# REPORT DOCUMENTATION PAGE

*Form Approved*
*OMB No. 0704-0188*



| 1. REPORT DATE *(DD-MM-YYYY)* | 2. REPORT TYPE | 3. DATES COVERED *(From - To)* |
|---|---|---|
| 09-02-2015 | Master's Thesis | 21-07-2014 to 12-06-2015 |

**4. TITLE AND SUBTITLE**
**Expanding Combat Power Through Military Cyberpower Theory**

**5a. CONTRACT NUMBER**

**5b. GRANT NUMBER**

**5c. PROGRAM ELEMENT NUMBER**

**6. AUTHOR**
Sean C. G. Kern, 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**

**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**
Military theory is a primary component of operational art. Early military theorists reasoned about the maritime, air, and land domains generating frameworks, models, and principles for warfare. Today, these theories assist strategists and planners to think about, plan for, and generate joint combat power. Unfortunately, no standard military theory for cyberspace operations exists, although elements for such a theory do. A codified theory for military cyberpower will provide the descriptive language necessary for articulating the roles for cyberspace operations in joint operations and serve as a foundation to provide the explanatory and predictive power necessary for a Joint Force Cyber Component Commander (JFCCC) to assess the operational environment as a precursor for providing his best military advice to the Joint Force Commander (JFC). Generating essential combat power is critical for addressing a number of contemporary operational problems, the most challenging of which is adversary anti-access and aerial denial (A2/AD) strategies and capabilities. A codified theory of military cyberpower is a prerequisite for success against this and other operational challenges.

**15. SUBJECT TERMS**
**Cyber; Joint Force Cyber Component Commander; Joint Force Commander; Military Cyberpower Theory**

| 16. SECURITY CLASSIFICATION OF: | | | 17. LIMITATION OF ABSTRACT | 18. NUMBER OF PAGES | 19a. NAME OF RESPONSIBLE PERSON |
|---|---|---|---|---|---|
| a. REPORT | b. ABSTRACT | c. THIS PAGE | Unclassified Unlimited | 55 | 19b. TELEPHONE NUMBER *(include area code)* |
| Unclassified | Unclassified | Unclassified | | | 757-443-6301 |

*NATIONAL DEFENSE UNIVERSITY*

*JOINT FORCES STAFF COLLEGE*

**JOINT ADVANCED WARFIGHTING SCHOOL**


# EXPANDING COMBAT POWER THROUGH MILITARY CYBERPOWER THEORY

by

Sean C. G. Kern

Lieutenant Colonel, United States Air Force

**EXPANDING COMBAT POWER THROUGH MILITARY CYBERPOWER THEORY**

by

Sean C. G. Kern

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: _____

02 April 2015

**Thesis Adviser:** Signature: _____
**Stephen Rogers, Colonel, USA**

**Approved by:** Signature: _____
**John Torres, Colonel, USAF**
**Committee Member**

Signature: _____
**Sterling Pavelec, PhD**
**Committee Member**

Signature: _____
**Robert Antis, PhD**
**Director, Joint Advanced Warfighting School**

## ABSTRACT

Military theory is a primary component of operational art. Early military theorists like Alfred Thayer Mahan, Guilio Douhet, and Lidell Hart reasoned about the maritime, air, and land domains respectively, generating frameworks, models, and principles for warfare. Today, these theories assist strategists and planners to think about, plan for, and generate joint combat power. Unfortunately, no standard military theory for cyberspace operations exists, although elements for such a theory do. A codified theory for military cyberpower will provide the descriptive language necessary for articulating the roles for cyberspace operations in joint operations and serve as a foundation to provide the explanatory and predictive power necessary for a Joint Force Cyber Component Commander (JFCCC) to assess the operational environment as a precursor for providing his best military advice to the Joint Force Commander (JFC).

Generating essential combat power is critical for addressing a number of contemporary operational problems, the most challenging of which is adversary anti-access and aerial denial (A2/AD) strategies and capabilities. The *Joint Operational Access Concept* notes three trends in the operating environment that will likely complicate the challenge of opposed access, one of which is the emergence of cyberspace as an increasingly important and contested domain. The implication is that cyberspace operations are becoming ever more central in assisting the JFC in generating combat power to disrupt, degrade, and defeat enemy A2/AD capabilities. To be successful against challenges posed by A2/AD environments, the JFC must fully integrate cyberspace operations into joint operations. A codified theory of military cyberpower is a prerequisite for success against this and other operational challenges.

## TABLE OF CONTENTS

# CHAPTER 1: THE CHAIRMAN'S VISION FOR CYBERSPACE OPERATIONS

*"To us who have only armies and navies, it must seem strange that the sky, too, is about to become another battlefield no less important than the battlefields of land and sea. But from now on we must get accustomed to this idea and prepare ourselves for new conflicts to come. If there are nations which can exist untouched by sea, there are certainly none which exist without the breath of air."*[1]

Italian Air Marshall Giulio Douhet

## Introduction

The Chairman's 2012 *Capstone Concept for Joint Operations 2020* states that joint forces in current day employ cyberspace operations as adjuncts rather than as integral parts of joint operations. The Chairman asserts that the joint force can expand combat power if it fully integrates cyberspace operations with joint operations.[2] This is a significant problem given the highly contested nature of the cyberspace domain and the reliance of the joint force on unfettered access to the cyberspace domain. To resolve this operational problem, the joint force must answer two questions. First, why does the joint force employ cyberspace operations as adjuncts to joint operations? Second, what can the joint force do to better integrate cyberspace operations with joint operations, resulting in expanded combat power?

The responsibility to generate combat power rests with the Joint Force Commander (JFC). Using his operational art, the JFC is responsible for integrating

---

[1] Giulio Douhet, *The Command of the Air*, translated by Dino Ferrari (Washington, DC: Office of the Air Force History, 1983, originally published 1942).
[2] U.S. Joint Chiefs of Staff, *Capstone Concept for Joint Operations: Joint Force 2020* (Washington, DC: Joint Chiefs of Staff, 12 September 2012), 7.

cyberspace operations with joint operations to expand combat power.[3] Of course, the JFC relies upon his component commanders' creative imaginations to recommend proper employment of forces, plan and coordinate operations, and accomplish assigned missions. Based on these recommendations, the JFC integrates operations to generate combat power. To whom does the JFC turn to for cyberspace operations recommendations? There is no answer in doctrine. *Joint Publication 3-12 (R), Cyberspace Operations*, does depict a Combatant Command (CCMD) Joint Cyberspace Center (JCC) in its cyberspace command and control organizational construct, but it does not address the leadership of the JCC or consider a component commander construct for cyberspace operations.[4]

Although JFCs have many years of practical experience and military education in employing joint force, this is not the case for cyberspace operations.[5] There is a lack of shared cyberspace knowledge and an agreed upon operational approach that links cyberspace missions and actions and places them in the larger context of joint operations.[6] This makes the JFC even more reliant upon a senior officer that can recommend, plan, and coordinate cyberspace operations in support of the JFC's operational approach. Without a Joint Force Cyberspace Component Commander (JFCCC), it is unlikely that the JFC would be able to integrate cyberspace operations at a level on par with the other domains, resulting in a perpetual adjunct role for cyberspace

---

[3] Joint Publication 5-0, *Joint Operational Planning*, defines operational art as the application of creative imagination by commanders and staff—supported by their skills, knowledge, and experience.
[4] Joint Publication 3-12(R), *Cyberspace Operations* (Washington, DC: Joint Chiefs of Staff, 5 February 2013), IV-7.
[5] Brett T. Williams, "Ten Propositions Regarding Cyberspace Operations," *Joint Forces Quarterly* 61 (2nd quarter 2011): 11-17.
[6] Brett T. Williams, "The Joint Force Commander's Guide to Cyberspace Operations," *Joint Forces Quarterly* 73 (2nd quarter 2014):12-20.

operations and sub-optimal combat power. Lack of a JFCCC is the primary reason the joint force employs cyberspace operations as adjunct to joint operations.

It is not the intent of this research to provide justification for a JFCCC, which others have already argued.[7] Nor is it the intent of this research to present a methodology to integrate cyberspace operations into a JFCs operational approach, as others have addressed this as well.[8] However, there is a dearth of studies addressing the skills, knowledge, and experience needed of a JFCCC to make the recommendations the JFC requires.

Assuming the JFC chose to designate a JFCCC, a ready pool of candidates does not exist.[9] A JFCCC should be knowledgeable of military cyberpower theory and lessons from historical cyber conflict. A JFCCC should have expertise in DoD Information Network Operations (DODIN Ops), Defensive Cyberspace Operations (DCO), and Offensive Cyberspace Operations (OCO). A JFCCC should have experience on Joint Staff, United States Cyberspace Command (USCYBERCOM) or CCMD operations and planning staffs. Cyberspace operations will cease to be adjunct to joint operations when the Department of Defense (DoD) develops future JFCCCs using this professional development framework.

To aid the joint force in implementing the proposed professional development framework, this research will focus on military cyberpower theory and its application.

---

[7] Martin Stallone, *Don't Forget the Cyber! Why the Joint Force Commander must integrate cyber operations across other warfighting domains, and how a Joint Force Cyberspace Component Commander will help,* Monograph, Newport, RI: Naval War College, May 4, 2009.
[8] Williams S. Angerman, "Cyber Power for the Joint Force Commander: An Operational Design Framework," Master's thesis, Joint Advanced Warfighting School, 2014.
[9] Williams, "Ten Propositions," 11-17.

Military cyberpower theory provides a framework, models, and principles used to assess and explain the operational environment and make predictive judgments that then guide strategy and plan development. By viewing the operational environment through the lens of military cyberpower theory, the JFCCC will be in the position to provide his best military advice to the JFC, resulting in integrated cyberspace operations and expanded combat power. This research seeks to expand upon earlier cyberpower theory development efforts, with an emphasis on the military component.

## Cyberspace Operations Role in Expanding Combat Power

The ultimate goal of this research is to develop a preliminary theory for military cyberpower theory that will aid the JFCCC and the joint force in integrating cyberspace operations into joint operations. It may be difficult for some to equate cyberspace operations with combat power. Personnel rarely observe the effects of cyberspace operations, unlike the effects generated by kinetic operations. However, the JFCCC, through expert knowledge and application of military cyberpower theory, will be able to place cyberspace operations in the context of combat power and express cyberspace operations' relevance to the JFC and his fellow component commanders. A review of joint doctrine's discussion of combat power and an exploration of the role of cyberspace operations in the Chairman's *Joint Operational Access Concept* are good starting points from which to explore cyberspace operations' potential contribution to joint force combat power.

Joint doctrine is silent regarding the direct relationship between cyberspace operations and combat power. *JP 1-02* defines combat power as, "the total means of destructive and disruptive force which a military unit or formation can apply against an

opponent at a given time."[10] The key words are destructive and disruptive. Although *JP 3-12(R)* does not refer to combat power, it does describe direct denial effects achieved through cyberspace attack, which include, in part, the ability to destroy and disrupt adversary targets. *JP 3-12(R)* addresses DCO, but does not consider its impact in protecting and enabling combat power generated in other domains.[11]

The primary doctrinal source on combat power is *JP 3-0, Joint Operations*. The JFC is the central focus. It notes that the JFC, "seeks decisive advantage using all available elements of combat power to seize and maintain the initiative, deny the enemy the opportunity to achieve its objectives, and generate in the enemy a sense of inevitable failure and defeat." [12] The discussion of combat power in JP 3-0 leaves the reader with a sense that there is a bias to operations and effects in the physical domains. For example, JP 3-0 discusses the relative combat power that military forces can generate in terms of delivering forces and materiel. JP 3-0 extols the value of long-range air and sea operations as effective force projection when timely or unencumbered access to the area of operations is not available. Doctrine also discusses combat power in the context of mass, maneuver, economy of force, and surprise. There are no examples of generating combat power through cyberspace operations.

In addition to doctrinal references to combat power, the Chairman also publishes operational concepts which provide broad visions for how joint forces will operate in

---

[10] U.S. Joint Chiefs of Staff, *DOD Dictionary of Military and Associated Terms*, Joint Publication 1-02 (Washington, DC: Joint Chiefs of Staff, 8 November 2010, as amended through 15 August 2014), 43.
[11] U.S. Joint Chiefs of Staff, *Cyberspace Operations*, Joint Publication 3-12(R) (Washington, DC: Joint Chiefs of Staff, 5 February 2013), II-5.
[12] U.S. Joint Chiefs of Staff, *Joint Operations*, Joint Publication 3-0 (Washington, DC: Joint Chiefs of Staff, 11 August 2011), xx.

response to specific challenges. For example, the Chairman's *Joint Operational Access Concept* calls for cross-domain synergy to overcome emerging anti-access and area-denial (A2/AD) challenges. Cross-domain synergy seeks to employ complementary capabilities in different domains such that each enhances the effectiveness and compensates for the vulnerabilities of others.[13] To this end, the JOAC specifically addresses the need for a greater degree and more flexible integration of cyberspace operations into the traditional air-sea-land battlespace. It identifies two combat power related tasks required to gain and maintain access in the face of armed opposition. The first is the combat task of overcoming an enemy's anti-access and area-denial capabilities through the application of combat power. The second is moving and supporting the necessary combat power over the required distances. Successful accomplishment of these tasks fundamentally depend upon the development of military cyberpower theory and the professional development of cyber mission forces with expert understanding and experience applying military cyberpower theory.

## Thesis and Paper Structure

Just as every domain has its own characteristics, operational challenges, and opportunities, the cyberspace domain is no exception. Implementing a JFCCC and a staff that have the skills, education, and experience to operationalize the domain, to overcome the challenges, and to leverage the opportunities is critical to expanding joint combat power. An essential requirement for successful integration of cyberspace operations in joint operations is a JFCCC with expert knowledge of military cyberpower theory gained

[13] U.S. Joint Chiefs of Staff, *Joint Operational Access Concept* (Washington, DC: Joint Chiefs of Staff, 17 January 2012), ii.

through education, combined with operational expertise gained through the application of military cyberpower theory during operational and staff assignments.

Cyberspace operations are adjunct to joint operations because the JFC historically has not designated a cyber component commander that has an expert understanding and experience applying military cyberpower theory. Chapter 2 presents an expanded theory of cyberpower with emphasis on the military component of cyberpower. It serves as a starting point for continued military cyberpower theory development and as a foundation for cyber mission force professional development. Chapter 3 presents the application of military cyberpower theory in a hypothetical A2/AD scenario, suggesting how expert application of military cyberpower theory leads to expanded combat power. Chapter 4 concludes with recommendations and areas for future research.

## CHAPTER 2: AN EXPANDED "PRELIMINARY" THEORY OF MILITARY CYBERPOWER

*"Theory then becomes a guide to anyone who wants to learn about war from books; it will light his way, ease his progress, training his judgment, and help him to avoid pitfalls. Theory exists so that one need not start afresh each time sorting out the material and plowing through it, but will find it ready to hand and in good order. It is meant to educate the mind of the future commander."*[1]

Carl von Clausewitz

### Introduction

Military theory is a primary component of operational art. Early military theorists like Alfred Thayer Mahan, Guilio Douhet, and Lidell Hart reasoned about the maritime, air and land domains respectively, generating frameworks, models, and principles for warfare. Today, these theories assist strategists and planners to think about, plan for, and generate joint combat power. Unfortunately, no standard military theory for cyberspace operations exists, although elements for such a theory do. It follows then that when the Secretary of Defense established cyberspace as a warfighting domain, he created the requirement for a cyberpower theory. This requirement manifested in the 2006 Quadrennial Defense Review (QDR), which made a request of the National Defense University's (NDU) Center for Technology and National Security Policy (CTNSP) to develop a theory of cyberpower.

The 2006 QDR stated, "There is a compelling need for a comprehensive, robust, and articulate cyberpower theory that describes, explains, and predicts how our nation should best use cyberpower in support of U.S. national and security interests."[2] The

---

[1] Carl von Clausewitz, *On War*, trans. and ed. Michael Howard and Peter Paret (Princeton: Princeton University Press, 1976), 141.
[2] Stuart H. Starr, "Toward a Preliminary Theory of Cyberpower," *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: NDU Press, 2009), 44.

CTNSP published *Towards a (Preliminary) Theory of Cyberpower* in 2009, which articulated a cyberpower theory focused at the national level.[3]

This research adopts the theoretical framework employed by CTNSP. The following section highlights the key elements of the CTNSP framework. Subsequent sections expand upon this framework and provide additional emphasis on the military component.

## "Preliminary" Theory of Cyberpower

Constructing a theory starts with identifying and defining key terms, forming the foundation and lexicon for mutual understanding. The CTNSP, Stratton, Gray, Kuehl, and other theorists agree on three key terms for cyberpower theory: cyberspace, cyberpower, and cyber strategy. JP 1-02 provides a definition for cyberspace, but does not define cyberpower or cyber strategy.[4] CTNSP defines cyberpower as, "the ability to use cyberspace to create advantages and influence events in the other operational environments and across the instruments of power."[5] Kuehl offers a helpful theoretical distinction between cyberspace and cyberpower, observing that cyberspace is simply the domain, while cyberpower is a measure of the ability to achieve desired effects within the cyberspace domain.[6] Many authors reference Kuehl's definition for *cyber strategy*: "the development and employment of capabilities to operate in cyberspace, integrated and

---

[3] Ibid, 44.
[4] JP 1-02 defines cyberspace as a global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.
[5] Starr, "Preliminary Theory of Cyberpower," 51.
[6] Daniel T. Kuehl, "From Cyberspace to Cyberpower," *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: NDU Press, 2009), 38.

coordinated with the other operational domains, to achieve or support the achievement of objectives across the elements of national power."[7]

A theory helps structure discussions by categorizing the elements of the theory. For example, the CNTSP organized the key terms modeled on their broad conceptual framework, visualizing cyberspace as the base of a pyramid, upon which it placed cyberpower and cyber strategy in successive layers. This approach assists people in understanding the relationships of the theory's key tenets.

Once the theorist categorizes the theory's elements, a theory explains the categorized elements by summarizing relevant events and introducing additional constructs and models. "The challenge for the theorist," according to the CTNSP, "is to suggest and apply appropriate models that are useful for the decision maker and to delineate the range of their utility."[8]

Theory serves as a common means by which diverse communities can comprehensively treat key issues. Hearkening back to CTNSP's pyramid, the focus of this effort is to enable communication within the same level of the pyramid as well as enabling cross-level communication, which is significantly harder since each community has its own terminology, frameworks, and principles through which they assess the operational environment. As the common example proves, telling a Marine to "secure" a building will result in a different effect than directing a Soldier to do so. The lack of such a means for cross-level communication regarding cyberspace operations is the fundamental problem obstructing the successful integration of cyberspace operations.

---

[7] Ibid, 40.
[8] Starr, "Preliminary Theory of Cyberpower," 51.

Finally, a theory should anticipate key trends and activities. CTNSP considered four aspects of anticipation: identification of key cyberspace trends; research activities to study key trends; identification of major policy issues that decision makers will need to address; and assessment needs to support the formulation and analysis of policy options. This element speaks to the explanatory and predictive power of a sound theory and is a critical aspect of the JFCCC's ability to assess the operational environment through the lens of military cyberpower theory as a precursor for providing his best military advice to the JFC.

## "Expanded" Preliminary Theory of Military Cyberpower

Major General Brett Williams, former United States Cyber Command (USCYBERCOM) Director of Operations, provides a useful starting point from which to expand CTNSP's preliminary cyberpower theory:

> *"We need a theory for cyberspace operations that will allow us to understand the implications of employing cyberspace capabilities at the tactical, operational, and strategic levels. The theory must capture the ubiquitous nature of cyberspace and its relevance and interaction with government, commercial, and civilian sectors. Additionally, the theory must cover the complete spectrum from national security policy to detailed technical operations and account for the fact that the domain changes constantly."*[9]

This research expands upon the CTNSP preliminary cyberpower theory, further developing the military component at the strategic and operational levels since it will be the JFCCC's responsibility to translate strategic direction into operational plans. The military component focus is on integrating cyberspace operations with joint operations to

[9] Williams, "Guide to Cyberspace Operations," 12-20.

expand combat power. The following sections address additional terms, theoretical elements, and additional anticipatory issues for JFCCC consideration.

### *Additional Terms and Models*

In addition to the terms cyberspace, cyberpower, and cyber strategy, four additional terms and definitions are proposed: military cyberpower, military cyber strategy, key cyber terrain, and cyberspaces. The following definitions for military cyberpower and military cyber strategy reflect an emphasis on cyberspace operations mission areas and their contributions to joint operations and joint force combat power:

Military cyberpower: *the application of operational concepts, strategies, and functions that employ cyberspace operations (OCO, DCO, and DODIN operations) in joint operations to expand combat power for the accomplishment of military objectives and missions*.[10]

Military cyber strategy: *the development and employment of operational cyberspace capabilities integrated with other operational domain capabilities to expand combat power and accomplish the military objectives and missions of the JFC.*

Given the pervasive and ubiquitous nature of the cyberspace domain and the fact that the military relies heavily upon the commercial sector for interconnectivity, the concept of key terrain becomes especially critical in the context of military cyberpower theory. JP 3-12 does not define *key cyber terrain*, but does describe information technology in terms of links and nodes essential to friendly and adversary capabilities.

---

[10] Adapted from Elihu Zimet and Charles L. Barry, "Military Service Overview," *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: NDU Press, 2009), 285.

Key cyber terrain is the foundation from which the joint force preserves and projects military cyberpower and is therefore where an adversary will likely target.

Key cyber terrain: *any physical, logical, or persona element of the cyberspace domain, including commercial services, the disruption, degradation, or destruction of which constricts combat power, affording a marked advantage to either combatant*.[11]

Defining cyberspace as a global domain suggests homogeneity that does not exist in reality. There is not one cyberspace, but many cyberspaces.[12] These cyberspaces are in most cases interconnected by privately owned infrastructure. The DOD has over 15,000 networks, or cyberspaces, interconnected by commercial infrastructure that the DOD does not own or control. This has two significant implications. First, unlike in other domains, the joint force is not solely capable of generating its required military cyberpower; it relies on commercial services. Second, not all key cyber terrain will be under control of the joint force. For example, there is no current equivalent in cyberspace to the way in which the U.S. fully militarized U.S. airspace for the period immediately following the 9/11 terrorist attacks.

Military Cyberspaces: *Networks or enclaves wholly owned and operated by the DOD, interconnected by means that are outside the control or direct influence of the DOD.*

[11] This definition is derived from JP 1-02's definition for "key terrain."
[12] Colin Gray, *Making Strategic Sense of Cyber Power: Why the Sky is Not Falling* (Carlisle Barracks, PA: U.S. Army War College Strategic Studies Institute, April 2013), 15.

With the key terms identified and defined, models enable the theorist to explore the relationships among the concepts. Cyberspace strategists and cyberspace operations mission planners and operators must consider their efforts in the context of the three layers of cyberspace depicted in JP 3-12: physical, logical, and cyber-persona layers.[13] Figure 1 depicts the addition of new terms (left) and the relation of the cyberspace layers in the context of the overall friendly attack surface (right).

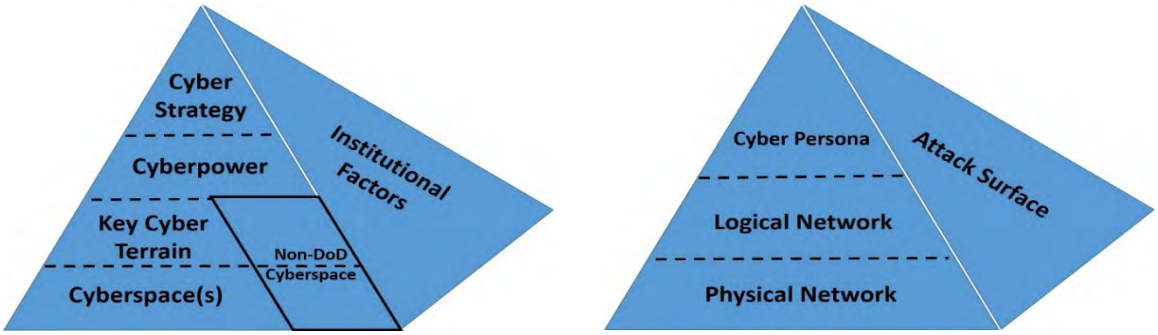


*Figure 1: Elements of Military Cyberpower Theory (l) and Cyberspace Domain Layers (r)*

With this framework for conceptualizing the cyberspace domain, the JFCCC can then consider the weighted effort of the cyberspace operations mission areas (Figure 2) in relation to the elements in Figure 1.[14] These operations comprise the JFCCC's cyber strategy and planning. Weighted effort, in priority order, would be DODIN operations, DCO-IDM, DCO-RA and OCO.

[13] JP 3-12(R), *Cyberspace Operations*, I-3.
[14] DODIN operations are responsible for designing, building, configuring, securing, operating, maintaining, and sustaining Department of Defense cyberspace domain from which to project military cyberpower. DCO Internal Defense Measures (DCO-IDM) are responsible for the mission assurance of key cyber terrain. OCO and DCO Response Actions (DCO-RA) are responsible for projecting cyberpower into neutral and adversarial cyberspace.

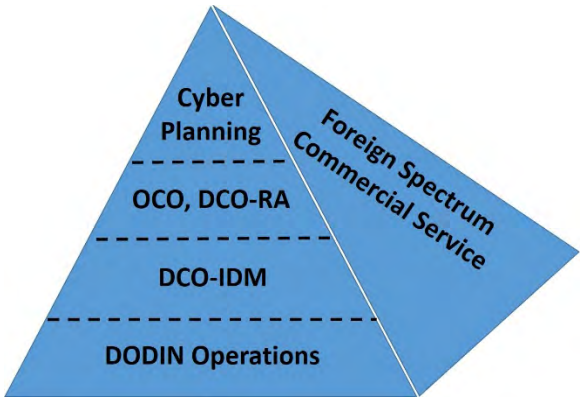


*Figure 2: Weighted Effort for cyberspace operations*

The joint force conducts cyberspace operations, like all joint operations, with adversaries in mind. This leads to a final structured discussion to characterize cyberspace adversaries and conceptualize adversarial operational planning and execution. Ultimately, this discussion gives the JFCCC and his staff the framework to assess risks to generating combat power.

The JFCCC and his staff assess cyberspace adversaries similar to adversaries in other domains, in terms of intent and capability. In the cyberspace domain, Lachow asserts that it takes two types of capabilities to conduct a cyber attack: technical and analytical. Analytical capability refers to the ability to analyze a potential target in order to identify its critical nodes and vulnerabilities and potentially its connections to other targets. Technical capability refers to knowledge of computer software and hardware, networks, and other relevant technologies.[15] He further categorizes cyber adversaries as simple, advanced, and complex, based in part on scope and scale of operations and potential effects achieved.

[15] Irving Lachow, "Cyber Terrorism: Menace or Myth?" *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: NDU Press, 2009), 443.

Adversaries can execute either opportunistic or targeted cyber attacks. The former is usually cybercrime-related, automated, and take the form of "smash and grab" operations where the adversary has no interest in maintaining persistent access. Targeted attacks are oriented against friendly key cyber terrain and may be persistent and stealthy; operators manually interact with target systems. These categories are not mutually exclusive as opportunistic attackers may gain access to high value systems and in turn seek to sell access to these high value systems to adversaries seeking targeted access (*e.g.*, nexus of cybercrime and state-sponsored cyber operations). Although the JFCCC should consider the full range of possible threats, manmade and natural, to his assigned Joint Operational Area (JOA), the focus of this research is on manmade threats. Figure 3 shows the relationships between adversary capability, targeting type, and persistence.

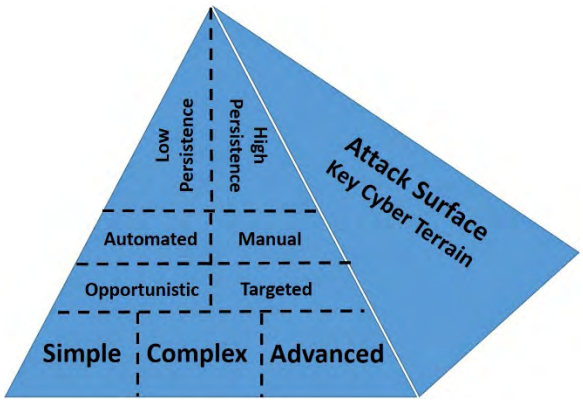


*Figure 3: Cyber Adversary Characterization*

Cyberspace adversaries share common strategic and operational concepts with adversaries in other domains, one of which is the concept of a kill chain. Visualizing a cyber kill chain enables the JFCCC to understand the way in which the adversary plans and conducts cyber operations. The Cyber Kill Chain depicted in Figure 4 provides a framework for the JFCCC to develop the appropriate strategy and corresponding operational plans to mitigate the adversarial threat. The ultimate goal is to detect and

defend against the adversary as early as possible in the chain, ideally prior to the adversary developing access.

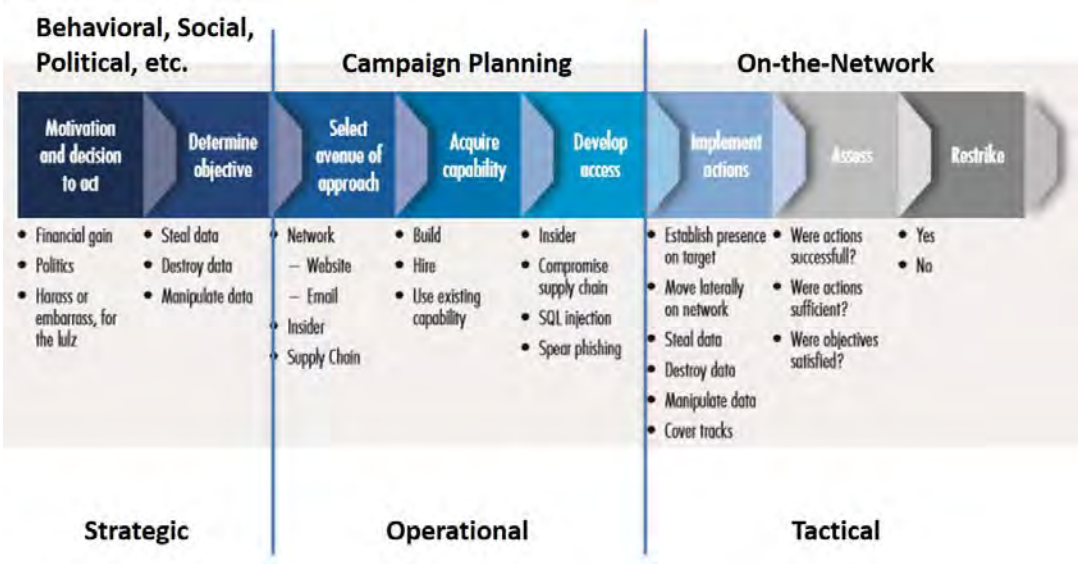


*Figure 4: Cyber Kill Chain*[16]

***Military Cyberpower Principles***

A theory of military cyberpower should include principles that inform the JFCCC's operational art. The true test of a theory is how well these principles are explanatory, predictive, and relevant over time.

The theory presented here contains nineteen principles, organized into three categories based on each principle's application to cyberspace operations. General principles apply across the full spectrum of cyberspace operations. Blue space principles apply to cyberspace operations within friendly cyberspace. Finally, red space principles apply to cyberspace operations that reach into adversarial cyberspace. Categorization of these principles is from a U.S. perspective, meaning red space is composed of a U.S.

[16] This cyber kill chain representation was adapted from an Intelligence and National Security Alliance whitepaper entitled "Strategic Cyber Intelligence" co-authored by this author. The whitepaper is available at http://www.insaonline.org/i/d/a/Resources/CyberIntel_WP.aspx.

adversary's cyberspaces. These principles are not exhaustive, culled from the author's professional experience and the works of others, but can serve as a foundation for future expansion of military cyberpower theory.

*General Principles*

Cyberspace Operations are Inherently Joint. No service has the preponderance of cyber mission forces nor the ability to command and control them. No service is unique in its use of the cyberspace domain.

Perpetual, Ambiguous Conflict. Actors in cyberspace are in a perpetual state of conflict that crosses geographic boundaries. Unlike the other domains where one can physically discern unambiguous threat indications and warning (I&W), operations in cyberspace are inherently ambiguous. Ambiguity complicates the concepts of war and warfare. Junio suggests this is the case because ambiguity, "may lead states to overestimate their potential gains, overestimate their stealth, and/or underestimate their adversary's skill."[17] The inverse may apply as well, creating very different conditions. States may underestimate their potential gains, underestimate their stealth, and/or overestimate their adversary's skills. Demchak warns that actions by non-state actors could lead to unintended escalation if one state misinterprets the action or uses it as cover for its own actions.[18]

---

[17] Timothy Junio, "How Probable is Cyber War? Bringing IR Theory Back Into the Cyber Conflict Debate." *Journal of Strategic Studies* 36, no. 1. February 2013. http://www.tandfonline.com/doi/full/10.1080/01402390.2012.739561#.VKhkFyvF_Sk (accessed January 3, 2015).

[18] Chris Demchak and Peter Dombrowski, "Cyber Westphalia: Asserting State Prerogatives in Cyberspace," *Georgetown Journal of International Affairs* (December 2013), 35.

Complexity, Penetration, and Exposure. Systems are becoming increasingly complex by almost every measure. Higher complexity begets a growth in vulnerabilities. Internet penetration is expanding in terms of people and devices connected to cyberspace. People and organizations are integrating more and more services delivered through cyberspace in their daily lives and operations, creating significant cyberspace exposure. Complexity, penetration, and exposure expand the attack surface by creating broader and deeper technical and process vulnerabilities, putting joint combat power at risk.

Speed and Global Reach. Cyberspace exhibits levels of speed and reach uncharacteristic of the other domains. Like other domains, cyberspace operations, especially offensive cyberspace operations, do require significant capability development, planning, reconnaissance, policy, and legal support prior to execution. However, once the JFC is authorized to act, cyberspace effects can be near instantaneous. The global cyberspace domain relegates geography to a subordinate consideration.

Cyber-Physical Interface Key to Kinetic Effects. To increase efficiency, critical infrastructure owners and operators connected their once-closed systems to the Internet. As a result, industrial control systems (ICS) and supervisory control and data acquisition systems (SCADA) are public-facing, providing more avenues of approach for an adversary. ICS and SCADA are the two primary means for cyber adversaries to achieve direct physical effects through cyberspace.

Strategic Attribution. From a strategic perspective, it may be more important to know "who is to blame?" than "who did it?"[19] This shift in perspective changes focus

[19] Jason Healey, "Beyond Attribution: Seeking National Responsibility for Cyber Attacks," The Atlantic Council Cyber Statecraft Initiative, entry posted February 22,2012,

from technical attribution, which is very difficult, to one of assigning responsibility to a nation state—more pointedly national decision makers—for either ignoring, abetting, or conducting cyberspace operations against the U.S., its allies, and key partners. At the strategic level, there are usually geo-political considerations that point to likely sources of cyber incidents.

Cyber Intelligence as Police Work. Cyber intelligence becomes very close to police work, looking for things that just do not look right by sifting through chatter to discern patterns of intelligence.[20] When DCO operators detect an adversary, it is difficult to assess adversarial intent. Is the adversary conducting reconnaissance, exfiltrating information, or instrumenting the network for a follow-on operation? A JFCCC must be able to assess cyber situational awareness beyond the joint operational area to understand fully the scope and scale of cyber risks to his theater of operations. This requires a high-level of integration and information sharing with relevant government and private sector cybersecurity organizations.

*Blue Space Principles*

Primacy of Defense. History shows that militaries are prone to favor offensive operations.[21] Yet, Gray, Williams, and Libicki argue that DCO, not OCO, should be the JFC's primary effort in cyberspace. Since the joint force builds its own cyberspaces, Gray contends that cyberspace operators can repair damage after an attack. Each repair hardens the system against future attacks, rendering enemy cyber capabilities

---

http://www.atlanticcouncil.org/publications/issue-briefs/beyond-attribution-seeking-national-responsibility-in-cyberspace (accessed January 3, 2015).

[20] Mark Lowenthal, *Intelligence: From Secrets to Policy*. 5ed. (Washington DC: Sage Press, 2013), 279. This is adapted from Lowenthal's description of the intelligence challenge posed by terrorism.

[21] Junio, "How Probable?"

increasingly ineffective. Offense can achieve surprise, but response and repair is routine for a well-organized and trained force. Cyberspace defense is difficult, but so is cyberspace offense.[22] As systems are hardened, an attacker must exploit multiple vulnerabilities to achieve the same effect as compared to earlier attacks that only required taking advantage of a single vulnerability.[23]

Convergence, Consolidation and Standardization. In peacetime, efficiency is valued over effectiveness. Core services are converging to Internet Protocol (IP) technologies. Smaller bandwidth network interconnections are converging to fewer massive bandwidth interconnections. The DOD is consolidating data centers and Internet access points, resulting in streamlined, consolidated service architectures. The DOD is also standardizing hardware and software. Convergence, consolidation and standardization create an efficient, homogenous military cyberspace environment that reduces the DOD attack surface overall and better postures cyber defenders to defend and preserve combat power. However, these efforts reduce system redundancy, limit alternative routes, and increase the number of chokepoints, making it easier for an adversary to identify and target friendly key cyber terrain.

Resilience. Resilience is the ability to continue military operations in a degraded cyber environment while quickly mitigating the impact of an attack. Much like the Quick Reaction Force construct in the physical domain, cyberspace operations require robust DCO-IDM capacity oriented in support of friendly key cyber terrain to mitigate the effects of adversarial cyberspace operations. In concert with these DCO-IDM efforts, the

---

[22] Gray, *Making Strategic Sense*, 45.
[23] Kim Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon* (New York: Crown Publishing, 2014), 106.

total force implements people, process, and technology measures, such as network minimize procedures or bandwidth management, to continue to operate in the degraded environment.

Increase Security, Decrease Freedom of Movement. In other domains, increased security usually implies greater freedom of movement. This concept is invalid for cyberspace since increased cybersecurity usually restricts options in cyberspace. For example, conducting mission planning on secure networks greatly reduces the access and therefore contributions of non-U.S. mission partners.

Decision Integrity. Assuring the integrity of operational information is essential to maintaining trust and confidence in the quality of decision-making. Making decisions based on wrong information degrades joint combat power. Cyber mission forces must baseline operational information, otherwise, it is impossible to assess if an adversary has made unauthorized changes. As Barry and Zimet observe, "The possession of accurate and timely knowledge and the unfettered ability to distribute this as information have always been the *sin qua non* of warfighting."[24]

Speed, Not Secrets. "Speed, not secrecy, will be the coin of the realm."[25] Adversaries are adept at compromising and extracting information from closed networks. In this environment, how long is it reasonable to expect secrecy? The days of having a high degree of confidence that secrets will remain secure are fleeting. Over-classification exacerbates this problem and negatively affects key cyber terrain analysis. The joint

[24] Zimet and Barry, "Military Service Overview," 286.
[25] Joel Brenner, *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare* (New York: Penguin Press HC, 2011), 199.

force should place value on the ability to make decisions before the adversary compromises key information.

Increased Reliance on Commercial Services. U.S. Central Command's 2014 posture statement noted the command is, "heavily reliant on host nation communications infrastructure across the Central Region."[26] Whereas a JFC can easily partition and militarize the other domains into internationally and nationally recognized, contiguous operational areas, cyberspace largely exists via private sector Internet Service Providers (ISP) interconnecting national and military cyberspaces. The JFCCC and his staff will have to consider this dynamic when attempting to define its "cyber Joint Operational Area."

*Red Space Principles*

Stealth and Utility. A cyberspace capability is effective as long as it can remain undetected and exploit an open vulnerability. If the adversary detects the cyber capability or mitigates the targeted vulnerability, the cyber capability is perishable. These characteristics may drive the timing of cyberspace operations based on the perceived utility.[27]

Arranging Operations. The *Joint Operational Access Concept* states that the critical support provided by cyberspace operations generally must commence well in advance of other operations, as part of efforts to shape the operational area. Even in the

[26] House Armed Services Committee, "Statement of General Lloyd J. Austin III Commander U.S. Central Command Before the House Armed Services Committee on the Posture of U.S. Central Command," 113th Congress, 1st sess., 2014.
[27] Robert Axelrod and Rumen Iliev, "Timing of Cyber Conflict," *Proceedings of the National Academy of Sciences of the United States of America* 111, no. 4 (January 2014), http://www.pnas.org/content/111/4/1298.abstract (accessed January 3, 2015).

absence of open conflict, operations to gain and maintain cyberspace superiority will be a continuous requirement, since freedom of action in cyberspace is critical to all joint operations.[28] Demchak offers a cautionary consideration, suggesting that if kinetic operations eventually take place, the U.S. may see the results of several decades of cyber "preparation of the battlefield," ranging from tainted supply chains to embedded malware.[29]

Scope and Scale of Effects. The most sophisticated cyber adversaries have the means to create regional disturbances involving multiple networks across multiple sectors (*e.g.*, electric, water, military command and control, etc.) for a short period. Alternatively, these adversaries can create local disturbances involving single networks or systems for a sustained period.[30] The intelligence functions must continually assess the intent and capabilities of potential adversaries in order to predict the potential scope and scale of effects.

Centralized Control, Centralized Execution. Because any point in cyberspace is logically equidistant to any other point in cyberspace, cyber forces are capable of deploying and surging virtually, without the required mobilization time and physical proximity to theater operations. This characteristic is a contributing factor to the centralized control, centralized execution model employed by United States Cyber Command (USCYBERCOM). This model affects the development of cyberspace experience across the joint force.

---

[28] U.S. Joint Chiefs of Staff, *Joint Operational Access Concept,*12.
[29] Peter Dombrowski and Chris Demchak, "Cyber War, Cybered Conflict, and the Maritime Domain," *Naval War College Review* (September 2014), 89.
[30] Sean Kanuck, "Cyber Intelligence and Secure Networks" (keynote address, AFCEA 2013 Spring Intelligence Symposium, Washington, DC, July 31, 2013).

Effects Uncertainty. Whereas the physical characteristics of the other domains are well understood and defined, cyberspace is a constantly changing, dynamic domain that is difficult to precisely model. Offensive cyberspace operators identify new vulnerabilities to exploit while defensive cyberspace operators identify new vulnerabilities to patch. These factors contribute to a level of doubt and uncertainty regarding the effectiveness of cyber capabilities (refer to the Principle of Stealth and Utility). Uncertainty makes cyber targeting and weaponeering more difficult than in other domains. Second and third order effects in cyberspace are difficult to model in contrast to the certainty the joint force enjoys with precision guided munitions for example. Lack of cyberspace operations education and experience in the joint force compounds uncertainty, thus creating a vicious circle of uncertainty, reluctance to employ, and lost opportunity to gain cyber experience, in turn leading to even greater uncertainty.

## Conclusion

The combination of key terms, frameworks, and principles serves as a foundation for an evolving military cyberpower theory. This theory serves as a building block to enhance both the explanatory and predictive power of the JFCCC's recommendations to the JFC. Application of the theory improves the soundness and timeliness of the JFCCC's recommendations. With expert understanding and application of this preliminary military cyberpower theory, the JFCCC and his staff will be better prepared to provide the JFC recommendations to integrate cyberspace operations in joint operations to preserve and project joint combat power.

## CHAPTER 3: APPLYING MILITARY CYBERPOWER THEORY

*A key antiaccess capability includes cyber attack capabilities designed to disrupt U.S. command and control systems and critical infrastructure, both civilian and military.*
*Joint Operational Access Concept*

### Introduction

With an understanding of military cyberpower theory presented in Chapter 2, the JFCCC will be poised to develop strategic and operational recommendations to the JFC to integrate cyberspace operations in joint operations. Proper application of military cyberpower theory will result in the joint force generating expanded combat power, forcing the opponent by means of disruption or destruction to accept the joint force's desired military endstates.

Although there is a rich history of cyber conflict, information in the open source does not offer a comprehensive historical example in which a military commander succeeded or failed to integrate cyberspace operations and the resulting impact on joint combat power. Such an example would be helpful in assessing the validity of the military cyberpower theory presented in Chapter 2. In the absence of such an example, it is necessary to construct a hypothetical scenario, based on current and emerging technology, operational concepts, and strategy, that will scrutinize the theoretical aspects of military cyberpower theory.

The hypothetical scenario presents an anti-access, area denial environment constructed to incorporate major considerations posed in the *Joint Operational Access*

*Concept* as well as to exercise a number of theoretical principles presented in the previous chapter.[1]

## Military Cyberpower Applied to a Chinese A2/AD Operational Environment

### *Strategic Context*

China is modernizing its military, preparing for a "local war under modern high-technology conditions."[2] This strategy places emphasis on development of effective A2/AD capabilities, including new cyber and space control technologies. This is a direct effort to counter U.S. operational and tactical superiority by threatening entry into the contested area of operation and hold at risk existing forward air bases and ports, especially in Japan and South Korea. For these reasons, Chinese A2/AD is a primary U.S. concern.

Key A2/AD capabilities include advanced intermediate- and medium-range conventional ballistic missiles (IRBM/MRBM), long-range land-attack and anti-ship cruise missiles (ASCM), diesel and nuclear powered submarines, fourth generation maritime strike aircraft, counter-space weapons, and offensive cyber capabilities. Supporting all of this is a full-spectrum command, control, communications, computer, intelligence, surveillance, and reconnaissance infrastructure capable of providing target quality location data.

China has arranged these capabilities in an overlapping, multilayered, combined offensive framework supporting China's offshore defense strategy. U.S. bases on

---

[1] Bryan Krekel, Patton Adams, and George Bakos, *Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage* (Washington, DC: U.S.-China Economic and Security Review Commission, 2012). This scenario is derived in part from this publication.
[2] Andrew Krepinevich, *7 Deadly Scenarios: A Military Futurist Explores War in the 21st Century* (New York: Bantam Dell, 2009), 169.

Okinawa are within range of a growing number of Chinese MRBMs; Chinese air-launched-cruise missiles can potentially reach Guam. China is enhancing its ability to detect U.S. and allied deployments in the region using space-based electronic intelligence (ELINT) satellites, signals intelligence collection, and land-based over the horizon radar. The Chinese military is improving its ability to move data from these collection systems over secure fiber optic cable to commanders at multiple locations and levels.

An essential prerequisite of China's growing A2/AD posture is the ability to control and dominate the information spectrum that supports all modern warfighting domains. Integrated Network Electronic Warfare (INEW) is the Chinese theory to describe the use of electronic warfare, computer network operations, and kinetic strikes to disrupt battlefield information systems that support an adversary's warfighting and power projection capabilities. China considers INEW one of the basic forms of integrated joint operations. The result of this approach is the creation of a "hard/soft kill matrix" of attacking forces.

The Chinese approach to INEW focuses on seizing the initiative by exploiting surprise, identifying and exploiting key enemy vulnerabilities, dismantling U.S. military communications networks and launching preemptive attacks where necessary. The net result is a climate of "disorientation and disintegration," creating blind spots that can be exploited.[3]

Key targets include enemy command and control and logistics networks in order to disrupt, degrade, or destroy the enemy's ability to operate effectively, cohesively, and in mutual support of one another early in the conflict. As one Chinese military officer

---

[3] Krepinevich, *7 Deadly Sins*, 169.

stated, “By striking directly at the ‘brains, heart, and nerve centers’ of the enemy’s systems, this method paralyzes powerful troop formations and makes them collapse without being attacked.”[4] Chinese military writings highlight the seizure of electromagnetic dominance in the early phases of a campaign as among the foremost tasks to ensure battlefield success. China can exploit and attack enemy networks prior to the start of kinetic operations, at a level below which would traditionally provoke a kinetic response or invoke defense treaty obligations (*e.g.*, 2007 cyber attacks against Estonia) and with little likelihood of attribution. China also recognizes the potential deterrent value of cyberspace operations as a means to manage the escalation of hostilities.

Diversion and deception are additional aspects of Chinese strategy. The Chinese can create disruptions that divert time, resources, and attention. Deception operations can also assist in diverting enemy combat power. Chinese military strategic and doctrinal writings on information confrontation stress attacking or shaping the adversary's perceptions, sometimes via the networks or systems themselves, with false or corrupted data during a conflict or crisis.[5]

***Current Situation***

China has been conducting cyberspace operations against the U.S. for years, mostly in the form of cyber espionage. For example, a private security firm published a report naming PLA Unit 61398 responsible for a 7-year cyber espionage campaign that stole hundreds of terabytes of information from at least 141 organizations spanning 20

[4] Ibid, 169.
[5] Krekel, *Occupying the Information High Ground*, 41.

major industries, 87 percent of which were from English speaking countries.[6] The same report assesses the unit's personnel strength from hundreds to possibly thousands assigned, including linguists, open source researchers, malware authors, industry experts, information technology staff, financial support, facility management, and logistics personnel. There may be as many as 40 other advanced persistent threat (APT) operations of similar scale and up to 250 groups of sophisticated non-state hackers in China.

As China continues to improve its A2/AD capabilities, it is increasingly becoming active in extending its territorial claims and influence. In 2014, China declared a new, expansive Area Defense Identification Zone (ADIZ), and since then it has increased its maritime presence in the South China Sea to challenge a number of territorial disputes with Japan, South Korea, and Vietnam.

In response to China's increased military activity in the region, the U.S. and partner nations have decided to conduct a short-notice combined air and naval exercise in the South China Sea. Although the scale of the exercise will be limited, the reduction of forward-based U.S. forces and overall force structure in the Pacific theater requires additional logistical support from outside the theater than was required for past exercises.

U.S. forces within range of Chinese A2/AD capabilities are on heightened alert. The Chinese have protested the upcoming exercise, labeling it an "unnecessary and inflammatory action." Although there have been no obvious disruptive or destructive cyber operations against the U.S. or its partners thus far, the possibility exists that China

---

[6] Mandiant, *APT1: Exposing One of China's Cyber Espionage Units* (Alexandria, VA: Mandiant, 2013), 21.

may show its displeasure by disrupting the exercise through application of its military cyberpower. Targets would likely include U.S. and partner command, control, and logistics networks. The Chinese could also seek to weaken or dismantle regional U.S. partnerships by threatening partner nation critical infrastructures.

### *The JFCCC Operational Assessment to the JFC*

The JFCCC's role is to assess the operational environment through the lens of military cyberpower theory, providing his best military advice to integrate cyberspace operations into joint operations thereby expanding the combat power of the joint force. The following sections present example application of the proposed military cyberpower theory presented in Chapter 2 to the operational challenge facing the JFCCC and the JFC. Note that not all principles presented in Chapter 2 apply in this operational scenario.

#### *Friendly Cyberspace Operations Mission Weight of Effort*

USPACOM's primary cyberspace operations mission is to preserve and enable combined air and naval combat power, while holding in reserve the right to project military cyberpower to target any adversary systems attempting to disrupt, degrade, or destroy U.S. cyberspaces. Cyberspace operations mission priorities should be DODIN operations, DCO-IDM, and DCO-RA.

This assessment applies to the current level of tension between China and the U.S. and its partners. No assessment is complete without considering the potential for increased tensions or the possibility of hostilities. In light of this more dangerous operational environment, the U.S. would alter its weight of effort to incorporate offensive cyberspace operations in cross-domain operations to disrupt, destroy, and defeat Chinese

A2/AD capabilities and their means to project force to provide maximum U.S. and partner operational advantage.

*Adversary Characterization and Arranging Operations*

USPACOM faces a determined and capable adversary. The Chinese have excellent technical and analytical capabilities, the intent to act, and the means to manually and persistently target specific U.S. military, partner, and commercial cyberspaces.

If the Chinese choose to conduct offensive cyberspace operations against the U.S. and its partners, they will likely attempt to do it pre-emptively, with the goal to stop the exercise before it begins. The Chinese can accomplish this in a number of ways. They may conduct cyber attacks against friendly cyberspaces and key cyber terrain. They may conduct cyber attacks against local commercial electric grids serving these cyberspaces. Finally, they could conduct physical attacks to isolate these cyberspaces from commercial internet service providers, although this is not likely at this time.

Although the Chinese can target friendly physical and logical cyberspace layers, the Chinese prefer to attack the persona layer as 91 percent of targeted attacks involve spear phishing emails. This style of attack is highly effective, as close to 50 percent of all spear phishing email recipients click on enclosed links, ten times the rate for standard spam emails.[7] Command personnel with privileged access to sensitive information as well as U.S. commercial partners need to be on heightened alert for this type of operation.

[7] FireEye, *Spear Phishing Attacks Whitepaper* (Milpitas, CA: FireEye, 2012), 5.

In addition to spear phishing, the U.S. and its partners may see distributed denial of service (DDOS) attacks to isolate U.S. and partner networks and systems. DDOS attacks can inundate fiber optic cables and routers, effectively isolating whole countries. This would be an effective attack against South Korea for example. In this case, it would be extraordinarily difficult to coordinate logistics and force projection with partner nations while under a DDOS attack.

*Adversary Cyberspaces and Key Cyber Terrain*

The U.S. will likely be the only partner nation with the capability to conduct offensive cyberspace operations. The U.S. needs to establish access to Chinese key cyber terrains that supports their A2/AD capabilities. Key targets should include Chinese early detection capabilities (*e.g.*, ELINT, SIGINT, over-the-horizon-radar) and their command and control networks and systems. The U.S. needs to blind Chinese military forces so they cannot feed targeting data to their advanced intermediate- and medium-range conventional ballistic missiles (IRBM/MRBM), long-range land-attack, and anti-ship cruise missiles (ASCM). Simultaneously, the U.S. should gain access to cyberspaces that support the planning and operation of these A2/AD capabilities. The ability to conduct offensive cyberspace operations on these targets relies heavily on current U.S. cyber intelligence on Chinese A2/AD systems.

*Friendly Cyberspaces and Key Cyber Terrain*

The Chinese will seek to disrupt or degrade U.S. and partner cyberspaces containing command, control, and logistics systems in theater as well as United States Transportation Command (USTRANSCOM) and its commercial partner cyberspaces.

Cyberspaces of concern in the USPACOM region include command, control, and logistics systems in Hawaii, Japan, Guam, Okinawa, South Korea, and Australia. If the U.S. and its partners cannot adequately defend its key cyber terrains, allied ability to project forces and combat power will be degraded. If the Chinese do not already have access to these cyberspaces and the systems contained within, they will seek to gain access.

There is also key cyber terrain that is not under direct military control or protection. As a result, non-military controlled key cyber terrains will likely be the preferred Chinese avenues of approach. Why gain access to a USTRANSCOM system to steal the Time Phased Force Deployment Listing (TPFDL) when the adversary can collect the data resident on commercial "soft targets?" The Chinese will exploit the trusted connections that commercial logistics providers have with USTRANSCOM systems. Unclassified commercial and DoD networks handle over 90 percent of USTRANSCOM's distribution and deployment transactions.[8] The Chinese may also target the commercial electric grid industrial control systems supporting these key cyber terrains as well.

*General Principles*

Perpetual, Ambiguous Conflict. It is possible for another nation or non-state actor(s) to conduct cyberspace operations against the U.S. and partner cyberspaces with the intent that such operations would be attributed to China, further exacerbating tensions.

[8] Krekel, *Occupying the Information High Ground*, 35.

Cyber Intelligence as Police Work. Given most information is digital, it is likely that sensitive information is duplicated and stored in multiple cyberspaces on multiple networks and systems, increasing Chinese avenues of approach. Effective cyber intelligence will be necessary to identify likely avenues of approach and if an outsider gains access, begin attribution to confirm Chinese cyber activities.

Speed and Global Reach. Cyber mission forces can surge and orient virtually to defend key cyber terrains. USPACOM cyberspaces and USTRANSCOM cyberspaces are equally within Chinese reach.

Initiative and surprise are key characteristics of cyberspace operations. Military power historically has tended to degrade over distance, but cyber capabilities are unaffected by distance.[9] This gives the U.S. the ability to maneuver directly against enemy key cyber terrains from strategic distance. This also means the U.S. can conduct cyber attacks against Chinese A2/AD in depth. The U.S. does not want to give the Chinese a chance to close their networks. Under heightened conditions, the Chinese can disconnect completely from the Internet, severely reducing U.S. cyber avenues of approach. Conversely, the U.S. does not have the means to disconnect from the Internet. Therefore, the Chinese can continue to use direct and indirect means to target U.S. key cyber terrain in theater as well as reachback to the U.S. homeland to cause significant damage and disruption.

Cyber-Physical Interfaces Key to Kinetic Effects. Physical destruction through application of military cyberpower is possible. The Shamoon virus destroyed 55,000

[9] U.S. Joint Chiefs of Staff, *Joint Operational Access Concept*, 7.

computers in Saudi Arabia's largest oil exporter.[10] Stuxnet destroyed 1000 Iranian centrifuges.[11] There are reports that explosions damaging oil pipelines in Russia and Turkey were the result of cyber attacks.[12] These types of cyberspace operations can be integrated with operations in other domains, greatly enhancing combat power effects. China likely has these capabilities and the capacity to conduct simultaneous, persistent cyberspace operations against many targets. The U.S. and its partners therefore need to monitor closely any potential for escalation.

Strategic Attribution. The Chinese will likely do all they can to remain stealthy in order to avoid attribution. However, given the heightened tensions, the U.S. and its partners should be confident that if offensive cyberspace operations take place against friendly key cyber terrain, China is the likely source. Note that this principle is in tension with the principle of Perpetual, Ambiguous Conflict.

*Blue Space Principles*

Primacy of Defense. DODIN operations and DCO-IDM oriented on cyberspaces hosting U.S. and partner command, control, and logistics networks and systems are critical to preserve the generation of combat power.

Convergence, Consolidation, and Standardization. Commercial communications and power providers serving friendly key cyber terrain must be technologically (*e.g.*, land

---

[10] Nicole Perlroth, "In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back," *The New York Times*, October 24, 2012, http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html?pagewanted=all&_r=0 (accessed January 3, 2015).
[11] David E. Sanger, "Obama Order Sped Up Attacks Against Iran," *The New York Times*, June 1, 2012, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all (accessed January 3, 2015).
[12] Jordan Robertson and Michael Riley, "Mysterious '08 Turkey Pipleline Blast Opened New Cyber War Era," http://www.bloomberg.com/news/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar.html (accessed January 3, 2015).

line and satellite) and geographically (*i.e.*, multiple paths) diverse. The U.S. must increase infrastructure redundancy to the maximum possible, eliminating cyber chokepoints. The U.S. should ensure it has multiple commercial power providers if possible and adequate backup power. For especially critical key cyber terrains, the U.S. and its partners must consider establishing hot-sites to which the JFC can quickly transfer command, control, and logistics operations if needed. Longer term, the acquisition community needs to develop alternative implementations of these key cyber terrains, using diverse operating systems, software, and infrastructure, which greatly increases an adversary's technical and analytical requirements.

Resilience. To mitigate the damage in the event Chinese cyberspace operators gain access to cyberspaces containing key cyber terrains, the JFCCC must orient Cyber Protection Teams on these locations to conduct DCO-IDM operations. This could be through virtual or on-location support. Personnel operating on, in, or through these cyberspaces need to be on heightened alert. Combat Mission Teams should be ready to conduct DCO-RA operations to trace back any attacks in the event the U.S. and its partners decide to act against the source adversary systems.

Decision Integrity. The Chinese will seek access to friendly cyberspace and key cyber terrains in order to steal information, gain intelligence, and infiltrate U.S. and partner cyberspaces with cyber capabilities to disrupt and destroy information to affect U.S. and partner decision integrity at a time of its choosing.

Increased Reliance on Commercial Services. U.S. reliance on commercial power, telecommunications, and logistics providers pose operational risk to the mission. Commercial telecommunications service providers interconnect military cyberspaces.

Using military satellite communications alleviates the dependence on commercial services, but has very limited relative bandwidth. Moving operations to military satellite communications would reduce the bandwidth available, reducing friendly freedom of movement in cyberspace.

*Red Space Principles*

Stealth and Utility. The U.S. will operate stealthily, to avoid direct technical attribution and to manage escalation of tensions. Short of direct hostilities, the U.S. will strive to use the lower end of their capabilities, reserving their most capable capabilities in the event of hostilities.

Arranging Operations. Arranging operations will be critical to effectively integrating cyberspace operations in joint operations. Even in the absence of any tension or conflict, the U.S. has been conducting cyber operations against enemy key cyber terrains to prepare the operational area in advance to facilitate access. The U.S. will conduct cyber operations in advance of kinetic operations and will continue cyberspace operations throughout escalation and conflict. The U.S. will seek to seize the initiative by conducting cyberspace operations integrated with other joint lines of operations.

Scope and Scale of Effects. Although the potential downtime due to Chinese offensive cyberspace operations is hard to assess, the U.S. has not seen instances where a large-scale outage lasts very long. Attackers are more effective at keeping specific networks or systems down, rather than multiple networks over a wide geographic area.

Effects Uncertainty. Cyberspace operations planners cannot predict precisely the effects of offensive cyberspace operations as compared to traditional combat arms planners. Cyberspace operational planners must consider risks to friendly or neutral

cyberspaces and key cyber terrain when planning missions against Chinese key cyber terrains.

## Conclusion

The preceding hypothetical scenario offers a high-level glimpse into the relevance and applicability of the military cyberpower theory terms, models, and principles presented in Chapter 2 by applying them in the context of an operational challenge. Although not all principles were directly applicable to the chosen scenario, it should be evident that the terms, models, and principles provide the necessary predictive and explanatory power by which the JFCCC can assess the operational environment as a precursor for providing his best military advice to the JFC.

# CHAPTER 4: Summary, Recommendations, and Conclusion

## Thesis Summary

This thesis investigated and offered a solution to the operational problem identified in the Chairman's *Capstone Concept of Joint Operations 2020* of the poor integration of cyberspace operations in joint operations and its corresponding negative impact on generating joint combat power. Two factors contribute to this problem. First, organizationally the joint force does not commonly designate component commanders for cyber mission forces and therefore there is not a senior leader in place to provide best military advice for cyberspace operations to the JFC. Second, in contrast to other domains, senior leaders lack cyberspace operations education and experience to inform strategy and operational plan development. This research focused on the latter factor.

Developing education and experience in cyberspace operations should follow a pattern similar to the other domains. A JFCCC should be knowledgeable of military cyberpower theory and lessons from historical cyber conflict, accrue expertise in one or more of the cyber mission areas, and gain experience on Joint Staff, United States Cyberspace Command (USCYBERCOM) or CCMD operations and planning staffs. Cyberspace operations will cease to be adjunct to joint operations when the Department of Defense (DoD) develops future JFCCCs using this professional development framework.

A detailed discussion of the breadth and depth of these educational and experiential requirements are beyond the scope of this work. As such, this research specifically addressed the most undeveloped aspect of these requirements: military cyberpower theory.

The military cyberpower theory presented in Chapter 2 extended previous work on national cyberpower theory. First, it identified and defined four new key terms: military cyberpower, military cyberpower strategy, key cyber terrain, and cyberspaces. This work also proposed several new models to aid cyber strategists and planners, including key terms relationship model, weight of cyber mission effort model, a framework for characterizing cyber adversaries, and a cyber kill chain model. Finally, the author proposed nineteen military cyberpower theory principles.

The theoretical principles proposed here serve as building blocks to enhance both the explanatory and predictive power of the JFCCC's recommendations to the JFC. Application of the theory improves the soundness and timeliness of the JFCCC's recommendations. With expert understanding and application of this preliminary military cyberpower theory, the JFCCC and staff will be better prepared to provide the JFC recommendations to integrate cyberspace operations in joint operations to preserve and project joint combat power.

## Recommendations

In 1932, British Prime Minister Stanley Baldwin claimed that the "bomber will always get through."[1] History has proven him wrong. However, the adoption of this theoretical airpower perspective did drive acquisition, organization, and doctrine leading into World War II. Cyberspace operations share some similarities with the interwar years. Much remains undetermined about the role of cyberspace operations in joint operations and its contribution to joint combat power. Yet there are historic examples,

[1] UK.gov, "Past Prime Ministers: Stanley Baldwin," https://www.gov.uk/government/history/past-prime-ministers/stanley-baldwin (accessed January 3, 2015).

key trends, and operational problems that call for increased attention to the need for a military cyberpower theory and consequently, updates to doctrine, organization, and education to inculcate the military cyberpower principles presented here.

The Joint staff should update doctrine to reflect the growing importance of effectively integrating cyberspace operations in joint operations to expand joint combat power. The Joint Staff should update JP 3-12(R) to reflect the need for a JFCCC and incorporate aspects of the preliminary military cyberpower theory presented here. Likewise, the Joint Staff should update JP 3-0's description of combat power to broaden and deepen the relationship between cyberspace operations and combat power. Finally, the Joint Staff should update JP 1-02 to include the terms presented in Chapter 2.

Organizationally, the JFC should designate a JFCCC for most task force operations. However, depending on the forces assigned, it may be difficult for the JFC to identify a JFCCC candidate that has the preponderance of cyber forces and the best means to command and control those cyber forces. Just as USCENTCOM chose to have a theater Joint Force Air Component Commander (JFACC) rather than a JFACC for each named operation, perhaps a theater or global JFCCC would be appropriate (refer to the principle of Centralized Control, Centralized Execution). Further, organizations that must address A2/AD in their strategies and operational plans should conduct extensive exercises with a heavy emphasis on cyberspace operations.

Professional military education and advanced studies programs should include military cyberpower theory in the curricula and challenge students to conduct research to evolve military cyberpower theory. Joint Staff should incorporate the findings from these research efforts into future versions of joint doctrine.

## Conclusion

With expert understanding and application of military cyberpower theory, the JFCCC is poised to develop strategic and operational recommendations for the JFC to integrate and synchronize cyberspace operations in joint operations and achieve expanded combat power. The need for integrated cyberspace operations and its contribution to joint combat power is clearly illustrated in one of the most significant operational challenges the joint force will likely face in the future, which is gaining and maintaining operational access in the face of enemy A2/AD capabilities.

The *Joint Operational Access Concept* notes three trends in the operating environment that will likely complicate the challenge of opposed access, one of those being the emergence of cyberspace as an increasingly important and contested domain. This implication is that the JFCCC and his staff are becoming ever more central in assisting the JFC in generating combat power to disrupt, degrade, and defeat enemy A2/AD capabilities. If the joint force is going to be successful in future advanced A2/AD operations, the JFC must fully integrate cyberspace operations into joint operations. A prerequisite for success is the designation of a JFCCC with the requisite professional development, to include expert understanding of and experience applying military cyberpower theory.

## BIBLIOGRAPHY


Angerman, William S. "Cyber Power for the Joint Force Commander: An Operational Design Framework." Master's thesis, Joint Advanced Warfighting School, 2014. In Defense Technical Information Center, http://www.dtic.mil/docs/citations/ADA603670 [accessed October 2, 2014].

Axelrod, Robert and Rumen Iliev. "Timing of Cyber Conflict." Proceedings of the National Academy of Sciences of the United States of America, vol 111, no. 4 (January 2014): 1298-1303.

Brenner, Joel. *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare*. New York: Penguin Press HC, 2011.

Clausewitz, Carl Von. On War. trans. and ed. Michael Howard and Peter Paret. Princeton: Princeton University Press, 1976.

Demchak, Chris and Peter Dombrowski. "Cyber Westphalia: Asserting State Prerogatives in Cyberspace." Georgetown Journal of International Affairs (December 2013).

Dombrowski, Peter and Chris Demchak. "Cyber War, Cybered Conflict, and the Maritime Domain." Naval War College Review (September 2014).

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

FireEye. *Spear Phishing Attacks Whitepaper*. Milpitas, CA: FireEye, 2012.

Gray, Colin S. *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.

Healey, Jason Healey. "Beyond Attribution: Seeking National Responsibility for Cyber Attacks." The Atlantic Council Cyber Statecraft Initiative, entry posted February, 22,2012http://www.atlanticcouncil.org/publications/issue-briefs/beyond-attribution-seeking-national-responsibility-in-cyberspace (accessed January 3, 2015).

House Armed Services Committee. "Statement of General Lloyd J. Austin III Commander U.S. Central Command Before the House Armed Services Committee on the Posture of U.S. Central Command." 113th Congress, 1st sess., 2014.

Junio, Timothy J. "How Probable is Cyber War? Bringing IR Theory Back In to the Cyber Conflict Debate." *Journal of Strategic Studies* 36, no. 1. February 2013.

http://www.tandfonline.com/doi/full/10.1080/01402390.2012.739561#.VKhkFyvF_Sk (accessed January 3, 2015).

Kanuck, Sean. “Cyber Intelligence and Secure Networks.” Keynote address, AFCEA 2013 Spring Intelligence Symposium. Washington, DC, July 31, 2013.

Krekel, Bryan, Patton Adams, and George Bakos. *Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage*. Washington, DC: U.S.-China Economic and Security Review Commission, 2012.

Krepinevich, Andrew. *7 Deadly Scenarios: A Military Futurist Explores War in the 21st Century*. New York: Bantam Dell, 2009.

Kuehl, Daniel F. “From Cyberspace to Cyberpower: Defining the Problem.” In *Cyberpower and National Security*, by Starr, Wentz, and Kramer eds. Washington, D.C.: National Defense University Press, 2009.

Lachow, Irving. “Cyber Terrorism: Menace or Myth?” In *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz. Washington, DC: NDU Press, 2009.

Lowenthal, Mark. *Intelligence: From Secrets to Policy*. 5ed. Washington DC: Sage Press, 2013.

Mandiant. *APT1: Exposing One of China’s Cyber Espionage Units*. Alexandria, VA: Mandiant, 2013.

Stallone, Martin. Don’t Forget the Cyber! Why the Joint Force Commander must integrate cyber operations across other warfighting domains, and how a Joint Force Cyberspace Component Commander will help. Monograph. Newport, RI: Naval War College, May 4, 2009. In Defense Technical Information Center, http://www.dtic.mil/get-tr-doc/pdf?AD=ADA503117 [accessed October 2, 2014].

Starr, Stuart H. “Toward a Preliminary Theory of Cyberpower.” In *Cyberpower and National Security*, by Starr, Wentz, and Kramer eds. Washington, D.C.: National Defense University Press, 2009.

U.S. Joint Chiefs of Staff. *Capstone Concept for Joint Operations: Joint Force 2020*. Washington, DC: Joint Chiefs of Staff, 10 September 2012.

_____. *Cyberspace Operations*. Joint Publication 3-12(R). Washington, DC: Joint Chiefs of Staff, 5 February 2013.

_____. *DOD Dictionary of Military and Associated Terms*. Joint Publication 1-02. Washington, DC: Joint Chiefs of Staff, 8 November 2010, as amended through 15 August 2014.

_____. *Joint Operational Access Concept*. Washington, DC: Joint Chiefs of Staff, 17 January 2012.

_____. *Joint Operational Planning*. Joint Publication 5-0. Washington, DC: Joint Chiefs of Staff, 11 August 2011.

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

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

Williams, Brett T. "The Joint Force Commander's Guide to Cyberspace Operations." *Joint Forces Quarterly* 73 (2nd quarter 2014): 12-20.

Zetter, Kim. *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. New York: Crown Publishing, 2014.

Zimet, Elihu and Charles L. Barry. "Military Service Overview." In *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz. Washington, DC: NDU Press, 2009.

## VITA

Lieutenant Colonel Sean C. G. Kern is currently assigned to the Joint Advanced Warfighting School (JAWS) at the Joint Forces Staff College in Norfolk, VA. Colonel Kern received his commission through the United States Air Force Officer Training School in 1996. He is a master cyberspace operations officer with assignments in space operations, operational test and evaluation, tactical and base-level communications, and command and control systems. Colonel Kern has served in OPERATION IRAQI FREEDOM and OPERATION ENDURING FREEDOM, the latter as an expeditionary communications squadron commander at Kandahar Air Field, Afghanistan. His previous assignment was as Military Faculty, Information Resources Management College, National Defense University, where he developed and taught courses in cybersecurity, cyber intelligence, and cyber conflict. Colonel Kern is a graduate of the U.S. Air Force Institute of Technology and the National Intelligence University. He has authored a number of articles and been a panelist and guest speaker at several cybersecurity conferences.