectrum Penetration & Control**	**Cyber Protection**	**Cyber Fires**	**Virtual Coalition**	**Strategic Cyber Messaging**
	Operational Cyber Capabilities Available to JFC in Operational Design				
Cyber Decisive Points	***Spectrum Superiority in JOA***	***Cyber Integrity of Friendly Forces and Systems***	***Cyber Influence in JOA***	***(JFC Force Synergy) Coalition Situational Awareness, C2, and Information Sharing***	***(Win the info war) (Win hearts/minds) Resonate JFC Messages in JOA***
Cyber Functional Capabilities for Integration by Phase and with other Joint Functions within the Operational Design	(Phase I-IV): Collect adversary signals (***Intel***)	(Phase 0-V): Identify critical systems and access for JFC ops (***Intel, Protect***)	(Phase I-IV): Perform adversary system ISR (***Intel***) (Clandestine)	(Phase I-V): Allow partner contributions and access levels (***M&M, Sustain***)	(Phase I-III): Persuade key decision makers (***C2, Intel, Fires***)
	(Phase I-V): Deliver coalition frequency interoperability (***C2***)	(Phase 0-V): Provide situational awareness of system readiness (***Intel, Fires, Protect***)	(Phase I-IV): Shape JOA for joint operations (***All***) (Clandestine)	(Phase I-V): Share Coalition information securely (***Intel, Protect, M&M***)	(Phase I-III): Intimidate adversary force (***Intel, Fires***)
	(Phase I-V): Ready multi-spectral broadcasts (***C2, Fires***)	(Phase 0-V): Ensure redundancy of systems (***Protect***)	(Phase I-V): Leverage JOA data mining (***Intel***)	(Phase I-V): Promulgate and coordinate C2 activities (***C2***)	(Phase I-V): Disseminate information to wide audience (***M&M***)
	(Phase I-V): Extend Single Integrated Network Environment for coalition JOA ops (***All***)	(Phase 0-V): Protect and guarantee critical system availability and reliability (***All***)	(Phase II-III): Deny adversary service (***Fires***)	(Phase I-V): Facilitate JOA coalition planning & interoperability (***All***)	(Phase I-V): Shape coverage/ content of news cycle (***Intel***)
	(Phase II-III): Jam adversary systems (***Fires***)	(Phase 0-V): Protect friendly systems (e.g. passwords, firewalls, anti-virus) (***Protect***)	(Phase II-III): Deceive adversary (***Intel***) (Clandestine)	(Phase II-IV): Synchronize coalition joint force operations (***C2, Intel, Fires, M&M***)	(Phase I-V): Identify audience; target persuasive arguments & commitments (***Intel, Fires***)
	(Phase II-III): Mislead; spoof JOA activity/ signals (***Intel***) (Clandestine)	(Phase 0-V): Identify/marginalize cyber threats and manipulation (***Intel, Protect***)	(Phase II-III): Manipulate adversary data (***Intel, Fires***) (Clandestine)	(Phase II-V): Decentralize real-time JOA situational awareness & decision support (***Intel***)	(Phase I-V): Garner public support in JOA (***Intel, Fires***)
	(Phase II-III): Control JOA spectrum for decisive joint ops (***C2, Fires, Protect, M&M***)	(Phase 0-V): Reconstitute cyber capabilities (***All***)	(Phase II-III): Degrade/delay adversary capability (***Fires***)	(Phase IV-V): Provide system resources for population/civil authorities (***C2, Sustain, M&M***)	(Phase I-V): Reinforce JFC messages and talking points (***Intel, Fires***)
	(Phase II-V): Protect/amplify/ repeat friendly signals in JOA (***C2, Fires, Protect, M&M***)	(Phase I-IV): Accelerate response to denial of service (**C2, Protect, M&M**)			
	(Phase II-IV): Deny adversary spectrum/signals (***Fires***)				

Joint Functions Key:

C2 – Command & Control
Intel – Intelligence
Fires – Fires
Protect – Protection
Sustain – Sustainment
M&M – Movement & Maneuver

Table 1: JFC Cyber Operationalization Framework

Implications for JFC Cyber Framework

The cyber operationalization framework provides a vision and an organizing structure for the JFC, joint planners, and cyber enablers. Using the proposed framework empowers the JFC to not just identify and submit cyber targets and desired localized effects, but also to leverage the infosphere to achieve information/cyber superiority and shape beneficial battlespace conditions in all domains. The JFC must have capability to plan for and adapt to dynamic changes and opportunities in the JOA cyber environment. While a fledgling effort, the framework is designed to make the JFC the driver and strategic-operational director (not just the customer) of cyber power. The model for cyber operationalization integrating cyber elements (environment, command and control, weapons system, and operator) presented in Chapter 1 can serve as a basis for assessing implications of the JFC cyber framework.

Framework Relevance to Command and Control

The JFC and USCYBERCOM have inter-related cyber command and control responsibilities as well as inherent interests in cyber operations.[13] The JFC cyber framework lends itself to a balanced and reconciled command and control of cyber operations between the JFC and USCYBERCOM. A tightly knit (and probably virtually maintained) relationship must be fostered that allows shared situational awareness, responsiveness, collaborative decision making, and operational trust regarding JFC operational plans for cyber in all domains within the JOA. Using the framework to structure phased cyber operations, both the USCYBERCOM and the JFC must contribute to synchronized, unified planning, and execution. USCYBERCOM personnel (including subject matter experts and liaisons embedded in the JFC staff) should provide cyber policy oversight, tools and expertise, Title 10/Title 50 authority relationships, and

[13] Interests include the people, cyber identity, information, physical infrastructure, and geography associated with cyber operations within mission contexts in the JOA.

associated approved operational support for cyber capabilities.[14] The JFC should provide regional knowledge, operational art and design insights, priorities for cyber efforts, planning and execution coordination, and operational oversight/authority in the JOA. In this way, the proposed cyber operationalization framework should help shared cyber responsibilities ensuring operational authorization, JOA effects, and cross-domain cyber capabilities. The resulting operationally-balanced C2 relationship should focus effort and facilitate flexibility at the JFC level while reconciling strategic and global interests in employing cyber weapon systems.

Framework Relevance to Cyber Weapon System

The JFC cyber operationalization framework also lends itself to identifying cyber weapon system technology development areas. Some of the JFC cyber focus areas may not have ready cyber tools or existing operational capability to produce cyber effects. Cyber capabilities must be advanced not just for clandestine cyber hacking tools and traditional information assurance (i.e. encryption), but for other future cyber power requirements.[15] Each JFC focus area should have a functionally-designed cyber weapon system. A weapon system approach to cyber procurement and development has many advantages. Weapons systems have design parameters (data in, engagement with cyber domain, data out) that can target JFC cyber centers of gravity. Weapon systems have projectable lifecycle and budget considerations that can be incorporated into JFC operational plans.[16] Finally, while probably upgradable, weapons systems have version control (e.g. hardware and software) that will facilitate standardized joint training and cyber weapon system employment.

[14] This could be built into USCYBERCOM plans for Cyber Combat Mission Forces to be located at geographic CCMDs.

[15] Such as cyber situational awareness, alerting, aerial networking, spectrum transmission capabilities, mission readiness/assurance oversight, personal-to-enterprise communications, decision support, common operational picture visualizations, virtual coalition coordination, data-centric metadata, and fault tolerant/self-healing networks.

[16] Budget considerations could include development and sustainment of cyber weapon system hardware and software as “must pay” bills.

Framework Relevance to Cyber Operators

The cyber operationalization framework can be used to guide desired JFC joint cyber operator makeup in the JOA in terms of training, experience, and functional specialty integration. Per the framework operational objective requirements, the JFC can press Services and USCYBERCOM for organizing, training, and equipping the cyber force for JFC operations and focus areas. Generalized service career cyber training will have to be augmented with specialized joint cyber weapon system knowledge and JFC focus area core competencies. As the framework interprets cyber broadly, experience from many functional specialties and disciplines.[17] This expertise will have to be drawn from Service contributions to the joint force, reorganized traditional staffs, or via USCYBERCOM manpower assigned to JFC cyber operations.[18] Training should be formalized for specialized roles operating JFC cyber weapon systems with certification requirements to ensure knowledge and proficiency. Cyber operators aligned to the JFC cyber operational design framework will be highly focused on achieving cyber superiority and cyberspace effects as part of a joint team.

Framework Relevance to JFC Cyber Integration and Employment

The cyber operationalization framework is designed to align the cyber elements (environment, command and control, weapon systems, and operators) toward a clear purpose and integrate them for JFC mission planning and execution at the operational level. As a result, the JFC can more effectively integrate these framework cyber elements within an operational design. This aids the JFC in his cyber conception for an operational campaign, crystallizing

[17] Such as joint ops planners, cyber operations, intelligence, public affairs, weapon system SMEs, information operations, spectrum management, etc.

[18] Chuck Hagel, *Quadrennial Defense Review* (Washington, DC: U.S. Department of Defense, March 2014), 33. Cyber personnel may come from DoD Cyber Mission Forces that will be manned by 2016 including "Combat Mission Forces that support Combatant Commanders as they plan and execute military missions."

commander’s intent into executable mission objectives. Also, this cyber operationalization framework can act as a shared basis for decentralized cooperation between JFC planners and cyber operators. The framework allows dialogue between the JFC planners and cyber operators to identify common and complementary decisive points along the framework’s designated lines of operation and phases.   Functional capabilities related to achieving specific decisive points are also identified, then synchronized and integrated into the operational design.

Once the cyber planners has a full understanding of the operational design, they develop an adjunct to the JFC operational design that employs lines of effort (LOEs) defined by the JFC cyber focus areas to identify cyber-specific decisive points from the framework as well as linking specific cyber functional capabilities to JFC decisive points by phase. (See Figure 8 for a proposed JFC operational design for campaign planning). This helps align JFC planning efforts in time, space, and purpose not just in the cyber domain, but across all warfighting domains.

A Director CYBERFOR is posited as being authorized by the JFC for responsibility in three portions of the cyber domain battlespace to achieve JFC effects: physical, logical, and human. Other components are responsible for the physical domain (air, land, sea, space) as well. The operational design for cyber must reflect this multi-dimensional space and its integration with the roles of other components in controlling the decisive points laid out in the JFC’s operational design. The Director CYBERFOR overlays his design over the JFC’s operational design and defines LOEs that support the lines of operation (LOO) of the JFC. These LOEs have cyber decisive points that are identified to support the control of JFC decisive points in other LOOs. All of these LOEs are linked to the JFC’s decisive points directed at influencing the adversary center of gravity (COG). Once the adversary COG is influenced or neutralized and Phase IV begins, the cyber LOEs continue to match decisive points along the cyber LOEs with the JFC's decisive points focused now on accomplishing the operational objectives that support the achievement of the designated end state.

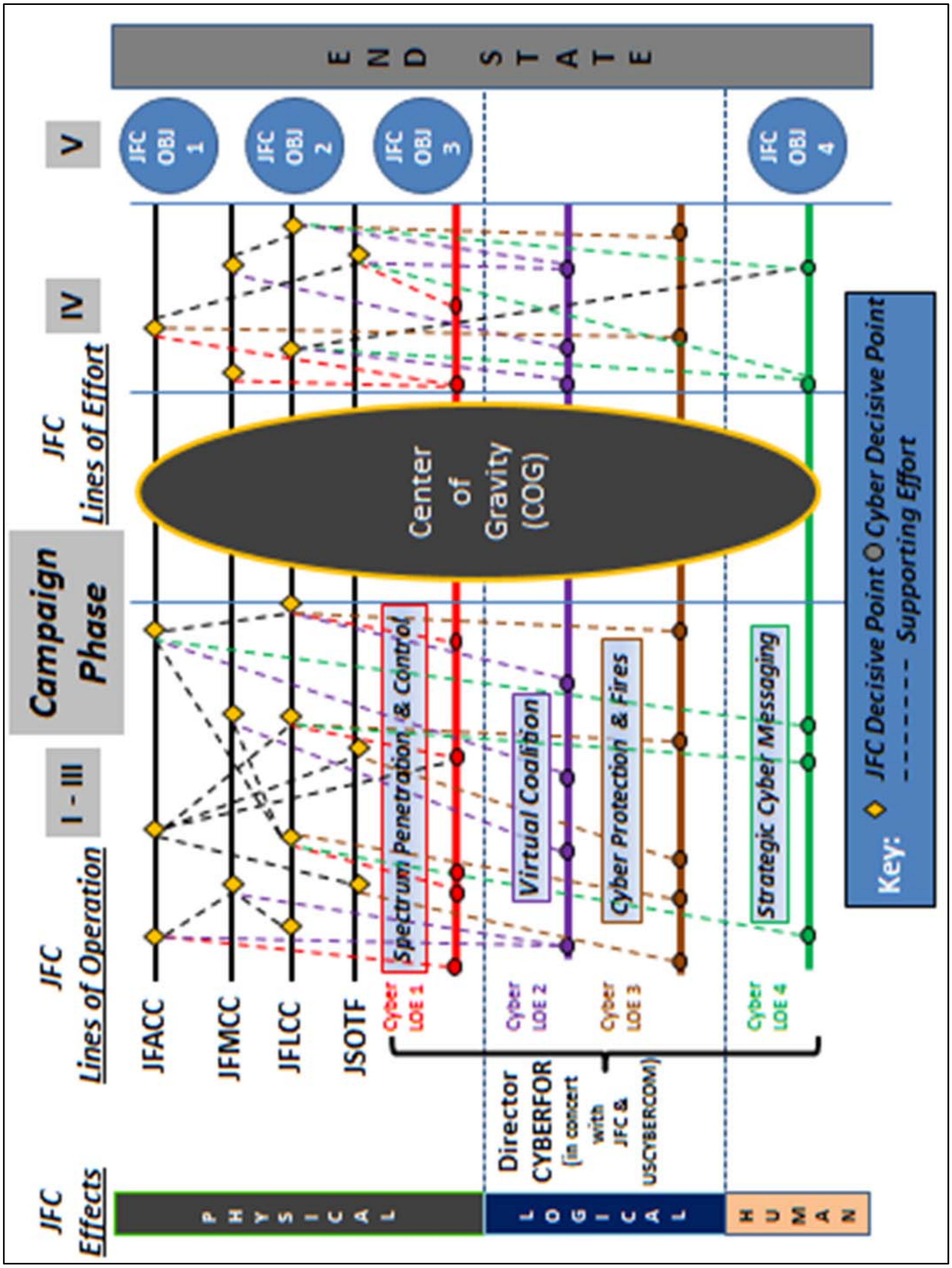


Figure 8: JFC Cyber Operational Design for Campaign

Collectively within this cyber framework and operational design, cross-functional cyber exploitation teams of operators employing the specialized cyber weapon system will work for the JFC to integrate cyber planning, analysis, coordination, and execution. These exploitation teams could be virtually integrated, if required, to support cooperation between geographically separated USCYBERCOM experts, weapon systems, and JFC staffs. USCYBERCOM dual Title 10/Title 50 relationships should be fully integrated via streamlined, responsive liaison relationships. Cyber operations will have to be balanced across offensive, defensive, and support capabilities in cyberspace and other warfighting domains. Across planning and execution of cyber operations, cyber exploitation teams would be discrete but decentralized functional hubs of activity synchronized with associated JOA mission operations cycles. The JFC may want to delegate some JOA cyber oversight given the nature of the disparate cyber operations, the required coordination and vectoring effort, and time constraints. The JFC would want to remain fully integrated in cyber operational design and execution, but could be relieved of significant management oversight. A Director CYBERFOR or empowered Joint Force Cyber Component Commander could help vector and direct cyber exploitation teams on JFC cyber focus area objectives, coordinate upcoming and ongoing cyber operations with USCYBERCOM, and harmonize cyber activities with JFC efforts in other joint functional areas or domains.[19]

[19] Stallone, *Don't Forget the Cyber!*, 15-17; Friberg, *U.S. Cyber Command Support to Geographic Combatant Commands*, 13-15.

CHAPTER 5

Conclusions & Recommendations

"Neither a wise man or a brave man lies down on the tracks of history
to wait for the train of the future to run over him."[1]

Dwight D. Eisenhower

"Strategic Initiative 1: DoD will treat cyberspace as an operational domain to organize, train, and equip so that DoD can take full advantage of cyberspace's potential."[2]

Department of Defense Strategy for Operating in Cyberspace

Thesis Summary, Assessment of Relevance, and Recommendations

This thesis addressed a medium-structured complex problem: overcoming JFC barriers to cohesively integrating cyber into campaign operational design. A JFC cyber operationalization framework utilized within operational design was proposed to empower the JFC to fully leverage cyber power in campaign conception, planning, and employment. The thesis approach taken was both descriptive and prescriptive. This thesis framed the JFC's dilemma of not having an integrated cyber operational approach to address needs of modern warfare. This research helped synthesize JFC framework for conceiving cyber forces in a campaign and organizing their capabilities for pragmatic mission planning and integrated execution. The proposed JFC cyber operationalization framework (in Table 1) attempts to improve and rebalance the JFC and USCYBERCOM

[1] TIME magazine, "National Affairs: Foreign Policy: Ike," October 6, 1952.

[2] U.S. Department of Defense, *Department of Defense Strategy for Operating in Cyberspace* (Washington, DC: U.S. Department of Defense, July 2011), 5.

working dynamic while meeting the JFC's operational cyber campaign requirements outlined in Chapter 2. Specific rationale to how this was accomplished is provided in Table 2 below.

Requirements for JFC Operational Cyber Campaign	**Met? (Yes/No)**	**Rationale**
1. Use cyber/info focus areas to achieve strategic objectives	Yes	Framework JFC cyber focus areas line up with campaign centers of gravity toward strategic objectives. Unifying framework will provide common reference for JFC and USCYBERCOM that will facilitate responsive, unified actions.
2. Align with theater engagement in all other JOAs and domains	Yes	Framework aligns to JFC plans (that inherently should align with COCOM and other theater JOA objectives and ROEs). Framework phased cyber operations provides the JFC with options across the range of conflict (deterrence, major combat operations, sustainment, etc.) Structure will also facilitate other inter-governmental and interagency alignment.
3. Incorporate regional theater expertise and integrate intelligence, information technology, and operations expertise	Yes	A more involved, integrated JFC staff provides regional and theater expertise to cyber operations planning. JFC planners and USCYBERCOM operators can integrate to form cyber exploitation teams. The framework improves cyber operational design processes; common framework more fully leverages teams from USCYBERCOM & JFC staffs; operators inherent to framework cyber operationalization.
4. USCYBERCOM provides tools and coordination in direct support of JFC	Yes	USCYBERCOM direct support relationship is required for JFC cyber operations. The JFC (in concert with USCYBERCOM) has ability to arrange his cyber exploitation teams and focus areas to support phased campaign objectives.
5. Cyber is a weapon system	Yes	The framework calls for development of standard cyber weapons systems designed around JFC focus areas. Standardized operator and cyber exploitation team training was proposed aligned with cyber weapon systems and JFC cyber operations roles.
6. Perform cyber activities at the operational level under both Title 10 (military action) and Title 50 (intelligence)	Yes	Designed as either inherent to JFC cyber exploitation teams granted authorities or liaison relationships with USCYBERCOM; framework assumes explicit cyber ops authorizations in line with JFC assigned missions. USCYBERCOM oversight of cyber operations policy will ensure global/national interests are preserved.
7. Ensure affordability (in terms of money and personnel)	Yes	Standardized cyber weapon systems are good "bang for buck" as they can be used across multiple JOAs; cyber operations can be less costly than other offensive operations as they can be more temporary and less kinetically damaging.

Table 2: Adjudication of JFC Operational Cyber Campaign Requirements

The proposed JFC cyber operationalization framework delivers relevant and positive contributions on many fronts. The framework as a conception and construct promotes improved JFC operational art and design. The framework puts the JFC as the individual responsible for planning and execution, not just as a customer requesting cyber targets, but also as a cyber shaper of the overall operational campaign. Cyber focus areas of cyber penetration and control, cyber protection and fires, virtual coalition, and strategic cyber messaging present the JFC an operational approach as well as a vision for organizing and operationalizing cyber forces and capabilities in ways that directly influence JOA mission success. Framework cyber operational objectives are designed to be flexibly phased in a campaign to provide the JFC options across the range of conflict that can be used independently or in concert with operations in other domains. Described cyber organization (including cyber exploitation teams integrating cyber domain situational awareness, JFC/USCYBERCOM command and control relationships, specialized cyber weapon systems, and trained operators) provides a powerful engagement capability for planning and JFC campaign effects. Finally, the framework provides a frame of reference promoting a balanced and more integrated working relationship between the JFC staff and USCYBERCOM for leveraging cyber power. Subsequent recommendations provide specific areas for improvements and further research.

Develop the Doctrine: Cyber as Joint Function and Cyber Operational Design

Reliance on cyber capabilities for modern and future operations makes establishing a cyber joint function a necessity for consideration and planning. Just as intelligence and command and control are enabling functions for all other joint functions, so is cyber. Cyber information system management is integral to offensive, defensive, and support operations; cyberspace domains and operations underwrite all other joint functional capabilities and will do so into the foreseeable future. A lack of cyber as a joint function should be further researched and submitted for inclusion in joint doctrine.

Also, further development regarding cyber operational design should be done to fill voids and address fragmented cyber planning and operations doctrine. Understanding of cyber power application of in doctrine by JFCs and cyber mission planners is critical to mission success. As one author notes:

> While doctrine is best acknowledged as a guideline, planners must grasp it *before* departing from it. In dealing with the problem sets posed by [offensive cyber operations], experience continues to indicate that planners out-think themselves when objectives are unclear or misunderstood, or when planning fails to follow an approach that is rational, logical, and sensical. Without a solid, doctrinal foundation by all involved, the ability to adapt to new concepts – particularly in cyberspace – will continue to result in disjointed planning and in an operational process that lacks full integration or synchronization.[3]

Given the need for and complexity challenge of higher-level JFC cyber operational integration, operational design is warranted. As put forward in this thesis, the proposed cyber operationalization framework applied within the JFC cyber operational design is recommended as a doctrinal addition.

Ready the Tools: Cyber Weapon System Development

This thesis recommends development of specialized cyber weapon systems specifically addressing JFC campaign objectives via focus areas as outline in proposed framework. Promoting development of specialized cyber tools is not new. However,

[3] Jason M. Bender, "Cyberspace: Deep Understanding of Offensive Cyber Ops Needed -- The Cyberspace Operations Planner," Fortuna's Corner web site. http://fortunascorner.com/2013/11/05/cyberspace-deep-understanding-of-offensive-cyber-ops-needed/ (accessed November 14, 2013).

cyber weapon systems designed around JFC cyber focus areas can directly shape JOA mission environments for success and open new operational possibilities. Additionally, a weapon systems approach to development and procurement provides advantages for planners, budgeters, and standardized training across the joint force.

Train the Force (As We Fight): Cyber Weapon System Training

The joint cyber force available for the JFC needs to be trained and ready. Specialized training for cyber operators and exploitation team planners is recommended to fully leverage specialized JFC cyber weapons systems. Cyber training and operational certification prior to mission engagement should be as realistic as possible with full role playing and exercises that develop proficiency and confidence. Cyber weapon system training needs to ensure the force understands capability limitations and operational employment considerations.

Organize for Success: Cyber Exploitation Teams with the JFC

Cyber exploitation teams are recommended to break specialized but compartmentalized pockets of cyber knowledge. Organizing for success is critical. This thesis recommends cross-functional cyber exploitation teams organized around JFC cyber focus areas and specially-designed campaign cyber weapon systems. Cyber exploitation teams should be data driven, process aligned, and center of gravity focused to systemically engage within cyberspace and systematically attain JFC phased campaign cyber objectives.

Traction in Cyberspace: Balanced JFC and USCYBERCOM C2

This thesis recommends all efforts to advance improved cyber operationalization between the JFC and USCYBERCOM. Progress should be facilitated along the cyber integration continuum measuring improvements from disunity to de-confliction to coordination to integration to full cyber coherence and cross-functional operational traction. Cyber command and control capabilities need to be balanced and responsibly shared for greatest effectiveness. If USCYBERCOM does not back the JFC's inherent operational or capability requirements, then the JFC loses a major means to shape campaign operations. The JFC and associated campaign cyber exploitation teams need to be fully integrated into cyber operational planning for realistic cross-domain employment, incorporation of regional expertise and campaign knowledge, and adaptation to risk and opportunities. Balancing JFC commander's intent and flexibility for JOA missions with cyber engagement policy and ROEs that protect global strategic interests is recommended for best long-term success in cyberspace.

Practice, Practice, Practice: Phased Cyber Operations in Peace and War

Cyber operations are here to stay as instruments of power and practice makes perfect. This thesis recommends continual development and practice of cyber operationalization in peacetime as well as lead into conflict. This framework focused on a JFC-led campaign with phased cyber objectives linked by operational design to strategic goals. Practice should include demonstrations and simulations delivering systemic and systematic effects in the physical, logical, and human layers of the cyberspace domain. The JFC cyber operational design framework is recommended for developing, testing, and assessing full-spectrum cyber campaign capabilities.

APPENDIX

Phased Campaign for a JFC

Explanation of JFC Campaign Phases

Phase 0 (Shape) is the phase where the JFC's theater environment is shaped by continuous normal and routine military activities. Phase 0 activities are designed to "ensure success by shaping perceptions and influencing the behavior of both adversaries and partner nations, developing partner nation and friendly military capabilities for self-defense and multi-national operations, improving information exchange and intelligence sharing, and providing U.S. forces with peacetime and contingency access."[1] Phase 0 activities are typically accomplished within the scope of the CCMD's Theater Campaign Plan (TCP).

Phase 1 (Deter) is the phase where the JFC's intent is to "deter undesirable action by demonstrating the capabilities and resolve of the joint force."[2] The JFC creates an increased readiness posture in response to the crisis at hand. Demonstration of capabilities and commitment seeks to stop adversary from current course of action (or perhaps delay to fully rationally consider the consequences). In addition to deterrence, Phase 1 activities prepare for scenarios where deterrence is unsuccessful and successive campaign phases are required.

[1] U.S. Joint Chiefs of Staff, *Joint Operation Planning*, JP 5-0, III-42.
[2] Ibid.

Phase II (Seize Initiative) is the phase where the JFC seeks "to seize initiative through the application of appropriate joint force capabilities."[3] The initiative is taken in order to set the conditions and tempo of following campaign actions. When friendly forces have the initiative, the JFC can influence conditions were adversaries capabilities are blunted and are relegated to a reactive mode. During this phase, "operations to gain access to theater infrastructure and to expand friendly freedom of action continue while the JFC seeks to degrade adversary capabilities with the intent of resolving the crisis at the earliest opportunity."[4]

Phase III (Dominate) is the phase where the JFC "focuses on breaking the enemy's will for organized for resistance or, in noncombat situations, control of the operational environment."[5] To successfully dominate, friendly forces overmatch adversary capabilities at the critical time and space. Depending on the circumstances in the domination phase, adversary resistance may continue. The JFC's domination activities intend to "fight through" to achieve objectives consistently despite adversary actions.

Phase IV (Stabilize) is the phase where the JFC shifts from sustained combat operations to stability operations. Campaign activities are designed to reestablish a safe and secure environment (e.g. restored local political, economic, and infrastructure stability). The JFC and joint forces will provide substantial support even if civilians are leading part or all of this phase.

Phase V (Enable Civil Authorities) is the phase where the JFC's joint force works to provide sustainable legitimacy for civil governance (working with civilian

[3] Ibid.
[4] Ibid., III-43.
[5] Ibid.

authorities). The goal is that the supported civilian authority will be able to regain its ability to govern and manage services and needs of its population.

Description of Notional JFC Cyber Campaign Using Thesis Framework

A brief and broad description of the notional JFC's campaign follows incorporating the proposed cyber operational design framework to standard phases found in doctrine (Phase 0--Shape; Phase I--Deter; Phase II--Seized Initiative; Phase III--Dominate; Phase IV--Stabilize; Phase V--Enable Civil Authorities).

The scenario envisioned for the JFC is a military confrontation between the JFC's coalition force and a rogue state. To begin the confrontation, a JFC has been appointed to deal with the crisis at hand within given JOA boundaries encompassing rogue state and potential access area. The JFC has been authorized to proceed with operations according to national approval and policy as well as geographic CCDR directives and ROE. Upon authorization, the JFC transitions from normal shaping activities found within the CCMD's Theater Campaign Plan to begin activities to handle the crisis.

During Phase I (Deter), the JFC expands a range of deterrent activities to demonstrate operational readiness and commitment. Spectrum penetration operations begin with the JFC expanding operational network coverage across the JOA. This is done through a mesh of space, terrestrial, maritime, and aerial networking involving communication and ISR. The goal is first to provide coverage and penetration for coalition C4I within a potential physical battlespace, and second, demonstrate increasing coalition activity within the region. Spectrum control may be demonstrated during this time to demonstrate periodic jamming or frequency denial capabilities to adversaries in small confrontations. Cyber protection activities will increase systems monitoring and security practice vigilance during this time to ensure JFC infrastructure and capabilities are not at risk during this period of increased international tension.

The JFC withholds cyber fires to during Phase I to maintain rogue nation stability during negotiations and allow rogue nation to comply with JFC or international conditions. Cyber fire preparations and target analysis increases during this time. Pre-existing software enterprise is adapted to coalition membership. A standard coalition classification is specified to enable authorized sharing of data feeds and mission info. Mission objective, intelligence, command and control, planning and situational awareness forums are established for coalition partner cooperation and collaboration. Strategic cyber messaging greatly increases allowing the JFC to address many audiences. The JFC explains his operational standup through news outlets, internet communities, radio missives to rogue state population and some specialized personal communiques to power brokers. Different cyber media are used for specific message targets, but all consistently specify behavior changes required to defuse the confrontation and avoid further escalation of crisis.

During Phase II (Seize Initiative), the JFC determines deterrence measures have failed and more muscular military operations are required. Spectrum penetration operations are maximized to allow frequency freedom of action within the JOA. Spectrum control operations (e.g. jamming) are used to deny the rogue state frequency freedom of actions for specified communications and weapons systems in contested and anti-access areas. Cyber protection operations are wary of rogue state “first strike.” Per authorization and coordination with USCYBERCOM, planned cyber fires are employed to access rogue state systems for ISR and future exploitation. Cyber contingency measures are readied for further escalation. The virtual coalition is in full force with coalition partners sharing intelligence, contingency plans, and operational products in preparation for imminent military operations. Strategic cyber messaging maintains consistent message reminding rogue state and domestic/foreign audiences how conflict began and can be resolved.

During Phase III (Dominate), the JFC is leveraging the preparation to the battlespace from cyber operations. Spectrum penetration and control continues to spread a 3-dimensional umbrella of frequency superiority for air superiority protected airspace, ISR, jamming, air/land/space networked communications, and near-space re-broadcasted PNT (position navigation timing) for precision guided munitions. While the rogue state does have its own jamming and anti-access/aerial-denial (AA/AD) systems, they are mitigated by JFC spectrum penetration and control approach. The JFC uses some aerial jammers to block rogue states military communications and substitutes prepared radio broadcasts. This not only signals superiority of the JFC's coalition forces, it pushes rogue state military communications to wired means. This is also a dilemma for the adversary as JFC cyber fires are creating unpredictable and mistrustful environment for rogue state through system degradation and denial of service. JFC cyber protection force is on high alert wary of rogue state counter-attack. The virtual coalition enterprise is used to provide real-time updates on cyber and other military domain operations. Shared situational awareness and open command & control channels offer the coalition ability to adapt to fluid battlefield conditions and take advantage of fleeting opportunities. Strategic cyber messaging is targeting media (e-mails & phones) of military and political leaders of the rogue state with personal messages pushing them to accept JFC demands.

As the rogue state gradually accedes to the coalition forces and capitulates to JFC demands, cyber operations are tapered to restore stability during Phase IV (Stabilize). The virtual coalition is used to synchronize friendly force stabilization efforts until civilian authorities can take over. Strategic cyber messaging (e-mail, web, phone, text) is used to broadcast widespread messaging regarding cessation of hostilities as well as instructions to both the civilian population and military forces within the JOA. Continuous messaging provides status updates and promotes expectation management during the stability transition.

During the transition to Phase V (Transition to Civilian Authorities) the JFC readies a portion of the virtual coalition hardware/software to be opened for interagency and non-government organization (NGO) use. The virtual coalition will be used to coordinate civilian authority actions and serve as foundational information services and command and control until local systems can be reestablished.

Shown in in Figure 9, the overall level of effort of campaign cyber operations is projected to reach its apex during the Phase II (Seize Initiative). This is consistent with the idea that once hostilities begin, all aspects of cyber may be maximized both to provide direct effects for the JFC as well as prepare battlespace for military activities in other domains. This is reflected in the dashed line showing other JFC operations and activities that peak during Phase III (Dominate).[6] Some operations, such as cyber protection go on during all campaign phases.

[6] Derived from Figure III-16 (Notional Operation Plan Phases) from U.S. Joint Chiefs of Staff, *Joint Operation Planning*, JP 5-0, III-39.

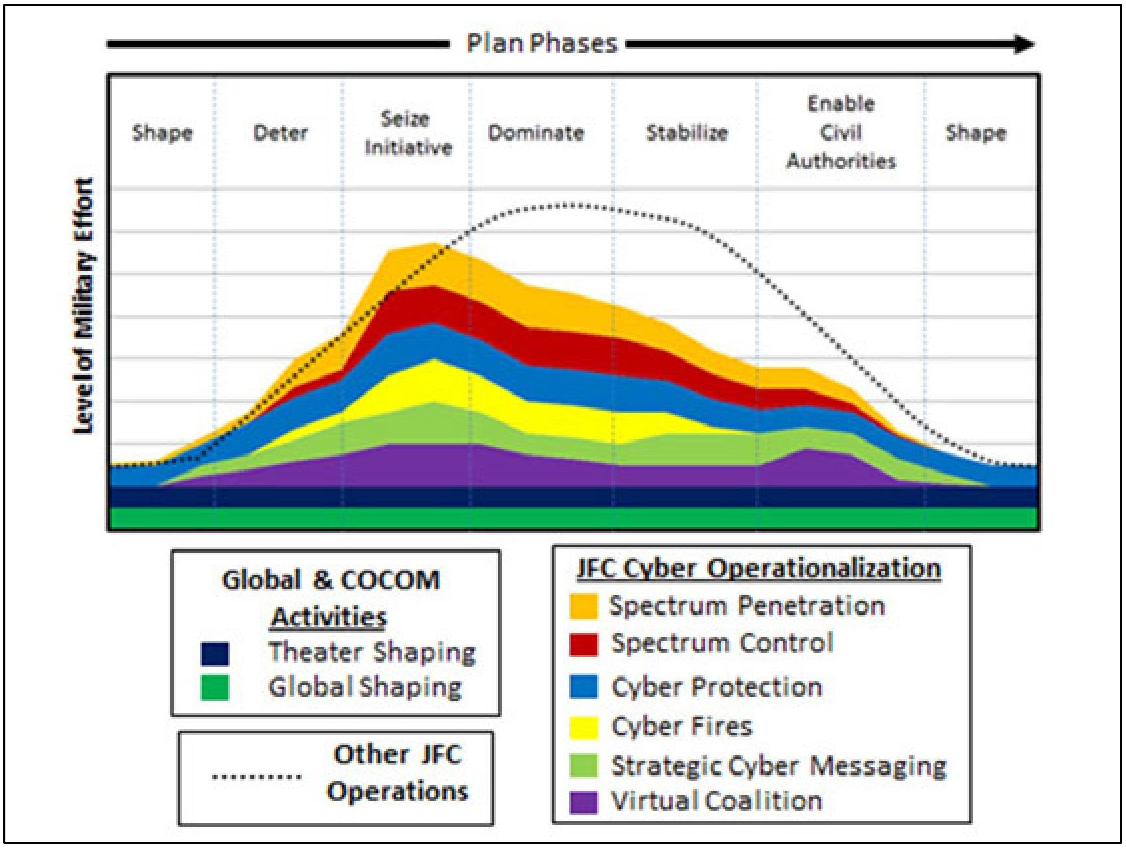


Figure 9: Notional JFC Campaign using Cyber Operationalization Framework

BIBLIOGRAPHY

Air Force Research Laboratory, Dr. Sarah Muccio, "Cyber Mission Assurance." Web page memo. http://www.wpafb.af.mil/shared/media/document/AFD-110516-046.pdf (accessed December 4, 2013).

Alexander, Keith B. "Building a New Command in Cyberspace." *Strategic Studies Quarterly* 5 , no. 2 (2011): 3-4.

Angerman, William S. *Coming Full Circle on Boyd's OODA Loop Ideas: An Analysis of Innovation Diffusion and Evolution*. Master's Thesis. Wright Patterson Air Force Base, OH: U.S. Air Force Institute of Technology, March 2004.

Bender, Jason M. "Cyberspace: Deep Understanding of Offensive Cyber Ops Needed -- The Cyberspace Operations Planner." Fortuna's Corner web site. http://fortunascorner.com/2013/11/05/cyberspace-deep-understanding-of-offensive-cyber-ops-needed/ (accessed November 14, 2013).

Bender, Jason M. "The Cyberspace Operations Planner: Challenges to Education and Understanding of Offensive Cyberspace Operations." *Small Wars Journal* 9, no. 11 (November 2013). http://smallwarsjournal.com/jrnl/art/the-cyberspace-operations-planner (accessed November 14, 2013).

Carter, Ashton B. "Department of Defense Directive 3000.06, Combat Support Agencies (CSAs)." Deputy Secretary of Defense Policy Directive, Washington, DC, June 27, 2013. http://www.dtic.mil/whs/directives/corres/pdf/300006p.pdf (accessed October 10, 2013).

Carter, Rosemary. "Offensive Cyber for the Joint Force Commander: It's Not That Different." *Joint Forces Quarterly* 66 (3rd quarter 2012): 22-27.

Cartwright, James. *Striking the Balance - Today's War, Tomorrow's Threats , Future Technology*. USSTRATCOM commander speech to Air Force Association in Orlando, FL, February 8, 2007. http://www.stratcom.mil/speeches/2007/4/AFA_Symposium/printable (accessed March 16, 2014).

Clarke, Richard A., and Robert K. Knake. *Cyber War: The Next Threat to National Security and What to Do About It*. New York, NY: Ecco, 2010.

Douhet, Giulio. *The Command of the Air.* Translated by Dino Ferrari. Washington, DC: Office of the Air Force History, 1983, originally published 1942.

Even, Shmuel, and David Siman-Tov. *Cyber Warfare: Concepts and Strategic Trends.* White Paper (Memorandum 117). Tel Aviv: Institute for National Security Studies, May 2012. http://mercury.ethz.ch/serviceengine/Files/ISN/152953/ipublicationdocument_singledocument/f3e19de1-bcf7-4d07-b088-f3d477b4329c/en/INSS+Memorandum_MAY2012_Nr117.pdf (accessed November 5, 2013).

Farwell, James P., and Rafal Rohozinski. "Stuxnet and the Future of Cyber War." *Survival: Global Politics and Strategy* 53, no. 1 (2011): 23-40.

Finn, Peter. "Cyber Assaults on Estonia Typify a New Battle Tactic." *Washington Post*, May 18, 2007.

Franz, George J. "Effective Synchronization and Integration of Effects Through Cyberspace for the Joint Warfighter." U.S. Cyber Command Director of Current Operations briefing to Armed Forces Communications and Electronics Association (AFCEA), Fort Meade, MD, August 14, 2012. http://www.afcea.org/events/tnlf/east12/documents/4V3EffSynchIntEffthruCybrspcforJtWarfighter_forpublicrelease.pdf (accessed February 22, 2014).

Friberg, Harry M. *U.S. Cyber Command Support to Geographic Combatant Commands.* Monograph. Carlisle Barracks, PA: U.S. Army War College, March 2, 2011.

Gates, Robert M. *Quadrennial Defense Review*. Washington, DC: U.S. Department of Defense, February 2010.

Gray, Colin. *Making Strategic Sense of Cyber Power: Why the Sky is Not Falling.* Monograph. Carlisle Barracks, PA: U.S. Army War College (Strategic Studies Institute), April 2013.

Hagel, Charles T. *Quadrennial Defense Review*. Washington, DC: U.S. Department of Defense, March 2014.

Hudson, Michael. "Cyber Workforce Development: Trained and Ready Cyber Teams." USCYBERCOM/J72 Training & Readiness Division briefing to Armed Forces Communications and Electronics Association (AFCEA), Fort Meade, MD, June 27, 2013. https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0CCcQFjAA&url=http%3A%2F%2Fwww.afcea.org%2Fevents%2Fcyber%2F13%2FAFCEAUnclassifiedJune2013V4Hudson.PPTX&ei=uNIXU7CGO5SBqQHF_YDYCQ&usg=AFQjCNFbgo5BuLxCwvldVzkShaWo9RDNIA&sig2=kZyGxZzKHCL45o6NgV2l5Q&bvm=bv.62577051,d.aWM (accessed February 6, 2014).

Kuehl, Daniel F. "From Cyberspace to Cyberpower: Defining the Problem." In *Cyberpower and National Security*, by Starr, and Wentz, eds. Kramer, 24-42. Washington, DC: National Defense University Press, 2009.

Lykke, Arthur F. “Toward an Understanding of Military Strategy.” In *Military Strategy: Theory and Application*, edited by Arthur Lykke. Carlisle Barracks, PA: U.S. Army War College, 1993.

Modelling & Simulation Journal. "Cyber Warfare is No Computer Game." *M & S Journal*, 2013: 1-48.

Ortiz, Christina. "U.S. Cyber Command to Recruit 4,000 new Cyber Soldiers." *ReadWrite.com*, January 31, 2013. http://readwrite.com/2013/01/31/us-cyber-command-to-recruit-4-000-cyber-soldiers#awesm=~oxGPQt9EGW4KyK (accessed February 15, 2014).

Owens, William A., Kenneth W. Dam, and Herbert S. Lin, eds. *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities.* Washington, DC: National Acadamies Press, 2009.

Phillips, Kyle G. "Unpacking Cyberwar: The Sufficiency of the Law of Armed Conflict in the Cyber Domain." *Joint Forces Quarterly* 90 (3rd quarter 2013): 70-75.

Reister, Brett. *Cyberspace: Regional and Global Perspectives.* Monograph. Carlisle Barracks, PA: U.S. Army War College, February 22, 2012.

Roulo, Claudette. "DOD Must Stay Ahead of Cyber Threat, Dempsey Says." *American Forces Press Service*, June 27, 2013.

Stallone, Martin. *Don't Forget the Cyber! Why the Joint Force Commander must integrate cyber operations across other war fighting domains, and how a Joint Force Cyberspace Component Commander will help*. Monograph. Newport, RI: Naval War College, May 4, 2009.

Starr, Stuart H. "Toward an Evolving Theory of Cyberspace." *Cryptology and Information Security Series (The Virtual Battlefield: Perspectives on Cyber Warfare)*, 2009: 18-52.

Stimson. *Strategic Agility: Strong National Defense for Today's Global and Fiscal Realities*. Washington, DC: The Stimson Center, September 2013. http://www.stimson.org/images/uploads/research-pdfs/Strategic_Agility_Report.pdf (accessed November 12, 2013).

U.S. Air Force Space Command. *Strategic Vision for an Air Force Single Integrated Network Environment.* Military White Paper. Peterson Air Force Base, CO: Headquarters, U.S. Air Force Space Command, 2011.

———. *The United States Air Force Blueprint for Cyberspace.* Military white paper. Peterson Air Force Base, CO: Headquarters, U.S. Air Force Space Command, 2009.

U.S. Department of Defense. *Department of Defense Strategy for Operating in Cyberspace.* Washington, DC: U.S. Department of Defense, July 2011.

U.S. Department of Defense Office of Public Affairs. *U.S. Cyber Command Fact Sheet.* Washington, DC: U.S. Department of Defense, May 25, 2010.

U.S. Joint Chiefs of Staff. *Doctrine for the Armed Forces of the United States.* Joint Publication 1. Washington, DC: U.S. Joint Chiefs of Staff, March 25, 2013.

———. *Joint Operations*. Joint Publication 3-0. Washington, DC: U.S. Joint Chiefs of Staff, August 11, 2011.

———. *Joint Cyberspace Operations*. Joint Publication 3-12. Washington, DC: U.S. Joint Chiefs of Staff, February 5, 2013.

———. *Joint Operation Planning*. Joint Publication 5-0. Washington, DC: U.S. Joint Chiefs of Staff, August 11, 2011.

———. *Joint Electromagnetic Spectrum Management Operations*. Joint Publication 6-01. Washington, DC: U.S. Joint Chiefs of Staff, March 20, 2012.

U.S. Government Accountability Office. *Defense Department Cyber Efforts: DOD Faces Challenges In Its Cyber Activities*, by Davi M. D'Agostino and Gregory C. Wilshusen. GAO-11-75. 2011. http://www.gao.gov/new.items/d1175.pdf (accessed October 7, 2013).

———. *Defense Department Cyber Efforts: More Detailed Guidance Needed to Ensure Military Services Develop Appropriate Cyberspace Capabilities*, by Davi M. D'Agostino. GAO-11-421. 2011. http://www.gao.gov/assets/320/318604.pdf (accessed October 7, 2013).

Weiner, Norbert. *Cybernetics or Control and Communication in the Animal and the Machine*. Cambridge, MA: MIT Press, 1948.

Williams, Brett T. *Cyberspace Operations*. USCYBERCOM/J3 presentation at the Joint Advanced Cyber Warfare Course 11 in Linthicum, MD, June 25, 2013.

Williams, Brett T. "Ten Propositions Regarding Cyberspace Operations." *Joint Forces Quarterly* 61 (2^{d} quarter 2011): 11-17.

VITA

Lieutenant Colonel William S. Angerman is currently assigned to the Joint Advanced Warfighter School (JAWS) at the Joint Forces Staff College in Norfolk, VA. Colonel Angerman is a United States Air Force Academy graduate, Class of 1995. He is a master cyber operator and space professional with assignments in communications, command and control, systems integration and space support. In addition to operations and staff assignments, he has deployed to Italy in support of the Balkan Combined Air Operations Center and Pakistan supporting Pakistan-Afghanistan border missions. His previous assignment was as commander, 22d Space Operations Squadron (22 SOPS/CC) at Schriever Air Force Base, Colorado where he oversaw operations for the $6.2 billion Air Force Satellite Control Network (AFSCN). In this role, he assured AFSCN mission access for satellite and launch operations in space and cyberspace domains. His squadron generated, scheduled and executed over 400 daily contacts for 154 satellites across 15 remote tracking station antennas at 7 global sites. Colonel Angerman is a distinguished graduate of the Air Force Institute of Technology and the Air Command and Staff College. He authored the earlier thesis, "*Coming Full Circle with Boyd's OODA Loop Ideas: An Analysis of Innovation Diffusion and Evolution*." He and his wife, Tana, are proud parents of two boys, Jacob and Zachary.