REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)* 03/31/2017	**2. REPORT TYPE** Master's Thesis	**3. DATES COVERED** *(From - To)* 07/21/2016 to 03/31/2017

4. TITLE AND SUBTITLE CLOSING THE GAPS: CYBERSECURITY FOR U.S. FORCES AND COMMANDS	**5a. CONTRACT NUMBER**
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S) ANDREW T. FERGUSON, LTC, USA	**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

Cyberattacks are an everyday event in the Department of Defense (DoD) and proper application of cybersecurity is the key to mission assurance for Combatant Commands and the military services. There are multiple cybersecurity policies and programs working to defend the network in depth, but there remain gaps and seams for adversaries to exploit due to a lack of knowledge, understanding, or concern from users at all levels of command. This paper will broadly examine the cyberspace environment, U.S. cybersecurity policy, and cybersecurity compliance, specifically using the Command Cyber Readiness Inspection (CCRI) program as an example of how to close some of the gaps and seams in DoD's cyber defense.

15. SUBJECT TERMS

Cybersecurity, CCRI, Cyberspace Operations

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			Andrew T. Ferguson
Unclassified	Unclassified	Unclassified	Unclassified Unlimited	64	**19b. TELEPHONE NUMBER** *(Include area code)* 757-579-8835

THIS PAGE INTENTIONALLY LEFT BLANK

NATIONAL DEFENSE UNIVERSITY

JOINT FORCES STAFF COLLEGE

JOINT ADVANCED WARFIGHTING SCHOOL

CLOSING THE GAPS: CYBERSECURITY FOR U.S. FORCES AND COMMANDS

by

Andrew T. Ferguson

Lieutenant Colonel, United States Army

THIS PAGE INTENTIONALLY LEFT BLANK

CLOSING THE GAPS: CYBERSECURITY FOR U.S. FORCES AND COMMANDS

by

Andrew T. Ferguson

Lieutenant Colonel, United States Army

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

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

Signature: ______________________

Andrew T. Ferguson, LTC, USA
30 March 2017

Thesis Advisor: Signature: ______________________

Keith Dickson, Ph.D.
Professor of Military Studies, JAWS
Thesis Advisor

Approved by: Signature: ______________________

Kevin Therrien, Col, USAF
Committee Member

Signature: ______________________

Stephen Rogers, Colonel, USA
Director, Joint Advanced Warfighting School

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Cyberattacks are an everyday event in the Department of Defense (DoD) and proper application of cybersecurity is the key to mission assurance for Combatant Commands and the military services. There are multiple cybersecurity policies and programs working to defend the network in depth, but there remain gaps and seams for adversaries to exploit due to a lack of knowledge, understanding, or concern from users at all levels of command. This paper will broadly examine the cyberspace environment, U.S. cybersecurity policy, and cybersecurity compliance, specifically using the Command Cyber Readiness Inspection (CCRI) program as an example of how to close some of the gaps and seams in DoD's cyber defense. The paper concludes by providing five recommendations to help improve the CCRI program and overall cybersecurity across DoD.

DEDICATION

I dedicate this to my wife and kids who have supported all of my efforts unconditionally. To my thesis advisors, Dr. Keith Dickson and Col Kevin (KT) Therrien (USAF), whose guidance and advice have been invaluable on this journey. To both the instructors and students of JAWS FY 16-17 Seminar One, you have all in some way helped me to expand both my knowledge base and overall vocabulary. And finally to all the cybersecurity professionals who defend the networks, your efforts have not gone unnoticed.

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

INTRODUCTION

The cyber domain in some ways is like the air domain, in being a realm that had no relevance for military planning until all of the sudden a new technology offered access to it.[1] – GEN Keith Alexander

Cybersecurity is the key to mission assurance for Combatant Commands (CCMDs) and the military services. Without a concentrated effort from all members of the Department of Defense (DoD) to comply with proper cybersecurity procedures, there is a high risk of both personal and national defense information becoming compromised and exploited. The United States Department of Defense Information Networks (DoDIN) are under constant threat of surveillance, exploitation, and attack by a multitude of different types of hostile actors. Cyberattacks are an everyday event in the Department of Defense.[2] The DoD has implemented multiple programs in an effort to increase the security posture of its networks.[3] One of these programs is the Command Cyber Readiness Inspection (CCRI) designed to evaluate a military installation's overall cybersecurity posture. The CCRI is DoD's primary cybersecurity compliance program and serves as an important line of defense. At present, the CCRI program does not ensure security across DoD networks, potentially exposing military installations and commands to a myriad of cyber threats. CCRI requires adjustments to provide adequate

[1] Keith Alexander, "Statement for the Record, Commander, US Cyber Command" *House Armed Services Committee Statement*. (Washington, DC. 23 September 2010). http://www.defense.gov/home/features/2010/0410_cybersec/docs/USCC%20Command%20Posture%20Statement_HASC_22SEP10_FINAL%20_OMB%20Approved_.pdf (accessed February 19, 2017), 4.

[2] Sandra Erwin, "Defense CIO: Cybersecurity Improving But Innovation Lags" *National Defense Magazine.* August 8, 2016. DoD CIO Terry Halverson statement on the frequency of cyberattacks against the Pentagon. http://www.nationaldefensemagazine.org/blog/Lists/Posts/Post.aspx?ID=2268 (accessed 9 August 2016).

[3] Risk Management Framework (RMF), Cybersecurity Scorecards, "Hack the Pentagon," Command Cyber Readiness Inspection (CCRI), and Federal Information Security Management Act (FISMA) are different programs designed to detect network vulnerabilities for Federal and DoD networks.

oversight in order to protect the multitude of critical military networks. The goal of the CCRI is to make it as difficult, if not impossible, for a potential cyberspace adversary to impact information technology (IT) systems through both technical and procedural means. The Department of Defense must adjust its current Command Cyber Readiness Inspection program in order to maintain cybersecurity compliance and mission assurance.

This paper will broadly examine the cyberspace environment, U.S. cybersecurity policy, cybersecurity compliance, and use the CCRI program as an example of how to close some of the gaps in DoD's cyber defense. Chapter One begins by defining key terms regarding cyberspace, examining the adversaries and discussing why cyberspace and cybersecurity matters to the Combatant Commands. This chapter will also provide a brief history of the internet, examine how cyberspace is changing the characteristics of warfare, discuss the constantly contested nature of cyberspace, and examine the anarchistic nature of cyberspace by addressing whether the cyberspace environment is complex or complicated. Chapter Two reviews U.S. federal and military cybersecurity policy and exposes the limits of these policies. Chapter Three examines the role of CCRI as a mechanism of national security by using the three categories of inspection design, manning and expertise, and feedback enforcement mechanisms. Chapter Four provides five recommendations to help improve the CCRI program and overall cybersecurity in order to close some of the gaps and seams in DoD's cyber defense. A final conclusion reinforces the fact that the biggest challenge for cybersecurity is that if it is working effectively, the threat is marginalized and cybersecurity remains an afterthought; but if it fails, the potential effects could be catastrophic and worthy of headlines.

CHAPTER 1: THE CYBERSPACE ENVIRONMENT

The events of every age must be judged in the light of its own peculiarities.[4]- Carl Von Clausewitz

Defining Cyberspace and Cyberspace Operations

"Cyber" is a prefix, not a word. When people refer to "cyber," it is understood to mean cyberspace. Cyberspace has multiple definitions. National Security Presidential Directive-54/Homeland Security Presidential Directive-23 (NSPD-54/HSPD-23) defines cyberspace as "the interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries."[5] Cyberspace is defined in Joint Publication (JP) 3-12 as "a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[6] It further describes cyberspace in terms of three layers: a physical network, a logical network, and a cyber-persona[7].

A more useful definition is the one developed by Rain Ottis and Peeter Lorents from the Cooperative Cyber Defense Center of Excellence in Estonia. Ottis and Lorents posit that "cyberspace is a time-dependent set of interconnected information systems and

[4] Carl von Clausewitz, *On War*, (New York: Everyman's Library, 1993), 717.
[5] George W. Bush, *National Security Presidential Directive-54/Homeland Security Presidential Directive-23*. (Washington, DC: Presidential Memorandum, 2008), 3.
[6] U.S. Joint Chiefs of Staff, *Cyberspace Operations*, Joint Publication 3-12(R), V.
[7] Ibid, V.

the human users that interact with these systems."[8] This definition includes three important factors that the JP 3-12 definition does not fully encompass: technology, people, and time. This paper will use the Ottis and Lorents definition because it includes the realizations that people who interface with the network are part of cyberspace, and that cyberspace itself is an ever-changing domain over time.

Cyberspace operations is defined in JP 3-0 as the "employment of cyberspace capabilities where the primary purpose is to achieve military objectives or effects in or through cyberspace."[9] JP 3-12 expands on JP 3-0 by separating cyberspace operations into three categories: Offensive Cyberspace Operations (OCO), Defensive Cyberspace Operations (DCO), and Department of Defense Information Networks (DoDIN).[10] DCO has two subcategories: Response Action (RA) and Internal Defense Measures (IDM).[11] DCO-IDM are "actions [internal to the DoDIN] to dynamically reestablish, re-secure, reroute, reconstitute, or isolate degraded or compromised local networks to ensure sufficient cyberspace access for Joint Force Command (JFC) forces."[12] JP 3-12 specifically defines DoDIN operations as "actions taken to design, build, configure, *secure*, operate, maintain, and sustain DOD communications systems and networks in a way that creates and preserves data availability, integrity, confidentiality, as well as user/entity authentication and non-repudiation."[13] The focus of this paper is to

[8] Rain Ottis, and Peeter Lorents, *Cyberspace: Definition and Implications*. In Proceedings of the 5th International Conference on Information Warfare and Security. Academic Publishing Limited. Dayton. April 2010.

[9] U.S. Joint Chiefs of Staff, *Joint Operations*, Joint Publication 3-0, defined in the Glossary section on pg. GL-8.

[10] JP 3-12(R), vii. This paper will only examine OCO in regard to the threat from cyberspace adversaries, not from the perspective of U.S. capability.

[11] This paper will not be examining DCO-RA as it requires personnel with special skill-sets that most organizations do not employ and the CCRI does not measure any activities in this subcategory.

[12] JP 3-12(R), II-3.

[13] Ibid, II-3. Secure is italicized by author for emphasis.

understand the cyberspace environment, cybersecurity policy, DoDIN operations, and the CCRI program in relation to DoD's ability to protect its networks from its adversaries.

Who are the cyberspace adversaries? (4+1 plus two more)

Cybersecurity and the proper application of the CCRI is significant to DoD because the threat is real, constant, and comes from a multitude of vectors. Sun Tzu wrote in the *The Art of War,* "if you know the enemy and know yourself, you need not fear the result of a hundred battles."[14] It is imperative to know the enemy because there are hundreds of cyber battles fought each day, and in order to thwart these attacks, the enemy's intentions must be understood. Senior military leaders have stated that China, Russia, Iran, and North Korea are all increasing their capabilities within the cyber domain.[15] Violent extremists along with hacktivists and insider threats are also part of the enemy arrayed against the DoDIN (a more detailed account of each of the listed cyberspace threats is included as part of Appendix A).

Mission Assurance for the Combatant Commands

The Joint Operating Environment 2035 (JOE 2035) forecasts that cyberspace will be contested as "adversaries may also attempt to conduct a strategic cyber campaign directly against the U.S. homeland focused on degrading critical systems and assets"[16] over the next two decades. One of the overarching themes of JOE 2035 is the concept of contested norms in which "adversaries will credibly challenge the rules and agreements

[14] Sun Tzu, *The Art of War,* trans. By Samuel B. Griffith (London: Oxford University Press, 1963), 84.
[15] Jim Garamone, DoD News, Defense Media Activity "*Dunford Details Implications of Today's Threats on Tomorrow's Strategy*" Published Aug. 23, 2016. NDU President's Lecture Series. https://www.defense.gov/News/Article/Article/923685/dunford-details-implications-of-todays-threats-on-tomorrows-strategy/ (accessed 24 August 2016).
[16] U.S. Joint Chiefs of Staff, *Joint Operating Environment 2035: The Joint Force in a Contested and Disordered World*. Washington, DC: U.S. Joint Chiefs of Staff. July 14, 2016, 35.

that define the international order."[17] As more nations and people in the southern hemisphere become connected through the Internet, the global digital divide[18] will be reduced by individuals who do not have the same cultural background as most Western democracies. Global cyberspace governance is inherently weak and as cyberspace expands, new types of adversaries with different worldviews and perspectives will become more prevalent. For example, USPACOM will have to work through China's aggressive use of cyber lawfare as it continues to draft new laws "to preserve cyberspace sovereignty, national security and societal public interest."[19] USCENTCOM and USSOCOM will continue their efforts to counter extremist groups' use of the cyberspace for recruiting and misinformation.

JOE 2035 also predicts that "some states may also integrate cyber warfare capabilities at the operational and tactical levels of war."[20] USEUCOM/SACEUR will face a significant challenge in Russia who has already displayed its ability to integrate offensive cyberspace operations with other kinetic types of warfare. The CCRI's ability to help all of the CCMDs with mission assurance will be critical because Combatant Commands have broad continuing missions in specific geographic or functional areas that ensure U.S. security interests; and as a result, it is imperative that cybersecurity is encapsulated into the culture of these organizations.

[17] U.S. Joint Chiefs of Staff, *Joint Operating Environment 2035*, ii.

[18] According to Dr. Melanie Heely and Leela Damodaran of Loughborough University, the global digital divide is national differences in Internet use and development due to economic, technological, regulatory and political characteristics of countries. The majority of the countries which lag behind Internet usage and development are geographically located along the equator and in the southern hemisphere, especially Africa and South America.

[19] U.S. Joint Chiefs of Staff, *Joint Operating Environment 2035*, 35.

[20] Ibid, 36.

Understanding the Nature of the Cyberspace Environment

Harry R. Yarger, a professor of National Security Policy at the U.S. Army War College, stated in his book, *Strategic Theory for the 21st Century* that "strategy is subordinate to the nature of the strategic environment."[21] It is therefore imperative to understand the cyberspace environment prior to developing any strategy to operate inside of it.

A brief overview of networking and the Internet

In *A History of the Internet and the Digital Future*, John Ryan expressed the need to examine what has happened in the recent past in an effort to project the future of cyberspace:

> Three characteristics have asserted themselves throughout the Internet's history, and will define the digital age to which we all must adjust: the Internet is a centrifugal force, user-driven, and open. Understanding what these characteristics mean and how they emerged is the key to making the great adjustment to the new global commons.[22]

The Internet has seen three significant periods starting with the developmental years (1969-1991) in which networking was still being developed by governmental and academic institutions. The early commercial years (1992-2006) involved simple file sharing, email, and static web pages with an exponential growth of public users across the globe. It was during this period many of the original architects of the Internet believed their vision of "open architecture networking" had come to fruition.[23] The current period, known as Web 2.0 (2007-present), consists of self-generated content through social media and video sharing sites like YouTube. Wireless capability, mobile devices, and the

[21] Harry R. Yarger, *Strategic Theory for the 21st Century: The Little Book on Big Strategy.* (Carlisle PA: U.S. Army War College Strategic Studies Institute, 2006), 7.
[22] Johnny Ryan. *A History of the Internet and the Digital Future* (UK: Reaktion Books, 2010), 8.
[23] Ibid, 24.

expansion of networking to cars, airplanes, watches, and home appliances highlight the idea that this is not just a digital age, but a *networked* digital epoch.

Cyberspace is changing the characteristics of War

Carl von Clausewitz wrote, "every age had its own kind of war, its own limiting conditions, and its own peculiar preconceptions."[24] There has been a shift from the twentieth century industrial age to the twenty-first century digitally networked information age. Cyberspace has now become a great equalizer enabling almost anyone with a laptop and network connectivity to become a combatant in this part of the Information Domain. John B. Sheldon, a professor at the School of Advanced Air and Space Studies, has observed that "cyber power can be used in peacetime and war because it is stealthy and covert, it is relatively cheap, and its use favors the offense but is difficult to attribute to the perpetrator."[25] The interdependence of the space and cyberspace domains are now shaping how the digitally networked information age conducts warfare.

One important concept of cyberspace is the rapid nature of technical advancement commonly referred to as Moore's Law. Moore's Law simply states that, "every eighteen months, processing power doubles while cost holds constant."[26] This is like having an M-16 rifle that has a maximum effective range of 300 meters and the opposition procures a new rifle every eighteen to twenty-four months that can fire twice as far. If DoD does not factor Moore's Law as part of the procurement cycle for cyber defense, it will create gaps and weaknesses for the adversaries to exploit.

[24] Clausewitz, *On War*, 717.

[25] John B. Sheldon, "Toward a Theory of Cyber Power: Strategic Purpose in Peace and War" in *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, ed. Derek S. Reveron, (Washington, DC: Georgetown University Press, 2012), 210.

[26] Larry Downes and Chunka Mai, *Unleashing the Killer App*, (Boston: Harvard Business School Press, 1998), 21.

By making some analogies to the domains of land, sea, air, and space, the concepts of cyberspace and cybersecurity may be easier to realize. Admittedly, there are some cyberspace pundits who believe that analogies are not useful in explaining cybersecurity. For example, Thomas Rid, the author of the book, *Cyber War Will Not Take Place*, believes that "a subject that pervades, if not distorts, many other publications on cyber security [is] analogies."[27] However, using analogies of what is already known in order to explain unknown concepts is a tried and true method at all levels of education. Without the use of analogies, the necessary time to educate about bandwidth, firewalls, and encryption becomes too consuming for military leaders with calendars managed in fifteen minute increments. Even Rid admits that using analogies, metaphors, and historical references may be useful to describe cyberspace on some level and "make it easier to understand a problem" yet cautions that, "at some point a metaphor will begin to fail."[28] With this understanding, a few analogies and historical references from the classical war theorists will be examined.

The nineteenth century naval strategist, Julian S. Corbett made the assertion that one "cannot conquer the sea because it is not susceptible to ownership."[29] A similar statement can be made for the Internet. The Internet is part of the global commons just like air, sea, and space. The concept of information dominance that was formerly sought after by both the Navy and Air Force is highly unlikely. The dynamic and pervasive nature of cyberspace makes the concept of 'dominance' unrealistic. Corbett made the supposition that "the normal position is not a commanded sea, but an uncommanded

[27] Thomas Rid, *Cyber War Will Not Take Place*, (London: Oxford University Press, 2013), 163.
[28] Ibid, 164.
[29] Julian S. Corbett, *Some Principles of Maritime Strategy*, (London: Longmans, Green and Company, 1911), 93.

sea."[30] It can be derived from this statement that a more realistic goal would be the concept of mutual uncontrollability where if one side cannot achieve or sustain control, then it is vital that the other side cannot achieve or sustain control either. In early 2016, both the Navy and the Air Force accepted these conclusions and replaced the term 'domination' with 'warfare' in regards to cyberspace operations. Corbett's observations on naval warfare can also be applied to warfare in the digital networked world:

> The object of naval warfare is the control of communications, and not, as in land warfare, the conquest of territory. The difference is fundamental. True, it is rightly said that strategy ashore is mainly a question of communications, but they are communications in another sense. The phrase refers to the communications of the army alone, and not to the wider communications which are part of the life of the nation.[31]

The critical dependence on maintaining the lines of communication through digital networking capability is now an imperative to both the nation as a whole and the military which defends it.

Similar to Clausewitz's description of a "remarkable trinity," cybersecurity also has its versions of a primary and secondary (opposing) trinity. The concepts of Confidentiality, Integrity, and Availability are known as the CIA triad of information security, or in this case, the primary cybersecurity trinity. The opposing trinity consists of Disclosure, Alteration, and Destruction (DAD) are the basic goals of cyberspace adversaries. Defining and explaining the primary cybersecurity trinity will also help to explain its opposing trinity. Confidentiality seeks to prevent the unauthorized disclosure of information.[32] Integrity seeks to prevent unauthorized modification of information.[33]

[30] Corbett, *Principles of Maritime Strategy*, 93

[31] Ibid, 94.

[32] Eric Conrad, Seth Misenar and Joshua Feldman, *CISSP Study Guide*, (Waltham: Syngress Publications, 2012), 519.

[33] Conrad, *CISSP Study Guide*, 529.

Availability ensures that information is available when needed.[34] Computer users' expectations are that their computer will work, will be able to connect to the Internet (or other authorized network), and that any data on the hardrive, Internet, or shared data site can be accessed at will. Releasing classified information to Wikileaks is an example of Disclosure. Stuxnet is an example of Alteration or an unauthorized modification when the operating instructions for Iran's centrifuges were modified in order to cause damage. Physically breaking equipment, creating a Distributed Denial of Service (DDoS), jamming the electromagnetic spectrum, or finding other ways to disrupt information flow are all methods of Destruction. CIA and DAD are in constant opposition to each other and thus, help to describe the constantly contested nature of the cyberspace environment.

The Constantly Contested Nature of Cyberspace

The cyberspace environment is in a constant state of contention. It can be used as an instrument of both national power and a weapon of war. The nature of cyberspace as part of the information domain is different from other warfighting domains. The nature of the cyberspace favors the offense exponentially more than the defense. Offensive cyber power has the ability to produce both kinetic and non-kinetic effects against adversaries such as the destruction of information, theft of intellectual property, modification of data, and the alteration or disruption of system operations. Considering that skilled and some not-so skilled operators in cyberspace can execute one or all the listed effects, the defense of cyberspace is constant and expensive, requiring more than a whole of government approach, but rather a very deliberate and contentious effort from all of society. Even as a firm believer in the strength of the defense, Julian Corbett

[34] Ibid, 515.

admitted, "the side which takes the initiative has usually the better chance of securing advantage by dexterity or stealth."[35] For example, a single laptop can probe entire networks in milliseconds. Individual members of loosely affiliated hacktivist groups such as Anonymous can disrupt nation states and Fortune 500 companies or help influence movements like the Arab Spring. Hacktivists are the cyberspace version of guerillas, applying Mao Tse Tung's principle of "unity of the opposites" which states that the dispersion of forces in guerrilla warfare, similar to loosely affiliated hacktivist groups, is useful "to confuse the enemy and preserve the illusion of guerillas as ubiquitous."[36] It is the ungoverned nature of cyberspace that allows hacktivists to employ a myriad of guerilla tactics and effectively employ DAD concepts across the network.

Anarchy

Cyberspace, specifically the World Wide Web or the Internet, was initially conceived to be ungoverned or anarchistic. The original founders of the Internet contemplated four ground rules:

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; later 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 simple and avoiding complicated adaptation and recovery from various failure modes.
4. There would be no global control at the operations level.[37]

[35] Corbett, *Some Principles of Maritime Strategy*, 35.
[36] Mao Tse Tung. *On Guerrilla Warfare*, trans. Samuel B. Griffith II, (Champaign, Il: University of Illinois Press, 2000), 25.
[37] Barry M. Leiner et al., "A Brief History of the Internet" *ACM SIGCOMM Computer Communication Review*, (Oct 2009): 24.

These four rules provided fairly easy access for anyone wanting to build onto the Internet, allowing it to grow quite rapidly and provide a free flow of ideas and information. However, this open architecture lends itself to a myriad of security threats. "The Internet's architects did not design the network or its protocols to handle the level of sensitive data and economic activity that they routinely carry today. The network has scaled to hundreds of millions of users around the globe."[38] Indeed, the current pace of growth for the Internet is 5.5 million devices per day.[39] However, the lack of governance creates problems from both ethical and legal standpoints. The legal community is attempting to develop professionals who can apply the law to cyberspace. The Internet was never intended to be governed inherently creating an environment that is difficult, if not impossible, to regulate.

Is cyberspace complex or complicated?

It is the ungoverned nature of cyberspace that many pundits refer to it as complex; however, the physical layer of cyberspace is merely complicated. A complicated system is linear and deterministic, provides the same outputs when the same inputs are provided, and requires human intervention and interaction. Conversely, a complex system has components that interact with each other and adapt, the whole is indistinguishable from the sum of the parts, and does not require human interaction.[40] The fact that cyberspace is man-made creates a significant difference in that particular strategic environment. This may create a false sense of control over this environment because even though the

[38] Franklin D Kramer, *Cyberpower and National Security* (Washington, DC: National Defense University Press, 2009), 204.

[39] Gartner Corporation. Press Release. "*Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent From 2015*" November 10, 2015. http://www.gartner.com/newsroom/id/3165317 (accessed 29 December 2016).

[40] Definitions for complicated and complex systems provided by JFSC JAWS faculty during ST6630-08 lecture, 20 September 2016.

domain is man-made and linear in nature, it still has anarchistic characteristics. While some professionals will argue that cyberspace has moved from being complicated to complex, even referring to it as an ecosystem; cyberspace is only a time-dependent set of interconnected information systems that humans interact with in order to process information. There is no doubt that cyberspace is an ever growing and complicated system of systems; however, it was still created by humans and it is imperative that this fact be kept in mind when defining the nature of cyberspace. There are some experts who feel that the inclusion of the human dimension is what make cyberspace complex and there is validity to their arguments. The debate on whether cyberspace is complicated or complex is useful to expand the discussion and educational process involved with trying understanding the nature of cyberspace.

Since before the turn of the century, the nature of cyberspace has been debated. Its increased usage across all elements of national power make it an important element of national security. Being perceptive of how cyberspace is changing the characteristics of war, its anarchistic nature, and the contestation that resides among its many facets are all important factors that national security leaders need to understand about operating within cyberspace. A broader understanding of the lexicon, key actors, and strategic end states provide stakeholders and cybersecurity professionals a common frame of reference to develop effective network defenses. With a greater understanding comes an imporved ability to develop policy and strategy to secure the DoDIN and provide mission assurance.

CHAPTER 2: U.S. CYBERSECURITY POLICY

If fundamental cybersecurity and identity issues are not addressed, America's reliance on digital infrastructure risks becoming a source of strategic liability.[1] *- White House Cybersecurity National Action Plan*

In a complicated and anarchistic environment, the Department of Defense must defend itself against a wide array of cyber adversaries. Since the turn of the century, the United States has developed numerous policies and strategies to mitigate threats in the man-made domain of cyberspace. This chapter reviews federal and military policy on cyberspace over the past twenty-one years and highlights some points of concern.

Historical Analysis of Federal Policy on Cybersecurity (1995-2016)

One of the first federal government documents that references cybersecurity prior to the 21st century was President Bill Clinton's 1995 National Security Strategy (NSS). The 1995 NSS noted that there was a new transnational "threat of intrusion to our military and commercial information systems."[2] This acknowledgement of a new type of threat was the beginning of U.S. cyberspace policy and strategy.

The first significant federal policy document that addresses cybersecurity as a stand-alone topic was the 2003 National Strategy to Secure Cyberspace. It provided three main objectives in cyberspace for the United States: prevent cyberattacks against critical infrastructures, reduce national vulnerabilities to cyberattack, and minimize the damage

[1] White House Press Office, *Cybersecurity National Action Plan Fact Sheet*, Washington, D.C. February 2016. https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan (Accessed 29 Aug 2016).

[2] William Clinton, *National Security Strategy,* (Washington DC: Government Printing Office, February 1995), 8.

and recovery time from cyberattacks that do occur.[3] This document designated the newly formed Department of Homeland Security (DHS) as the federal government's integrator for cyberspace directing that "DHS will become a federal center of excellence for cybersecurity and provide a focal point for federal outreach to state, local, and nongovernmental organizations including the private sector, academia, and the public."[4] This strategy document also designated federal agency leads to support critical infrastructure in cyberspace. Of the thirteen different critical infrastructure sectors listed, DoD was lead to only one, the Defense Industrial Base.[5]

The 2004 National Military Strategy was one of the first strategic documents to refer to cyberspace as a domain.[6] The 2017 National Defense Authorization Act (NDAA) designated USCYBERCOM as separate functional Combatant Command (CCMD), making cyberspace the only domain to have its own specifically associated CCMD. This action is a clear indicator of the important cyberspace operations has with regards to U.S. national security.

The National Military Strategy for Cyberspace Operations (NMS-CO) produced in 2006 was designed to be the overarching military strategy to ensure United States military superiority in cyberspace and a reference document to plan execute, and resource cyberspace operations.[7] It consisted of five parts: 1) strategic context to provide

[3] George Bush, *National Strategy to Secure Cyberspace.* (Washington DC: Government Printing Office. February 2003), 14.
[4] Ibid, x.
[5] Ibid, 16.
[6] Over the better part of a decade there has been much conceptual debate about whether cyberspace is a domain, a warfighting domain, a global domain within the information environment, an operational domain, an environment, or merely a transport mechanism for information. Cyberspace can be visualized as all of these concepts.
[7] U.S. Joint Chiefs of Staff, *National Military Strategy for Cyberspace Operations*. (Washington, DC, December 2006), ix.

definitions and characteristics of cyberspace; 2) threats and vulnerabilities assessment to create a common understanding; 3) strategic considerations in order to identify priorities in cyberspace; 4) a military strategic frame work that develops the ends, ways and means; and 5) implementation plan and measurement mechanisms to meet strategic goals.[8] The 2006 NMS-CO also made it clear that DoD deemed its role in cyberspace paramount above all others:

> Although partner departments and agencies have responsibilities to secure portions of cyberspace, only DoD conducts military operations to defend cyberspace, the critical infrastructure, the homeland, or other vital US interests. If defense of a vital interest is implicated, DoD's national defense mission takes primacy even if that would conflict with, or subsume, the other support missions.[9]

It can be assumed that the strong language used in the 2006 NMS-CO was to validate that DoD would serve as a backstop against any cyber threats while the nation determined how to best defend itself in cyberspace.

In an effort to codify the nation's strategy on cyberspace, President George W. Bush signed National Security Presidential Directive-54 / Homeland Security Presidential Directive-23 (NSPD-54/HSPD-23) in early 2008. This directive can be considered a cornerstone document for cybersecurity in the federal government. It reinforced already established policy for protecting information and data entrusted to the federal government, provided guidance on how threat information would be shared, defined key terms (especially cybersecurity), and most importantly, laid out the roles and responsibilities for each of the federal agencies giving them specific tasks and

[8] Ibid, 1.
[9] Ibid, 1-2.

deadlines.[10] This document, along with the disruptive effects of Buckshot Yankee[11] on military networks later that year, cemented both the federal government and the military's necessity to put an emphasis on cybersecurity.

JP 3-12 was first published in February 2013 as a secret document, but later released in an unclassified version. It was intended to be the comprehensive "joint doctrine for the planning, preparation, execution, and assessment of joint cyberspace operations across the range of military operations."[12] Supplanting the NMS-CO, JP 3-12 became the definitive document governing military cyberspace operations. JP 3-12 tried to define the roles and responsibilities of USSTRATCOM and USCYBERCOM, the other CCMDS, and the military services.

- Commander, United States Strategic Command (CDRUSSTRATCOM), has overall responsibility for DODIN operations and defense in coordination with CJCS, the Service Chiefs, and CCDRs. CDRUSSTRATCOM is responsible for Cyberspace Operations (CO) to secure, operate, and defend the DODIN, and to defend US critical cyberspace assets, systems, and functions as directed by the President or SecDef, against any intrusion or attack, and does so through a subunified command, USCYBERCOM.[13]

- Other Combatant Commanders operate and defend tactical and constructed networks within their commands; and, integrate CO capabilities into all military operations; integrate CO into plans (concept plans and operation plans [OPLANs]); and work closely with the joint force, USSTRATCOM/USCYBERCOM, Service components, and DOD agencies to create fully integrated capabilities.[14]

- Service Chiefs [Services] will provide CO capabilities for deployment/support to CCMDs as directed by SecDef; and, remain

[10] NSPD-54 / HSPD-23, 3-14.
[11] In 2008, Operation Buckshot Yankee was DoD's effort to remove malicious code from both unclassified and classified networks caused by an infected USB flahdrive being inserted into military computers.
[12] JP 3-12(R), i.
[13] Ibid, ix.
[14] Ibid, ix.

> responsible for compliance with USSTRATCOM's direction for operation and defense of the DODIN.[15]

A common theme among the roles and responsibilities is the concept of "operate and defend." Notable omissions from the roles and responsibilities listed in JP 3-12 are the DoD Chief Information Officer (CIO) and the Defense Information Security Agency (DISA). Both of these organizations had historically been responsible for operating and defending the Global Information Grid (GIG), which is now known as the DoDIN. The DoD CIO has responsibility to make policy regarding operating and defending the DoDIN, specifically:

> The DoD CIO is the Principal Staff Assistant and senior advisor to the Secretary of Defense for information technology (IT) (including national security systems and defense business systems), information resources management (IRM) and efficiencies. The DoD CIO is responsible for all matters relating to the DoD information enterprise, including communications; spectrum management; network policy and standards; information systems; *cybersecurity*; positioning, navigation, and timing (PNT) policy; and the DoD information enterprise that supports DoD command and control (C2).[16]

Cybersecurity is one of the myriad of tasks that the DoD CIO must oversee. DISA is a direct reporting unit to the DoD CIO, and not only has the burden to operate and defend the DoDIN, but to design and engineer it as well. DISA is the "provider for defensive cyberspace and IT combat support for the DoD"[17] and "provides, operates, and assures command and control and information-sharing capabilities and a globally accessible enterprise information infrastructure in direct support to joint warfighters, national level leaders, and other mission and coalition partners across the full spectrum of military

[15] Ibid, ix.

[16] U.S. Department of Defense. DoD Directive 5144.02: *Department of Defense Chief Information Officer (DOD CIO)*. (Washington, DC. November 21, 2014), 1-2. Italics added by author for emphasis.

[17] *Defense Information Security Agency Strategic Plan 2015-2020.* http://www.disa.mil/~/media/Files/DISA/About/Strategic-Plan.pdf (accessed 13 February 2017), 4.

operations."[18] While the DoD CIO and DISA are mentioned in JP 3-12, it is important that the next doctrinal update of JP 3-12 specifies the roles and responsibility of the DoD CIO and DISA in cyberspace.

DoD Instruction 8500.01, dated March 2014 titled *Cybersecurity*, was written and signed by the DoD CIO in order to solidify specific cybersecurity policy directives. First, it consolidated a multitude of previous DoD Directives (DoDDs) into a singular DOD Instruction (DoDI). Second, it ensured that all electronic data meets the required levels of confidentiality, integrity, and availability (Cybersecurity Triad). Third, it codified the DoD CIO's role to monitor, evaluate, and provide advice to the Secretary of Defense regarding all DoD cybersecurity activities along with developing and establishing DoD cybersecurity policy and guidance. Finally, it reaffirmed that DISA is a direct reporting unit to the DoD CIO, and directed DISA to conduct both command cyber readiness inspections (CCRIs) and operational risk assessments in support of USSTRATCOM.[19] At the time, USCYBERCOM was still a sub-unified combatant command subordinate to USSTRATCOM, and therefore, was not referenced in DoDI 8500.01.

The year 2015 saw multiple federal and DoD policies on Cybersecurity released. First, was President Barack Obama's NSS which, for the first time, had an entire section dedicated to cybersecurity:

> As the birthplace of the Internet, the United States has a special responsibility to lead a networked world. Prosperity and security increasingly depend on an open, interoperable, secure, and reliable Internet. Our economy, safety, and health are linked through a networked

[18] DISA, "Our Work / DISA 101." http://www.disa.mil/About/Our-Work (accessed 13 February 2017).
[19] U.S. Department of Defense Assistant Secretary of Defense for Networks and Information Integration ((ASD(NII))/Chief Information Officer. DODI 8500.01, *Cybersecurity*. (Washington, DC. March 14, 2014), http://www.dtic.mil/whs/directives/corres/pdf/850001_2014.pdf. (accessed August 20, 2016).

> infrastructure that is targeted by malicious government, criminal, and individual actors who try to avoid attribution.[20]

Later that year, Congress passed the Cybersecurity Information Sharing Act (CISA), codifying several cybersecurity items. First, it reaffirmed that DHS was the federal lead for cybersecurity and was to act as the central repository for information gathering and sharing. Second, it protected agencies and corporations that share information from liability. Third, CISA limited the amount of information sharing that the federal government was allowed to do with the commercial sector; the only exception being the Defense Department.[21] Fourth, CISA did not require agencies or corporations to share information, warn other organizations of a threat, or act on threat warnings. Finally, while it encouraged private organizations to defend itself in cyberspace, CISA specifically prohibited any type of retribution by private organizations.[22]

The 2015 DoD Cyber Strategy listed three missions for the Defense Department in cyberspace: Defend Department of Defense systems, networks, and information; defend the U.S. homeland and U.S. national interests against significant cyberattacks; and provide cyber support to military operations and contingency plans.[23] DoD has begun to recognize the multitude of cybersecurity risks, emphasizing defense as two of its three missions in cyberspace. This concern is reflected in the Cyber Strategy's assessment of the DoDIN and its indefensible nature:

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

[21] Chapter 19 (Cyber Matters) of Title 10, United States Code directs that all cleared U.S. defense contractors are required to rapidly report breaches of network security to the DoD. Section 391(c)(2): Rapid reporting.—The procedures established pursuant to subsection (a) shall require each operationally critical contractor to rapidly report to the component of the Department designated pursuant to subsection (d)(2)(A) on each cyber incident with respect to any network or information systems of such contractor.

[22] 114th U.S. Congress, *Cybersecurity Act of 2015*, (Washington, DC. December 16, 2015), Section 101-111.

[23] U.S. Department of Defense, *Department of Defense Cyber Strategy*, (Washington, DC. April 2015), 3.

> While DoD cannot defend every network and system against every kind of intrusion – DoD's total network attack surface is too large to defend against all threats and too vast to close all vulnerabilities – DoD must take steps to identify, prioritize, and defend its most important networks and data so that it can carry out its missions effectively.[24]

This is the first document that acknowledges the military's inability to defend all of its networks in their entirety, reinforcing the military contradiction that offense has the advantage over defense in cyberspace.

In an attempt to meet the requirements of the DoD Cyber Strategy, the DoD Cybersecurity Discipline Implementation Plan (DoD CDIP), released in 2015 and later amended February 2016, highlighted the need for increased scrutiny on cybersecurity because, "inspections [such as CCRI] and incidents across the Department of Defense (DoD) reveal a need to reinforce basic cybersecurity requirements identified in policies, directives, and orders."[25] In February of 2016, the DoD Inspector General (IG) began an audit to "gauge how well agencies have corrected vulnerabilities identified by Command Cyber Readiness Inspections."[26] The DoD CDIP is divided into four lines of effort:

1. Strong authentication - degrade the adversaries' ability to maneuver on the DoDIN
2. Device hardening - reduce internal and external attack vectors into DoDIN
3. Reduce attack surface - reduce external attack vectors into DoDIN
4. Alignment to cybersecurity / computer network defense service providers - improve detection of and response to adversary activity[27]

These four lines of effort work to mitigate the risks identified in the DoD Cyber Strategy and increase the CIA tenets in the cybersecurity triad. The DoD CDIP directs

[24] Ibid, 13.

[25] U.S. Department of Defense, *DoD Cybersecurity Discipline Implementation Plan,* (Washington, DC. October 2015) (amended February 2016), 3.

[26] Sean Lyngaas, "Pentagon IG to Audit Cyber Readiness" *Federal Computer Week*, February 3, 2016. https://fcw.com/articles/2016/02/03/pentagon-cyber-oversight.aspx (accessed 21 December 2016).

[27] U.S. DoD, *DoD Cybersecurity Discipline Implementation Plan*, 3.

commanders to complete specific tasks across each of the four lines of efforts in order to create a layered defense in depth across the DoDIN.

It is clear that the federal government, especially DoD, must secure its networks. Over the past twenty-one years, both the quantity and quality of policy regarding cybersecurity has increased. While there still remains gaps and seams in some aspects of cybersecurity, there also appears to be overlap between agencies such as DHS and DoD. U.S. cybersecurity policy needs to mature and make the necessary refinements that will help to achieve federal unity of effort.

Policy Concerns

There are five major policy concerns in the realm of cybersecurity: inconsistent terminology, overlapping mission objectives, poor unity of command and unity of effort, confusion in understanding the nature of cyberspace, and the voluntary approach of cybersecurity measures used and implemented by both DoD and DHS.

Terminology

The first issue is inconsistent terminology among federal agencies. The primary example is the interchangeable usage of the terms "cybersecurity" and "information assurance." DoDI 8500.01, *Cybersecurity*, states that DoD, "adopts the term 'cybersecurity' as it is defined in National Security Presidential Directive-54/Homeland Security Presidential Directive-23 (Reference (m)) to be used throughout DoD instead of the term 'information assurance (IA).'"[28] The directive articulates that "'cybersecurity' means prevention of damage to, protection of, and restoration of computers, electronic

[28] U.S. Department of Defense Assistant Secretary of Defense for Networks and Information Integration ((ASD(NII))/Chief Information Officer, DODI 8500.01, *Cybersecurity*, Washington, DC. March 14, 2014. http://www.dtic.mil/whs/directives/corres/pdf/850001_2014.pdf. (accessed November 27, 2016), 1.

communications systems, electronic communication services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and non-repudiation."[29] The term "information assurance" does not appear in NSPD-54/HSPD-23. Although the directive to change from "Information Assurance" to "Cybersecurity" has been in place for three years, military organizations such as USCYBERCOM continue to use "information assurance" because other federal agencies have not yet adopted the term "cybersecurity" as directed by NSPD-54/HSPD-23. This undoubtedly leads to confusion and wasted effort making it difficult to communicate complicated ideas because the lexicon is not consistent across all the federal agencies.

Overlapping Missions

According to NSPD-54/HSPD-23, "the Secretary of Homeland Security shall lead the national effort to protect, defend, and reduce vulnerabilities of Federal systems and the Secretary of Defense shall provide support to the Secretary of Homeland Security with respect to such assignment."[30] However, the mission objectives of both DHS and DoD do not appear to be complementary. DHS has been directed by the President to defend the all Federal networks, yet its cybersecurity mission statement reads "the Department of Homeland Security (DHS) has the mission to provide a common baseline of security across the federal civilian executive branch and to help agencies manage their cyber risk."[31] The inclusion of the term "civilian" in the mission statement suggests that DoD is not included under DHS's umbrella of support. Conversely, the DoD makes it

[29] *NSPD-54/HSPD-23*, 3.

[30] Ibid, 5.

[31] U.S. Department of Homeland Security, *DHS cybersecurity webpage*, https://www.dhs.gov/einstein (accessed 27 November 2016).

appear that one of its primary missions is to defend all the nation's networks. DoD's 2015 Cyber Strategy it states that "DoD must be prepared to defend the United States and its interests against cyberattacks of significant consequence."[32] It amplifies this statement by declaring that,

> *In concert* with other agencies, the United States' Department of Defense (DoD) is responsible for defending the U.S. homeland and U.S. interests from attack, including attacks that may occur in cyberspace . . . The Defense Department has developed capabilities for cyber operations and is integrating those capabilities into the full array of tools that the United States government uses to defend U.S. national interests, including diplomatic, informational, military, economic, financial, and law enforcement tools.[33]

DoD's cyber strategy does not appear to recognize DHS as the lead and the use of the words "in concert" as opposed to "in support of" suggests a leadership role with regards to defending the United States homeland in cyberspace. The difference in mission statements could be a result of cultural nuances among the organizations; however, both agencies should reexamine their mission statements in order to prevent confusion during a time of crisis and conform to the presidential directive.

Unity of Effort and Unity of Command

United States Cyber Command (USCYBERCOM) was established in 2010 and is focused on three main tasks which are to defend the DoDIN, provide support to combatant commanders for execution of their missions around the world, and strengthen the nation's ability to withstand and respond to cyberattack.[34] These tasks support the DoD Cyber Security Strategy; however, because there is no direct command relationship

[32] DoD Cyber Strategy 2015, 5.

[33] Ibid, 2. Italicized by author for emphasis.

[34] USSTRATCOM Website, https://www.stratcom.mil/factsheets/2/Cyber_Command/ (accessed 15 October 2016).

between USCYBERCOM and DISA, the missions begin to overlap in relation to the defense of the DoDIN. This basic lack of unity of command is also revealed by the lack of clear lines of responsibility among the DoD CIO, USCYBERCOM, and DISA. A 2015 OMB report found that DoD had not implemented Internet Protocol version 6 (IPv6), the next generation protocol for maintaining cybersecurity, and that the DoD CIO, USCYBERCOM, and DISA had failed to put together an effective, coordinated effort and did not use available resources to guide the DOD-wide transition toward IPv6.[35] This is an example of how the pace of technological change continues to befuddle large bureaucratic organization while the lack of unity of command and unity of effort only complicate the efforts to meet U.S. cybersecurity goals.

Confusion in understanding the nature of cyberspace

JP 3-12 makes the assertion that "[cyber operations] take place in a complex environment: large parts of cyberspace are not under any nations' control; the array of state and non-state actors is extremely broad; the costs of entry are low; and technology proliferates rapidly and often unpredictably."[36] Even though this environment is extremely complicated, labeling it as complex advances the mistaken idea that it is uncontrollable and cannot be expected to produce predicable outcomes.

The Department of Homeland Security creates even greater problems by describing cyberspace as an ecosystem in its memorandum *Strategic Principles for Securing the Internet of Things (IoT), version 1* using phases such as "promoting

[35] Jacob Fischler, "Pentagon Solicits $475M Omnibus Cybersecurity Contract" *Law360*, (May 1, 2015) https://www.law360.com/articles/650741/pentagon-solicits-475m-omnibus-cybersecurity-contract (accessed 12 December 2016).
[36] JP 3-12, I-1.

transparency across the IoT ecosystem."[37] The comparison of cyberspace with an ecosystem is a clever way to convey a system, but it does not describe cyberspace accurately and one instance when analogies fail. Cyberspace is not a natural system, ecosystems survive without human interaction -- cyberspace cannot. Even accepting the concept that human interface and the cognitive domain make cyberspace complex, it does still not equate to an ecosystem. This undisciplined use of terms and analogies only serves to confuse the true nature of cyberspace.

Voluntary Compliance

The potential for a cyberattack on infrastructure is a looming threat. Disruption of power grids, attacks on nuclear power generation, and the interference with water or sewage treatment plants are all threats that could have significant effect on the population. This is a concern because DHS has noted that "cybersecurity and physical security are increasingly interconnected."[38] DHS has established a program known as the Critical Infrastructure Cyber Community Voluntary Program (C3VP) "to establish a voluntary program to encourage use of the Framework for Improving Critical Infrastructure Cybersecurity to strengthen critical infrastructure cybersecurity."[39] Cybersecurity experts understand the connective nature of cyberspace and recognize that a risk to one is a risk to all. However, a voluntary program is not very helpful to secure the network since any organization that does not comply still leaves those organizations who have complied vulnerable.

[37] Department of Homeland Security, *Strategic Principles for Securing the Internet of Things (IoT)*, https://www.dhs.gov/news/2016/11/15/dhs-releases-strategic-principles-securing-Internet-things (accessed 19 December 2016).
[38] DHS, *Protecting Critical Infrastructure*. https://www.dhs.gov/topic/protecting-critical-infrastructure (accessed 13 February 2017).
[39] Ibid.

Within DoD, the largest illustration of voluntary compliance that relates to cybersecurity risk is the employment of Enterprise Email. Email is one of the big threats to cybersecurity due to the human factor involved. An untrained or unsuspecting user can easily fall victim to any number of malicious and sophisticated email ploys, who can then unintentionally and inadvertently infect their coworkers and friends. The concept of having a single email service provider responsible for providing the overarching security reduces the potential points of entry and shrinks an adversary's attack surface.

As advertised on DISA's website, "the Department of Defense (DOD) Enterprise Email (DEE) service provides secure cloud-based email to the DOD enterprise that is designed to increase operational efficiency and facilitate collaboration across organizational boundaries."[40] Currently DISA provides enterprise email services to the Army, Joint Staff, and all of the CCMDs except USSOCOM and USCYBERCOM. The U.S. Coast Guard also uses DEE for secure email. The Air Force, Navy, Marine Corps, and most of the Defense Agencies except DISA and DFAS have not migrated to using DEE. The resistance to migrate to a single email service provided by DoD not only runs contradictory to the three principles of cybersecurity - confidentiality, integrity, and availability - but also runs contradictory to the concepts of jointness, cost efficiency, and unity of effort. It is ironic that the joint headquarters specifically tasked with the defense of the network, USCYBERCOM, does not use DEE. The fact that the Services, Defense Agencies, and CCMDs can voluntarily comply with DoD's initiative to provide a secure and unified method of email service illustrates the difficulty in establishing any systematic cyber defense.

[40] DISA, *DOD Enterprise Email*. http://www.disa.mil/enterprise-services/applications/dod-enterprise-email (accessed 13 February 2017).

Cybersecurity policy has been developed based on the national interest of keeping U.S. federal networks secure. These policies are the baseline that drives cybersecurity strategy and the programs that implement that strategy. While the policies and strategies are not perfectly aligned, when they are complied with, they provide a significant framework in which DoD can build towards defending the DoDIN and supporting other federal agencies.

CHAPTER 3: COMMAND CYBER READINESS INSPECTION (CCRI)

We need a cybersecurity renaissance in this country that promotes cyber hygiene and a security centric corporate culture applied and continuously reinforced by peer pressure.[1]
– James Scott from the Institute for Critical Infrastructure Technology

The CCRI program is the lynchpin between the commands, their day-to-day activities in cyberspace, and the defensive strategy of DoD. It is the mechanism that ensures that commands are able to operate securely in cyberspace to meet national security policy and cybersecurity requirements. Military installations are required to be inspected once every three years. The program will be examined through three categories: Inspection Design, Manning and Experience, and Feedback Enforcement Mechanisms. Looking at CCRI through these three lens provides a snapshot of how federal policy and strategic guidance is being implemented at the operational level.

Inspection Design

The Command Cyber Readiness Inspection is overseen by the DoD Chief Information Officer (CIO) and executed by the Defense Information System Agency (DISA). Defined by DISA's website, a CCRI is "a formal inspection conducted under the direction of USCYBERCOM's Enhanced Inspection Program."[2] Prior to 2010 and the establishment of USCYBERCOM, the Command Cyber Readiness Inspection was a "quick look" methodology for conducting compliance validations for the CCMDs, Services and Agencies on both NIPRNet and SIPRNet as directed by the Joint Task Force

[1] James Scott, "Cerber & KeRanger: The Latest Weaponized Encryption" Institute for Critical Infrastructure Technology, 8 March 2016. http://icitech.org/cerberkeranger/ (accessed 20 Feb 2017).
[2] Defense Information Security Agency, "Information Assurance (IA) Analysis." https://www.disa.mil/Cybersecurity/Analytics/IA-Analysis (accessed 15 October 2016).

– Global Network Operations' (JTF-GNO) Enhanced Inspection Program.[3] This approach is still used and only provides a snapshot in time, instead of seeking to drive sustainable compliance.

The CCRI was formally established in 2011 through Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6510.01F which tasked USSTRATCOM to "oversee DOD Cyber Security Inspection Program [later referred to as CCRI] to maintain and determine compliance with security policy, procedures, and practices."[4] The same memo directed the Director of DISA to "provide CCRI support with Information Assurance (IA) trained and certified personnel to conduct security inspections as requested by USSTRATCOM."[5] USSTRATCOM in turn, delegated oversight of the CCRI program to USCYBERCOM. Nevertheless, USCYBERCOM is not perceived to have full authority or responsibility for CCRI, leading some organizations undergoing inspections to potentially downplay the importance of the program. Organizations that have recently undergone a CCRI have made statements that they were "challenged by Defense Information Systems Agency (DISA) inspectors"[6] and that the CCRI was a "comprehensive network inspection aimed at improving security of the Department of Defense Information Network[s] and is conducted by Defense Information Systems Agency."[7] This perception of the CCRI as a three-star level initiative instead of a four-

[3] DISA, *Customer Support*, http://www.disa.mil/Services/DISA-Europe/Customer-Support (accessed 13 February 2017).
[4] U.S. Department of Defense, Chairman of the Joint Chiefs of Staff Instruction 6510.01F: Information Assurance (IA) and Computer Network Defense (CND). February 9, 2011 (Current as of 9 Jun 2015), B-6.
[5] Ibid, B-12.
[6] USSOUTHCOM Public Affairs Office and J6, "SOUTHCOM Achieves Cyber Readiness Success" https://extranet.southcom.mil/Apps/Home/(S(3w3rfjt3yt4yogx2msuf2xk1))/Spotlight/News/frm_Read.aspx?ID=375 (accessed 18 September 2016).
[7] United States Air Force, Tyndall Air Force Base "Command Cyber Readiness Inspection" http://www.tyndall.af.mil/AboutUs/CommandCyberReadinessInspection.aspx. (accessed 22 August 2016).

star command program detracts from the importance of the program. It would be more useful if the CCRI was branded as a USCYBERCOM program in order to communicate its importance to overall national security. By branding the CCRI as a functional Combatant Command program, it would be received as a commander's program instead of a J-6 (Command, Control, Communications, and Computers) staff inspection. This would encourage more leadership emphasis on proper cybersecurity practices across commands and build towards a culture of compliance.

Manning and Expertise

Manning and expertise for cybersecurity continues to be a problem at all levels of DoD. First, there remains a significant shortfall in the number of trained cybersecurity professionals. Although there has been approved growth in organizations such as USCYBERCOM, at the operational and installation level where the majority of CCRIs are conducted, personnel cuts continue to force organizations to hire contractors to provide cybersecurity and help pass CCRIs. When outside contracted support is leveraged in order to pass inspections, it creates unforecasted spending and a misperception about the cybersecurity abilities of organizations, thereby providing a false assessment. Companies such as SecureStrux and Tapestry Technologies offer contractor assistance to pass the CCRI. One advertisement claims "We have helped our clients achieve some of the highest CCRI scores in the DoD. Since the beginning of 2015, all of our Defense Security Service [SecureStrux] customers have achieved an Excellent or Outstanding CCRI grade."[8] Since sites continue to pass inspections but are taking cuts to cybersecurity personnel, it leaves the impression that those personnel are not needed,

[8] SecureStrux. "CCRI and SAV Whitepaper." http://www.securestrux.com/wp-content/uploads/2016/05/CCRI-and-SAV-White-Paper.pdf (accessed 20 August 2016).

when in fact it is just the opposite. Since sites are taking cuts, they must hire external contractors from companies such as SecureStrux and Tapestry if they expect to pass the inspection creating a loop which continues to exacerbate the manning issues.

The CCRI highlights the absence of physical security, operational security, and cybersecurity knowledge the common user has. To ensure users were ready for the CCRI, one installation's webpage specifically listed cyber security advice in order to get users to "cram for the test." Examples of the directions listed were reboot unclassified workstations daily to allow security patch compliance, turn on SIPR workstations for at least six continuous hours weekly, properly label disc media, do not use wireless devices in classified areas, remove common access cards or SIPR token cards before leaving the computer, and never share passwords, personal identification numbers, CACs or token cards.[9] Though it is good that organizations are providing this information in preparation for the CCRI, the mere fact that it must be reemphasized indicates that DoD still has much work to do in building a culture that understands and appreciates the importance of cybersecurity.

Feedback Enforcement Mechanisms

The CCRI is intended to harden targets in cyberspace and increases deterrence against the multitude of cyberspace threats. The CCRI is intended to reinforce the cybersecurity triad by validating proper procedures, technical compliance, and a culture of awareness. There is a significant amount of surging to ensure proper compliance and attainment of an acceptable "snapshot" of the cybersecurity posture. Upon completion of the CCRI, the inspectors will provide an outbrief to the Senior Mission Commander

[9] Robert Register, "Command Cyber Readiness Inspection: Know Your Role," *North West Florida Daily News*. August 14, 2015.

with the results of the inspection. The current scoring mechanism is a grading scale from 0-100 points with any score below 70 percent considered failing. However, this type of scoring methodology feeds the attitude that an organization can peak for an inspection then fall back into normal routines rather than addressing specific threats, procedural issues, equipment shortfalls, or cultural concerns.

The results of the CCRI are forwarded to the military component's cyber headquarters, those being ARCYBER, AFCYBER, MARFORCYBER, FLTCYBERCOM. The military services' cyber headquarters are responsible to ensure the correction of major deficiencies within a specified timeline after completion of the inspection. Early in 2016, the DoD IG published a memo entitled *Audit of Corrective Actions on Command Cyber Readiness Inspection Deficiencies.* The objective of the memo was "to determine whether DoD Components are adequately correcting deficiencies identified during Command Cyber Readiness Inspections (CCRI) and whether DoD Components' Headquarters are using CCRI results to identify systemic deficiencies and improve component-wide cyber security"[10] This memorandum clearly indicated that even though there are feedback mechanisms in place, those mechanisms have not been effective to fully correct deficiencies, establish procurement priorities, or drive sustainable compliance.

The organizations that oversee and implement the CCRI understand the limitations and short-comings of the program. There are already efforts to operationalize the program and convert it to the Command Cyber Operational Readiness Inspection (CCORI) using more of a risk assessment scoring methodology as opposed to a

[10] U.S. Department of Defense. Inspector General Memorandum: *Audit of Corrective Actions on Command Cyber Readiness Inspection Deficiencies,* (Washington, DC. February 2, 2016), 1.

percentage grade.[11] While this addresses some of the inspection design and feedback issues mentioned, it still does not address any personnel or material requirement concerns. More importantly, it takes leadership, not an inspection, to inculcate a culture of cybersecurity into an organization.

[11] Defense Information Security Agency, "Command Cyber Operational Readiness Inspection (CCORI) Program: Mission Impact Analysis Process Guide." (Fort Meade, MD. 24 September 2016), 2.

CHAPTER 4: RECOMMENDATIONS

Without preparedness, superiority is not real superiority and there can be no initiative either. Having grasped this point, a force that is inferior but prepared can often defeat a superior enemy by surprise attack.[1] – Mao Tse Tung

Cyberspace is an ever-changing environment, constantly contested, and unlikely to have a global governing body anytime soon. Any free and open system can become a dangerous tool for nefarious actors resulting in "the possibility of infection by numerous varieties of malicious code, such as viruses, spyware, worms, and bots."[2] The federal government continues to work through all the partnership agreements and bureaucracy to achieve the unity of effort required to safeguard the nation's networks. While DoD has technical overmatch in the other domains of land, sea, air, and space, it has not fully resourced the cyberspace domain as a part of the information environment to achieve some level of superiority in the most contested domain on the planet. Even though the CCRI is a useful program, it only provides a snapshot of the organization's compliance levels the time of the inspection. USCYBERCOM needs to take a larger role in CCRI management and begin to fully develop programs that operationalize cybersecurity like the CCORI and work with CCMDs and military services to internalize new mentality and culture. Agencies must understand the hazards and threats that reside in cyberspace, prioritize the manning and resourcing of cyber defense, and vigorously comply with policy and directives realizing that a threat to one is a threat to all.

[1] Mao Tse Tung. *Selected Works of Mao Tse Tung, Vol II.* (Peking: Foreign Language Press, 1965), 165-166.

[2] Franklin D Kramer, *Cyberpower and National Security*. (Washington, DC: National Defense University Press, 2009, 204.

Inspect Every Two Years

The nature of cyberspace as an open, anarchistic environment that is continuously growing in its complications requires that that CCRI needs to be more visible and more active in ensuring compliance. The first recommendation is to have inspections for sites every two years instead of three. By increasing the frequency of inspections, it helps to build sustainable compliance. With less time to digress and move backwards to non-compliance, sites will be more apt to maintain a better cybersecurity posture. Organizations will better compensate for Moore's Law by inspecting every two years and will need to prioritize their budgets more towards improving technologies and ensuring those technologies comply with cybersecurity policies. Not only would cybersecurity personnel have to remain current with regulations, but the standard user would internalize proper cybersecurity habits. Increased frequency of inspections will require partnership with other agencies in order to overcome the increased requirement on funding, personnel, and resources. The added benefit of increased partnership with other federal agencies will be stronger ties towards achieving a cybersecurity unity of effort.

Standardization of Technologies and Services across the DoDIN

Network security seeks to limit seams and gaps in the network. Having different types of proprietary technologies creates those seams and gaps at the lowest levels of the network. DoD needs to develop more Joint Enterprise Level Agreements (JELA) in an effort to standardize technologies, protect the network, and support enterprise level compliance monitoring. Both Cisco and Microsoft have JELA's with DoD. Cisco's JELA covers all of DoD while Microsoft only covers the Army, Air Force, and select CCMDs (USSTRATCOM, USTRANSCOM, and USNORTHCOM). McAfee also has a

JELA with DoD, which enables military members to get McAfee anti-virus free for home use, positively expanding network security to service members' families. Finally, all services and CCMDs need to transition to DISA provided email services in order to increase security and reduce costs.

Move to Biometrics

Currently, the military uses the common access card (CAC) to allow and verify a user's identity on the network. Use of the CAC is a cumbersome process and cannot always ensure validation of a user. The DoD CIO recently stated in an interview that "we are on a two-year journey to get rid of the CAC card. The CAC card is not the future of security. What the government needs is a common identity standard that assures me you're you, but also that you have the access."[3] The use of biometrics, retina or fingerprint scans, is one way to move away from the CAC, remove a CCRI check, and increase both the security of the network and convenience for the user.

A counter argument to biometrics is that it is too costly. While this may be true initially, more electronic devices are being developed with biometric scanners already in place. Various organizations within DoD already have laptops with fingerprint scanners embedded into the hardware. Cost for biometric hardware and software continue to fall as companies that have agreements with the government must still compete with Apple products that have already integrated biometrics into its iPhones and iPads. This is the opportune time for DoD to develop a strategy to move towards biometric access control for its IT systems over the next three to five years.

[3] Sandra Erwin, "Defense CIO: Cybersecurity Improving But Innovation Lags," *National Defense Magazine,* August 8, 2016. http://www.nationaldefensemagazine.org/blog/Lists/Posts/Post.aspx?ID=2268 (accessed 9 August 2016).

Concentrated Effort to Map the DoDIN

The DoDIN is a network of networks. The Army operates the LandWarNet, the Navy operates the Navy Marine Corps Internet (NMCI), the Air Force operates the AFNet, the National Guard Bureau (NGB) operates the GuardNet, there are multiple CCMD networks, plus additional networks based on classification level such as CENTRIX, SIPRNET, and JWICS. Each of these networks have separately managed networks underneath their primary architecture. Due to the ever changing nature of computer networks, it is difficult to develop useable network maps. There are numerous blind spots in the DoDIN and a network that cannot fully account for all its parts is a dangerous situation.

A concentrated effort needs to be made to map all portions of DoDIN, catalog it, continuously update it, and ensure those maps are properly classified and secured. The technology already exists to monitor and map networks continually; however, it is difficult to procure a common tool familiar and affordable to all. While this may be one of the more difficult recommendations to implement, due to procurement restrictions and varying opinions on technology options, it is the most important one from a classical sense in order to "know yourself."[4] USCYBERCOM and DISA need to lead this effort with full support from all military services and CCMDs if DoD is serious about defending the all of its disparate networks.

Create Unity of Effort internally and with other federal agencies

DoD needs to examine its current organizational structure for cyberspace operations. At this time, USCYBERCOM does not have direct command authority over

[4] Sun Tzu, *Art of War*, 84.

DISA, the architect and engineer of the DoDIN. Creating a direct chain of command relationship between USCYBERCOM and DISA would provide better unity of command, and thereby unity of effort, for all aspects of cyberspace operations. The DoD CIO would remain as the policy maker and principal staff advisor to the SecDef on matters of cybersecurity, but the USCYBERCOM would be the execution arm of all cyberspace operations. This adjustment in the command and control structure would provide a clear line of responsibility for CCRI directly to USCYBERCOM.

If one of DoD's primary cybersecurity missions is to defend the U.S. homeland and U.S. national interests against cyberattacks, then greater partnership is required from the DoD with all federal agencies. The Department of Homeland Security stated in its 2011 Blueprint for a Secure Cyber Future that, "through partnership with the Department of Defense (DOD), a secure cyberspace will support the United States' execution of its critical national defense mission responsibilities."[5] NSPD-54/HSPD-23 makes it clear that DHS has the responsibility to protect, defend, and reduce vulnerabilities across the federal networks, and one of the ways DoD can establish a proper supporting relationship is by increased partnership with other federal agencies. In order for that partnership to be most effective, DoD and other federal agencies must prescribe to a common lexicon for cyberspace operations. All federal agencies must adopt a more aggressive attitude towards developing a cybersecurity partnership to secure the networks of the United States.

These recommendations are intended to help improve overall cybersecurity posture of the DoDIN. Cyberspace continues to evolve, and so must the ways in which it

[5] Janet Napolitano, *Blueprint for a Secure Cyber Future*, (Department of Homeland Security: Washington, D.C., November 2011), 7.

is defended. President Barack Obama in speaking about the importance of cybersecurity observed that "it's hard, and it constantly evolves because the technology so often outstrips whatever rules and structures and standards have been put in place, which means that government has to be constantly self-critical and we have to be able to have an open debate about it."[6] This paper is intended to help begin that debate. Examining the nature of cyberspace, deconstructing cybersecurity policy, assessing current programs, and providing recommendation are all part of the iterative process of advancement. All of these efforts are to help the dedicated cybersecurity professionals who continue to find innovative ways to protect the nation's networks.

[6] Barack Obama, "Remarks by the President at the Cybersecurity and Consumer Protection Summit." Washington DC: The White House Office of the Press Secretary. February 13, 2015. https://obamawhitehouse.archives.gov/the-press-office/2015/02/13/remarks-president-cybersecurity-and-consumer-protection-summit (accessed 19 February 2017).

CHAPTER 5: CONCLUSION

When future historians ask who built this Information Age, it won't be any one of us who did the most important part alone. The answer will be, 'We all did, as Americans.'[1] – President Barack Obama

How the United States and its military defends itself in cyberspace from the constant threats of surveillance, exploitation, and attack by a multitude of different types of hostile actors continues to be studied. Successful cyberattacks on the Pentagon as recently as 2015 prove that the military's information is valuable and continues to be at risk. An analysis of current cybersecurity policies indicates that a dedicated effort is necessary to improve network defense and ensure effective security across all the CCMDS and military services in the ever changing cyberspace domain. This paper has analyzed the cyberspace environment, the current federal policies on cybersecurity, and taken an in-depth look into one of DoD's primary compliance programs, the Command Cyber Readiness Inspection. Examining the cyberspace environment and exploring the nature of cyberspace provides context for understanding problems with cyber defense as it exists today. The policy analysis helps determine the strategic direction. The examination of the CCRI, which has been one of the mainstays of cybersecurity, has shown that it is currently inadequate and needs to be significantly improved along with major changes in oversight, compliance, command responsibilities, and unity of effort.

This paper makes five recommendations on how to improve the CCRI and cybersecurity not only within the DoD, but for other federal agencies as well. The first recommendation is to have a CCRI like-program that runs every two years instead of

[1] Barack Obama. "Remarks by the President at the Cybersecurity and Consumer Protection Summit." Washington DC: The White House Office of the Press Secretary. February 13, 2015.

three in an effort to keep up with the rapid pace of technological changes. Second is to standardize more of technologies across the DoDIN in order to reduce the gaps in an open architecture and reduce the amount of training time required for IT professionals. The third recommendation is to move to biometric identity authentication which will simultaneously increase ease of use and network security. The fourth recommendation is to prioritize mapping the DoDIN in order to better understand and visualize the network architecture and reduce threat gaps across all of the DoD networks. The final recommendation is to partner with other federal agencies to help prevent cybersecurity violations of the past by having outside agencies provide hard looks at cybersecurity procedures and then utilize the best business practices from each agency.

Examining cyberspace and cybersecurity from a strategic perspective through the environment, policy, and inspection process is useful to inform, educate, and influence stakeholders and everyone who operates in cyberspace. The analysis shows the need to establish a culture of cybersecurity as the centerpiece of defense in the digital networked age. Closing the gaps and seams across networks can only happen by establishing a cybersecurity culture and doing the right things, the right way in cyberspace. Vigilance across all aspects of cybersecurity is essential to the mission assurance of the Department of Defense and the national security of the United States of America.

APPENDIX A - Cyberspace Threats

This appendix provides broad analysis of the current adversaries that threaten the United States in the cyberspace domain.

China

China's Third Department of the People's Liberation Army's (3PLA) is reported to have over 100,000 personnel working all three facets of cyberspace operations: OCO, DCO, and DoDIN. Five personnel within 3PLA are wanted by the United States Department of Justice for stealing corporate secrets of a military nature.[1] Formed in the 1930s as part of the Communist Red Army, 3PLA intercepted telegrams and radio enemy messages and is credited with helping Mao Zedong's rebel forces win power in 1949.[2] The 2015 United States National Security Strategy specifically references the Chinese threat: "On cybersecurity, we will take necessary actions to protect our businesses and defend our networks against cyber-theft of trade secrets for commercial gain whether by private actors or the Chinese government."[3]

North Korea

North Korea's Bureau 21 has been accused by U.S. intelligence agencies as the culprits behind the Sony Pictures hack in November of 2014.[4] Also in July 2009, South Korea accused another North Korean Cyber unit, Unit 110, of infecting over 100,000 computers in both the United States and South Korea. Their actions brought down

[1] James T. Arreddy, Paul Maozu, and Danny Yadron, "Military Organization 3PLA Is Tasked With Monitoring World-Wide Electronic Information" *Wall Street Journal.* 7 July 2014. http://www.wsj.com/articles/chinas-spy-agency-has-broad-reach-1404781324 (accessed October 12, 2016).
[2] Ibid.
[3] Barack Obama. *National Security Strategy*, 24.
[4] David Lee, "Bureau 121: How Good are Kim Jong-Un's Elite Hackers?" BBC News, 29 May 2015. http://www.bbc.com/news/technology-32925503 (accessed October 11, 2016).

servers in the United States Treasury Department, Secret Service, Federal Trade Commission, and Department of Transportation while simultaneously flooding Korean banking and government websites in a Denial of Service (DoS) attack.[5]

Iran

Iran is unique because of the highly publicized Stuxnet attack in 2010 carried out against it purportedly by Israel and the United States. This successful attack made Iran aware of the true nature of offensive cyberspace operation and Iran has now seriously invested in training and technology to be a significant actor in cyberspace. Iran's Cyber Defense Command, Gharargah-e Defa-e Saiberi, was established in November 2010 and operates under the supervision of the Passive Civil Defense Organization, an independent unit of the Iranian Joint Staff.[6]

Russia

Little is written about actual Russian cyber units. The Russian FSB, formerly known as the KGB, appears to lead the majority of Russia's cyber activity. In August 2013, the Moscow Times reported that Russia is standing up a military cyber warfare unit. In this article Andrei Grigoryev, the head of the Foundation for Advanced Military Research at the time stated, "Cyber space is becoming our priority . . . the decision to create a cyber-security command and a new branch of the armed forces has already been made."[7] Historically, Russia has effectively used non-state actors to execute its cyberattacks. Jarno Limnéll, a professor of cybersecurity at Aalto University in Finland identifies some of these Russian cyber personas as APT28, the Dukes, Red October,

[5] Richard Clarke, *Cyber War: The Next Threat to National Security and What to Do About It,* (New York: Harper Collins Publishers, 2010), 24-27.

[6] Vladimir Platov, "Iran and Modern Cyber Warfare" *New Eastern Outlook.* December 22, 2014.

[7] Ria Novosti, "Military Creating Cyber Warfare Branch" *Moscow Times.* August 21, 2013.

Snake, and Energetic Bear.[8] The DNC hacks in July 2016 have been attributed to Russia based on the sophistication of the attacks, all the IP addresses were from Russian servers, and the fact that no actions were taken on Russian holidays.[9] According to cybersecurity experts at the Center for Cyber Security Sciences in London, the assumed goals of the DNC attack were "to demonstrate that Russia is on top of its game in this kind of shadowy warfare. Another was to embarrass the Democrats and undermine the presidential election process at a critical time. A third was to test U.S. security measures."[10]

Non-State Violent Extremists

Beginning in 2006, there has been a rise in the use of cyberspace from extremist and terrorist organizations.[11] There appears to be much literature written about how non-state violent extremist are using the cyberspace domain. Of interest is what Joseph Nye writes about how cyberspace is easily accessed by non-state actors, "The low price of entry, anonymity, and asymmetries in vulnerability means that smaller actors have more capacity to exercise hard and soft power in cyberspace than in many more traditional domains of world politics."[12] The ease of access into this new man-made domain has shifted the balance of power towards non-state actors especially as the nature of warfare has changed over the past fifty years.

[8] Jarno Limnéll, "The West Must Respond to Russia´s Increasing Cyber Aggression." *Defense One*, June 15, 2016.

[9] Brian Ross, "'Beyond a Reasonable Doubt,' Russians Hacked DNC" *ABC News*, July 25, 2016. http://abcnews.go.com/International/reasonable-doubt-russians-hacked-dnc-analyst/story?id=40863292 (accessed 15 October 2016).

[10] Ruben Johnson, "US has fallen dangerously behind Russia in cyber warfare." *Business Insider*. July 27, 2016), http://www.businessinsider.com/us-behind-russia-cyber-warfare-2016-7 (accessed 14 Oct 2016).

[11] Franklin D. Kramer, *Cyberpower and National Security*, 565.

[12] Joseph Nye, "Cyber Power" Cambridge, MA: President and Fellows of Harvard College, May 2010. http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA522626 (accessed 15 Oct 2016).

Hacktivists

Hacktivists pose the most unconventional threat to the DoDIN. The lure of accessing government secrets and uncovering government conspiracies can be very tempting to these cyber adversaries. Anonymous is likely the most widely known group of hacktivists, but most individual hacktivists are not as easy to identify. Hacktivism becomes extremely dangerous for the DoD when these skilled cyberspace players are supported by nation states with nefarious agendas. It is also dangerous to U.S. allied partners. In 1998, during the Kosovo Campaign, the Serb Black Hand Group (Crna Ruka) conducted Denial of Service attacks against computers owned by the North Atlantic Treaty Organization (NATO).[13] Activities such as these highlight the need to adjust national and defense cyber policy to include trusted allies.

Insider threats

Insider threats are the most dangerous cyber adversary faced by the Department of Defense. "Whether malicious insiders are committing espionage, making a political statement, or expressing personal disgruntlement, the consequences for DOD, and national security, can be devastating."[14] There are two ways in which members within an organization can create damage. First, insider threats can expose critical or sensitive data to the outside world. Insiders who expose information can impose a significant amount of damage on all levels of national security. For example, PFC Bradley Manning was able to provide classified information to WikiLeaks and damaged the United States

[13] Dorothy Denning, "The Rise of Hacktivism" *Georgetown Journal of International Affairs*. (September 8, 2015) http://journal.georgetown.edu/the-rise-of-hacktivism/ (accessed 15 Oct 2016).
[14] JP 3-12, IV-10.

efforts and credibility. Second, insider threats can damage the network through physical or virtual sabotage. As JP 3-12 makes clear, "because insiders have a trusted relationship with access to the DoDIN, any malicious activity can be much more far reaching than external entities attempting to gain access."[15] The insider threat is more than individuals with a nefarious agenda. The insider threat is also users who are ignorant of cybersecurity policy or lackadaisical about its application. It is imperative that these users are properly educated and embrace a mindset of cybersecurity.

[15] JP 3-12, IV-10.

BIBLIOGRAPHY

Alexander, Keith. "Statement for the Record, Commander, US Cyber Command" *House Armed Services Committee Statement*. Washington, DC. 23 September 2010. http://www.defense.gov/home/features/2010/0410_cybersec/docs/USCC%20Command%20Posture%20Statement_HASC_22SEP10_FINAL%20_OMB%20Approved_.pdf (accessed February 19, 2017).

Arreddy, James T., Paul Maozu, and Danny Yadron. "*Military Organization 3PLA Is Tasked With Monitoring World-Wide Electronic Information*." Wall Street Journal. 7 July 2014. http://www.wsj.com/articles/chinas-spy-agency-has-broad-reach-1404781324 (accessed October 12, 2016).

Bush, George W. National Security Presidential Directive #54 / Homeland Security Presidential Directive #23: *Cyber Security*. Washington, DC. White House Memorandum. January 8, 2008.

____. *National Strategy to Secure Cyberspace*. Washington DC: Government Printing Office. February 2003.

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

Clausewitz, Carl. *On War*. New York: Everyman's Library, 1993.

Clinton, William J. *National Security Strategy*. Washington DC: Government Printing Office. February 1995.

Conrad, Eric, Seth Misenar, and Joshua Feldman. *CISSP Study Guide*. Waltham: Syngress Publications, 2012.

Corbett, Julian S. *Some Principles of Maritime Strategy*. London: Longmans, Green and Company, 1911.

Denning, Dorothy. "The Rise of Hacktivism." *Georgetown Journal of International Affairs*. (September 8, 2015) http://journal.georgetown.edu/the-rise-of-hacktivism/ (accessed 15 Oct 2016).

Defense Information Security Agency. "Information Assurance (IA) Analysis." https://www.disa.mil/Cybersecurity/Analytics/IA-Analysis (accessed 15 October 2016).

_____. "Command Cyber Operational Readiness Inspection (CCORI) Program: Mission Impact Analysis Process Guide." Fort Meade, MD. 24 September 2016.

_____. "Command Cyber Readiness Inspection (CCRI) Program." https://disa.deps.mil/ext/cop/FS-CCRI/inspections/SitePages/Command_Cyber_Readiness_Inspection_(CCRI)_Program.aspx (accessed 15 October 2016).

_____. *Defense Information Security Agency Strategic Plan 2015-2020.* http://www.disa.mil/~/media/Files/DISA/About/Strategic-Plan.pdf (accessed 13 February 2017).

_____. *DOD Enterprise Email.* http://www.disa.mil/enterprise-services/applications/dod-enterprise-email (accessed 13 February 2017).

_____. "Our Work / DISA 101." http://www.disa.mil/About/Our-Work (accessed 13 February 2017).

Douhet, Giulio. *The Command of the Air*. ed. Joseph Patrick Harahan and Richard H. Kohn. Tuscaloosa: University of Alabama Press, 2009.

Downes, Larry, and Chunka Mui. *Unleashing the Killer App.* Boston: Harvard Business School Press, 1998.

Erwin, Sandra I. "Defense CIO: Cybersecurity Improving But Innovation Lags," *National Defense Magazine.* August 8, 2016. http://www.nationaldefensemagazine.org/blog/Lists/Posts/Post.aspx?ID=2268 (accessed 9 August 2016).

Fischler, Jacob. "Pentagon Solicits $475M Omnibus Cybersecurity Contract" *Law360.* May 1, 2015. https://www.law360.com/articles/650741/pentagon-solicits-475m-omnibus-cybersecurity-contract (accessed 12 December 2016).

Garamone, Jim. "*Dunford Details Implications of Today's Threats on Tomorrow's Strategy.*" DoD News, Defense Media Activity. Published Aug. 23, 2016. NDU President's Lecture Series.

https://www.defense.gov/News/Article/Article/923685/dunford-details-implications-of-todays-threats-on-tomorrows-strategy/ (accessed 24 August 2016).

Gartner Corporation. "*Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent From 2015*" Press Release. November 10, 2015. http://www.gartner.com/newsroom/id/3165317 (accessed 29 December 2016).

Heeley, Melanie, and Leela Damodaran. *"Digital Inclusion: a review of international policy and practice."* Loughborough, UK: Loughborough University, 2009.

Jasper, Scott. *Conflict and Cooperation in the Global Commons: A Comprehensive Approach for International Security*. Washington, DC: Georgetown University Press, 2012.

Johnson, Ruben. "US has fallen dangerously behind Russia in cyber warfare." *Business Insider* (July 27, 2016) http://www.businessinsider.com/us-behind-russia-cyber-warfare-2016-7 (accessed 14 Oct 2016).

Kramer, Franklin D. *Cyberpower and National Security*. Washington, DC: National Defense University Press, 2009.

Lee, David. "Bureau 121: How Good are Kim Jong-Un's Elite Hackers." *BBC News*. 29 May 2015. http://www.bbc.com/news/technology-32925503 (accessed October 11, 2016).

Leiner, Barry, Vinton G. Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts, and Stephen Wolff, "A Brief History of the Internet" *ACM SIGCOMM Computer Communication Review* Vol. 39 (Oct 2009): 22-31.

Libiki, Martin C. *Cyberdeterence and Cyberwar*. Arlington, VA: RAND Corporation, 2009.

Limnéll, Jarno. "The West Must Respond to Russia´s Increasing Cyber Aggression." *Defense One*, June 15, 2016. http://www.defenseone.com/ideas/2016/06/west-must-respond-russias-increasing-cyber-aggression/129090/ (accessed 14 Oct 2016).

Lubold, Gordon and Paletta, Damian. "Pentagon Sizing Up Email Hack of Its Brass." *Wall Street Journal*. August 7, 2015. http://www.wsj.com/articles/pentagon-sizing-up-email-hack-of-its-brass-1438989404 (accessed 18 August 2016).

Lyngaas, Sean. "Pentagon IG to Audit Cyber Readiness" *Federal Computer Week*, February 3, 2016. https://fcw.com/articles/2016/02/03/pentagon-cyber-oversight.aspx (accessed 21 December 2016).

Mao Tse Tung. *On Guerilla Warfare*, Translated by Samuel B. Griffith II. Champaign, Il: University of Illinois Press, 2000.

_____. *Selected Works of Mao Tse Tung, Vol II*. Peking: Foreign Language Press, 1965.

Napolitano, Janet. *Blueprint for a Secure Cyber Future*. Department of Homeland Security. Washington, DC, November 2011.

Novosti, Ria. "Military Creating Cyber Warfare Branch." *The Moscow Times*. August 21, 2013. https://themoscowtimes.com/news/military-creating-cyber-warfare-branch-26921 (accessed 14 October 2016).

Nye, Joseph S. Jr. *Cyber Power*. Cambridge, MA: President and Fellows of Harvard College, May 2010. http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA522626 (accessed 15 Oct 2016).

Obama, Barrack. *National Security Strategy*. Washington DC: Government Printing Office. February 2015.

_____. "Remarks by the President at the Cybersecurity and Consumer Protection Summit." Washington DC: The White House Office of the Press Secretary. February 13, 2015. https://obamawhitehouse.archives.gov/the-press-office/2015/02/13/remarks-president-cybersecurity-and-consumer-protection-summit (accessed 19 February 2017).

Ottis, Rain, and Peteer Lorents, *Cyberspace: Definition and Implications*. In Proceedings of the 5th International Conference on Information Warfare and Security. Academic Publishing Limited. Dayton. April 2010.

Platov, Vladimir. "Iran and Modern Cyber Warfare." *New Eastern Outlook*. December 22, 2014. http://journal-neo.org/2014/12/22/rus-iran-i-kibervojny/ (accessed October 12, 2016).

Register, Robert. "Command Cyber Readiness Inspection: Know Your Role." *North West Florida Daily News*. August 14, 2015. http://www.nwfdailynews.com/article/20150814/news/150819520 (accessed 18 September 2016).

Rid, Thomas. *Cyber War Will Not Take Place.* London: Oxford University Press, 2013.

Ross, Brian, et al.. "'Beyond a Reasonable Doubt,' Russians Hacked DNC, Analyst Says." *ABC News*. Jul 25, 2016. http://abcnews.go.com/International/reasonable-doubt-russians-hacked-dnc-analyst/story?id=40863292 (accessed 15 October 2016).

Ryan, Johnny. *A History of the Internet and the Digital Future.* United Kingdom: Reaktion Books, 2010.

Scott, James. *Cerber & KeRanger: The Latest Weaponized Encryption.* Washington, DC: Institute for Critical Infrastructure Technology. 8 March 2016. http://icitech.org/cerberkeranger/ (accessed 20 Feb 2017).

SecureStrux. "CCRI and SAV Whitepaper" http://www.securestrux.com/wp-content/uploads/2016/05/CCRI-and-SAV-White-Paper.pdf (accessed 20 August 2016).

Sheldon, John B. "State of the Art: Attackers and Targets in Cyberspace." *Journal of Military Strategic Studies.* Volume 14, Issue 2. 2012.

_____. "Toward a Theory of Cyber Power: Strategic Purpose in Peace and War" In *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, edited by Derek S. Reveron, 207-224. Washington, DC: Georgetown University Press, 2012.

Sun Tzu. *The Art of War.* Translated by Samuel B. Griffith. London: Oxford University Press, 1963.

United States Air Force, Tyndall Air Force Base. "Command Cyber Readiness Inspection" http://www.tyndall.af.mil/AboutUs/CommandCyberReadinessInspection.aspx (accessed 22 August 2016).

U.S. Congress. *Cybersecurity Act of 2015.* 114th Congress. Washington, DC. December 16, 2015.

U.S. Department of Defense. *The Department of Defense Cyber Strategy*. Washington, DC. April 2015.

U.S. Department of Defense. DoD Directive 5144.02: *Department of Defense Chief Information Officer (DOD CIO).* Washington, DC. November 21, 2014.

U.S. Department of Defense. Chairman of the Joint Chiefs of Staff Instruction 6510.01F: *Information Assurance (IA) and Computer Network Defense (CND).* Washington, DC. February 9, 2011 (Directive Current as of 9 Jun 2015).

_____. CJCSI 6211.02C: *Defense Information Services Network (DISN): Policy and Responsibilities.* Washington, DC. July 9, 2008.

U.S. Department of Defense Assistant Secretary of Defense for Networks and Information Integration ((ASD(NII))/Chief Information Officer. *DoD Cybersecurity Discipline Implementation Plan,* October 2015 (amended February 2016) http://dodcio.defense.gov/Portals/0/Documents/Cyber/CyberDis-ImpPlan.pdf (accessed August 20, 2016).

_____. DODI 8500.01, *Cybersecurity.* Washington, DC. March 14, 2014 http://www.dtic.mil/whs/directives/corres/pdf/850001_2014.pdf. (accessed November 27, 2016).

U.S. Department of Defense. Inspector General Memorandum: *Audit of Corrective Actions on Command Cyber Readiness Inspection Deficiencies.* Washington, DC. February 2, 2016.

_____. *DHS Cybersecurity Webpage*. https://www.dhs.gov/einstein (accessed 27 November 2016).

_____. *Protecting Critical Infrastructure.* https://www.dhs.gov/topic/protecting-critical-infrastructure (accessed 13 February 2017).

U.S. Department of Homeland Security. *DHS Releases Strategic Principles For Securing The Internet Of Things* https://www.dhs.gov/news/2016/11/15/dhs-releases-strategic-principles-securing-Internet-things (accessed 19 December 2016).

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

______. *Cyberspace Operations*, Joint Publication 3-12(R). Washington, DC. February 12, 2013.

______. *Joint Operating Environment 2035: The Joint Force in a Contested and Disordered World.* Washington, DC. July 14, 2016.

______. *National Military Strategy for Cyberspace Operations (U).* Washington, DC. December 2006.

U.S. Navy Cyber Forces. *Commander's Cyber Security and Information Assurance Handbook.* Revision 2. Norfolk, VA. 26 February 2013.

U.S. Navy CYBERFOR Public Affairs Office. "USS Abraham Lincoln Passes First Underway Cyber Inspection." *InfoDomain: The Professional Magazine of Navy Cyber Forces.* Fall 2011.

USSOUTHCOM Public Affairs Office and J6. "SOUTHCOM Achieves Cyber Readiness Success." USSOUTHCOM. https://extranet.southcom.mil/Apps/Home/(S(3w3rfjt3yt4yogx2msuf2xk1))/Spotlight/News/frm_Read.aspx?ID=375 (accessed 18 September 2016).

USSTRATCOM. "USCYBERCOM Fact Sheet." USSTRATCOM. https://www.stratcom.mil/factsheets/2/Cyber_Command/ (accessed 15 October 2016).

Williams, Brett T. "The Joint Force Commander's Guide to Cyberspace Operations." *Joint Force Quarterly* 73, 2d Quarter 2014 (1 April 2014): 12-19. http://ndupress.ndu.edu/Media/News/News-Article-View/Article/577499/jfq-73-the-joint-force-commanders-guide-to-cyberspace-operations/ (accessed August 22, 2016).

White House Press Office. *Cybersecurity National Action Plan Fact Sheet.* Washington, D.C. February 2016. https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan (Accessed 29 Aug 2016).

Yarger, Harry R. *Strategic Theory for the 21st Century: The Little Book on Big Strategy.* Carlisle PA: U.S. Army War College Strategic Studies Institute, 2006.

VITA

Lieutenant Colonel Drew Ferguson (USA) is currently attending the National Defense University's Joint Advanced Warfighting School. He graduated from Abilene Christian University and awarded a branch-detailed commission in the Infantry in 1995. He was a platoon leader in the 82nd Airborne Division and later the 35th Signal Brigade (Airborne). He deployed to El Salvador with the 46th Corps Support Group (Airborne) for Operation Fuerte Apoyo (Strong Support) as part of JTF-Aguila. His previous assignments include S-6 for 2-9 Infantry Regiment; S-6 for 2-82 Field Artillery Battalion; and Commander of Delta Company, 13th Signal Battalion. He has three combat deployments to include OIF 2, OIF 06-08, and OIF 9 all as part of the 1st Cavalry Division (Multi-National Division-Baghdad) G-6 staff. His other staff assignments include the Army CIO/G-6, the U.S. Army Cyber Center of Excellence Capabilities Development Integration Directorate, and the Brigade S-3 for 93d Signal Brigade. He was the Battalion Commander of the 442d Signal Battalion in Fort Gordon, GA. LTC Ferguson holds a Bachelor of Arts in Human Communication from ACU and a Masters in Policy Management from Georgetown University. He is married with two children.