

REPORT DOCUMENTATION PAGE					Form Approved OMB No. 0704-0188	
The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.						
1. REPORT DATE (DD-MM-YYYY) 03/31/2017		2. REPORT TYPE Master's Thesis			3. DATES COVERED (From - To) 08/01/2016 to 06/16/2017	
4. TITLE AND SUBTITLE UNTYING OUR HANDS: RECONSIDERING CYBER AS A SEPARATE INSTRUMENT OF NATIONAL POWER				5a. CONTRACT NUMBER		
				5b. GRANT NUMBER		
				5c. PROGRAM ELEMENT NUMBER		
6. AUTHOR(S) LtCol Carl Priechenfried, USMC				5d. PROJECT NUMBER		
				5e. TASK NUMBER		
				5f. WORK UNIT NUMBER		
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)				8. PERFORMING ORGANIZATION REPORT NUMBER		
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) Joint Forces Staff College Joint Advanced Warfighting School 7800 Hampton Blvd Norfolk, VA 23511-1702				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 Not for Commercial Use without the express written permission of the author.						
14. ABSTRACT Military considerations significantly influenced development of U.S. national cyber capabilities, resulting in the current U.S. strategic approach that identifies cyber as a military capability. While this strategic approach offers advantages with regard to resourcing, the application of military power is limited by domestic law, international treaty law, and international customary law. Reconsidering cyber as a separate instrument of national power by legally distinguishing cyber activity from an armed attack and consolidating national cyber capabilities within a single, civilian-led organization within the executive branch avoids these limitations and provides additional cyber employment options to national strategic decision-makers.						
15. SUBJECT TERMS Cyber, Instruments of National Power, U.S. Grand Strategy, DIME						
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON	
a. REPORT	b. ABSTRACT	c. THIS PAGE			Carl C. Priechenfried	
Unclassified	Unclassified	UNCLASS	Unclassified Unlimited	58	19b. TELEPHONE NUMBER (Include area code) 910-650-7259	

This page intentionally left blank.

NATIONAL DEFENSE UNIVERSITY
JOINT FORCES STAFF COLLEGE
JOINT ADVANCED WARFIGHTING SCHOOL



**UNTYING OUR HANDS: RETHINKING CYBER AS AN
INSTRUMENT OF NATIONAL POWER**

By

Carl Priechenfried

Lieutenant Colonel, United States Marine Corps

Not for Commercial Use without the express written permission of the author

This page intentionally left blank.

**UNTYING OUR HANDS: RETHINKING CYBER AS AN
INSTRUMENT OF NATIONAL POWER**

By

Carl Priechenfried

Lieutenant Colonel, United States Marine Corps

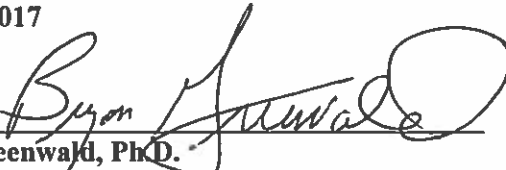
A paper submitted to the Faculty of the Joint Advanced Warfighting School in partial satisfaction of the requirements of a Master of Science Degree in Joint Campaign Planning and Strategy. The contents of this paper reflect my own personal views and are not necessarily endorsed by the Joint Forces Staff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

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

Signature: 

21 April 2017

Thesis Advisor:

Signature: 
Bryon Greenwald, Ph.D.
Professor, JAWS

Approved by:

Signature: 
James Golden, Col, USAF
Committee Member

Signature: 
Stephen Rogers, COL, USA
Director, Joint Advanced Warfighting School

This page intentionally left blank

ABSTRACT

Current cyber thought reflects a heavy military influence in the prevailing discussion of *cyber war* and *cyber warfare*. While acknowledging the military roots of the development of cyber and recognizing that developing cyber capabilities via military mechanisms offered initial advantages, the continued global expansion of and reliance upon digitized societies calls for an objective, unconstrained analysis and consideration of cyber independent of the military lens to promote comprehensive understanding of cyber power and afford the widest possible range of options to strategic decision makers.

This thesis seeks to reframe the strategic discussion of U.S. cyber power. Specifically, this thesis proposes a new strategic approach to cyber by considering it as an instrument of national power separate and independent from the military instrument. This new strategic approach to cyber has conceptual, legal, and organizational implications. Conceptually, the argument for cyber builds on similar previous arguments for expanding the instruments of national power to include such national capabilities as law enforcement, financial, and intelligence. Legally, this approach requires the U.S. to change its position equating cyber aggression with armed attacks. Organizationally, this approach calls for the creation of a single, civilian-led cyber agency that combines and consolidates the cyber functions of the Office of the Director of National Intelligence, Department of Homeland Security, Federal Bureau of Investigation, and some of the cyber capabilities resident within the Department of Defense. This thesis concludes that a new strategic approach to cyber would provide a wider range of strategic cyber options, including expanded cyber defense of civilian government infrastructure and more freedom of action for offensive cyber activity by avoiding limitations commensurate with the application of military force.

ACKNOWLEDGEMENTS

I am indebted to many people who supported my research and writing efforts. The Joint Advanced Warfighting School faculty enabled my success during this year by challenging me to both broaden and deepen my professional military education. I am particularly grateful for the thoughtful suggestions and discussions offered by my thesis advisor, Dr. Bryon Greenwald, and my faculty advisor, Col Doug Golden. Their careful review of my thesis drafts and other efforts along the way ensured a valuable journey of discovery on a topic for which I had little prior knowledge. My classmates provided an honest sounding board for my thesis presentation while at the same time offering camaraderie and encouragement.

Finally, I dedicate this effort to my wife and my three children. They give meaning and purpose to my life and I strive every day to earn their love and respect.

Any errors in this work are my own.

TABLE OF CONTENTS

CHAPTER 1: THE INCREASING IMPORTANCE OF CYBER POWER	1
With Dependency Comes Vulnerability	2
Cyber Limitations	3
Cognitive Limitations	3
Organizational Limitations	4
Legal Limitations	4
Thesis and Paper Structure	5
Terminology	7
CHAPTER 2: THE MILITARY PARADIGM OF U.S. NATIONAL CYBER POWER	9
Military Role in Cyber Power Development	12
Military Influence on Cyber Thought	12
Cyber Literature	12
Cyber as an Operating Domain	15
The Sea, the Sky, and the Heavens	16
National Cyber Organizations	19
Consequences of Military Influence on Cyber Power Employment	22
CHAPTER 3: INSTRUMENTS OF NATIONAL POWER	25
Assessing the Value of the Instruments of National Power Paradigm	26
Instruments of National Power	27
DIME	28
DIME-FIL	29
CHAPTER 4: CYBER AS AN INSTRUMENT OF NATIONAL POWER	32
The Idea	33
Requirements	34
Implications	38
Analysis	40
CHAPTER 5: CONCLUSION	45
BIBLIOGRAPHY	48
VITA	54

This page intentionally left blank

CHAPTER 1: THE INCREASING IMPORTANCE OF CYBER POWER

*This world—cyberspace—is a world that we depend on every single day ... [it] has made us more interconnected than at any time in human history.*¹

President Barack Obama, May 29, 2009

The creation of interconnected, or networked, computers in the late 1960s and the subsequent development and implementation of a non-proprietary open-network information repository and recall architecture in the 1990s opened the dawn of a global information age as transformative to societies today as the introduction of the modern printing press was to European society in the fifteenth century. In today's globally-connected and increasingly digital world, computers and technology are ever-present; in fact, it is hard to conceive of a time when such was not the case.

The spread of global digitization almost defies comprehension. In just over forty years, the use of email grew from zero (1970) to almost 40 trillion a year (2014). In twenty-two years, websites grew from one (1991) to over 30 trillion (2013). According to Cisco, the internet service provider behemoth, by 2020 approximately 40 billion devices will connect to the internet.² The Miniwatts Marketing Group, a site used by several prominent cyber scholars, estimates that as of June 2016 50.1% of the global population, or 3,675,824,813 out of 7,340,159,492 people, used the internet.³ It is no exaggeration to acknowledge that

¹ U.S. President, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* (Washington DC: Government Printing Office, May, 2011), 3.

² P. W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (Oxford: Oxford University Press, 2014), 2.

³ Author Derek Reveron cited this website using 2011 data in a book he edited titled *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World* (Washington DC: Georgetown University Press, 2012), 6. Miniwatts Marketing Group, "Internet World Stats: Usage and Population Statistics," <http://www.internetworldstats.com/stats.htm> (accessed November 28, 2016).

modern societies are quickly becoming dependent on the services and benefits provided by global digitization.

With Dependency Comes Vulnerability

While the rewards of this global digitization are many, the dark side of this dependency is the increasing likelihood of exploitation from criminals or other nefarious actors. As of 2014, malicious actors have hacked 97% of Fortune 500 companies.⁴ In his 2016 annual worldwide threat assessment to Congress, James Clapper, the Director for National Intelligence, highlighted this concern by discussing cyber and technology threats.

The consequences of innovation and increased reliance on information technology in the next few years on both our society's way of life in general and how we in the Intelligence Community specifically perform our mission will probably be far greater in scope and impact than ever. Devices, designed and fielded with minimal security requirements and testing, and an ever-increasing complexity of networks could lead to widespread vulnerabilities in civilian infrastructures and US Government systems.⁵

This is not the first time that the concern over cyber vulnerabilities has merited mention in national security dialogue. In 2000, the National Intelligence Council highlighted the emergent threat of adversarial use of information technology as a key trend by 2015, although they admittedly missed the mark by failing to predict how central such technology would become for most first-world nations and thus the vulnerability such dependency would create.⁶ In early 2001, President Clinton appointed the first Special Advisor to the President

⁴ Singer and Friedman, *Cybersecurity and Cyberwar*, 2.

⁵ Director of National Intelligence (DNI) James R. Clapper, *Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community*, provided to the House Permanent Select Committee on Intelligence (February 25, 2016), 1-4.

⁶ National Intelligence Council, "Global Trends 2015: A Dialogue about the Future with Nongovernment Experts," (Langley: National Foreign Intelligence Board, December 13, 2000), https://www.dni.gov/files/documents/Global%20Trends_2015%20Report.pdf (accessed December 28, 2016), 32-3.

for Cyber Security. The importance of that position and the importance of cyber security to the nation has only increased since then.

Cyber Limitations

Cognitive Limitations

Beyond the technical vulnerabilities, other limiting factors associated with current U.S. national cyber capabilities generate concern. One such limitation is cognitive in nature. It is important to remember that despite the rapid proliferation of information technology, the digital age is less than fifty years old. This relative newness has significant implications, especially for the current generation of senior strategic decision-makers and how they relate to, and make decisions about, digital technology. As Singer and Friedman note:

Our most senior leaders, now in their sixties and seventies, likely did not even become familiar with computers until well into their careers, and many still today have only the most limited experience with them. As late as 2001, the Director of the FBI did not have a computer in his office, while the U.S. Secretary of Defense would have his assistant print out e-mails to him, write his response in pen, and then have the assistant type them back in ... a full decade later the Secretary of Homeland Security, in charge of protecting the nation from cyberthreats, told us at a 2012 conference, “Don’t laugh, but I just don’t use e-mail at all.” ... And in 2013, Justice Elena Kagan revealed the same was true of eight out of nine of the United States Supreme Court justices, the very people who would ultimately decide what was legal or not in this space.⁷

While today’s youth may be “digital natives,” the majority of today’s senior leaders are, at best, characterized as “digital immigrants.”⁸ As a result, those that direct strategic policy and issue strategic guidance are perhaps the least prepared to address the strategic considerations of cyber power despite the growing importance of this national capability.

⁷ Singer and Friedman, *Cybersecurity and Cyberwar*, 5.

⁸ *Ibid.*, 4.

Organizational Limitations

Another challenge facing current U.S. national cyber capabilities is the assignment of cyber responsibilities to multiple national agencies. While the Defense Department has a subordinate command explicitly named U.S. Cyber Command, other executive branch entities have designated cyber responsibilities. These include the Office of the Director for National Intelligence, the National Security Agency within the Defense Department, the Federal Bureau of Investigation, and the Department of Homeland Security. The specific responsibilities of each of these entities will be discussed later. It suffices to say that these large bureaucratic organizations, each with separate missions, cultures, and approaches towards cyber operations, challenge the ability to optimize national cyber capabilities.

Legal Limitations

Another limitation with regard to use of national cyber capabilities specific to the Department of Defense is legal in nature. The U.S. use of military force is generally constrained through several broad legal frameworks. Consistent with Article 51 of the United Nations (UN) Charter, the U.S. reserves the right to employ offensive military force for self-defense, but other legitimate offensive uses are *de facto* limited by international law and the principles of *jus ad bellum*. Some scholars argue that *jus ad bellum* analysis is insufficient to address cyber, but there are currently no prospects for development of a comprehensive international legal treaty due to “fundamental differences among the world’s major cyber-powers about the scope of activities that should be prohibited under an international cyber attack agreement.”⁹ In this absence, Reese Nguyen developed a *jus ad*

⁹ Reese Nguyen, “Navigating Jus Ad Bellum in the Age of Cyber Warfare,” *California Law Review* 101, no. 4 (August 1, 2013), 1111. To be fair, other legal scholars argue the opposing position that “the basic tenets of the law of armed conflict are sufficient to address the most important issues of cyberwar” and that the real difficulty lies not in the lack of a legal framework but instead “relates to the technical ability to determine the necessary

bellum analytical framework, proposing that cyber attacks constitute armed attack (and therefore justify responsive force from the aggrieved nation) “only when intended to cause irreversible disruption or physical damage to a cyber-physical system.”¹⁰ Despite his careful analysis, this definition leaves considerable room for interpretation; for instance, how does one prove the “intention” to cause irreversible disruption or physical damage? In any case, the U.S. in 2011 chose to define cyber actions as armed attacks and declared its right to respond militarily to cyber aggression, however broadly or ill-defined, thus placing cyber firmly in a military paradigm with regard to the use of force. Federal law also limits application of military force within the U.S. except under exceptional and very specific circumstances.¹¹

Thesis and Paper Structure

Given the massive proliferation of digital technology and its influence on every facet of life, it is time to remove cyber as a mere domain of military operations and elevate consideration of the country’s cyber capabilities to the level of an instrument of national power operating alongside the military, diplomatic, economic, and informational instruments of national power. This paper examines the idea of treating cyber power as a national instrument separate and distinct from the military instrument to enable a more comprehensive understanding of national capabilities and provide additional options to strategic decision-

facts which must be applied to the law to render legal judgments.” Charles Dunlap, “Ch. 13: Perspectives for Cyberstrategists on Cyberlaw for Cyberwar,” in *Conflict and in Cyberspace: The Challenge to National Security*, ed. Panayotis A. Yannakogeorgos and Adam B. Lowther (New York: Taylor and Francis Group, 2014), 212.

¹⁰ Nguyen, “Navigating Jus Ad Bellum,” 1125.

¹¹ The Posse Comitatus Act is codified in 18 U.S.C. § 1385; civil defense is codified in Code of Federal Regulations 32 § 182-185. Cornell University Law School Legal Information Institute, <https://www.law.cornell.edu/cfr/text/32/chapter-I/subchapter-I> (accessed December 28, 2016).

makers. Chapter 2 presents an analysis of the current military context for U.S. national cyber power capabilities. This analysis first focuses on the significant military influence on the development of cyber concepts, theories, and actualization of national capabilities. This portion of the paper includes a brief review of current strategic cyber literature to demonstrate the pervasiveness of military considerations and terminology. This section also includes a discussion of cyber power realities, specifically the concept of cyber as a military operational domain and the actualization of national cyber capabilities within the U.S. military organizational structure. The analysis then evaluates the consequences of the military influence on strategic cyber power use, specifically identifying three constraints on the use of strategic cyber power resulting from this military influence. This chapter concludes with a summary of the net constraining effects that result from national cyber capabilities as a component of the military instrument of national power.

Chapter 3 advances the analysis of national cyber capabilities by conducting a comparative analysis of the doctrinal instruments of national power. This chapter begins by evaluating the value of the paradigm by which the instruments of national power are evaluated. The chapter next analyzes each of the doctrinal instruments to demonstrate how the abstract concept of a national power tangibly manifests. Subsequently, the chapter summarizes the recent arguments for expanding the framework from four to seven instruments of national power. Lastly, this chapter concludes by analyzing cyber as a separate instrument of power. This analysis makes use of the instantiation of the existing instruments as examples for comparing cyber power instantiation. The analysis also compares the arguments for the seven-instrument construct to an eight-instrument construct

that includes cyber power. This chapter concludes with an analysis of the consequences of treating cyber power as a separate instrument.

Chapter 4 concludes this paper by summarizing the argument for treating cyber power as a separate instrument of national power. This chapter also includes recommendations and areas for future research.

Terminology

Before beginning the analysis, it is necessary to understand the key terms used in this paper, especially given the varying uses and connotations in existing literature.¹²

- **Cyber** – “computer or digital interactions.”¹³ This term is drawn from Herbert Wiener’s coinage of the term “cybernetics,” defined as “the study of messages as a means of controlling machinery and society.”¹⁴ The term cybernetics is derived from the Greek word “kybernetes” which means “pilot; governor,” thus the term is used to describe not just a theory of communication, but also one of control.¹⁵ In U.S. military doctrine, cyber is a “three-legged stool” of operating military computer networks, defending military computer networks, and attacking adversarial computer networks.¹⁶

¹² This key terms section is significantly influenced by the comprehensive analysis of cyber terminology use in recent literature provided by Brandon Valeriano and Ryan C. Maness in chapter two of their book on cyber. Brandon Valeriano and Ryan C. Maness, *Cyber War versus Cyber Realities: Cyber Conflict in the International System* (Oxford: Oxford University Press, 2015), 21-33.

¹³ Ibid., 22. Valeriano and Maness acknowledge that this term has come into broad use as a normative function despite its technical origin.

¹⁴ Norbert Wiener, *Cybernetics: Or Control and Communication in the Animal and the Machine*, 2d. rev. ed. (Paris: MIT Press, 1961), as quoted by Patrick Jagoda, “Speculative Security,” in *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, ed. Derek S. Reveron (Washington, DC: Georgetown University Press, 2012), 21-22.

¹⁵ The definition for cybernetics was found in Merriam-Webster’s online web site, “Cybernetics,” Merriam-Webster, <https://www.merriam-webster.com/dictionary/cybernetics> (accessed February 17, 2017). A very similar definition, as well as the description of cybernetics as pertaining both to communication and control, is provided by Jagoda, “Speculative Security,” 22.

¹⁶ U.S. Department of Defense, *Joint Publication 3-12(R) Cyberspace Operations*, (Arlington: U.S. Department of Defense, February 5, 2013), II-2 to II-3.

- **Cyber attack** – attack directed against computers or digital networks.
- **Cyber conflict** – “the use of computational technologies for malevolent and destructive purposes in order to impact, change, or modify diplomatic and military interactions among states.”¹⁷
- **Cyber power** – “the ability to control and apply typical forms of control and domination of cyberspace.”¹⁸
- **Cyber space** – “the global domain within the information environment consisting of the interdependent network of information technology (IT) infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.”¹⁹
- **Cyber war** – “an extension of policy by actions taken in cyber space by state or non-state actors that either constitute a serious threat to a nation’s security or are conducted in response to a perceived threat against a nation’s security.”²⁰

¹⁷ This definition focuses on the effects intended by malevolent activity in cyberspace and is limited to state actors, whereas the preceding definition pertains to both state and non-state actors. Valeriano and Maness, *Cyber War versus Cyber Realities*, 32.

¹⁸ The author attempted to craft his own definition of cyber power, “the ability to influence the behavior of others through the use of computer or digital interactions or networks to achieve a desired outcome,” by combining D. Robert Worley’s definition of power, “the ability to influence the behavior of others to achieve a desired outcome,” with the above definition for cyber. This definition was broad and focused on the effects manifested by and through digital networks rather than on the networks themselves. However, Valeriano and Maness demonstrate how the impact of state manifestations of cyber power in this context “has failed to demonstrate a true and actual change in state-to-state interactions.” Ryan C. Maness and Brandon Valeriano, *New Sources of Power: Russia’s Coercive Cyber and Energy Policy* (unpublished manuscript), as quoted in Valeriano and Maness, *Cyber War versus Cyber Realities*, 25. D. Robert Worley, *Orchestrating the Instruments of Power: A Critical Examination of the U.S. National Security System* (Raleigh: Lulu Press Inc., 2012), 275.

¹⁹ U.S. Department of Defense, *JP 3-12(R) Cyberspace Operations*, I-1.

²⁰ Although many definitions are provided in literature, the author prefers this version as it most closely appreciates the political purpose of war as described by the premier military theorist Carl von Clausewitz. Paulo Shakarian, Jana Shakarian, and Andre Ruef, *Introduction to Cyber-Warfare: A Multidisciplinary Approach* (Amsterdam: Elsevier, Inc., 2013), 2.

CHAPTER 2: THE MILITARY PARADIGM OF U.S. NATIONAL CYBER POWER

*Consistent with the United Nations Charter, states have an inherent right to self-defense that may be triggered by certain aggressive acts in cyberspace ... When warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country.*¹

U.S. International Strategy for Cyberspace, 2011

*A State that is the target of a cyber operation that rises to the level of an armed attack may exercise its inherent right of self-defense. Whether a cyber operation constitutes an armed attack depends on its scale and effects ... The International Group of Experts agreed that any use of force that injures or kills persons or damages or destroys property would satisfy the scale and effects requirement.*²

2013 Tallinn Manual, Part I, Chapter 2, Section 2, Rule 13

The internet traces its origins to a U.S. military research initiative in the 1960s to link scientists throughout the U.S. to the few powerful supercomputers then available to support defense-related research.³ Although the first instantiation of the network on October 29, 1969, was to link four civilian research sites together, the Department of Defense's Advanced Research Projects Agency (ARPA, later renamed DARPA) funded and controlled this research effort until they declared the network operational in 1975. Subsequent to this declaration, DARPA passed control of the network to the Defense Communications Agency. However, this transfer in no way signified DARPA's end in this capability. Indeed, DARPA-funded research efforts continued to drive the academic and business research communities to expand both the capacities and capabilities of internetted computers throughout the 1970s and 1980s.

¹ U.S. President, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* (Washington DC: Government Printing Office, May, 2011), 10-14.

² Michael N. Schmitt, ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge: Cambridge University Press, 2013), 54-55.

³ Patrice Flichy, "New Media History," in *Handbook of New Media: Student Edition*, rev. ed., edited by Leah A. Lievrouw and Sonia M. Livingstone (London: Sage Publishing, 2006), 189.

Without delving into the technical details of the internet's growth during this time, it is important to recognize the profound influence defense researchers and scientists wielded over the burgeoning internet. One key concept underlying the internet since its foundation is the idea of open-architecture networking. Using this concept, introduced by Robert Kahn shortly after his arrival to DARPA in 1972, the "choice of any individual network technology was not dictated by a particular network architecture but rather could be selected freely by a provider and made to interwork with the other networks through a meta-level 'Internetworking Architecture.'"⁴ Thus, the networks could be custom designed to meet specific user-defined environments and requirements rather than conform to a universal standard. Another common feature of today's internet that owes its origin to DARPA is the Transmission Control Protocol/Internet Protocol (TCP/IP) that serves as a common communications protocol enabling open-architecture networking. TCP/IP was adopted as the defense standard in 1980, a decision that enabled defense to begin sharing the protocol base with both military and non-military communities prior to effecting a deliberate ARPANet transition to this protocol in 1983.⁵ These and other ideas set the stage for the internet as it is known today.⁶ The ease of access enabled by the open architecture design led to both the

⁴ Barry M. Leiner, Vinton G. Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts, and Stephen Wolff, "Brief History of the Internet," Internet Society, <https://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet> (accessed December 28, 2016), 3.

⁵ This transition was significant in that the ARPANet formed the primary internetwork at the time, thus this transition required several years of planning to effect a single, consolidated, simultaneous shift of the entire network. Ibid., 4.

⁶ In many ways, Robert Kahn's initial thinking about the desired characteristics of an "internetwork" proved foundational for the internet's current characteristics. In addition to the two examples already provided, Kahn developed four ground rules that were critical to his, and therefore DARPA's, internet development efforts. "1) Each distinct network would have to stand on its own and no internal changes could be required to any such network to connect it to the Internet. 2) Communications would be on a best effort basis. If a packet didn't make it to the final destination, it would shortly be retransmitted from the source. 3) Black boxes would be used to connect the networks; these would later be called gateways and routers. There would be no information retained by the gateways about the individual flows of packets passing through them, thereby keeping them

widespread popularity and thus adoption of the network while also foundationally embedding vulnerabilities that are now inherent and inescapable.

Perhaps as a result of these origins, and perhaps in part due to the obvious military command and control advantages conferred by use of the internet, strategic decision makers regard national cyber capabilities predominantly within a military paradigm. The consequences of considering cyber capabilities within a military paradigm demand further analysis, for these consequences are both many and profound. These consequences manifest in the development of strategic concepts and theories regarding the application of cyber power. They also include the imposition of an artificial separation between Defense Department and other government and civilian cyber sectors due to *posse comitatus*, a limitation on the use of military offense cyber capabilities in ambiguous circumstances short of declared war due to *jus ad bellum* principles, and the reluctance to use offensive cyber capabilities due to a perception of these capabilities as a last-resort option. Ultimately, these consequences result in a constrained understanding and treatment of national cyber power and thus limit the development of cyber options for strategic decision-makers.

This chapter explores the influence of the military paradigm in the development of a current understanding of national cyber capabilities and the commensurate effects of this military paradigm on employment of these capabilities. First, this chapter provides a brief historical summary of the U.S. defense community's role in development of the internet and cyber space. Next, the chapter demonstrates the pervasive influence of the internet's military origins on the development of cyber power concepts and theories. Specifically, this section of the chapter demonstrates the prevalence of military terminology and concepts in published

simple and avoiding complicated adaptation and recovery from various failure modes. 4) There would be no global control at the operations level. Ibid, 4.

cyber power literature. This also shows how strategic policy documents conceptualize cyber power as a military capability and a military operating domain. Third, this chapter evaluates the effects of the military paradigm with regard to cyber power employment, identifying limitations on the use of strategic cyber power and second-order effects of these limitations. This chapter concludes with a summary of the net constraining effects that result from national cyber capabilities as a component of the military instrument of national power.

Military Role in Cyber Power Development

The military's role in the creation of the initial internet and its design characteristics have been discussed above. One feature not previously mentioned, however, is the ability to separate military and civilian networks that was enabled by the adoption of the TCP/IP as the internet standard in the 1980s. As Derek Reveron notes, "In some sense, there has always been an implicit national security purpose for the Internet."⁷ Although it is a widely-held misperception that DARPA's internet development efforts were associated with the military's need for a command and control system that would survive a nuclear attack, there was nonetheless an obvious military advantage of a system that provided redundant, reliable, remote access to critical computer systems and capabilities.

Military Influence on Cyber Thought

Cyber Literature

The tremendous global growth of digitization over the last two decades mirrors the profusion of literature published regarding cyber capabilities. Indeed, it is an exciting time

⁷ Derek Reveron, ed, *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, (Washington DC: Georgetown University Press, 2012), 7.

for cyber. That said, a large body of recent cyber literature reveals a heavy military influence on cyber considerations. The term *cyberwar* figures prominently in published cyber titles. A useful anthology of twenty-first century cyber case studies also shows this heavy military influence, organizing its primary sections around “cyber attack,” “cyber espionage and exploitation,” and “cyber operations for infrastructure attack.”⁸ Martin Libicki, a prolific cyber author, has published multiple books, articles, and RAND reports on cyber topics that share a common frame of military reference in discussing cyber *attack* and *defense*.⁹ Richard Clarke, a former Assistant Secretary of State and the first Special Advisor to the President for Cyber Security in 2001, shows how deep-rooted the evaluation of cyber as a military instrument is in his easy-to-read 2010 book *Cyber War: The Next Threat to National Security and What to Do About It*.¹⁰

A smaller body of cyber literature addresses the strategic considerations of cyber capabilities. In a chapter of a 2012 RAND report, Libicki compares cyberwar to nuclear war, drawing out the similarities and differences between the two and their respective influences on strategic stability (alert reaction cycles, first-strike capabilities and escalation, the security dilemma, and neutrality versus ambiguity). He concludes his analysis by demonstrating a gap between cyber operation facts and perceptions that consequently may further destabilize cyber crises.¹¹ Several works seek to take an empirical approach towards analysis of conflict in the cyber domain. Danny Steed notes that although “plentiful in volume, [cyber warfare

⁸ Paulo Shakarian, Jana Shakarian, and Adnrew Ruef, eds., *Introduction to Cyber-Warfare: A Multidisciplinary Approach* (Amsterdam: Elsevier, 2013).

⁹ Several examples of his work include the following: Martin C. Libicki, Lillian Ablon, and Tim Web, *The Defender’s Dilemma: Charting a Course Toward Cybersecurity* (Santa Monica: RAND Corporation, 2015); “Cyberwarfare as a Confidence Game,” *Strategic Studies Quarterly* (Spring 2011): 132-46; and *Defending Cyberspace and other Metaphors* (Washington, DC: National Defense University, 1997).

¹⁰ Richard A. Clarke and Robert K. Knake, *Cyber War: The Next National Security Threat and What to Do About It* (New York: HarperCollins, 2010).

¹¹ Martin C. Libicki, *Crisis and Escalation in Cyberspace* (Santa Monica: RAND Corporation, 2012), 123-45.

literature] is also desperately impoverished in terms of its quality, particularly in generating strategic understanding.”¹² In assessing the state of current cyber thinking, he attributes this lamentable lack of strategic thought and subsequent separation of thinking into two diametrically opposed schools of thought, the “hyperbolic” and the “skeptical,” to a lack of empirical data to form a basis for strategic analysis.¹³ On the basis of three prominent case studies that he asserts provide sufficient quantity and quality of data to enable empirical analysis, he offers three “strategic certainties” to guide future thinking on cyber: cyber warfare will grow in strategic significance; cyber warfare will not be a strategically decisive instrument; and, cyber warfare will remain strategically ambiguous.¹⁴ The first point is generally accepted, but the second point is arguable in the Iran 2010 case study, and the last point is a wild card subject to ongoing technological developments regarding anonymity versus identification in this space. Nonetheless, his effort is a welcome one to forge a path through an otherwise operationally-focused body of cyber literature.

Of all the works on cyber power, one that stands out in providing a strategic-level evaluation of cyber capabilities is *Cyber War Versus Cyber Realities: Cyber Conflict in the International System* by Brandon Valeriano and Ryan C. Maness. Similar to Steed, Valeriano and Maness also take an empirical approach to their analysis, basing their evaluation and conclusion on an eleven-year data set of inter-state cyber conflict compiled from 2001 to 2011 that consists of 111 total cyber incidents within 45 broader cyber disputes.¹⁵ Aside from the use of the term *cyber war* in the title—a deliberate use to separate

¹² Danny Steed, “The strategic implications of cyber warfare,” in *Cyberwarfare: a multidisciplinary analysis*, ed. by James Green (London: Routledge, 2015), 74.

¹³ Steed, “Strategic Implications,” 75-6.

¹⁴ *Ibid.*, 89-92.

¹⁵ Brandon Valeriano and Ryan C. Maness, *Cyber War Versus Cyber Realities: Cyber Conflict in the International System* (Oxford: Oxford University Press, 2015), 8.

this term and associated line of thinking from their analysis—this work elevates the strategic analysis of cyber to nest within international relations. While they acknowledge the potential for conflict that can cause both kinetic and non-kinetic damage, their analysis of unclassified cyber incident data demonstrates that the perception of imminent catastrophic cyber danger does not match current empirical realities. Instead, cyber conflict is highly contextual to ongoing geostrategic conflicts and sources of friction, both regionally and globally. The most “severe” incidents identified by the authors (Iran Stuxnet; Russian infiltration of the American eastern seaboard power grid; and Chinese theft operations against American, Japanese and Indian militaries) do not show “escalation in terms of the basic rate at which the tactic has been used” through 2013. Restraint mechanisms exist, although they have not evolved into a broadly recognized normative system.¹⁶

Cyber as an Operating Domain

To promote an understanding of cyber, it is useful to compare the cyber domain to the other recognized military operating domains and identify any cyber domain characteristics shared with the other domains as well as characteristics peculiar only to this domain. This paper examines the maritime, air, and space domains to compare the development of domain understanding and subsequent theoretical evolution in an effort to derive lessons applicable to the still-nascent understanding and theoretical development of cyber.¹⁷

¹⁶ Valeriano and Maness, *Cyber War Versus Cyber Realities*, 214.

¹⁷ The land domain is excluded from consideration as the effort to understand and operate in the land domain dates back thousands of years to theorists and historians such as Sun Tzu and Thucydides, whereas the development of the subsequent maritime, air, and space domains occurred in the modern age and thus provides clearer bases for comparison to cyber.

The Sea, the Sky, and the Heavens

Early modern efforts to comprehend the maritime domain demonstrate the limited role ascribed to this domain. Prior to the seminal works of Alfred Thayer Mahan and Sir Julian Corbett to articulate the role of the maritime domain in not only enabling but also waging war, the predominant view of the maritime domain was either an obstacle or a bridge to land warfare. During the Peloponnesian War, contests for power were determined on land.¹⁸ Sir Francis Bacon in 1597 attributed the sea with affording one the option of “tak[ing] as much or as little of the war as he will;” in other words, describing the domain as a bridge enabling access to warfare.¹⁹ While Alfred Thayer Mahan is considered one of the most preeminent naval theorists for his recognition of the role of the navy both during war and in promoting commerce during times of peace, it was Sir Julian Corbett who articulated a broader appreciation of the maritime domain as a “general concept relating to the overall use of a state’s forces in war” and envisioned “the navy’s role in the overall strategy and in relation to forces from other armed services.”²⁰ This understanding of the maritime domain coupled with the advent of technologies that allowed navies to break from their dependence on the wind greatly expanded the concept of two-dimensional war. The maritime domain was no longer a bridge or barrier, but a domain for maneuver in its own right on more equal terms with the formerly predominant land domain.

¹⁸ Thucydides wrote that Athens was able to hold out for an additional ten years against not only its original enemy but a coalition of former Greek allies and the Persian Empire, even after losing its premier source of military strength, namely its fleet. Clearly, the fleet was a source of strength for the Athenian Empire, but was not in itself the decisive component of military power. Thucydides, *History of the Peloponnesian War*, trans. by Charles Foster Smith (Cambridge: Harvard University Press, 1930), 2.65.12-3, quoted in Donald Kagan, *Thucydides: The Reinvention of History* (New York: Penguin Books, 2009), 75.

¹⁹ Jan Angstrom and J. J. Widen, *Contemporary Military Theory: The Dynamics of War* (New York: Routledge, 2015), 129.

²⁰ Angstrom and Widen, *Contemporary Military Theory*, 130.

Continued technological advances in the early twentieth century led to the expansion of war into the air domain with the advent of powered flight. Early theoretical efforts by Giulio Douhet and William Mitchell to understand this domain following World War I showed the war's influence on their thinking as revealed by their view of air power as predominantly offensive and their assertion that airpower in and of itself could produce strategic effects.²¹ This domain opened a third physical dimension for maneuver that could bypass existing two-dimensional warfare capabilities, which fundamentally altered the character although not the nature of war.

Finally, continued technological advances in the post-World War II era opened space to man. Similar to the opening of the air domain but differing in scale, man's ascendance into space greatly extended the opportunity for three-dimensional maneuver. Similar to the other domains, this new domain was physical. Like the air domain, man was challenged to enter and remain in this domain, and the threshold to access it was sufficiently great that only a few nations have been able to muster sufficient resources to access it on a regular basis. However, the space domain differed greatly from the air domain and, to a lesser extent, the maritime domain with regard to the concept of territoriality. The U.S. decision not to protest the 1957 overflight of the Soviet Union's Sputnik satellite demonstrated the nature of this domain as the first truly global common, although the resource threshold required to access this domain was so high that this domain until very recently remained the province solely of nations and nation-approved commercial entities (e.g., commercial telecommunications and imagery satellites). Some of the ongoing challenges with development of a coherent space theory relate to both previous domains as well as cyber. Among those challenges are

²¹ Ibid, 149. Giulio Douhet, *The Command of the Air*, 2d ed., trans. by Dino Ferrari (North Stratford: Ayer Company Publishers, Inc., 2002), 251.

questions about what priority should be given to the space domain relative to the other domains, how should limited resources be allocated to this domain, and to what extent should operations in this domain be independent of or synchronized with operations in other domains.²² The lessons with regard to the gradual understanding and theoretical development of these previous domains may inform the immature literature on the cyber domain.

The cyber domain exists as a global common, much like the maritime and space domains. Alfred Thayer Mahan wrote on the global commons as a means to “advance commerce through a secure, networked infrastructure that connects global enterprise across the commons,” which could as easily describe cyberspace today as the maritime domain of which he was writing in the late nineteenth century.²³ Indeed, Mahan’s work informed the ideas of network-centric warfare and the concepts of both space and cyberspace as separate domains successfully advocated by Admiral Arthur K. Cebrowski in the late 1990s.²⁴ However, cyber differs from the aforementioned domains in several distinct and important ways. Cyberspace may be the only truly global common in which anyone who accesses it at any location can have global reach and effects. Also, the entry cost to access this domain is fundamentally lower and decreasing every day due to global digitization trends. Stephen McPherson and Glenn Zimmerman identify several other characteristics peculiar to cyberspace, including “the departure from the mechanical to the electronic,” the “highly asymmetric nature of cyberspace,” and the “unparalleled level of integration” between

²² Dana J. Johnson, Scott Pace, and C. Bryan Gabbard, *Space: Emerging Options for National Power* (Santa Monica: RAND, 1998), 75-7.

²³ Alfred Thayer Mahan, *The Influence of Sea Power Upon History* (Charleston: Bibliolife, 2007), 51, as quoted by Steven H. McPherson and Glenn Zimmerman, “Cyberspace Control,” in *Securing Freedom in the Global Commons*, ed. Scott Jasper (Stanford: Stanford University Press, 2010), 85.

²⁴ Steven H. McPherson and Glenn Zimmerman, “Cyberspace Control,” 87.

military operations almost entirely reliant upon civilian-run systems.²⁵ These unique characteristics, when considered in tandem with society's growing reliance upon the internet, suggest a fundamental change in the character of conflict.

National Cyber Organizations

Cyber capabilities exist within numerous executive branch departments, offices, agencies, and bureaus. Within the Defense Department, U.S. Cyber Command (CYBERCOM) under U.S. Strategic Command (STRATCOM) is assigned responsibilities to:

direct the operations and defense of specified Department of Defense information networks and; prepare to, and when directed, conduct full spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries.²⁶

CYBERCOM is collocated and shares its commander with the National Security Agency, the latter which provides the signals intelligence, cyber intelligence, and cyber research and development (R&D). In recognition of the growing importance of cyber by both Congress and the Defense Department, the 2017 National Defense Authorization Act submitted to Congress includes the proposal to remove CYBERCOM from under STRATCOM and establish it as an independent Functional Combatant Command equivalent to STRATCOM, U.S. Transportation Command, and U.S. Special Operations Command. The Department of Homeland Security (DHS) "has the lead for the federal government for securing civilian government computer systems" while also working collaboratively with industry and state

²⁵ Ibid, 88.

²⁶ U.S. Department of Defense, Cyber Command Fact Sheet (September 30, 2016) <http://www.stratcom.mil/Media/Factsheets/Factsheet-View/Article/960492/us-cyber-command-uscycbercom/> (accessed December 28, 2016).

and local governments to “secure critical infrastructure and information systems.”²⁷

Investigative actions for cyber attacks are the primary responsibility of the Department of Justice’s Federal Bureau of Investigation (FBI), which serves as the “lead federal agency for investigating cyber attacks by criminals, overseas adversaries, and terrorists.”²⁸ The Office of the Director for National Intelligence (ODNI) also has a role in supporting and coordinating intelligence support for malicious cyber actions.

This division of labor with regard to cyber capabilities is sub-optimal. It violates the military principle of unity of command that directs, “The operation of all forces under a single responsible commander who has the requisite authority to direct and employ those forces in pursuit of a common purpose.”²⁹ Although this is a military-specific definition, the concept of aligning capabilities under the purview of a single decision-maker is broadly applicable to various national-level capabilities, demonstrated by the Cabinet-level Secretaries serving as unity of command examples for their respective areas of assigned responsibility (e.g., diplomacy, treasury, defense, and homeland defense). In the absence of a single appointed decision-maker for cyber issues, decision-making and strategy is determined instead through a less timely and less efficient process of cooperation and collaboration to build consensus. This process also lacks a mechanism for resolving differences short of elevating the issue to a higher level, which again requires time to prepare arguments reflecting each position for due consideration and determination by the higher authority.

²⁷ U.S. Department of Homeland Security, “Core Missions: Safeguard and Secure Cyberspace,” (March 21, 2016) <https://www.dhs.gov/safeguard-and-secure-cyberspace> (accessed December 28, 2016).

²⁸ Federal Bureau of Investigations, “What We Investigate: Cyber Crime,” <https://www.fbi.gov/investigate/cyber> (accessed December 28, 2016).

²⁹ U.S. Department of Defense, *Joint Publication 1-02 Department of Defense Dictionary of Military and Associated Terms* (Arlington: U.S. Department of Defense, November 8, 2010 (as amended through February 15, 2016)), 252.

Over the past several years, the executive branch has taken action in light of the severity of the threat, the increasing vulnerability of the nation, and the inefficient federal government posture to respond to cyber incidents. In 2015, President Obama directed the ODNI to establish the Cyber Threat Intelligence Integration Center to develop, implement, and coordinate intelligence sharing capabilities to enhance shared situational awareness at the lowest possible levels of classification among US government and private entities.³⁰ In mid-2016, President Obama took further, more far-reaching actions to improve federal government cyber responsiveness by issuing Presidential Policy Directive-41. This directive distinguished three cyber incident “response areas” and designated corresponding lead agencies for each area; Department of Justice and the FBI acting through the National Cyber Investigative Joint Task Force for “threat response,” DHS acting through the National Cybersecurity and Communications Integration Center for “asset response,” and ODNI acting through the Cyber Threat Intelligence Integration Center for “intelligence support and related activities.”³¹ While PPD-41 served to formalize the delineation of responsibilities between these agencies, this directive had two distinct disadvantages. First, the PPD failed to include CYBERCOM within the framework for cyber incident response despite known and growing adversarial state capabilities by Russia, Iran, North Korea, China, and others. Second, by cementing the cyber division of labor among multiple agencies, the directive

³⁰ U.S. President, *Presidential Memorandum: Establishment of the Cyber Threat Intelligence Integration Center*, (Washington DC: Government Printing Office, February 25, 2015), <https://www.whitehouse.gov/the-press-office/2015/02/25/presidential-memorandum-establishment-cyber-threat-intelligence-integrat> (accessed December 28, 2016).

³¹ U.S. President, *Presidential Policy Directive-41: United States Cyber Incident Coordination* (Washington DC: Government Printing Office, July 26, 2016), <https://www.whitehouse.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident> (accessed December 28, 2016). An FBI news release issued simultaneous to PPD-41 offered a clear and succinct explanation of the PPD, posted to their web site. Federal Bureau of Investigation, *Countering the Cyber Threat New U.S. Cyber Security Policy Codifies Agency Roles* (July 26, 2016), <https://www.fbi.gov/news/stories/new-us-cyber-security-policy-codifies-agency-role> (accessed December 28, 2016).

consequently solidified the challenges inherent in working through multiple agencies, centers, and joint task forces that leads to diffused national responsiveness.

Consequences of Military Influence on Cyber Power Employment

As referenced in the 2011 International Strategy for Cyberspace, the U.S. reserves the right to respond militarily to a cyber attack *when warranted* (emphasis added). This italicized phrase is significant, as it alludes to the legal justification required to legitimize a military response. Legal limitations associated with the use of military force were briefly discussed in chapter one; this section explores the consequences of the limitations. One consequence is the hesitation to act without a legal determination or justification, which is often problematic given the challenges of attribution for activity that occurs in the truly global common region of cyberspace. This consequence, while subtle, is both far reaching and critical, as it undermines the military principles of speed and tempo and is habit-forming. While lawyers (and strategic decision-makers) demand precise information upon which to base their judgments, the fog of war first described by Carl von Clausewitz remains an inherent feature of today's battlefield that must be accepted rather than fought. Charles Dunlap accurately stated that such technical requirements and specificity have “a direct analogy to the central conundrum faced by military decision makers fighting in more traditional battlespaces—that is, the need to make quick decisions based on imperfect data.”³² A second consequence of the legal limitations on the use of military force is the creation of a conceptual, and in many cases, an actual separation between national cyber capabilities. Fred Taylor and Jerry Carter

³² Charles Dunlap, “Cyberstrategists on Cyberlaw for Cyberwar,” in *Conflict and Cooperation in Cyberspace: The Challenge to National Security*, eds. Panayotis A. Yannakogeorgos and Adam B. Lowther (New York: Taylor and Francis Group, 2014), 212.

note that while “military cyberspace operations in the public-private arena rightfully raises important privacy and civil liberties issues among Americans,” success—defined as national security—requires “modernization of authorities and organizational relationships” across the range of government (both uniformed and civilian) and private sectors to provide security while protecting privacy and civil liberties.³³

In the current paradigm, employment of cyber is thus subject to the *jus ad bellum* principles that are commonly accepted to provide legal justification and thus legitimacy for going to war. Several authors directly address these legal considerations. As James A. Green notes, “...the *Tallinn manual* represents the majority view in the literature on this point, which is that the existing rules of international law are applicable to the threat posed by cyber warfare.”³⁴ Another author shifts analysis to consideration of the applicability of *jus in bello* to cyber activities, finding that “much of that body of law is framed in general terms that may be applied regardless of technological advances.”³⁵ George Lucas continues this exploration of the possibility of an “ethical cyber war,” raising important, yet paradigm-reinforcing, questions such as what constitutes use of force in this space and how the level of this force is measured (to assess damage and prepare proportional or reasonable responses).³⁶

³³ Fred Taylor, Jr. and Jerry Carter, “Cyberspace Superiority Considerations” in *Conflict and Cooperation in Cyberspace: The Challenge to National Security*, eds. Panayotis A. Ynnakogeorgos and Adam B. Lowther (New York: Taylor and Francis Group, 2014), 19.

³⁴ The report referenced here is the *Tallinn manual on the international law applicable to cyber warfare*, a report prepared by an international team at the request of the NATO Cooperative Cyber Defence Centre of Excellence. Although an academic, non-binding work, this manual follows an established precedence for issuing such works that can have an outsized impact on how states and organizations approach such issues. James A. Green, “The regulation of cyber warfare under the *jus ad bellum*,” in *Cyber Warfare: A multidisciplinary analysis* (London: Routledge, 2015), 96-7.

³⁵ Heather A. Harrison Dinniss, “The regulation of cyber warfare under the *jus in bello*,” in *Cyber Warfare: A multidisciplinary analysis* (London: Routledge, 2015), 125-6.

³⁶ George R. Lucas, Jr., “Can There be Ethical Cyber War?” in *Conflict and Cooperation in Cyberspace: The Challenge to National Security*, ed. by Panayotis A. Ynnakogeorgos and Adam B. Lowther (Boca Raton: Taylor & Francis Group LLC, 2014), 196-7.

The challenges inherent in the application of military force are particularly acute in the cyber domain. Just War theory and the U.S. strategic culture takes a binary approach to what is and is not war. However, Lisa Nemeth identifies the ambiguous nature of cyber activity in considering malicious cyber incidents such as Stuxnet, Estonia, and Sony pictures. In asking the question whether such incidents can be considered acts of war, she notes that, “cyber activity, by its anonymity, potential covertness, and the use of proxies,” blurs the border between war and peace.³⁷ This ambiguity, and the challenges in satisfying precise information requirements required to render clear legal judgments, elevates the use of offensive cyber tools to the highest levels of strategic decision-making. As a result, cyber is often perceived as a tool of last resort. In the short term, this hesitation to use cyber leads to opportunity loss. In the longer term, the reluctance to use cyber tools prevents the development of the kind of experience necessary to create the required wide pool of subject matter experts needed to chart the nation’s course in the twenty-first century.

This chapter explored the many ways in which the U.S. military played a role in the development and growth of the internet. It also explored the consequences of the military’s important, and initially central, role. The military’s influence over the development and the current understanding of the internet is both pervasive and widespread. As a result, the military lens through which strategic decision-makers view the cyber environment colors their perspective and unintentionally limits their consideration of options. As a waypoint in developing the argument that the U.S. should consider cyber an instrument of national power, separate and distinct from its current subset of military power. The next chapter explores the ways in which America applies its current instruments of national power.

³⁷ Lisa Nemeth, “Cyber and the American Way of War” (master’s thesis, Joint Forces Staff College, 2015), 26.

CHAPTER 3: INSTRUMENTS OF NATIONAL POWER

*Political power in the international sphere may be divided, for purpose of discussion, into three categories...But power is an indivisible whole; one instrument cannot exist for long in the absence of the others.*³⁸

Edward H. Carr, 1939

The previous chapter explored the current understanding of U.S. national cyber capabilities. It demonstrated how the military paradigm both dominates and limits the understanding for considering U.S. strategic cyber power. While the historical military origins of U.S. cyber power provide a ready explanation for the current use of this paradigm, there is not a requirement *per se* to maintain this paradigmatic view. Cyber power competitors (and allies) of the U.S. demonstrate different views.³⁹ While it exceeds the scope of this paper to compare U.S. cyber power capabilities to those of the other leading cyber powers, it is important to recognize that there is precedence for considering national cyber capabilities as separate and distinct from national military capabilities.

This chapter builds on the previous chapter's analysis of cyber power as a military capability by conducting a comparative analysis of the framework used to analyze and evaluate manifestations of U.S. national power. Referred to as "instruments," the various components of national power categorized in U.S. military doctrine are diplomatic,

³⁸ Edward H. Carr, *The Twenty-Years' Crisis 1919-1939: Introduction to the Study of International Relations* (New York: HarperCollins, 1964), 108.

³⁹ While Russian military doctrine has addressed cyber considerations through their focus on information warfare since the 1990s, Russia takes an internal security-focused approach through the use of the Russian Federal Security Service, or FSB, as well as cultivating state-friendly and state-dominated commercial entities to lead their cyberspace monitoring efforts. Additionally, evidence suggests the Kremlin will provide a supportive environment for cyber "mercenaries" who benefit from state covert sponsorship in return for their targeting of Russian adversaries. Nikolas K. Gvosdev, "The Bear Goes Digital: Russian and its Cyber Capabilities," in *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, ed. by Derek S. Reveron (Washington DC: Georgetown University Press, 2012), 178-182.

informational, military, and economic capabilities (also known by its acronym DIME).⁴⁰

This chapter first discusses the value of the national power instruments concept to demonstrate explicitly the value behind the framework. Next, the chapter analyzes each instrument to link the concept of DIME to its actualization. This portion of the chapter addresses the emergent concept that adds several additional instruments to the list, including financial, intelligence, and law enforcement capabilities (either DIME-FIL or MIDLIFE). This study assesses the arguments held forth by proponents of this expanded concept for their applicability in supporting the case for cyber as another instrument of national power. This chapter then proceeds to propose and analyze the concept of cyber as a stand-alone instrument of national power.

Assessing the Value of the Instruments of National Power Paradigm

In order to consider cyber as a separate instrument of national power, one must first comprehend what value lies in identifying such instruments and how these instruments are instantiated. Political scientist D. Robert Worley defines power “...in the context of foreign affairs... [as]the ability to influence the behavior of others to achieve a desired outcome.”⁴¹ Writing over seventy years ago, E. H. Carr provided a useful deconstruction of political power into military power, economic power, and power over opinion along with the caution included in the opening quotation in this chapter that “... power is an indivisible whole; one

⁴⁰ U.S. Department of Defense, *Joint Publication 1-0 Doctrine for the Armed Forces of the United States* (Arlington: U.S. Department of Defense, March 23, 2013), I-4.

⁴¹ D. Robert Worley, *Orchestrating the Instruments of National Power: A Critical Examination of the U.S. National Security System* (Raleigh: Lulu Press Inc, 2012), 275.

instrument cannot exist for long in the absence of others.”⁴² His seminal work established the foundation for distinguishing distinct categories of national power.

Worley dedicates a full chapter to identifying and describing the four instruments of national power. He starts the chapter by offering the idea that “the notion of instruments of national power is an abstraction” and that the notion’s value lies in serving as “quick jumping off points on the way to discussing the concrete capabilities of the departments and agencies that house the instruments.”⁴³ For most of the post-World War II twentieth century, these instruments correlated directly to separate and distinct executive branch agencies, namely the U.S. Department of State, the former U.S. Information Agency (USIA), the U.S. Department of Defense, and the U.S. Agency for International Development.⁴⁴ Worley’s descriptions of each instrument are useful to understand how the nation employs the instruments and thus what utility the instrument holds for the nation.

Instruments of National Power

Joint Publication (JP) 1-0, *Doctrine for the Armed Forces of the United States*, provides the current framework for military strategists and practitioners to understand the instruments of national power known as DIME. These instruments are described as tools used “by appropriate government officials” for the application of sources of power, often at the direction of the National Security Council.⁴⁵ This doctrinal description reinforces Worley’s description that the concept’s value rests on the explicit actualization of an agency

⁴² Edward H. Carr, *The Twenty-Years’ Crisis*, 108.

⁴³ Worley, *Orchestrating*, 275.

⁴⁴ With the disestablishment of USIA in 1999, currently there is no single agency responsible for the information instrument of national power. Ibid, 275.

⁴⁵ U.S. Department of Defense, *Joint Publication 1-0 Doctrine for the Armed Forces of the United States* (Arlington: U.S. Department of Defense, March 23, 2013), I-4.

or department exclusively dedicated to the capability. Thus, the capability becomes a tool when a cadre of people are created who are trained in its use.

DIME

The military instrument demonstrates perhaps the clearest and most direct correlation between description and uses. The military instrument represents the use of force by not only the Department of Defense, but also the Coast Guard and civilian intelligence agencies authorized to conduct paramilitary operations either directly or through surrogates to influence behavior.⁴⁶ Military operations range across a spectrum from hard, coercive force as seen in conventional warfare to soft, attractive force as demonstrated by humanitarian assistance and disaster relief operations.

The diplomatic instrument includes all national negotiations pursued with other states either directly or via international organizations such as the United Nations. The State Department leads the national effort to conduct diplomacy, but is certainly not alone in doing so. The U.S. military supports and conducts extensive diplomatic efforts through its participation in such organizations as the North Atlantic Treaty Organization and through regional engagements by Geographic Combatant Commanders.⁴⁷

The economic instrument includes economic sanctions, foreign aid, trade controls and policies, and foreign development efforts. The sheer size of the U.S. economy and the dollar's *de facto* role as the global currency baseline means that "every move in U.S. economic, fiscal, and monetary policy has global effect."⁴⁸

⁴⁶ Worley, *Orchestrating*, 177-9.

⁴⁷ Ibid, 286-8.

⁴⁸ Ibid, 281-4.

The informational instrument is the most problematic to discuss. Worley defines the information instrument to include information collection of and dissemination to foreign audiences. This definition excludes government information exchanges otherwise accounted for within the diplomatic instrument, but it includes intelligence functions regarding information collection, processing, analysis, and synthesis. The information instrument can be further categorized by its intended audience. When used for domestic purposes, it is referred to as public affairs. For foreign audiences, it is referred to as public diplomacy.⁴⁹

Each of these instruments receives strategic direction and is employed by the executive branch of government via its organizational construct, with the exception of the information instrument which lacks a corresponding agency or department since the closure of the U.S. Information Agency in 1999. This hierarchical model allows for effective direction, guidance, and application of each instrument by strategic decision makers. Admittedly, this construct presents some challenges in integrating and synchronizing the application of all instruments to yield whole-of-government approaches and maximize the manifestation of national power. Nonetheless, this model allows for development of deep expertise in each instrument by its practitioners.

DIME-FIL

More recently, the argument emerged for expanding the DIME concept. The main thrust of this argument lies in the value inherent in leveraging other areas of national capability that strategic decision-makers can wield as tools in pursuit of the country's national objectives given the increasing complexity of the twenty-first century. The idea of expanding DIME is discussed at the senior service and joint war colleges as part of their

⁴⁹ Worley, *Orchestrating*, 278.

curriculum and its merit is generally, albeit informally, accepted. Although the expanded concept is currently not reflected in current military doctrinal publications, this is unsurprising given that doctrine often lags behind concept formulation, analysis and debate, and acceptance.⁵⁰

Perhaps the foremost argument for expanding DIME addresses three additional instrumentalities including financial, intelligence, and law enforcement (known alternately by the acronyms DIME-FIL or MIDLIFE). The financial instrument targets the specific means by which insurgents acquire and distribute capital, including both formal and informal banking and monetary exchange systems such as hawalas used in Iraq and elsewhere in the Middle East. The intelligence instrument relates to continuous operations especially relevant at the lowest tactical levels in the fluid counterinsurgency operating environment to develop the situation and generate the intelligence that allows forces to take actions against adversaries. The law enforcement instrument is regarded as peculiar to counterinsurgency, where “national and international laws can be brought to bear to restore order domestically and ensure the legitimacy of a friendly government” waging a counterinsurgency.⁵¹

⁵⁰ Interestingly, the term MIDLIFE was used in Interim Field Manual FMI 3-07.22, *Counterinsurgency Operations*, but this interim manual expired in October 2006 and was replaced by FM 3-24, which references only the traditional four instruments of power included in DIME. MIDLIFE/DIME-FIL was also explicitly mentioned in the 2006 National Strategy for Combating Terrorism and the 2006 National Military Strategic Plan for the War on Terrorism. Jack D. Kem, "Understanding the operational environment: the expansion of DIME," *The Free Library* (April 1, 2007), [https://www.thefreelibrary.com/Understanding the operational environment: the expansion of DIME.-a0213693824](https://www.thefreelibrary.com/Understanding+the+operational+environment:+the+expansion+of+DIME.-a0213693824).

⁵¹ For the description of the financial, intelligence, and law enforcement instruments, this section used the following two primary sources. Cale Horne, Stephen M. Shellman, and Brandon Stewart, “Nickel and DIMEing the Adversary: Does it work or PMESII them off?” University of Georgia and College of William & Mary: Violent Intranational Political Conflict & Terrorism Research Lab, undated. http://citation.allacademic.com/meta/p253278_index.html (accessed December 29, 2016). Jack D. Kem, "Understanding the operational environment: the expansion of DIME," *The Free Library* (April 1, 2007), [https://www.thefreelibrary.com/Understanding the operational environment: the expansion of DIME.-a0213693824](https://www.thefreelibrary.com/Understanding+the+operational+environment:+the+expansion+of+DIME.-a0213693824) (accessed December 29, 2016).

The argument for including these additional capabilities as national power instruments came to the fore as the U.S. began to conduct major counterinsurgency operations in Iraq beginning in 2004 for the first time since the Vietnam Conflict in the 1970s and existing doctrinal concepts were found wanting. DIME was a Cold War toolset that was effective in characterizing capabilities appropriate for state-on-state engagement and competition. In its application against asymmetric adversaries such as insurgent organizations, however, the toolset proved insufficient. The nature of the battlefield had changed, and more capabilities and levers were needed. In short, as the character of conflict changed, the need was identified for additional tools and capabilities by which to compete.

Given the argument for new approaches and levers of national power due to the changing character of conflict, the next chapter will propose a new strategic approach regarding national cyber capabilities. It will then proceed to identify the requirements for and subsequently explore the implications of this new approach. The chapter will conclude with an examination of the risks and benefits associated with this approach.

CHAPTER 4: CYBER AS AN INSTRUMENT OF NATIONAL POWER

The Task Force notes that the cyber threat to U.S. critical infrastructure is outpacing efforts to reduce pervasive vulnerabilities, so that for the next decade at least the United States must lean significantly on deterrence to address the cyber threat posed by the most capable U.S. adversaries. It is clear that a more proactive and systematic approach to U.S. cyber deterrence is urgently needed.¹

Craig Fields, Chairman, Defense Science Board, February, 2017

Chapter two of this thesis briefly summarized the military influence in cyber development that underpins the current U.S. strategic approach to cyber in which cyber is considered a military instrument of national power. Chapter three explored the concept of instruments of national power. Most importantly, it highlighted the argument for expanding the existing concept of national power (DIME) that was advanced in the mid-2000s as a result of the U.S. experiences waging war against an asymmetric adversary to show how the changing character of conflict calls for new concepts when existing doctrine proves inadequate.

This chapter explores the requirements, implications, risks, and benefits of adopting cyber as a separate instrument of national power. It identifies what would need to change legally and organizationally in order to actualize the concept. Given these changes, this section then projects and analyzes the implications for cyber employment in both offensive and defensive applications. The chapter concludes by weighing the risks and benefits associated with this proposal.

¹ U.S. Department of Defense, *Final Report of the Defense Science Board (DSB) Task Force on Cyber Deterrence*, by James N. Miller and James R. Gosler, endorsement memo by Craig Fields (Washington, DC: Department of Defense, February, 2017).

The Idea

Considering cyber as a separate instrument of national power builds upon the argument that America should modify and adapt its existing instruments in response to changes in the character of conflict. Moreover, the nation's increasing dependency on and vulnerability to cyber activities mandates its assessment as a separate instrument rather than a subordinate component of the military instrument. This is not as novel a concept as it may first appear. In 2014, Fred Taylor Jr. and Jerry Carter argued that "the U.S. government must have a unified effort to advance cyberspace capabilities through national priority, policy, legislation, and organization."² While they acknowledged that recent domestic and international legislation and policy have made progress articulating and clarifying U.S. and international positions regarding cyberspace, they cautioned that further work was required to define, prioritize, and enhance U.S. cyber capabilities to support strategic objectives for cyberspace superiority.

Others have added their voice to the growing chorus for this need to further grow and synchronize U.S. cyber capabilities. A September 2016 Senate Armed Services Committee hearing "illustrated disagreements between members of Congress, senior cyber officials and private technology companies about the best way to cooperate on preventing not only future cyberattacks, but (also) physical attacks planned using encrypted communication."³ In late 2016, a senior NSA official publicly discussed the need to consolidate national cyber capabilities. Highlighting the inefficiencies inherent in a system in which cyber capabilities are distributed among multiple agencies and departments, Curtis Drake, NSA's deputy

² Taylor and Carter, "Cyberspace Superiority Considerations," 18.

³ Mohana Ravindranath, "McCain to White House: If You Won't Establish a Cyber Defense Policy, Congress Will," *Defense One*, September 14, 2016, <http://www.defenseone.com/politics/2016/09/mccain-white-house-if-you-wont-establish-cyber-defense-policy-congress-will> (accessed November 22, 2016).

national manager for national security systems, stated his belief that “we need to rethink how we do cyber defense as a nation” and identified that combining capabilities within the NSA, the FBI, and the Homeland Security Department into one cyber defense organization would provide inherent advantages over the current trifurcated system.⁴ Most recently, the Defense Science Board (DSB) Task Force on Cyber Deterrence released the results of a two-year study effort into cyber deterrence and capabilities needed to support both deterrence and conflict in this operational domain. Disconcertingly, the DSB Chairman noted in his endorsement of this report that the threat is “outpacing (U.S.) efforts to reduce pervasive vulnerabilities” and he implies that current efforts lack both proactivity and synchronization.⁵ Clearly, a new approach is needed to combat this growing threat.

Requirements

The next question to address is what it means to seek a new approach. It is one thing to discuss cyber as an instrument of national power abstractly, but how would such a decision actualize in the real world? This paper identifies two requirements, one legal and one organizational, to implement this concept. Legally, the U.S. would have to modify its current legal position that equates adversarial cyber action as an armed attack. Organizationally, this proposal requires the consolidation of cyber capabilities into a single, civilian-led executive

⁴ At the time this article was published, Curtis Drake was the NSA’s deputy national manager for national security systems. He provided these remarks during an address at the American Enterprise Institute. During his remarks, he advocated for the unification of the cyber defense components of the NSA, FBI, and DHS to provide more effective and timely cyber defense. Joseph Marks, “The US Needs One Cyber Defense Agency-Not Three, a Top NSA Official Says,” *Defense One*, October 19, 2016, <http://www.defenseone.com/technology/2016/10/us-needs-one-cyber-defense-agencynot-three-top-nsa-official-says/132474/> (accessed November 22, 2016).

⁵ Craig Fields, the DSB Chairman, made this comment in his endorsement memo of the Task Force’s final report. U.S. Department of Defense, *Final Report of the Defense Science Board (DSB) Task Force on Cyber Deterrence*.

branch agency or department. These two changes, if enacted, would transform this idea into a strategic approach with tangible applications and wide-ranging implications.

As mentioned briefly in chapter one and highlighted in the opening quote of chapter two, the U.S. position on cyber aggression is clear; the U.S. reserves the right to act in self-defense to this as it would to any other hostile threat directed against the country.⁶ This position, equating cyber attacks to the status of an armed attack, is somewhat unique internationally.⁷ Because the U.S. frames hostile cyber action as an armed attack, the U.S.'s application of offensive cyber capabilities is considered the same. In seeking to promote a rules-based international order, the U.S. seeks broad legitimacy for any application of offensive military power. Thus, the U.S. use of its offensive cyber is broadly constrained to only the most extreme situations.

Without delving into an in-depth discussion on the misleading nature of terminology associated with cyber, a key concept in elevating cyber to its own instrument of national power is to remove cyber from the military paradigm. The nation's position thus conflicts with the idea of separating cyber considerations from strictly military frameworks and would need to be modified. Admittedly, the wording is vague and thus provides room for interpretation by strategic decision-makers, but at the same time such vague language undermines the deterrent effects that more specific language could achieve. Except in select

⁶ U.S. President, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* (Washington DC: Government Printing Office, May, 2011), 10-14.

⁷ An "armed attack" is a specific legal term in international customary and treaty law that triggers the threshold for a state's inherent right to use military force for self-defense. Karl Zemanek, "Armed Attack," *Max Planck Encyclopedia of Public International Law* (Oxford University Press, October, 2013), <http://opil.ouplaw.com> (accessed March 6, 2017). The reasons for which the U.S. took this aggressive legal position were not stated in the 2011 strategy, but the DSB Chairman's conclusion that "for the next decade at least the United States must lean significantly on deterrence" suggests that this position represented a clear deterrence signal to the nation's adversaries and competitors. U.S. Department of Defense, "Final Report of the Defense Science Board (DSB) Task Force on Cyber Deterrence," by James N. Miller and James R. Gosler, (Washington, DC: Department of Defense, February, 2017).

circumstances where the scale and effects of such attacks cross the international customary law criteria, the U.S. should counter cyber aggression as it does aggression in the other instruments of national power--through a holistic, whole-of-government approach that includes use and synchronization of all instruments including cyber. As an unclassified paper relying solely on publicly-available sources, this thesis cannot account for any U.S. actions that may have occurred or may be occurring in the classified space. However, the dearth of literature addressing U.S. offensive cyber actions other than the alleged involvement in the Stuxnet virus suggests either that the U.S. capabilities are not used frequently or, alternately, that the capabilities are so advanced as to largely avoid compromise.

In addition to the aforementioned legal change, adopting cyber as a non-military instrument of national power would also require an organizational change. Recognizing the accuracy of Worley's comment that "the named instruments are merely quick jumping off points on the way to discussing the concrete capabilities of the departments and agencies that house the instruments," this paper proposes consolidating the disparate national cyber capabilities within one agency.⁸ The organizational approach for which the senior NSA official quoted previously recently advocated is the clear solution to address many of the current challenges inherent in optimizing US national cyber power.

Such an organization would combine the cyber intelligence, research, and development capabilities of the National Security Agency and the investigative capabilities of the FBI (who, incidentally, often rely on subject matter experts from the NSA for technical

⁸ Worley, *Orchestrating*, 275.

support to their investigations).⁹ Such a consolidation would also occur between the ODNI's Cyber Threat Intelligence Integration Center, National Cyber Investigative Joint Task Force, and National Cybersecurity and Communications Integration Center. This consolidation would not obviate the functions of threat response, asset response, and intelligence support. However, this consolidation would enhance the responsiveness in all three areas by removing the organizational and bureaucratic barriers to information sharing and reaction responses that currently exist between these entities and their parent agencies, departments, and bureaus.

How would this agency be formed? While there could be many ways to do so, this analysis proposes that the personnel required to man this hypothetical organization be directly transferred from their respective current agencies and the capabilities and responsibilities of each agency be transferred in whole to the new agency. While a transition and probably a phased approach would likely be required given the broad scope of activity such a transfer would entail, ultimately this consolidation is intended to yield efficiencies not just in process and speed of operations, but also in resource requirements given the capability overlap and capacity redundancy that likely exists between the three organizations; their subordinate watch floors, centers, and task forces; and the liaisons each organization maintains with others.

It is important to note that this organization is civilian in nature and not a military command. Inherent in the idea of elevating cyber to consideration as a separate instrument of

⁹ Of note, this proposal for consolidation does not include the Defense Department's USCYBERCOM, as the military must retain a robust cyber capability given its increasing reliance on digital, interconnected technologies. However, the consolidation of national cyber capabilities into a civilian-led executive branch department would include a significant shift in resources, with a majority directed towards the civilian-led organization to reflect the priority for a non-military national cyber capability.

national power is the idea that doing so offers additional options and avoids some of the limitations associated with the use of military force. Thus, this organization is not a “defense” entity, but instead is an agency empowered with a range of capabilities and options appropriate for the full spectrum of cyber operations.

Implications

Implementing a new strategic approach by adopting a new legal position regarding cyber use and consolidating national cyber capabilities into a single civilian-led institution has implications for cyber power applications. Considered in toto, these implications expand the range of options for cyber power use. However, these implications also have adverse second-order consequences that will be discussed subsequently.

From an offensive cyber power perspective, lowering the legal significance placed on cyber activity thus lowers the threshold for its use. Taking the argument to the extreme, one could posit that cyber is in fact not an act of force at all and instead should be considered as a capability equivalent to information or economics. This position is not without precedent. Michael Schmitt, in his consideration of whether cyber activity merits legal consideration as an act of force, observed that with regard to the UN charter, “cyber operations do not fit neatly” into the instrument-based (i.e., force rather than effect’s based) paradigm used by the framers to characterize and outlaw actions due to cyber’s “non-forceful” nature.¹⁰ He further illustrates this point by using the historical example of the UN General Assembly’s rejection of the inclusion of economic or political pressure as “force,” finding that, “a cyber operation

¹⁰ Michael Schmitt, “Cyber Operations and the *Jus Ad Bellum* Revisited,” *Villanova Law Review* 56, no. 3 (Villanova: Villanova University School of Law Digital Repository, 2011), 573, <http://digitalcommons.law.villanova.edu/vlr/vol56/iss3/10> (accessed March 6, 2017).

that involves such coercion is definitely not a prohibited use of force. Psychological cyber operations...intended solely to undermine confidence in a government or economy illustrate such actions.”¹¹ This line of reasoning for offensive cyber use as something other than a military act of force thus avoids the constraints placed on the use of offensive military power.

Defensively, consolidating national cyber capabilities into a single civilian organization best postures the nation to protect and defend against this critical threat. First, this approach avoids the procedural and legal limitations on applying military capabilities domestically.¹² As mentioned previously, the technical and R&D expertise currently resides predominantly within the military. *Posse comitatus* and other federal laws constrain the use of military personnel and capabilities within the United States for the enforcement of domestic policies or non-emergency homeland defense except within exceptional, narrowly-defined purposes. Thus, the bulk of the cyber expertise available is sub-optimally available for defense of the nation’s critical civilian infrastructure.

Second, consolidating cyber capabilities within a single organization creates a specific focus to defend against this threat. Within the civilian-led government organizations whose current responsibilities include cyber (FBI and DHS), cyber is only one of many portfolios requiring attention. An organization specifically chartered to focus on cyber power will enable a focus not just on the current issues today, but also a focus on advocacy to

¹¹ Schmitt, “Cyber Operations and the *Jus Ad Bellum*,” 574.

¹² Military doctrine addresses the provision of military capabilities for domestic use “in response to requests for assistance from civil authorities for domestic emergencies, law enforcement support, and other domestic activities, or from qualifying entities for special events.” Although permitted by doctrine and law, this publication’s emphasis on the unique challenges and requirement for expert legal advice when providing defense support to civil authorities reveals the non-routine and carefully-controlled nature of such operations. U.S. Department of Defense, *Joint Publication 3-28 Defense Support of Civil Authorities* (Arlington: U.S. Department of Defense, July 31, 2013), vii-xii.

comprehensively improve the national cyber posture across a wide spectrum of areas (e.g., policy, resourcing, training and education, capability development, and capacity growth).

Analysis

Elevating cyber as a separate instrument of power by adopting a legal position downgrading the strategic significance of the use of cyber and focusing national capabilities in a civilian agency confers both advantages and disadvantages that demand analysis.

First, reconsidering cyber as a non-military instrument of power avoids the entanglements associated with the application of offensive military force resulting from *jus ad bellum* principles and other legal constraints. U.S. strategic culture holds a binary view regarding war and peace that is constraining upon ambiguous activity in the borders. The Chairman of the Joint Chiefs of Staff, in an address to students attending the National Defense University, acknowledged the limitations inherent in separating military actions into distinct phases at the strategic level. Cyberspace as a domain affords adversaries the opportunity to exploit ambiguity for their benefit. Sidestepping the limitations inherent in the use of military force enables additional cyber power application in this ambiguous environment without being encumbered by the strategic significance associated with offensive military power.

Second, the decreased strategic significance of cyber use by separating it from military power will lead to increased use of cyber. As best can be determined in unclassified, publicly-available literature, current national cyber capabilities are treated as tools of last resort, reserved for sparing use only against the highest priority adversaries for which other options do not exist. This methodology for use is inconsistent with the whole-of-government

approach typically favored and emphasized in national strategic documents that generally seek the orchestrated application of all instruments of national power for synergistic effect. Decreasing the strategic significance of cyber will allow the more frequent application of cyber power against a broader range of adversaries.

Third, increased use of cyber confers its own advantages in both short- and long-term perspectives. The decreased strategic significance of cyber logically assumes a similarly decreased echelon at which the cyber use decision is made, which will positively affect the timeliness of the decision-making process and thus better posture the nation to take advantage of opportunities that move at the digital speed. In the longer term, the broader range of actors employing and making cyber decisions will lead to the development of a cadre of leaders with greater expertise and familiarity in applying national cyber capabilities.

Fourth, the creation of a single agency responsible for the full spectrum of cyberspace operations will optimize national capabilities. Although it may initially sound counterintuitive to discuss creation of a (likely large) governmental bureaucracy and optimized capabilities in the same sentence, the current diffusion of responsibilities among multiple bureaucratic entities stifles full achievement of the nation's potential and frustrates the need to synchronize efforts. Curtis Duke publicly acknowledged the challenges inherent in the existing trifurcated national cyber schema. He specifically criticized the lack of timeliness involved in investigating incidents due to the "days or even a week before government officials complete the paperwork to get NSA on site" and additional delays resulting from addressing such questions as;

Who's going to be in charge? Is it always going to be a criminal matter? Or, when it's non-national security is it DHS and when it's national security is it

NSA? ... By the time we get that all sorted out, we're at a disadvantage when it comes to an adversary.¹³

While the consolidation of responsibilities into a single agency will incur short-term costs due to the sheer scope of the effort required, the initial idea is that this consolidation would require at most an insignificant net growth and likely a slight decrease in the size of the personnel necessary to form and support this agency as they already exist in the disparate organizations currently executing cyber responsibilities.

Despite the obvious advantages, this proposal also contains some inherent disadvantages that merit discussion. First, and perhaps foremost, is the issue of risk. This thesis argues that the current U.S. strategic approach framing cyber as a military instrument of national power and equating cyber to an armed attack is intended to send an aggressive deterrence signal to mitigate adversary exploitation of this significant vulnerability. Any change to this strategic approach that downgrades the strategic significance associated with cyber activity thus confers increased risk to the U.S. that cannot be ignored. This risk may be mitigated in part by adopting a more ambiguous legal position that walks back from the current posture while still retaining the right to claim self-defense if deemed appropriate, but it must be recognized that any shift from the current aggressive position inherently carries some inescapable amount of increased risk.

Second, if history is any indication, the rapid formation of a large government bureaucracy comes with considerable challenges that will be rife with friction and may incur a temporary overall decreased national cyber effectiveness while capabilities are consolidated into a single organization.¹⁴ While careful planning and adopting a phased approach to

¹³ Marks, "One Cyber Defense Agency—Not Three."

¹⁴ Although it exceeds the scope of this paper, an examination of the Department of Homeland Security's establishment would serve as an excellent case study for comparison to this proposal.

capability transfers may mitigate some of this friction, hiccups will inevitably occur in this process. Additionally, a bureaucracy, once formed, can assume a life of its own. This is neither positive nor negative at the outset, but this internal momentum may potentially lead to a cultural, operational, organizational, and/or cognitive biases and rigidity that may not keep pace with the dynamic, fluid nature of cyberspace without careful, conscious management to mitigate these potential concerns.

Third, another disadvantage of this proposal is the vulnerability inherent in a centralized model for national cyber capabilities. While affording a smaller conceptual topology for adversaries to attack, having all national cyber capabilities consolidated into a single organization makes the agency more vulnerable if penetrated, especially if this penetration occurs as a result of insider threat. The dysfunction of disjointed processes and procedures stemming from multiple agencies responsible for cyber can counterintuitively afford some small measure of protection, albeit at a cost of efficiency and effectiveness. An appropriate analogy to this is the nation's national voting process being controlled at the state versus the federal level. The use of over fifty separate processes to conduct national elections may not be the most efficient process, but it protects the overall outcome from a single actor or single penetration.

Lisa Nemeth highlights another friction point that may be a fourth potential disadvantage in her discussion of cyber's impact on the American Way of War. She explores the requirement for much greater civil-military integration to a degree not previously experienced that will be a consequence of elevating cyber as a separate instrument of national power. Such a shift will not obviate the military requirement to conduct cyber operations; the military is far too dependent on information and command and control systems to fully

transfer cyber responsibilities to a civilian agency. However, with the ability to conduct cyberspace operations in ambiguous operating environments coupled with the military's overseas commitments and forward-deployed posture, the military will remain intimately involved with cyber operations. The difference will be the civilian direction and leadership, not just at the strategic levels but potentially at the operational and even tactical levels as well. As Nemeth identifies, "Cyber will alter the American way of war to not just view its actions as political instruments, but to conduct them as such—with increased civilian involvement in military affairs to control the political linkage" in a way that may challenge military leaders unaccustomed to civilian control of operations at the operational and even tactical levels.¹⁵

A fifth and final disadvantage for discussion is the costs associated with creation of another executive-branch organization. As mentioned earlier, this proposal assumes only an insignificant personnel cost on the basis that the personnel currently working cyber in the multitude of government organizations will form the body of this new, consolidated cyber organization. However, the infrastructure requirements necessary to support the full range of offensive and defensive cyber capability development and maintenance will likely incur major costs, as the security requirements will necessitate new infrastructure builds of both buildings and networks to house this consolidated cyber force. Although these costs may be small in comparison to the potential damage an adversary or adversaries can afflict upon the nation given the current cyber vulnerabilities, the current U.S. fiscal climate along with high government deficit and spiraling debt will prove a major legislative obstacle to overcome to bring this proposal to full fruition.

¹⁵ Nemeth, "Cyber and the American Way of War," 28.

CHAPTER 5: CONCLUSION

*Cyber threat is one of the most serious economic and national security challenges we face as a nation.*¹

President Barak Obama, 2014

*The need to identify a lead agency to address a threat is based on the global nature of the problem, the ability to communicate and exercise control forces, the magnitude of the stakes in a cyber conflict, and uncertain collateral effects of cyberspace activities. Until the US government establishes an effective comprehensive cybersecurity framework, implements policy, grants authorities, and provides resources to address limitations in capacity, capability, and cognizance... [U.S.] strategic cyberspace superiority will be limited.*²

Fred Taylor and Jerry Carter, 2014

Current cyber thought reflects a heavy military influence in the prevalent discussion of *cyber war* and *cyber warfare*. This thesis attempts to reframe the discussion of cyber as a national instrument of power separate but equal to that of the military and information instruments, borrowing from and building upon a small minority of authors to explore cyber capabilities unconstrained by the limitations inherent in the use of military force. Although advantages in initially developing cyber capabilities via military mechanisms were obvious, the continued global expansion of and reliance upon digitization calls for an objective analysis and consideration of cyber to promote comprehensive understanding of these capabilities and to afford the widest possible range of options to strategic decision makers pursuing national goals.

¹ U.S. President, “Cyber Security,” White House website, <http://www.whitehouse.gov/issues/foreign-policy/cybersecurity> (accessed March 3, 2014), as quoted in Brandon Valeriano and Ryan C. Maness, *Cyber War versus Cyber Realities: Cyber Conflict in the International System* (Oxford: Oxford University Press, 2015), 2.

² Taylor and Carter, “Cyberspace Superiority Considerations,” 24.

Worley's *Orchestrating the Instruments of Power* provides a useful starting point in explaining the concept of instruments of national power as an abstraction whose utility lies in mapping the concept to the agency and/or mechanism for leveraging the power.

This then builds to the argument that elevating cyber as an instrument of national power allows for the effective application of this instrument across the full range of cyberspace operations, combining the investigative, intelligence, and operational arms into a single element protecting all aspects of national society rather than being sub-optimally divided into separate elements that bleed away unity of effort.

This thesis proposes considering cyber as an instrument of national power separate and independent from the military instrument. It also proposes moving away from the current U.S. position that equates cyber aggression as a military action, and specifically an armed attack, to avoid the offensive operations limitations commensurate with the application of military force. To actualize this concept, the thesis proposes downgrading the strategic and legal significance currently associated with cyber power and creating a single, civilian-led, executive branch cyber organization that combines and consolidates the cyber functions of the ODNI, DHS, FBI, and some of the cyber capabilities resident within the Department of Defense's NSA and USCYBERCOM to create unified cyber action.

Cyberspace as a domain affords the ability to operate with near-full anonymity, presents almost insurmountable obstacles to establish attribution, and enables covert and proxy activity, all of which support ambiguity. Foundational characteristics of cyberspace, specifically its open-architecture network, render cyberspace permanently vulnerable to malicious actors. Given the nation's increasing reliance (and dependency) on cyberspace, these challenges are unavoidable in the near term. As a result, the need to successfully

operate in cyberspace represents a recent change in the character of warfare. Much as major counterinsurgency operations required new (and not-so-new) doctrinal concepts and ideas to be developed and updated, so too does the dependency on cyberspace similarly require new concepts and ideas to enable greatest freedom of movement and range of strategic options in order to achieve strategic security objectives. The fog of war is alive and well in cyberspace. It is time to recognize and embrace this fact conceptually and posture the nation's capabilities accordingly in order to safeguard the nation and guarantee achievement of national security objectives.

BIBLIOGRAPHY

- Angstrom, Jan, and J. J. Widen. *Contemporary Military Theory: the Dynamics of War*. London and New York: Routledge, 2015.
- Butler, Sean C. "Refocusing Cyber Warfare Thought." *Air and Space Power Journal* 27, no. 1 (January-February 2013): 44-57.
<http://search.proquest.com.nduezproxy.idm.oclc.org/docview/1318929576?accountid=12686> (accessed August 29, 2016).
- Carr, Edward Hallett. *The Twenty Years' Crisis, 1919-1939: An Introduction to the Study of International Relations*. London: Macmillan & Co. Ltd, 1946.
- Clarke, Richard A., and Robert K. Knake. *Cyber War: the Next Threat to National Security and What to Do About It*. New York: HarperCollins, 2010.
- Corbett, Julian. *Some Principles of Maritime Strategy*. Breiningsville, PA: Dodo Press, 2011.
- Director of National Intelligence. *Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community*, provided to the House Permanent Select Committee on Intelligence (Washington DC: Government Printing Office, February 25, 2016).
https://www.dni.gov/files/documents/Newsroom/Testimonies/HPSCI_Unclassified_2016_ATA_SFR-25Feb16.pdf (accessed November 28, 2016).
- Douhet, Giulio. *The Command of the Air*. 2d ed. Trans. by Dino Ferrari. North Stratford: Ayer Company Publishers, Inc., 2002. (New York: Coward-McCann, Inc., 1942).
- Flichy, Patrice. "New Media History." In *Handbook of New Media: Student Edition*. Rev ed. Ed. by Leah A. Lievrouw and Sonia M. Livingstone. London: Sage Publishing, 2006.
https://books.google.co.uk/books?id=NZ3ktyGA0rwC&pg=PA253&dq=ARPANET&hl=en&sa=X&redir_esc=y#v=onepage&q=ARPANET&f=false (accessed Oct 14, 2016).
- Gray, Colin S. *Another Bloody Century: Future Warfare*. London: Phoenix, 2005.
- Green, James A., ed. *Cyber Warfare: a Multidisciplinary Analysis*. New York: Routledge, 2015.

- Horne, Cale, Stephen M. Shellman, and Brandon Stewart, "Nickel and DIMEing the Adversary: Does it work or PMESII them off?" University of Georgia and College of William & Mary: Violent Intranational Political Conflict & Terrorism Research Lab, undated.
- Hughes, Rex. "A Treaty for Cyberspace." *International Affairs* 86, no. 2 (March 2010): 523-541. <http://www.jstor.org/stable/40664079> (accessed August 29, 2016).
- Jasper, Scott, ed. *Securing Freedom in the Global Commons*. Stanford: Stanford University Press, 2010.
- Johnson, Dana J., Scott Pace, and C. Bryan Gabbard. *Space: Emerging Concepts for National Power*. Santa Monica: RAND, 1998.
- Kagan, Donald. *Thucydides: the Reinvention of History*. Reprint ed. New York: Penguin Books, 2010.
- Kem, Jack D. "Understanding the operational environment: the expansion of DIME." *The Free Library* (April 1, 2007). [https://www.thefreelibrary.com/Understanding the operational environment: the expansion of DIME.-a0213693824](https://www.thefreelibrary.com/Understanding+the+operational+environment:+the+expansion+of+DIME.-a0213693824) (accessed December 29, 2016).
- Leiner, Barry M., Vinton G. Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Lawrence G. Roberts, and Stephen S. Wolff. "Brief History of the Internet." Internet Society. <https://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet> (accessed December 28, 2016).
- "The Past and Future History of the Internet: The Science of Future Technology." *Communications of the ACM* 40, no. 2 (February 1997), 102-108.
- Libicki, Martin C. *Crisis and Escalation in Cyberspace*. Santa Monica: RAND, 2012.
- "Cyberspace is not a warfighting domain." *ISJLP* 8 (2012): 321.
- "Cyberwarfare as a Confidence Game." *Strategic Studies Quarterly* (Spring 2011): 132-46.
- *Defending Cyberspace and other Metaphors*. Washington, DC: National Defense University, 1997.

- "Why Cyber War Will Not and Should Not Have Its Grand Strategist." *Strategic Studies Quarterly* 7, no. 4 (2013): 23-39. *International Security & Counter Terrorism Reference Center*, EBSCOhost (accessed October 30, 2016).
- Libicki, Martin C., Lillian Ablon, and Tim Webb. *The Defender's Dilemma: Charting a Course Toward Cybersecurity*. Santa Monica: RAND Corporation, 2015.
- Lynn, William J. "Defending a New Domain: The Pentagon's Cyberstrategy." *Foreign Affairs* 89, no. 5 (September/October 2010): 97-108.
<http://www.jstor.org/stable/20788647> (accessed August 29, 2016).
- Mahan, Alfred T. *The Influence of Sea Power upon History 1660-1783*. New York: Dover Publications, 1987.
- Marks, Joseph. "The US Needs One Cyber Defense Agency-Not Three, a Top NSA Official Says." *Defense One*, October 19, 2016,
<http://www.defenseone.com/technology/2016/10/us-needs-one-cyber-defense-agencynot-three-top-nsa-official-says/132474/> (accessed November 22, 2016).
- Martin, Laurence, ed. *Strategic Thought in the Nuclear Age*. London: Heinemann, 1979.
- McGuffin, C., and P. Mitchell. (2014). "On domains: Cyber and the practice of warfare." *International Journal* 69, no. 3 (2014): 394-412.
<http://dx.doi.org/10.1177/0020702014540618> (accessed August 29, 2016).
- National Intelligence Council. "Global Trends 2015: A Dialogue about the Future with Nongovernment Experts." (Langley: National Foreign Intelligence Board, December 13, 2000).
https://www.dni.gov/files/documents/Global%20Trends_2015%20Report.pdf (accessed December 28, 2016).
- Nemeth, Lisa. "Cyber and the American Way of War." Master's thesis, Joint Forces Staff College, 2015.
- Nguyen, Reese. "Navigating Jus Ad Bellum in the Age of Cyber Warfare." *California Law Review* 101, no. 4 (August 1, 2013): 1079-1129.
- Nye, Joseph S, Jr. *Soft Power: the Means to Success in World Politics*. New York: PublicAffairs, 2005.

Ravindranath, Mohana. "McCain to White House: If You Won't Establish a Cyber Defense Policy, Congress Will." *Defense One* (September 14, 2016).
<http://www.defenseone.com/politics/2016/09/mccain-white-house-if-you-wont-establish-cyber-defense-policy-congress-will> (accessed November 22, 2016).

Reveron, Derek S., ed. *Cyberspaces and National Security: Threats, Opportunities, and Power in a Virtual World*. Washington, DC: Georgetown University Press, 2012.

Ridout, Tim. "Building a Comprehensive Strategy of Cyber Defense, Deterrence, and Resilience." In *The Fletcher Forum of World Affairs* 40, no. 2 (Summer, 2016): 63-83.
<http://search.proquest.com.nduezproxy.idm.oclc.org/docview/1804900059?accountid=12686> (accessed August 29, 2016).

Schmidt, Lara. "Perspective On 2015 Dod Cyber Strategy." Testimony presented before the House Armed Services Committee, Washington, DC, September 29, 2015.
<http://www.rand.org/> (accessed August 29, 2016).

Schmitt, Michael N. "Cyber Operations and the *Jus Ad Bellum* Revisited." *Villanova Law Review* 56, no. 3 (Villanova: Villanova University School of Law Digital Repository, 2011). <http://digitalcommons.law.villanova.edu/vlr/vol56/iss3/10> (accessed March 6, 2017).

----- ed. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press, 2013. <https://ccdcoe.org/research.html> (accessed October 30, 2016).

Shakarian, Paulo, Jana Shakarian, and Andrew Ruef. *Introduction to Cyber-Warfare: a Multidisciplinary Approach*. Boston: Syngress, 2013.

Shapiro, Lawrence A. "Multiple realizations." *Journal of Philosophy* 97, no. 12 (December 2000): 635-54.
<http://links.jstor.org/sici?sici=0022362X%28200012%2997%3A12%3C635%3AMR%3E2.0.CO%3B2-Q> (accessed June 27, 2006).

Singer, Peter W., and Allan Friedman. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford: Oxford University Press, 2014.

Singer, Peter W. "Cybersecurity's Human Side: How Can We Solve Our People Problem?"

- Defense One* (March 20, 2017).
http://www.defenseone.com/ideas/2017/03/cybersecuritys-human-side-how-can-we-solve-our-people-problem/136296/?oref=d_brief_nl (accessed March 21, 2017).
- Strassler, Robert B, ed. *The Landmark Thucydides: A Comprehensive Guide to the Peloponnesian War*. Rev. ed. New York: Free Press, 2008.
- Tikk, Eneken. “Establishing Rules for Cyber Security.” In *Conflict and Cooperation in the Global Commons*, ed. by Scott Jasper. Washington, DC: Georgetown University Press, 2012. <http://www.jstor.org/stable/j.ctt2tt578.20> (accessed August 29, 2016).
- Trias, E. D., Maj, & Capt B. M. Bell. “Cyber this, cyber that . . . so what?” *Air & Space PowerJournal* 24, no. 1 (2010): 90-100.
<http://search.proquest.com.nduezproxy.idm.oclc.org/docview/374942529?accountid=12686> (accessed August 29, 2016).
- U.S. Department of Defense. *The Department of Defense Cyber Strategy*. Arlington: U.S. Department of Defense, April, 2015.
<http://www.defense.gov/news/d20110714cyber.pdf> (accessed August 29, 2016).
- Defense Science Board. *Final Report of the Defense Science Board (DSB) Task Force on Cyber Deterrence*, by James N. Miller and James R. Gosler. Washington, DC: Department of Defense, February, 2017.
- *Joint Publication 1-0 Doctrine for the Armed Forces of the United States*. Arlington: U.S. Department of Defense, March 25, 2013.
- *Joint Publication 1-02 Department of Defense Dictionary of Military and Associated Terms*. Arlington: U.S. Department of Defense, November 8, 2010 (as amended through February 15, 2016).
- *Joint Publication 3-0 Joint Operations*. Arlington: U.S. Department of Defense, August 11, 2011.
- *Joint Publication 3-12(R) Cyberspace Operations*. Arlington: U.S. Department of Defense, February 5, 2013.
- *Joint Publication 3-28 Defense Support of Civil Authorities*. Arlington: U.S. Department of Defense, July 31, 2013.
- U.S. Department of Homeland Security. “Core Missions: Safeguard and Secure Cyberspace.”

- (March 21, 2016) <https://www.dhs.gov/safeguard-and-secure-cyberspace> (accessed December 28, 2016).
- U.S. President. *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*. Washington DC: Government Printing Office, May, 2011.
- *Presidential Memorandum -- Establishment of the Cyber Threat Intelligence Integration Center*. Washington DC: Government Printing Office, February 25, 2015. <https://www.whitehouse.gov/the-press-office/2015/02/25/presidential-memorandum-establishment-cyber-threat-intelligence-integrat> (accessed December 28, 2016).
- U.S. President. *Presidential Policy Directive-41: United States Cyber Incident Coordination*. Washington DC: Government Printing Office, July 26, 2016. <https://www.whitehouse.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident> (accessed December 28, 2016).
- *National Security Strategy*. Washington DC: Government Printing Office, February, 2015.
- Valeriano, Brandon, and Ryan C. Maness. *Cyber War Versus Cyber Realities: Cyber Conflict in the International System*. New York: Oxford University Press, 2015.
- Walzer, Michael. *Just and Unjust Wars: A Moral Argument with Historical Illustrations*. 5th ed. New York: Basic Books, 2015.
- Yannakogeorgos, Panayotis A., and Adam B. Lowther, eds. *Conflict and Cooperation in Cyberspace: The Challenge to National Security*. Boca Raton: Taylor and Francis, 2014.
- Zemanek, Karl. "Armed Attack." *Max Planck Encyclopedia of Public International Law*. Oxford: Oxford University Press, October, 2013. <http://opil.ouplaw.com> (accessed March 6, 2017).

VITA

Lieutenant Colonel Carl C. Priechenfried is currently assigned to the Joint Advanced Warfighting School at the Joint Forces Staff College in Norfolk, VA. Lieutenant Colonel Priechenfried was commissioned a Ground Intelligence Officer in 1997 upon graduation from the University of North Carolina at Chapel Hill. LtCol Priechenfried has served in leadership and staff positions at all echelons of the Marine Corps' operating forces from the platoon, company, and battalion levels to the Marine Expeditionary Unit, division, Marine Expeditionary Force (MEF), and Service Component levels. In addition to two deployments to Iraq and one to Afghanistan (the latter two with U.S. and Coalition special forces commands) for Operations IRAQI FREEDOM and ENDURING FREEDOM, he has spent over two years deployed aboard Naval shipping with deployed Marine amphibious forces on three separate Marine Expeditionary Unit deployments. He has also served at U.S. Central Command and U.S. Marine Corps Forces Special Operations Command (MARSOC). Most recently, he commanded 2d Intelligence Battalion, II MEF from 2014-2016. He is a distinguished graduate of the USMC Command and Staff College and holds his Masters in Military Studies.