REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
28-04-2015	Master's Thesis	21-07-2014 to 12-06-2015

4. TITLE AND SUBTITLE

Strategic Uncertainty: Thinking About Tactical Level Cyberspace Operations

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

DANIEL J. RUDER, Colonel, USA

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

Joint concepts describe that the growing capabilities of cyberspace operations will further transform how the tactical force will fight during Joint operations in the future, by integrating cyberspace operations down to lower tactical levels to achieve new levels of cross-domain synergy. Although the concept of integrated offensive and defensive cyberspace operations at tactical echelon commands is unproven, joints concepts suggest that this new approach to cyberspace operations is potentially feasible, suitable, and acceptable. While it may be entirely appropriate to pursue the desired outcomes outlined in joint concepts, and in line with the Chairman's vision, it is not prudent to do so without fully understanding the potential strategic challenges and consequences of these pursuits. This leads to the primary question addressed in this paper: What are the potential strategic environmental challenges for integrating cyberspace operations at the tactical level of war as part of the Capstone Concept for Joint Operations 2020 concept of globally integrated operations? This paper's thesis is that a better understanding of the strategic environmental challenges to integrate cyberspace operations to the lowest tactical levels will provide defense leaders and Joint Force Commanders with a better understanding to shape the successful integration of cyberspace operations into tactical echelon force. This paper employs Howard Winton's framework for considering the challenges to military change and examines the inherent tensions surrounding adaptation of new capabilities in the military. The paper concludes with insights of the tensions involved in military adaptation in cyberspace and provides four recommendations to inform and assist defense leaders and Joint Force Commanders to meet the Chairman's vision for cyberspace integration at lower levels in the force. The four recommendations are: 1) to empower the Geographic Combatant Commands with control authorities over cyberspace capabilities; 2) to communicate to national policy makers the strategic utility of future military cyberspace requirements; 3) to develop technical cyberspace situational awareness capabilities at all echelons; and 4) to task organize, versus assign, cyber forces to the tactical level units.

15. SUBJECT TERMS

Cyberspace Operations, Joint Concepts, Strategic Challenges, Tactical Level

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

(This Page Intentionally Left Blank)

NATIONAL DEFENSE UNIVERSITY

JOINT FORCES STAFF COLLEGE

JOINT ADVANCED WARFIGHTING SCHOOL

STRATEGIC UNCERTAINTY: THINKING ABOUT TACTICAL LEVEL CYBERSPACE OPERATIONS

by

Daniel J. Ruder

Colonel, U.S. Army

(This Page Intentionally Left Blank)

Strategic Uncertainty: Thinking About Tactical Level Cyberspace Operations

by

Daniel J. Ruder

Colonel, U.S. Army

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: _____
25 May 2015

Thesis Adviser: Signature: _____
Stephen C. Rogers, Colonel, USA
Thesis Advisor

Approved by: Signature: _____
David C. Rodearmel, J.D., LL.M
Committee Member

Signature: _____
Dr. Robert M. Antis, PhD
Director, Joint Advanced Warfighting School

(This Page Intentionally Left Blank)

ABSTRACT

Joint concepts describe that the growing capabilities of cyberspace operations will further transform how the tactical force will fight during Joint operations in the future, by integrating cyberspace operations down to lower tactical levels to achieve new levels of cross-domain synergy. Although the concept of integrated offensive and defensive cyberspace operations at tactical echelon commands is unproven, joints concepts suggest that this new approach to cyberspace operations is potentially feasible, suitable, and acceptable.

While it may be entirely appropriate to pursue the desired outcomes outlined in joint concepts, and in line with the Chairman's vision, it is not prudent to do so without fully understanding the potential strategic challenges and consequences of these pursuits. This leads to the primary question addressed in this paper: What are the potential strategic environmental challenges for integrating cyberspace operations at the tactical level of war as part of the Capstone Concept for Joint Operations 2020 concept of globally integrated operations?

This paper's thesis is that a better understanding of the strategic environmental challenges to integrate cyberspace operations to the lowest tactical levels will provide defense leaders and Joint Force Commanders with a better understanding to shape the successful integration of cyberspace operations into tactical echelon force. This paper employs Howard Winton's framework for considering the challenges to military change and examines the inherent tensions surrounding adaptation of new capabilities in the military.

The paper concludes with insights of the tensions involved in military adaptation in cyberspace and provides four recommendations to inform and assist defense leaders and Joint Force Commanders to meet the Chairman's vision for cyberspace integration at lower levels in the force. The four recommendations are: 1) to empower the Geographic Combatant Commands with control authorities over cyberspace capabilities; 2) to communicate to national policy makers the strategic utility of future military cyberspace requirements; 3) to develop technical cyberspace situational awareness capabilities at all echelons; and 4) to task organize, versus assign, cyber forces to the tactical level units.

(This Page Intentionally Left Blank)

ACKNOWLEDGEMENTS

This thesis is an attempt to synthesize a number of ideas I encountered while attending the Joint Advanced Warfighting School (JAWS), studying the profession of arms while understanding the challenges that may characterize the future Joint operational environment. During my tenure at JAWS, I was exposed to numerous concepts and takeaways from the lessons that educated my thinking on the future of the Joint Force. Equally important, the guided discussions and student deliberations generated diverse opinions with respect to Joint Force planning and the uncertainties that lie ahead facing Joint Force requirements.

I am particularly indebted to Colonel John Torres (USAF) and Colonel Chris Rogers (USA), for their instruction as the JAWS faculty leads in the elective course *Leading the Joint Force: Development and Future Prospects*. Their experience, insights, and wisdom greatly enhanced my understanding of the Joint Force, from its historical context to its future prospects. In addition, I am grateful to my classmates for the vigorous discussions concerning not only Service and Allied nation perspectives on joint warfighting, but also their perspectives regarding future Joint Force transformation requirements.

I would like to express my gratitude to Colonel Pete Yeager (USMC), my JAWS Seminar II faculty lead, and again to Colonel Chris Rogers, as my Thesis Advisor. Their mentorship, advice, and assistance throughout my tenure at JAWS remained vitally important to any success I have had in the program. I also want to express an appreciation to my Seminar II classmates, for freely offering many bold and innovative ideas on just about every topic. Every day in Seminar was interesting, offering valuable insights into our profession of arms from unique joint and allied perspectives.

(This Page Intentionally Left Blank)

TABLE OF CONTENTS

CHAPTER 1: INTRODUCTION 1
CHAPTER 2: THE CYBERSPACE ENVIRONMENT 5
Future Challenges 9
CHAPTER 3: UNCERTAINTIES OF INTEGRATING TACTICAL LEVEL CYBERSPACE OPERATIONS 13
The Influence of Strategic Requirements and Technology 14
The Influence of Political and Social Values 20
The Influence of Military Service Values and Norms 24
The Influence of Mission Command 27
CHAPTER 4: CONCLUSIONS AND RECOMMENDATIONS 33
Conclusions 33
Recommendations 36
Empower the Geographic Combatant Commands with Control Authorities 37
Communicate the Strategic Utility of Future Military Cyberspace Requirements 37
Develop Cyber Situational Awareness Capabilities at all Echelons 38
Task Organize Cyber Forces to the Tactical Level 39
GLOSSARY: KEY MILITARY TERMS 42
FREQUENTLY USED ABBREVIATIONS: 43
BIBLIOGRAPHY 44
VITA 48

(This Page Intentionally Left Blank)

CHAPTER 1: INTRODUCTION

> All human institutions must inevitably deal with the tension between continuity and change, between preserving that which has met the needs of the past and adapting to the challenge of change in a confusing present and uncertain future.[1]
>
> *Harold R. Winton*

Over the last decade, the U.S. military has expanded operations from its traditional domains of land, air, maritime, and space, to include cyberspace. Specifically, in July of 2011, the Department of Defense codified cyberspace as an operational domain in its own right, when the department published its first ever *Strategy for Operating in Cyberspace*.[2] While all five operational domains are inherently interdependent, the Joint Force's ability to operate effectively within the cyberspace domain is *the* vital thread that interconnects operations in and across the other four domains.[3]

While the Department of Defense has clearly articulated the vital importance of this new domain, the Chairman of the Joint Chiefs of Staff has expressed significant concern over the joint force's ability to exploit the capabilities inherent in this critical domain. In his 2012 *Capstone Concept for Joint Operations 2020 (CCJO),* the Chairman stated that joint forces employ cyberspace operations as adjuncts rather than as integral parts of joint operations. He asserts, however, that integrating these capabilities, just as the joint force has learned how to integrate special operating and general-purpose forces, will generate the potential to expand combat power and dramatically increase the effectiveness of other standing capabilities.[4]

---

[1] Harold Winton, and David Mets, eds., *The Challenge of Change: Military Institutions and New Realities, 1918-1941* (University of Nebraska Press, 2000) xi.

[2] Cherl Pellerin, "DOD Releases First Strategy for Operating in Cyberspace," *DoD News Article, July 14, 2011,* (Accessed April 2, 2015). http://www.defense.gov/news/newsarticle.aspx?id=64686

[3] U.S. Joint Chiefs of Staff, *Capstone Concept for Joint Operations: Joint Force 2020,* (Washington, DC: Joint Chiefs of Staff, September 10, 2012), 2-3, 5.

[4] Ibid., 7.

Joint operating concepts, such as the CCJO, guide future force development by proposing new approaches and capability requirements for military challenges envisioned in the future security environment.[5] Guided by these joint concepts, the military Services contribute to the intellectual and analytical study of the future military challenges by exploring innovative joint or Service-unique concepts in support of defense priorities. By comparison, the process of military adaptation may present itself in the form of these future force concepts. It is necessary to note that the new military approaches described within joint concepts are based on the synthesis of strategic guidance and direction contained in, inter alia, defense strategic guidance, the National Military Strategy, the Unified Command Plan, and the Chairman's Risk Assessment.[6] Joint concepts are informed by strategic guidance and thus guarded against change that may be viewed as radical or impractical.

If the Services are to develop the subordinate concepts and capabilities, and the joint force is to learn how to integrate them to meet the Chairman's vision, then the total force will have to, by necessity, become inherently comfortable with relying more on cyberspace to conduct operations in and across the air, land, sea, and space domains. Moreover, the joint force will also have to fulfill the joint concepts' other assertions that operations in all domains will require synchronization and integration to create cross-domain synergy at *increasingly lower levels* in the Joint Force.[7] These concepts envision

[5] Joint Chiefs of Staff, *Guidance for Development and Implementation of Joint Concepts* (Washington DC: The U.S. Joint Chiefs of Staff, 22 November 2013), A-1 – A-5.

[6] Ibid. The Capstone Concept for Joint Operations (CCJO) informs development of subordinate joint and Service concepts.

[7] U.S. Joint Chiefs of Staff, *Capstone Concept for Joint Operations*, 7. See also U.S. Joint Chiefs of Staff, *Joint Operational Access Concept*, Version 1.0 (Washington, DC: Joint Chiefs of Staff, January 17, 2012), ii, 30. The *JOAC* requires tactical echelon units to exploit opportunities in cyberspace against adversaries with the inclusion of offensive and defensive cyberspace operations integrated increasingly lower tactical levels.

that the growing capabilities of cyberspace operations will further transform how the tactical force will fight during joint operations in the future, by integrating cyberspace operations down to the *lower tactical levels* to achieve new levels of cross-domain synergy.

While the concept of integrated offensive and defensive cyberspace operations at lower tactical levels is unproven, joint concepts suggest that this new approach to cyberspace operations is potentially suitable, feasible, and acceptable for achieving strategic and political goals in the future. Indeed, the principles of joint concept development requires synthesis of strategic guidance by the Joint Staff.[8] While it may be entirely appropriate to pursue the desired outcomes outlined in joint concepts, and in line with the Chairman's vision, it is not prudent to do so without fully understanding the potential strategic challenges and unintended consequences of these pursuits. This leads to the primary question addressed in this paper: What are the potential strategic environmental challenges for integrating cyberspace operations at the tactical level of war as part of the CCJO's future concept of globally integrated operations?

In this paper, I intend to prove that by better understanding the strategic environmental challenges of integrating cyberspace operations to the lowest tactical levels, Joint Force Commanders will have a better understanding of the requirements and associated methods to shape how the future Joint Force 2020 will integrate cyberspace operations into the tactical force.

To accomplish this, Chapter 2 will address the prominent challenges of the cyber domain by defining, describing, and discussing the cyberspace domain and the challenges

[8] Joint Chiefs of Staff, *Guidance for Development and Implementation of Joint Concepts,* A-1–A-5.

existing between the current cyber environment and the environment envisioned by multiple joint concepts. Chapter 2 also describes what cyberspace operations consist of, and what "tactical level" refers to in context of conducting cyberspace operations. Building upon these assertions, this will set conditions for an analysis of the challenges inherent with such change in Chapter 3.

The military instrument of national power exists to serve national interests, and the political and social value placed on the military's increased role in cyberspace requires understanding its political and social dimensions. Howard Winton has developed a framework that accounts for these specific dimensions and the inherent tensions surrounding military change and the adaptation of new capabilities in the military. The third chapter of this paper will employ Winton's framework to addresses the potential implications for adapting tactical cyberspace operations in that context.

The paper concludes with insights of the tensions involved in military adaptation in cyberspace and provides four recommendations to inform and assist defense leaders and Joint Force Commanders to meet the Chairman's vision for cyberspace integration at lower levels in the force. The four recommendations are: 1) to empower the Geographic Combatant Commands with control authorities over cyberspace capabilities; 2) to communicate to national policy makers the strategic utility of future military cyberspace requirements; 3) to develop technical cyberspace situational awareness capabilities at all echelons; and 4) to task organize, versus assign, cyber forces to the tactical level units.

CHAPTER 2: THE CYBERSPACE ENVIRONMENT

Although no longer the province of science fiction, defining cyberspace is surprisingly difficult. Once referred to as a "notional environment" and then a "nervous system--the control system for the country," the definition of cyberspace has been open to change by the Department of Defense (DoD) on four occasions.[1] The DoD settled on its current definition for cyberspace in 2008, and defined it as a "global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[2] This dictum characterizes the technical elements of cyberspace; however, Dr. Daniel Kuehl draws the distinction that the cyberspace domain is more than an electronic paradigm of interconnectivity between computers and networked technologies. The platforms that comprise cyberspace reside in the physical world, with shared relationships to human users that affect "human behavior and decision-making."[3] Franklin Kramer adds that cyberspace capabilities are also an element of national power, and inclusive of societal activities.[4] Thus, it is necessary to understand the cyberspace context in terms of having political and societal implications.

---

[1] Daniel T.Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," in *Cyberpower and National Security*, ed. Franklin Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, D.C.: National Defense University, 2009), 28.

[2] U.S. Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms,* Joint Publication 1-02 (Washington, DC: Joint Chiefs of Staff, November 8, 2010, as amended through January 15, 2015), 58.

[3] Kuehl, From Cyberspace to Cyberpower, 28. Kuehl adds that the technologies created that use cyberspace are physical platforms analogous to military vehicles, ships, aircraft, and satellites used in the other physical domains.

[4] Franklin Kramer, "Cyberpower and National Security: Policy Recommendations for a Strategic Framework," in *Cyberpower and National Security*, ed. Franklin Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, D.C.: National Defense University, 2009), 11-12.

Cyberspace capabilities are also transforming the way the Joint Force conducts military operations from the strategic to the tactical levels. Indeed, due in part to the pace of technological change, the Joint Force's dependency on cyberspace capabilities will grow exponentially over the next decade, from its reliance on networked technologies to communicate, to its ability to deploy and maneuver forces in joint operations.[5] Cyberspace capabilities constantly evolve, and the U.S. military has aggressively moved to understand, adapt to, shape, and invest in this operating environment to meet the future demands of the Joint Force and Combatant Commanders.[6] As described in the opening chapter, cyberspace is an operational domain. All five domains are interdependent and all have unique characteristics that demand a synchronized and coordinated examination of the Joint Force's role, issues, and requirements.[7]

According to joint doctrine, the range of cyberspace operations includes three mission sets: DOD Information Network operations (DODIN), defensive cyberspace operations, and offensive cyberspace operations. In describing the range of cyberspace operations, it is useful to understand them in context of the traditional warfighting capabilities of mobility, protection, and firepower. Mobility is a characteristic of DOD Information Network Operations, defined as "actions taken to design, build, configure, secure, operate, maintain, and sustain DOD communications systems and networks in a way that creates and preserves data availability, integrity, [and] confidentiality."[8]

---

[5] U.S. Joint Forces Command, *The Joint Operating Environment (JOE) 2010* (Suffolk, VA: U.S. Joint Forces Command, February 18, 2010), 34.

[6] Department of Defense, *Quadrennial Defense Review Report* (Washington, DC: 2014), x.

[7] U.S. Joint Chiefs of Staff, *The National Military Strategy of the United States of America 2011: Redefining America's Military Leadership* (Washington, DC: U.S. Joint Chiefs of Staff, February 8, 2011), 3, 9.

[8] U.S. Joint Chiefs of Staff, *Cyberspace Operations*, Joint Publication 3-12(R), (Washington, DC: U.S. Joint Chiefs of Staff, February 12, 2013), II-3.

Mobility can be viewed as the movement of data and content across the DoD information environment. Tactical echelon military units that deploy with, install, operate, and maintain digital networks conduct DODIN operations.

Protection is a characteristic of defensive cyberspace operations (DCO) and is applicable to all units that provide cybersecurity measures for military networks. The execution DCO includes "passive and active cyberspace defense operations to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities, and other designated systems."[9] Defensive cyberspace operations include two subcategories that add the characteristic of firepower to defending networks. Internal Defense Measures (DCO-IDM) are those conducted within the boundaries of the DoD ".mil" domain, or within a military unit's network perimeter within the DODIN, and "include actively hunting for advanced internal threats as well as the internal responses to these threats."[10] The other subcategory of DCO is Response Actions (DCO-RA), "those deliberate, authorized defensive actions which are taken external to the DODIN to defeat ongoing or imminent threats to defend DOD cyberspace capabilities or other designated systems."[11] Similar to combining the elements of protection and firepower, DCO-RA characterizes some of the required capabilities identified for lower tactical levels in the future force. Today, however, DCO-RA "require authorization within applicable rules of engagement as those operations could result in the use of force."[12]

The element of firepower best characterizes offensive cyberspace operations (OCO). The conduct of OCO "project[s] power by the application of force in and through

[9] Ibid., II-2.
[10] Ibid., II-3.
[11] Ibid.
[12] Ibid.

cyberspace. …[and] will be authorized like offensive operations in the physical domains."[13] Since OCO are deliberate offensive actions taken external to the DODIN, the Joint Publication for *Cyberspace Operations* cautions that the "growing reliance on cyberspace around the globe requires carefully controlling OCO, requiring national level approval. This requires commanders to remain cognizant of changes in national cyberspace policy and potential impacts on operational authorities."[14] Similar to DCO-RA, OCO capabilities characterize the required capabilities described in Joint concepts for lower tactical levels in the future force.

The term "tactical level" in this paper refers to an echelon in the Joint Force versus a specific method of cyberspace operations. Joint doctrine describes the three levels of warfare as strategic, operational, and tactical, which recognizes that military operations are designed and executed with resources and tasks assigned to the appropriate levels of command associated to the operation.[15] While tactical echelon commands can range from those under command of a two-star general or flag officer, to a company commander, it is the lowest level echelon most often characterized by the concentration of military force and offensive tactics to achieve military objectives. Joint concepts that stipulate the devolution of cyberspace operations to new lower levels is thus considered in this paper in context of integrating cyberspace capabilities to tactical echelon commands in support of tactical missions and plans in those units.

---

[13] Ibid., II-2.

[14] U.S. Joint Chiefs of Staff, *Cyberspace Operations,* Joint Publication 3-12(R), II-7-8.

[15] U.S. Joint Chiefs of Staff, *Doctrine for the Armed Forces of the United States,* Joint Publication 1, I-7-8. At the strategic level, policy and strategic obejctives are developed by the President, National Security Staff, and Secretary of Defense, inter alia. At the operational level, Combatant Commanders and Joint Force Commanders establish military operational objectives that link strategic objectives to tactical tasks and actions.

The differences in the types of cyber targets and the purpose of achieving effects on those targets presents a useful distinction between cyberspace operations conducted at the strategic and tactical echelons. A study conducted by the Center for Strategic and International Studies (CSIS) suggested that *strategic* targets could include "major national command and control networks" and those that can have an effect on the minds and thinking of potential adversaries.[16] Strategic targets inherently require long lead times in planning and preparation before execution is possible. Cyberspace operations at the tactical level, conducted by tactical echelon commanders, have a more limited focus and potentially require less time to plan and execute. For example, tactical echelon commanders "might wish to use cyber capabilities in a more limited sense (e.g., to deny local communications for a limited period of time, disrupt a maneuver lane by shutting down traffic signals in a portion of a city, or suppress a tactical weapons targeting system)."[17] Tactical commanders are also likely "to employ cyber attacks as part of shaping activities in support of local scheme of maneuver or fires and to be confronted with fleeting or "pop-up" targets that are difficult to anticipate in advance."[18]

Future Challenges

The priority for offensive and defensive cyberspace operations is apparent in the *Joint Operational Access Concept (JOAC).* The JOAC requires tactical echelon units to exploit opportunities in cyberspace against adversaries, with the inclusion of joint offensive and defensive cyberspace operations integrated at increasingly lower tactical

[16] Maren Leed, "Offensive Cyber Capabilities at the Operational Level - The Way Ahead," *Center for Strategic & International Studies*, (2013), 3.
[17] Ibid.
[18] Ibid.

levels.[19] The *JOAC* envisions maneuvering in and through cyberspace and penetrating enemy digital networks, effectively operationalizing cyberspace at the tactical level. The JOAC also acknowledges that offensive cyber fires must be managed and coordinated with fires originating in the other domains, but challenges of control must be resolved.

> "While that is true today for traditional nonlethal fires such as electronic jamming, it may not be true for certain cyber and space capabilities, which today are controlled by supporting functional combatant commands. This concept envisions that control of such capabilities in the future will devolve to lower echelons to make the fires more responsive to the needs of operational commanders. The precise level to which that control can appropriately devolve remains to be determined."[20]

Fortunately, that examination is underway, as the military Services have begun assessing the viability of integrating cyberspace capabilities and cyberspace operations down to their tactical echelon units. The U.S. Marine Corps and the U.S. Army have stated their intent to explore the potential of making the full range of cyberspace capabilities organic to their tactical units. The U.S. Army Cyber Command, for example, envisions a concept that would include attaching "cyberteams" to tactical brigade and lower units, while the Marine Corps Cyber Command envisions placing "cyber Marines" down to the Marine Air Ground Task Force (MAGTF) tactical level, and perhaps even in lower units.[21] However, the clarity of Army and Marine Corps' vision to integrate

[19] U.S. Joint Chiefs of Staff, *Joint Operational Access Concept*, ii, 30.

[20] Ibid., 30.

[21] James Sanborn, "Tactical Hackers: Cyber Steps Up its Roles on the Battlefield," *Marine Corps Times* (1 September 2014): 18-19, and Joe Gould, "Ground Commanders with Cyber Skills: Leaders Consider Adding New Offensive Tactics to CTC Rotations," *Army Times* (1 July 2014). An Army Brigade is a tactical echelon unit and can be employed on independent or semi-independent operations and is normally commanded by a Colonel (O-6) with 21-25 years in service. A MAGTF is also a tactical echelon organization, with a flexible structure that can vary in size and can operate independently or as part of a larger coalition. The MAGTF is a temporary organization formed for a specific mission and can be commanded by Lieutenant Colonel (O-5), when organized as a battalion, and up to a two-star general officer when organized as a division.

cyberspace operations into tactical operations is blurred by the uncertainty of whether control over cyberspace capabilities can devolve to that level.

Defense analysts, too, are evaluating cyber-themed scenarios that address the potential of cyberspace operations conducted at the tactical echelons. While their observations express multiple viewpoints from the military Services, the results thus far have been far from conclusive without systematic experimentation.[22] Among the multiple viewpoints, some challenge the viability of cyberspace operations at the tactical level. Those concerns include the fact that the Defense Department (DoD) does not have a clear understanding of how offensive cyberspace operations would actually be employed at the tactical level. That rationale is based on the idea that DoD has only focused previously on the strategic and operational level employment of those capabilities.[23] That rationale is supported to some degree in that policy and strategy documents have tended to emphasize cyber defense, and to a much lesser extent cyber offense, both in terms of national security and military priority. The Deputy Secretary of Defense has even expressed concerns "that cyberspace is at risk of being militarized," and defense strategy has purposely stressed cyber defense rather than offense.[24] Other viewpoints express concern that offensive cyberspace operations generate effects that are difficult to control, and even more difficult to predict, that it could lead to unintended consequences across the range of diplomatic, informational, military, and economic environments.[25]

[22] Leed, "Offensive Cyber Capabilities at the Operational Level - The Way Ahead," 8-9.
[23] Ibid, 4.
[24] Lynn, William J. "Deputy Secretary of Defense Speech." *U.S. Department of Defense*. http://www.defense.gov/ speeches/speech.aspx?speechid=1593 (accessed September 9, 2014).
[25] Leed, Offensive Cyber Capabilities at the Operational Level, 3.

Among the challenges that current Joint concepts identify for future Joint Force operations, is how to employ cyberspace capabilities in relevant ways into the next decade and beyond. Henry Kissinger acknowledges that cyberspace is strategically indispensable and he appropriately captured the challenge when he wrote, "cyberspace challenges all historical experience."[26] Likewise, the rapid advancements in technology has resulted in cyberspace capabilities that exist today, but have "outstripped strategy and doctrine."[27] Addressing the future challenges to adapt cyberspace operations to lower levels therefore requires understanding the inherent uncertainties that affect military adaptation.

[26] Henry Kissinger, *World Order*, (New York, NY: Penguin Press, 2014), 344.
[27] Ibid.

CHAPTER 3: UNCERTAINTIES OF INTEGRATING TACTICAL LEVEL CYBERSPACE OPERATIONS

> Of all the many policies our citizens deserve--and need--to understand, none is so important as those related to our topic today--the uses of military power. …In today's world, the line between peace and war is less clearly drawn than at any time in our history. …War may be different today than in Clausewitz's time, but the need for well-defined objectives and a consistent strategy is still essential.[1]
>
> The Honorable Casper W. Weinberger
> Secretary of Defense, 1984

What are the strategic challenges for employing offensive and defensive cyberspace operations at the tactical level of war? This is a challenging question for two reasons: the concept itself is unproven and the answer depends on a range of interdependent variables external and internal to the military. Unlike doctrine, which reflects extant capabilities and guides current joint forces during operations, joint concepts propose solutions to problems where "existing doctrinal approaches and joint capabilities are deemed inadequate."[2] While it is not feasible today for tactical level commanders to control cyberspace capabilities, such as offensive cyber fires, the JOAC's vision of decentralizing that control to lower echelons is not constrained by existing "policy, treaties, laws, or technology."[3] Thus, unconstrained by factors in the strategic environment, the concept of cyberspace operations at the tactical level of war entails a degree of inherent uncertainty. Such uncertainty might involve potential policy changes for the rules of engagement in cyberspace, flexibility needed with cyberspace legal

[1] Casper Weinberger, "The Uses of Military Power," *Remarks to the National Press Club* (Washington DC, November 28, 1984) http://www.pbs.org/wgbh/pages/frontline/shows/military/force/ weinberger.html (accessed September 7, 2014).

[2] Joint Chiefs of Staff, *Doctrine for the United States Armed Forces*, (Washington DC: The U.S. Joint Chiefs of Staff, 25 March 2013) JP 1, VI-3, VI-9.

[3] Joint Chiefs of Staff, *Guidance for Development and Implementation of Joint Concepts* (Washington DC: The U.S. Joint Chiefs of Staff, 22 November 2013), A-3. Joint concepts consider these factors during development, but are not limited by them.

authorities and decentralizing control, and the potential of technology to enable or even alter the concept. Cyberspace also affects human behavior and decision-making, as noted previously, therefore American society's understanding, and desire, of the uses of military cyberpower could affect future national policy that govern those capabilities. If not examined, these external drivers of uncertainty could "negate or marginalize the desired improvements in the operational capability."[4]

To understand the uncertainty and tensions that might influence constructs for employing cyberspace operations at lowers levels, it is necessary to consider the fundamental factors that influence change in the military. In the introductory pages of the book *The Challenge of Change,* Dr. Winton highlights the importance of critical factors in both continuity and change that affect military adaptation. Those tensions exist between preserving what has traditionally worked in the past during war and the pressures to adapt new means of warfighting in an uncertain future.[5] Dr. Winton's framework considers the challenges to military change along three primary factors: the external tensions generated by strategic requirements and technology, the external tensions generated by the political and social values of the state, and the internal characteristics of the military itself. The following section elaborates on Dr. Winton's framework in the context of potential challenges to integrate cyberspace operations at the tactical level.

The Influence of Strategic Requirements and Technology

The first step of Winton's framework emphasizes the importance of understanding of the changing character of warfare in its political, social and military

[4] Joint Chiefs of Staff, *Guidance for Joint Concepts,* A-5.
[5] Winton, and Mets, eds. *The Challenge of Change*, xi.

contexts.[6] The process involves ascertaining reasonable answers to questions such as "where the armed force is likely to fight, against whom, under what circumstances, and for what purposes."[7] These questions also point to the necessity for interpreting what future conflict might entail, which the *CCJO* and the *JOAC*, suitably address. The endemic uncertainty of future conflict, however, poses the risk of misinterpreting future threats and thus preparing Joint Force concepts for the wrong type of war.[8] Indeed, these strategic calculations are not new and highlight what Carl von Clausewitz concluded about war, that war is political, "an instrument of policy."[9] Both Clausewitz and Sun Tzu probed the strategic calculations regarding the role of force, the method of employing force, and what ideal victory looks like, all within the context of formulating strategic policies and guidance for waging war.[10]

Current strategic guidance acknowledges the requirement to dominate in the cyberspace domain and directs the Joint Force to retain the foundational capabilities to prevail against progressively more capable adversaries.[11] The circumstances for future conflict in cyberspace centers on the fact that the cyberspace domain presents symmetrical and asymmetrical advantages for the United States, as well as to its potential adversaries. More importantly, cyberspace is increasingly becoming a more contested *battlespace* domain in which conflict will increasingly occur.[12] As the CCJO notes:

---

[6] Ibid., xi-xii.

[7] Ibid., xiii.

[8] Ibid., xii.

[9] Carl Von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1989), 30.

[10] See Michael Handel, "Comparing Sun Tzu and Clausewitz." In *Masters of War: Classical Strategic Thought*, 3rd Rev. and Expanded ed. (London: Frank Cass, 2001), 21-22.

[11] Barack Obama, *National Security Strategy* (Washington, DC: Government Printing Office, February 2015), 8, 12.

[12] Richard Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (New York: Harper Collins, 2010), 69-70.

> [The proliferation of cyberspace weapons] will grant more adversaries the ability to inflict devastating losses. These threats place our access to the global commons at risk, target our forces as they deploy to the operational area, and can even threaten forces at their points of origin. …Adversaries will not only have more advanced capabilities in every domain. More of them will have the ability to simultaneously fight across multiple domains. Space and cyberspace will play a particularly important role in the years ahead. As these domains figure more prominently in the projection of military power, operations in them will become both a precursor to and integral part of armed combat in the land, maritime and air domains.[13]

While strategic guidance is suitable to consider new military approaches to dominate in cyberspace, the United States is meanwhile grappling with important U.S. foreign policy implications of offensive cyber power.[14] The proliferation of offensive cyber capabilities is fundamentally changing the character of warfare and more nations, states, and non-state actors are increasing their ability to exploit cyberspace. As the National Committee on American Foreign Policy (NCAFP) surmised, "offensive cyber capabilities are increasingly being incorporated into the military equation of major and minor powers and by non-state actors. …serious challenges remain, including reaching agreement on how (and no longer if) the UN Charter, international law and the laws of arm conflict apply in this new age."[15] Thus, there are potentially larger implications in the U.S. foreign policy realm if the Nation's military increases its offensive cyberspace capabilities as a fires projection capability at the tactical level.

The role of the military in cyberspace, whether in support of military objectives or in support of political expediency in other national matters, shapes the degree to which

[13] U.S. Joint Chiefs of Staff, *Capstone Concept for Joint Operations,* 2.

[14] George Schwab, "Cybersecurity: Challenge and Resposnse, A New Generation Speaks Out," International Committee on American Diplomacy, (Novemeber 6, 2013) 9. http://www.ncafp.org/ncafp/wp-content/uploads/2013/12/NCAFP-Cyber-Roundtable_Cybersecurity-Challenge-Response_Nov6.13.pdf (accessed November 12, 2014).

[15] Ibid.

offensive and defensive strategies and capabilities are needed in military operations. Cyberspace commentators often cite former Deputy Secretary of Defense William Lynn on his frank assessment that "in cyberspace, the offense has the upper hand. …in an offense-dominant environment, a fortress mentality will not work. The United States cannot retreat behind a Maginot Line of firewalls or it will risk being overrun. Cyber warfare is like maneuver warfare, in that speed and agility matter most."[16] Irrespective of being overrun or outflanked in cyberspace, the primacy of the offensive in cyberspace, as Lynn describes, strikes into the often-debated topic concerning cyberspace strategies and the rationale for either an offensive or a defensive dominant approach. The approach matters, in a strategic context, because the offense or defense approach influences how other nation-states and societies perceive the United States will use their cyberspace capabilities. Even in light of potential future power balances in cyberspace, the uncertain strategic requirements of national policy could affect realizing the full benefit of tactical level cyberspace operations in the Joint Force.

In theory, the perception of a nation's offense-defense balance can create a security dilemma. How other nations and actors understand the offensive-defensive balance of a particular nation can shape perceptions of how that nation intends to employ their capabilities. The offense-defense debate highlights the theory that when a nation adopts technical capabilities that favor the offense, the nation's military strategies will become predominantly offensive oriented. Conversely, a nation with stronger defensive

[16] William J. Lynn, "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs*, (September/October 2010), http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain (accessed December 2, 2014).

technical capabilities will tend to devise defensively oriented military strategies.[17] Robert Jervis, in *Cooperation Under the Security Dilemma*, asserts that nations with a militarily superior offensive technical capability tend to engage in short duration conflicts and seek to minimize the costs endured. Offensive superiority also favors the advantage of initiative in conflict, making preemptive action a valid strategic consideration.[18] In question then, is whether increasing the technical capability of the tactical force to conduct offensive and defensive response actions in cyberspace has any bearing on national level policy or generates a new level of strategic uncertainty.

In a roundtable report by the National Committee on American Foreign Policy, U.S. and international speakers suggested that the United States does not have a coherent strategy for cyberspace. On one hand, U.S. strategies emphasize, "a peaceful and stable cyberspace; and the other heavily focused on developing military and intelligence cyber capabilities or exploiting cyberspace for political or strategic effect, thus sending confusing signals to other countries."[19] The report highlights that there is a wider international perception that the cost benefit ratio of conducting cyberspace operations to achieve U.S. objective verses deployment of U.S. forces, favors a U.S. offensive approach in cyberspace. These perceptions of the United States follow that after more than a decade of war, the Nation is weary of further troop deployments and favors offensive cyberspace operations as an attractive alternative.[20] Martin Libicki, a prominent

[17] For detailed review of offensive-defensive theory, see Stephen Van Evera, *Causes of War: Power and The Roots of Conflict*, (New York: Cornell University Press, 1999), and Robert Jervis, "Cooperation Under the Security Dilemma," *World Politics*, Vol. 30, Issue 2 (January 1978) 161–214.

[18] Jervis, "Cooperation Under the Security Dilemma," *Politics*, Vol. 30, No. 2 (January 1978) 187-193. Jervis also contends with factors of geography, that geographically isolated countries are less likely to pose a security dilemma for their neighbors.

[19] Schwab, Cybersecurity: Challenge and Resposnse, 9.

[20] Ibid., 8.

cyber analyst, suggests that if an offense-defense cyberspace balance favors the offense, arguably "the damage from a cyberattack would be unacceptable or the resources that must be spent on defense are unaffordable. The United States therefore has no recourse but to hit back after the fact."[21]

Compared to strategic uncertainty, "technological uncertainty is equally perverse."[22] The impact of technology on future warfare is perhaps less predictable today than at any point in history. For example, the employment of airpower in 1918 and its tactical advantages was measurably offset with development of antiaircraft artillery countermeasures that followed afterwards. In comparison, nations with less material wealth to confront the United States militarily will bolster their capabilities in cyberspace as an alternative to achieve their political goals. Jervis asserts that if offensive has the advantage, status quo nations or actors will still seek offensive weapon capabilities.[23] However, the status quo from a technological perspective is difficult to determine and Jervis contends that the distinction between offensive and defensive weapons, or capabilities, is difficult to define.[24] Although Defensive Cyberspace Operations – Response Actions can create cyber effects similar to offensive cyberspace operations, nation-states, groups and individuals might not distinguish the difference between U.S. offensive and defensive cyberspace capabilities. Is essence, both capabilities render attack-like effects. To Jervis' point, Kissinger is remindful that "the history of warfare

[21] Martin Libicki, *Cyberdeterrence and Cyberwarfare* (Santa Monica, CA: RAND, 2009), 35. Libicki does not argue in favor of an offensive dominant military approach in cyberspace. This quote from Libicki was one element of a broader contrast between cyberdefense, cyberdeterrence, cyberretaliation, and cyber warfare. Libicki argures in favor of military cyberdefense strategies, and offensive cyberretaliation should only be on element of an approach among the uses of all elements of national power.

[22] Winton, and Mets, eds. *The Challenge of Change,* xiii.

[23] Jervis, Cooperation Under the Security Dilemma, 201.

[24] Ibid.

shows that every technological offensive capability will eventually be matched and offset by defensive measures."[25] From the security dilemma perspective, this could become a challenge to the concept of integrating offensive cyberspace capabilities into the tactical force if tensions over international power balances dominate the national cyberspace policy debate. Therefore, national support for growing the military cyberspace capabilities at even lower levels in the Joint Force must also be understood in terms of the political and societal value placed on military cyberspace adaptation.

The Influence of Political and Social Values

The second general observation is that adaption in military affairs is contextual, influenced by the political and social structure in which the military resides. Winton observes that the "dictates of the political and social values of the state" drive military adaptation, influenced by factors such as cultural norms and perceptions regarding the military's role in society, and resource availability.[26] Historical references also support Winton's observations and general conclusions that the level of national investment in a military change is subject to the political will to do so, the popular desire of society to support the change, and the imperatives of national interests.

The influence of communist party reforms in the early twentieth century and its political and social popularity amongst workers in Russian society, as Dennis Showalter explains, was decisive in the revolutionary transformation of the Soviet Army and Soviet society into a total "warfare state."[27] J.F.C. Fuller also cites that from its inception, the Soviet Red Army's purpose extended beyond solely military purposes. The Red Army

[25] Kissinger, *World Order*, 346.
[26] Winton, and Mets, eds. *The Challenge of Change,* xiii, xv.
[27] Dennis Showalter, "Military Innovation and the Whig Perspective of History," in The Challenge of Change: Military Institutions and New Realities, 1918-1941 (University of Nebraska Press, 2000) 222.

served as a political and social revolutionary instrument for international class warfare to unite the proletariat in a new Communist society organized in a struggle against capitalism.[28] The relationship between the military and society was also evident in the case of reform in the German army during the interwar period. As Showalter describes, the ideology of National Socialism acted as a "bridge between a small professional force" in Germany's Wehrmacht army, "…and a cohort of young men willing to seek military service as a rite of passage denied to them by the Versailles Treaty."[29] The prevailing cultural norms in the German army staff during the interwar period emphasized critical thought, strategic acumen, and examination of lessons from previous wars. James Corum highlights that the prevailing German *political*, *social*, and *military culture* coalesced in ways, for right or wrong, that supported the German army's concept development for future warfare and highlighted the importance of anticipating future requirements for military adaptation.[30]

Today, a similar relationship and interaction between political and social values, or behavior, is so significant and unpredictable, as Colin Gray describes, that those factors alone could invalidate military force planning derived from concepts. Yet, military planners often underappreciate the political and social interactions on force planning and fail to realize that the approaches designed in military force planning are subject to political approval. The military instrument of national power exists to serve national interests, and "there is no evading specification either of how American society

[28] J.F.C. Fuller, *The Conduct of War, 1789-1961* (New Brunswick, NJ: Rutgers University Press, 1961), 202-204.

[29] Showalter, "Military Innovation and the Whig Perspective of History," 230-231.

[30] James Corum, "A Comprehesnive Approach to Change, Refrom in the German Army in the Interwar Period," in The Challenge of Change: Military Institutions and New Realities, 1918-1941 (University of Nebraska Press, 2000) 37, 63-64.

needs to be served or, more realistically, the method by which American society can proceed to determine the service that it needs."[31] This caution from Gray resonates when considering that the political value placed on national cybersecurity measures has not always found coherence with the value that citizenry places on the topic. For example, the Edward Snowden revelations on U.S. intelligence agencies' surveillance programs heightened tensions between the United States, its allies, and the international community almost overnight.[32] Domestically, calls sounded for placing new restrictions on the DoD's use of cyberspace operations in the aftermath of Snowden's leaks.[33]

Clearly, cyberspace has become an integral underpinning to national security and an integral element of society's life and vital to its infrastructure. Strategic guidance addresses this vital relationship between protecting national security in cyberspace while safeguarding the society's civil liberties.[34] However, cybersecurity issues frequently feature in news headlines, enmeshed with geopolitical and domestic social sensitivities. The issues span policy and proposed legislative actions, all designed to secure America's cyberspace infrastructure while balanced against protecting personal information and privacy rights. The government's role in protecting privately owned critical infrastructure in cyberspace "has been one of the most contentious issues in the debate about

[31] Colin Gray, *Explorations in Strategy*, (Westport, Conn.: Greenwood Press, 1996), 112-113.

[32] Zygmunt Bauman, et al., "After Snowden: Rethinking the Impact of Surveillance," *International Political Sociology*, (2014) 121-144. http://onlinelibrary.wiley.com/doi/10.1111/ips.12048/epdf (accessed November 12, 2014).

[33] Ellen Nakashima, "U.S. Cyberwarfare Force to Grow Significantly, Defense secrEtary Says," *The Washington Post*, (March 28, 2014), http://www.washingtonpost.com/world/national-security/us-cyberwarfare-force-to-grow-significantly-defense-secretary-says/2014/03/28/0a1fa074-b680-11e3-b84e-897d3d12b816_story.html (accessed November 12, 2014).

[34] Obama, *National Security Strategy*, 3.

cybersecurity legislation."[35] The tension created for potential military change rests on uncertainty whether political and social values will intersect in ways that support future increases military offensive cyber warfare capabilities, with control extended down to even lower levels.

Support for adaption in military affairs is nevertheless contextual. Even the "new normal" in the relationship between U.S. political and military systems created by the wars in Afghanistan and Iraq, as claimed by Andrew Bacevich, is subject to change. Politically, war was valued as an "open-ended enterprise" and it elevated the social popularity of the military to a hero status.[36] National investment in the changing needs of the military was thus valued as a political and social "sacred obligation."[37] Bacevich highlights the exemplary nature of our society's cultural norms and values, as well as our nation's policies of ensuring resource and material availability to our military, but that support was in context of fighting two simultaneous wars. Given the political and social tensions surrounding DoD's use of cyberspace operations, military force planners must consider the shifting of political and social imperatives of the day and the potential impacts on realizing joint concepts.

Another consideration is the impact of increasing the role of the military in cyberspace as a political instrument of national power. The increased capability of the DoD and U.S. military in cyberspace can influence political leaderships' preference for

[35] Congressional Research Service, *Federal Laws Relating to Cybersecurity: Major Issues, Current Laws, Proposed Legislation, Decemebr 12, 2014*, (Washington, DC: Government Printing Office, 2014), 13.

[36] Andrew Bacevich, *The New American Militarism: How Americans are Seduced by War* (New York: Oxford University Press, 2005) 235.

[37] Ibid.

military options, at the expense of potential political or diplomatic approaches.[38] The Snowden revelations regarding the PRISM surveillance program specifically exacerbated tensions concerning domestic and internal personal privacy rights. Snowden's disclosures raised concerns among many observers that U.S. intelligence agencies hacked into U.S. and foreign companies, and inserted backdoors in support of espionage efforts.[39] Undoubtedly, the Snowden revelations have hurt the trust between governments, but it points to greater questions of precedent, and the consequential effects of military cyberspace operations that can generate negative strategic outcomes, even inadvertently. In instances where cyber effects are not reversible, it may cast doubts on the potential utility for the tactical level force to use a cyber capability offensively, as well as domestic and international concerns over legal authorities and policy concerns.[40] Assuming however, that authorities remain tightly controlled, what other ways can control be established to enable tactical echelon cyberspace operations and greater cross-domain synergy at lower levels?

The Influence of Military Service Values and Norms

The Third general observation of uncertainty in military change proposed by Dr. Winton, is that military adaptation is influenced by Service culture, values, and norms. Military culture draws upon some of the characteristics of society from where forces originate, but in large part, military culture is influenced by the Services' role during wartime.[41] During war, Service cultures mature and shape the paradigms for how the

[38] Ilai Saltzman, "Cyber Posturing and the Offense-Defense Balance," *Contemporary Security Policy*, 34:1, http://dx.doi.org/10.1080/13523260.2013.771031 (accessed November 2, 2014) 43.
[39] Schwab, Cybersecurity: Challenge and Resposnse, 9-10.
[40] Leed, Offensive Cyber Capabilities at the Operational Level, 8.
[41] Winton, and Mets, eds. *The Challenge of Change*, xiv.

Services view themselves and their relationships with other Services. Inter-Service relationships during peacetime may act as internal drivers that affect the potential for uniformly adapting cyberspace operations across Joint Forces at the tactical level of war.

The land, maritime, and air domains each have unique operating environments that require Service-unique capabilities. Cyberspace is a global domain with its own unique characteristics; however, it crosscuts the other domains and is a shared space among all the Services. Two military authors recently stressed that current Service capabilities overlap so greatly that the focus of joint operations have shifted from "coordination along the seams of geographically defined Service boundaries *to integration of Service capabilities within shared domains.*" (emphasis in the original)[42] The DoD recognized in 2008 that because the combatant commands and military Services required the ability to operate in cyberspace "the domain does not fall within the purview of any particular department or component."[43] Yet, post-war trends historically portray a reduction in inter-Service coordination. Specifically, "the end of combat operations in Iraq and Afghanistan will remove a powerful impetus for inter-Service cooperation. Second, defense budget reductions could result in prioritization of unique Service requirements over joint requirements."[44] Arguably, this effect is already occurring in the military because of current force structure reductions and fiscal

[42] William O. Odom and Christopher D. Hayes, "Cross-Domain Synergy: Advancing Jointness," *Joint Force Quarterly* 73, no. 2 (April 1, 2014) 125. http://ndupress.ndu.edu/Media/News/NewsArticleView/tabid/7849/Article/577517/jfq-73-cross-domain-synergy-advancing-jointness.aspx (accessed November 18, 2014).

[43] U.S. Defense Science Board, "Creating an Assured Joint DoD and Interagency Interoperable Net-Centric Enterprise," *Report of the Defense Science Board Task Force on Achieving Interoperability in a Net-Centric Environment* (Washington DC: Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, March 2009), 9. www.acq.osd.mil/dsb/reports/ADA498577.pdf (accessed November 18, 2014).

[44] Odom and Hayes, "Cross-Domain Synergy," 127.

constraints. The risk of this post-war trend is an inability to achieve the levels of cross-domain synergy envisioned in current joint concepts.

Service culture tensions created by resource scarcity may also act as internal drivers that challenge an effective unified joint approach for integrating Service cyberspace capabilities at the tactical level. RAND analyst Dr. Adam Grissom cites resource scarcity as the central contention between inter-service relationships and military innovation. Dr. Grissom wrote, "on occasion, a new mission area may emerge in which none of the Services have a dominant advantage, or an old mission may be reopened for competition between the Services. The interService [sic] model posits that Services will compete to develop capabilities to address these contested mission areas, believing that additional resources will accrue to the winner. The result is innovation."[45] Daniel Kuehl describes Service competition in a similar vein, citing the relief of both the Secretary of the Air Force and the Air Force Chief of Staff in 2008 after they pronounced the stand-up of an Air Force Cyber Command. Although two years before U.S. Cyber Command was established, Daniel Kuehl concludes, "suspicion arose among the other Services that the Air Force's movement was a grab for cyber turf."[46]

Other examples demonstrate the importance of top-down guidance and the involvement of combatant commands to integrate military Service approaches to cyberspace operations. In 2011, in absence of formalized strategic guidance from U.S. Cyber Command, the military Services began pursuit of capabilities in support of their own cyberspace operations needs. The Government Accountability Office (GAO) found

[45] Adam Grissom, "The Future of Military Innovation Studies." *Journal Of Strategic Studies* 29, no. 5 (October 2006), 910-911. http://dx.doi.org/10.1080/01402390600901067 (accessed January 21, 2015).

[46] Daniel Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," in *Cyberpower and National Security* (Washington DC: National Defense University Press, 2009), 33-34.

that the Services had focused on their Service-centric needs and employed "disparate, Service-specific approaches to organize, train, and equip forces for cyberspace operations, and these approaches may not enable them to meet U.S. Cyber Command's mission needs."[47] The point taken from this example is that the military Services must integrate their cyberspace capabilities across all the joint warfighting functions, specifically in terms of achieving meaningful outcomes and synergy in globally integrated operations.

The Influence of Mission Command

What are challenges for the employment of tactical cyberspace operations under the concept of mission command? General Martin Dempsey, the Chairman of the Joint Chiefs of Staff, forewarns commanders that "decentralization will occur beyond current comfort levels and habits of practice." However, the Chairman's intent for the Joint Force is clear, that "resident in the central figure of the commander, the ethos of mission command is a critical enabler of success."[48] As cyberspace operations become more central to the way tactical forces will maneuver in future combat, operational and strategic commanders are being challenged to embrace the concept of calculated risk taking. The decade of lessons learned during the wars in Afghanistan and Iraq have taught military leaders the value of adaptation and decentralization, permitting

[47] Government Accountability Office. *Defense Department Cyber Efforts: More Detailed Guidance Needed to Ensure Military Services Develop Appropriate Cyberspace Capabilities, May 2011*, (Washington, D.C.: U.S. Government Printing Office, 2011), 17. The issues identiified in this GAO report take years to correct; e.g., the issues concerning Cyber Workforce Management, workforce qualification, normalizing command and control of the cyberspace operational domain are expected to be completed in calendar 2015.

[48] Martin Dempsey, *Mission Command Whitepaper*, (Washington, DC: Joint Chiefs of Staff, April 3, 2012), 4.

commanders operating at the tactical level the freedom of action to exploit fleeting opportunities.

Mission command is a guiding principle in the *CCJO* and the *JOAC*. Both concepts call for empowering units at the lowest possible level as the military evolves to the Joint Force required in 2020. Joint doctrine describes mission command as "the conduct of military operations through decentralized execution based upon mission-type orders. … successful mission command demands that subordinate unit leaders at all echelons exercise disciplined initiative and act aggressively and independently to accomplish the mission."[49] The *CCJO* clarifies the future requirement for mission command, stating, "globally integrated operations requires a commitment to the use of mission command. …Mission Command is the most appropriate command philosophy for the increasingly uncertain future."[50] Under a mission command philosophy, subordinates are delegated the authority to make decisions "wherever possible", allowing subordinates the freedom to exercise initiative based on their understanding of the higher commander's intent."[51] However, the *CCJO* acknowledges that "[i]t is important to note that while mission command is the preferred command philosophy, it is not appropriate to all situations. Certain specific activities require more detailed control, such as the employment of nuclear weapons or other national capabilities, air traffic control, or activities that are fundamentally about the efficient synchronization of resources."[52]

[49] U.S. Joint Chiefs of Staff, *Joint Operations,*Joint Publication 3-0, (Washington, DC: Joint Chiefs of Staff, 11 August 2011), II-2.
[50] U.S. Joint Chiefs of Staff, *Capstone Concept for Joint Operations*, 4.
[51] Ibid.
[52] Ibid., 5.

Cyberspace operations fit into this category, where detailed control of cyberspace operations may require inhibiting elements of the mission command philosophy.

The relevance of cyberspace to future military operations described in the *CCJO* and the *JOAC* reflects the tremendous reliance on technical superiority. History however has shown that reliance on technology alone does not guarantee that the Joint Force can act faster and more effectively than a potential adversary can. While not ignoring the larger policy context of current restrictions on using cyber capabilities offensively, the technologies that have enabled offensive cyberspace operations and defensive cyberspace response actions have also led to greater centralization of control over those cyberspace capabilities. The rationale for centralized control over offensive and defensive response cyberspace operations reflects that effects generated from these operations might extend well beyond the target and not limited to a specific geographic area, such as within a combatant command's area of responsibility. Joint doctrine further acknowledges that "[b]ecause of transregional considerations or the requirement for high-demand, low-density resources, [cyberspace operations and cyber personnel] may be coordinated, integrated, and synchronized with centralized execution from a location outside the AOR of the supported commander."[53] Offensive cyberspace operations and defensive cyberspace operations may also rely on similar capabilities, thus requiring the need for centralized control over both of those capabilities.[54] Such detailed control may inhibit cyberspace operations in a mission command environment and the ability to create effects that enable cross-domain synergy as envisioned in current joint concepts.

[53] U.S. Joint Chiefs of Staff, *Cyberspace Operations*, JP 3-12R, I-7.
[54] Ibid.

In a focus paper titled *Insights and Best Practices: Mission Command and Cross-Domain Synergy,* General (Retired) Gary Luck and the Joint Staff J7 Deployable Training Division elaborated on recent insights concerning mission command. According to General Luck, understanding and applying the many laws, policies, and directives associated with various types of operations is necessary to operationalize a mission command philosophy. He elaborates by stating, "[l]ack of a shared understanding of these authorities and their limitations can result in loss of legitimacy, trust, cohesion, and tendency to retain centralized control."[55] Regarding the future for Joint Force cyberspace operations, the two key legal authorities that apply are Title 10 U.S. Code (USC), Armed Forces, and Title 50 (USC), War and National Defense.[56] Yet, understanding the distinction between these legal authorities is often difficult, which can complicate indoctrinating a mission command philosophy over cyberspace operations.

Although Title 10 and Title 50 USC refer to separate chains of command between the armed forces and intelligence agencies, USCYBERCOM and the National Security Agency (NSA), respectively, one four-star general heads both organizations. This has created very complicated lines of authority between Title 10 and Title 50 authorities.[57] "Under Title 50, a "covert action" is subject to presidential finding and Intelligence Committee notification requirements. Traditional military activity, although undefined, is an explicit exception to the Title 50 USC covert action definition in Section 913 as the identity of the sponsor of a traditional military activity may be well known."[58] A 2015

[55] Gary Luck, *Insights and Best Practices Focus Paper: Mission Command and Cross-Domain Synergy* (Suffolk, VA: Joint Staff J7, March 2013), 1.

[56] U.S. Joint Chiefs of Staff, *Cyberspace Operations,* JP 3-12(R), III-2.

[57] Congressional Research Service, *Cyber Operations in DOD Policy and Plans: Issues for Congress, January 5, 2015*, *CRS Report 43848* (Washington, DC: Government Printing Office, 2015), 16-17.

[58] CRS Ibid. According to the Department of Defense Dictionary of Military and Associated Terms, Joint Publication1-02, a clandestine operation is defined as one "sponsored or conducted by governmental

CRS report highlights the ambiguity that exists between Title 50 intelligence authority for "covert action" and Title 10 military authority for "clandestine action". The distinction between covert and clandestine is necessary because "the provision distinguishes between approval and reporting requirements for military-directed cyberspace operations and those conducted by the intelligence community."[59] To General Luck's observation, unclear authorities and lines of command may complicate the military commander's ability to operationalize a mission command philosophy and execute offensive and defensive cyberspace operations.

Andru Wall, in his article *Demystifying the Title 10-Title 50 Debate: Distinguishing Military Operations, Intelligence Activities & Covert Action,* describes the complexity between Title 10 and Title 50 authorities through an assessment of the killing of Osama Bin Laden by U.S. Navy SEALs in 2011. According to Wall, the Central Intelligence Agency Director characterized the operation to kill or capture bin Laden as a Title 50 covert operation, yet a military commander of the Joint Special Operations Command actually commanded the raid. He goes on to state that the "Title 10-Title 50 debate is the epitome of an ill-defined policy debate with imprecise terms and mystifying pronouncements."[60] Wall casts an important observation regarding military transparency, highlighting the requirement to ensure that military operations are conducted legally, under the appropriate governing authorities.[61] Without clarity and understanding

---

departments or agencies in such a way as to assure secrecy or concealment. A clandestine operation differs from a covert operation in that emphasis is placed on concealment of the operation rather than on concealment of the identity of the sponsor.

[59] Ibid., 17.

[60] Andru E. Wall, "Demystifying the Title 10-Title 50 Debate: Distinguishing Military Operations, Intelligence Activities & Covert Action," *Harvard National Security Journal* 3, no. 1 (September 2011): 85-142. *International Security & Counter Terrorism Reference Center*, EBSCO*host* (accessed November 2, 2014).

[61] Ibid., 140-141.

regarding the lawful use of offensive cyber weapons in support of military objectives, commanders may be unsure that their actions are consistent with applicable laws and policy, potentially inhibiting their freedom of action to exploit opportunities in cyberspace.

Joint Publication 3-12(R), *Cyberspace Operations* further notes the requirement for detailed control, citing that the "the growing reliance on cyberspace around the globe requires carefully controlling [offensive cyberspace operations], requiring national level approval."[62] Commanders executing integrated cyberspace operations at the tactical echelon would need to understand the lines of authority for cyber operations in order to know the types of operations are authorized, how control is established over those operations, and how far down they can be delegated in a mission command environment.

Fortunately, understanding the level that control over cyberspace capabilities can be decentralized is an effort that U.S. Cyber Command is currently exploring. The U.S. Cyber Command's premier annual Cyber Flag exercises includes a focus on understanding how to fully integrate cyberspace operations into coalition and joint operations at all levels, while understanding the potential new ways to command and control cyber forces. Cyber Flag exercise objectives include "rehearsing how a coalition will conduct command and control of cyberspace forces at the tactical and operational levels in response to a regional crisis."[63]

[62] U.S. Joint Chiefs of Staff, *Cyberspace Operations*, Joint Publication 3-12(R), II-7-8.

[63] U.S. Department of Defense, "'Cyber Flag' Exercise Tests Mission Skills," DoD News, November 12, 2014, http://www.defense.gov/news/newsarticle.aspx?id=123621 (accessed on January 17, 2015).

CHAPTER 4: CONCLUSIONS AND RECOMMENDATIONS

Conclusions

Does increasing the technical capability of the tactical force to conduct offensive and defensive response cyberspace operations have any bearing on national level policy or generates a new level of strategic uncertainty? The answer is yes. The Edward Snowden disclosures are one example that made it more difficult to assure allies and citizens at home that U.S. objectives in cyberspace focus principally on existential threats. The implications for foreign relations could shift to a focus on competition in cyberspace, lending to a security dilemma between nations. Prior to the Great War, and continuing throughout the Cold War, perceptions of the offense-defense balance were defining features for survival of nations. Perceptions of a U.S. offense-oriented cyberspace strategy may very well influence how other nation-states and societies value their investment in cyberspace capabilities. The likely response from the U.S. might be to control the proliferation of cyber warfare capabilities, while at the same time reconciling with its own concept of expanding cyberspace capabilities at all levels in its military. Bearing in mind the important national and international perceptions of misleading intent in U.S. cyberspace strategies, as well as the broader perception that the U.S. is predisposed to use cyberspace offensively, the concept of adding offensive cyber warfare capabilities to the tactical military force could receive blowback from the international community. This strategic uncertainty includes the specter of an international security dilemma, while imposing tensions in U.S. national policy and potential limiting factors for the authority of the Joint Force to conduct cyberspace operations at the tactical level. As stated earlier, these external drivers of strategic uncertainty could negate or

marginalize the desired effect of tactical level cyberspace operations and risk achieving the level of cross-domain synergy required in the Joint Force 2020 operating environment.

The evolving political and social values should factor into military force planning. National strategy captures the interests of protecting national security in cyberspace and the value of protecting society's civil liberties. The military clearly has a role in cyberspace, but a growing concern of over-militarizing cyberspace, or that the military could assume the cybersecurity responsibility of all Americans, could subject the Joint Force's cyber capabilities to greater social scrutiny for what society expects of its military. American society simply does not view cyberspace as primarily a military domain. Consequently, societal concerns over privacy and civil rights violations by intelligence agencies could diminish the value of the military's role in cyberspace.

Adapting increased military cyber warfare capabilities will require the political support and will to do so. Political will also relies on the popular desire of society to support the change also. The U.S. military will have to message its intent and requirement to political and societal elements for foundational cyberspace capabilities if it hopes to mitigate future uncertainty. Perhaps more importantly, early messaging may set the stage to allow policy makers to think differently about control over cyberspace authorities, and how control can devolve to lower levels in the Services.

The challenge of military Service cultures and norms is to avoid pursuit of disparate, narrowly focused, Service-centric concepts for cyber capabilities at the tactical levels. How the Services decide to approach their requirements to develop capabilities for cyberspace at the tactical level could affect the degree of technical and organizational

interoperability with USCYBERCOM and among the other Services. Failure to coordinate with USCYBERCOM, combatant commands, and among the Services' cyber components during concept development and joint experimentation could marginalize the ultimate effectiveness of cross-domain synergy and the operational approach described in Joint concepts. This risk of exacerbating the challenge of achieving synergy in globally integrated operations would detract from the approach of the *CCJO*, or worse, make one or more of the elements of globally integrated operations unattainable.

The assessment of mission command reveals a few conclusions. Currently, tactical level cyberspace operations do not lend themselves to the mission command philosophy, primarily because of the centrally controlled authorities over offensive and some defensive cyberspace operations. Future warfare may likely extend well beyond the province of military operations and the planning and execution of cyber fires can require significant interagency coordination and wide-ranging de-confliction ahead of time. The impact of those coordination requirements alone can negate much of the advantage in timing and tempo of cyberspace operations. From a mission command perspective, the tactical commander might not have the ability to attain the initiative in cyberspace or to seize fleeting opportunities in cyberspace that initiative in a mission command environment would otherwise provide.

Carefully controlling the exercise of authorities for offensive cyberspace operations requires detailed coordination between Title 10 and Title 50 lines of authority. The blurred lines between Title 10 and 50 authority may cause a tactical commander to either not be aware of a certain type of cyber capability or not be willing to consider cyberspace operations into the unit's operational planning. Intelligence concerns can also

arise should a tactical commander require effects on a target in or through cyberspace, yet the same target could also be a source for intelligence collection at the strategic level. Such a proposition could result in a form a cyberspace fratricide, intelligence loss, or will otherwise require a lengthy process of adjudication across several stakeholders. Achieving a coherent targeting process across all domains and levels of war will be paramount.

Arguably, there is no issue more important and less understood, than cyberspace operations in terms of national and strategic policy implications, national security concerns, societal values, and technological uncertainty. The unpredictable relationship and interaction between political and social values also suggests that political and social factors are subject to change. Future force concepts that envision increasing cyber warfare capabilities down to the lower tactical levels, while viewed as military imperatives, may not be valued politically and socially as acceptable military approaches in the future. These issues weigh on the challenges to adapt increased cyber capabilities into lower levels of the Joint Force.

Recommendations

Ensuring the future Joint Force has the capability to achieve cross-domain synergy requires commanders to become inherently more comfortable with relying on cyberspace operations conducted at increasingly lower levels. The challenge to this change is that the Joint Force must adapt to future joint cyberspace requirements in a strategic environment of inherent uncertainty. The four recommendations that follow, including areas for additional research, will assist defense leaders and Joint Force Commanders adapt the growing capabilities of cyberspace down to the tactical force.

Empower the Geographic Combatant Commands with Control Authorities

Assuming that authorities and control over cyberspace operations devolve to the tactical level, Combatant Commands must integrate operational and tactical level cyberspace operations within the theater. This new level of integration requires employment of joint cyber support and joint cyber targeting processes that extends from the strategic to tactical levels. Combatant Commands, responsible over regional areas of operations, will also require authorities to execute the range of cyberspace operations and enforce control measures over lower echelon units as a condition to exercise that authority. The timeframe to study the implications of authorities and control measures needed should begin in exercises, such as U.S. Cyber Command's Cyber Flag exercises, as a precursor to developing a detailed experimentation plan. From a joint capabilities integration perspective, the Geographic Combatant Commands, military Services and their Service cyber components, and U.S. Cyber Command must work together from the onset to achieve unity of purpose and unity of effort for cross-domain cyberspace operations at all levels.

An area for additional research includes the cyber training and education requirements for commanders. Commanders, especially at the tactical level, must understand the cyberspace capabilities available, how to operate within the corresponding legal constraints over offensive military cyber capabilities, and adapting cyberspace operations into an integrated targeting processes from the tactical to strategic levels.

Communicate the Strategic Utility of Future Military Cyberspace Requirements

Multiple viewpoints challenge the viability of cyberspace operations at the tactical level, not the least of which are political and societal perspectives. Thus, ensuring that

future force joint concepts are understood at the national policy level will shape viewpoints early and could alleviate any ambiguity about the future changes required in authorities to conduct cyberspace operations at lower levels. The DoD must describe joint concepts to national leaders and explain the requirements for the cyber-enabled tactical force, where that force is envisioned to likely fight, against whom, under what circumstances, and for what purposes. Key messages to national leaders and American society should establish a shared understanding that the utility of military force in cyberspace is a national capability for military purposes. Undoubtedly, other nation-states and societies are aware of U.S. strategies, doctrine, and future force joint concepts, all of which are available in the open-source medium. Thus, communicating the requirements for the cyber-enabled tactical force to a U.S. audience will potentially also shape international perceptions, and should be a consideration.

Ultimately, a future military cyberspace capability has to fit within how political leaders and society view the utility of the military capability. Defense leaders should consider that many in the domestic society are reasonably concerned over the revelations from Edward Snowden. Backlash over additional offensive cyber capabilities development and extension down to even lower levels in the Force is reasonable to expect. Thus, DoD must convey a clear understanding to its external audiences of the strategic purposes and utility of military cyberspace operations and each level of war.

Develop Cyber Situational Awareness Capabilities at all Echelons

Science and technology investment priorities should address the potential to estimate the chain consequences posed by offensive cyberspace operations. Cyber tools should be developed that can measure, with degrees of confidence, the potential order of

effects of employing offensive cyber capabilities. Technology investment priorities must lead to capabilities that provide commanders with cyberspace situational awareness and the capability to minimize collateral cyber effects. Such a capability may also increase the degree of acceptability to policy and decision makers to allow for decentralized control over cyber capabilities to lower levels. Moreover, the military's capability and processes to control cyber effects must integrate with other national capabilities, to include those of intelligence agencies and the Interagency. The potential outcomes would increase the strategic utility of military cyberspace operations and lead to even broader levels of cross-domain synergy across the whole-of-government.

The uncertain strategic political environment will nonetheless have a continuing influence over the ability to execute cyberspace operations in a mission command environment. The degree of integrating mission command principles and control over cyberspace operations is an area for additional research, and should be studied further and evaluated through Joint experimentation.

Task Organize Cyber Forces to the Tactical Level

Future limitations on military force structure, imposed by uncertain fiscal demands, may require innovative resourcing strategies to extend cyber forces to the tactical level without adding to personnel requirements in those units. Equally important, as increased cyber capabilities figure prominently in future tactical unit operations, resourcing strategies should consider ways to mitigate making critical trade-offs with other mobility, protection, and firepower combat power capabilities. In lieu of increasing the cyber force structure across tactical echelon units, the Joint Staff should consider increasing the personnel capability in the cyber support elements at each Geographic

Combatant Command. The result provides Combatant Commanders with the ability to selectively task organize cyber support personnel to lower echelons as planning and operations dictate. Moreover, such an approach would be less taxing on the overall military force structure requirements and could reduce concerns over decentralizing control over cyber capabilities.

For example, during operations, Combatant Commander's would have the capacity to task organize cyber support personnel to lower echelon commanders under tactical control authority. Combatant Commanders, however, retain operational control of those cyber forces at the Combatant Command or the Joint Force Cyber Component Commander level. Under this construct, Geographic Combatant Commanders could retain centralized control over cyber authorities while allowing cyber forces to distribute to lower tactical levels and support decentralized execution. This alternative may also support conditions for a mission command philosophy to emerge in context of executing cyberspace operations at tactical echelons.

Additional research is necessary towards studying the varied organizational structures that already exist in each Service and the best way to extend capabilities to the tactical level. The military Services are the force management proponents to resource cyber forces within their Services, to the U.S. Cyber Command, and to the Geographic Combatant Commands and must work together to determine feasible resourcing strategies in support of the Chairman's vision. The uncertainty of force structure limitations, however, will require a clear-eyed appraisal of the demand for cyber capability in tactical level units balanced against potential increases in man-power requirements, or trade-offs in other combat power capabilities.

These recommendations are not to suggest that suitable environmental conditions will exist or that current conditions will change to allow the tactical level Joint Force to adapt cyberspace capabilities in the future. Adversaries are adopting an offensive approach in cyberspace, which will continue to renew interest in realizing the potential for integrated cyberspace operations in support of the joint concepts. To the extent that rigorous debate continues on this topic at all levels and with internal and external stakeholders, there is potential to move ahead.

GLOSSARY: KEY MILITARY TERMS

Cross-Domain Synergy: The complementary vice merely additive employment of capabilities in different domains such that each enhances the effectiveness and compensates for the vulnerabilities of the others. (JOAC, 2012)

Cyberspace: A global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. (JP 1-02)

Cyberspace Fires: Depending on the objective, cyberspace fires can be offensive or defensive, supporting or supported. (JP 3-12(R))

Fires: The use of weapon systems to create a specific lethal or nonlethal effect on a target.

Joint Operations Area: An area of land, sea, and airspace, defined by a geographic combatant commander or subordinate unified commander, in which a joint force commander (normally a joint task force commander) conducts military operations to accomplish a specific mission. (JP 3-0)

Operational Area: An overarching term encompassing more descriptive terms for geographic areas in which military operations are conducted. Operational areas include, but are not limited to, such descriptors as: area of responsibility, theater of war, theater of operations, joint operations area, amphibious objective area, joint special operations area, and area of operations. (JP 3-0)

Joint Force: A general term applied to a force composed of significant elements, assigned or attached, of two or more Military Departments operating under a single joint force commander.

FREQUENTLY USED ABBREVIATIONS:

CCDR: Combatant Commander
CCJO: Capstone Concept for Joint Operations
CJCS: Chairman of the Joint Chiefs of Staff
DCO: Defensive Cyberspace Operations
DCO-RA: Defensive Cyberspace Operations Response Actions
DoD: Department of Defense
DODIN: Department of Defense Information Networks
JFC: Joint Force Commander
JOAC: Joint Operational Access Concept
JOE: Joint Operating Environment
NSA: National Security Agency
OCO: Offensive Cyberspace Operations
USCYBERCOM: United States Cyber Command

BIBLIOGRAPHY

Bacevich, Andrew. *The New American Militarism: How Americans are Seduced by War*. New York: Oxford University Press, 2005, 235.

Bauman, Zygmunt, et al. "After Snowden: Rethinking the Impact of Surveillance," *International Political Sociology*. 2014, 121-144. http://onlinelibrary.wiley.com/doi/10.1111/ ips.12048/epdf (accessed November 12, 2014).

Carl Von Clausewitz. *On War*, ed. and trans. Michael Howard and Peter Paret. Princeton, NJ: Princeton University Press, 1989.

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

Congressional Research Service. *Cyber Operations in DOD Policy and Plans: Issues for Congress, January 5, 2015*. Washington, DC: Government Printing Office, 2015.

———. Federal Laws Relating to Cybersecurity: Major Issues, Current Laws, Proposed Legislation, December 12, 2014, (Washington, DC: Government Printing Office, 2014).

Dempsey, Martin E. *Mission Command White Paper*. Washington, DC: U.S. Joint Chiefs of Staff, April 3, 2012.

Fuller, J.F.C. *The Conduct of War, 1789-1961*. New Brunswick, NJ: Rutgers University Press, 1961.

Gould, Joe. "Ground Commanders with Cyber Skills: Leaders Consider Adding New Offensive Tactics to CTC Rotations," *Army Times* (1 July 2014).

Government Accountability Office. "Defense Department Cyber Efforts: More Detailed Guidance Needed to Ensure Military Services Develop Appropriate Cyberspace Capabilities." *GAO Publication No. 13-255.* Washington, D.C.: U.S. Government Printing Office, May 2011, 17.

Gray, Colin S. *Explorations in Strategy*. Westport, Conn.: Greenwood Press, 1996. 112-113.

Grissom, Adam. "The future of military innovation studies." *Journal Of Strategic Studies* 29, no. 5 (October 2006): 905-934. *International Security & Counter Terrorism Reference Center*, EBSCO*host* (accessed January 25, 2015).

Hagel, Chuck. "FY15 Budget Preview." Secretary of Defense Speech. February 24, 2014. http://www.defense.gov/Speeches/Speech.aspx?SpeechID=1831 (accessed September 22, 2014).

Handel, Michael I. "Comparing Sun Tzu and Clausewitz." In *Masters of War: Classical Strategic Thought*, 3rd Rev. and Expanded ed. London: Frank Cass, 2001, 21-22.

Kuehl, Daniel T. "From Cyberspace to Cyberpower: Defining the Problem." In *Cyberpower and National Security*. Washington DC: National Defense University Press, 2009.

Jervis, Robert. "Cooperation Under the Security Dilemma." *World Politics*, Vol. 30, Issue 2, January 1978, 161–214.

Kramer Franklin. "Cyberpower and National Security: Policy Recommendations for a Strategic Framework." In *Cyberpower and National Security*. Washington, DC: National Defense University Press, 2009.

Leed, Maren. "Offensive Cyber Capabilities at the Operational Level - The Way Ahead," *Center for Strategic & International Studies*, (2013), 8-9.

Libicki Martin. *Cyberdeterrence and Cyberwarfare.* Santa Monica, CA: RAND, 2009.

Lynn, William J. "Defending a New Domain: The Pentagon's Cyberstrategy." *Foreign Affairs*. September/October 2010. http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain (accessed December 2, 2014).

Luck, Gary. *Insights and Best Practices Focus Paper: Mission Command and Cross-Domain Synergy*. Suffolk, VA: Joint Staff J7, March 2013, 1.

Obama, Barack. *National Security Strategy*. Washington DC: Government Printing Office, February 2015. www.whitehouse.gov/sites/default/files/docs/2015_ national_security_strategy.pdf (accessed on February 23, 2015).

———. *Sustaining U.S. Global Leadership: Priorities for 21st Century Defense.* Washington DC: Government Printing Office, January 3, 2012.

Odom, William O., and Christopher D. Hayes. "Cross-Domain Synergy: Advancing Jointness," *Joint Force Quarterly* 73, no. 2 (April 1, 2014): 125. http://ndupress.ndu.edu/Media/News/NewsArticleView/tabid/7849/Article/577517/jfq-73-cross-domain-synergy-advancing-jointness.aspx (accessed November 18, 2014).

Saltzman, Ilai. "Cyber Posturing and the Offense-Defense Balance." *Contemporary Security Policy*. 34:1, http://dx.doi.org/10.1080/13523260.2013.771031 (accessed November 2, 2014) 43.

Sanborn, James. "Tactical Hackers: Cyber Steps Up its Roles on the Battlefield," *Marine Corps Times* (1 September 2014): 18-19.

Schwab, George. "Cybersecurity: Challenge and Response, A New Generation Speaks Out." *International Committee on American Diplomacy*. Novemeber 6, 2013, 9. http://www. ncafp.org/ncafp/wp-content/uploads/2013/12/NCAFP-Cyber-Roundtable_Cybersecurity-Challenge-Response_Nov6.13.pdf wSMLDqg (accessed November 12, 2014).

Showalter, Dennis E. "Military Innovation and the Whig Perspective of History." In *The Challenge of Change: Military Institutions and New Realities, 1918-1941*. University of Nebraska Press, 2000.

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

———. *Joint Operational Access Concept.* Version 1.0. Washington DC: U.S. Joint Chiefs of Staff, January 17, 2012.

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

———. *Department of Defense Dictionary of Military and Associated Terms.* Joint Publication 1-02. Washington, DC: U.S. Joint Chiefs of Staff, November 8, 2010 (as amended through May 15, 2011).

———. *The National Military Strategy of the United States of America 2011: Redefining America's Military Leadership.* Washington DC: U.S. Joint Chiefs of Staff, February 8, 2011.

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

_____. *Quadrennial Defense Review Report.* Washington, DC: U.S. Joint Chiefs of Staff, 2014.

———. *Guidance for Development and Implementation of Joint Concepts.* Washington, DC: U.S. Joint Chiefs of Staff, 22 November 2013.

U.S. Department of Defense. "'Cyber Flag' Exercise Tests Mission Skills." DoD News, November 12, 2014. http://www.defense.gov/news/newsarticle.aspx?id=123621 (accessed on January 17, 2015).

U.S. Defense Science Board. "Creating an Assured Joint DoD and Interagency Interoperable Net-Centric Enterprise," *Report of the Defense Science Board Task Force on Achieving Interoperability in a Net-Centric Environment.* Washington DC: Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, March 2009. www.acq.osd.mil/dsb/reports/ADA498577.pdf (accessed on November 18, 2014).

U.S. Joint Forces Command. *The Joint Operating Environment (JOE) 2010.* Suffolk, VA: U.S. Joint Forces Command, February 18, 2010.

U.S. Library of Congress. *Cyber Operations in DOD Policy and Plans: Issues for Congress*, by Catherine Theohary and Anne Harrington, Congressional Research Service Report 43848. Washington, DC: Office of Congressional Information and Publishing, January 5, 2015, 16-17.

Murray, Williamson, and Allan R. Millett, eds. *Military Innovation in the Interwar Period*. New York: Cambridge University Press, 1996.

Van Evera, Stephen. *Causes of War: Power and The Roots of Conflict.* New York: Cornell University Press, 1999.

Wall, Andru E. "Demystifying the Title 10-Title 50 Debate: Distinguishing Military Operations, Intelligence Activities & Covert Action." *Harvard National Security Journal* 3, no. 1, September 2011, 85-142. EBSCOhost (accessed November 2, 2014).

Weinberger, Casper. "The Uses of Military Power," *Remarks to the National Press Club.* Washington, DC: November 28, 1984. http://www.pbs.org/wgbh/pages/frontline/ shows/military/force/ weinberger.html (accessed September 7, 2014).

Winton, Harold and David Mets, eds. *The Challenge of Change: Military Institutions and New Realities, 1918-1941*. University of Nebraska Press, 2000.

VITA

Most recently, Colonel Dan Ruder served a Division Chief for the US Army Cyber Center of Excellence, at Fort Gordon, Ga. His previous assignments include Commander of the 447th Signal Battalion and Deputy Brigade Commander of the 15th Regimental Signal Brigade at Fort Gordon. His operational and staff assignments include C5 Chief of Plans for the Multi National Corps-Iraq, C5 Chief of Plans for I Corps at Joint Base Lewis McChord, Lead Planner in the Commander's Initiatives Group (I Corps), G5 Lead Planner for Civil-Military Operation with Multi National Division Baghdad (1st Cavalry Division), and Deputy Plans Chief with the J6, SOCCENT, in Iraq. COL Ruder commissioned through ROTC (Distinguished Graduate) at Florida A&M University in 1994. He is a Signal Officer with four operational deployments that combine an array of operational planning, Signal, and Cyber experiences. Colonel Ruder holds advanced degrees in Information Technology Management, Military Art and Science, and Economics.