IGNORING A REVOLUTION IN MILITARY AFFAIRS:
THE NEED TO CREATE A SEPARATE BRANCH OF
THE ARMED FORCES FOR CYBER WARFARE

A thesis presented to the Faculty of the U.S. Army
Command and General Staff College in partial
fulfillment of the requirements for the
degree

MASTER OF MILITARY ART AND SCIENCE
General Studies

by

ANTHONY S. CARISTI, MAJOR, USA
B.A., Ball State University, Muncie, Indiana, 2006

Fort Leavenworth, Kansas
2017

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

1. REPORT DATE *(DD-MM-YYYY)* 9-06-2017	**2. REPORT TYPE** Master's Thesis	**3. DATES COVERED** *(From - To)* AUG 2016 – JUN 2017

4. TITLE AND SUBTITLE Ignoring a Revolution in Military Affairs: The need to Create a Separate Branch of the Armed Forces for Cyber Warfare	**5a. CONTRACT NUMBER** **5b. GRANT NUMBER** **5c. PROGRAM ELEMENT NUMBER**
6. AUTHOR(S) MAJ Anthony S. Caristi	**5d. PROJECT NUMBER** **5e. TASK NUMBER** **5f. WORK UNIT NUMBER**
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) U.S. Army Command and General Staff College ATTN: ATZL-SWD-GD Fort Leavenworth, KS 66027-2301	**8. PERFORMING ORG REPORT NUMBER**
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)	**10. SPONSOR/MONITOR'S ACRONYM(S)** **11. SPONSOR/MONITOR'S REPORT NUMBER(S)**

12. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for Public Release; Distribution is Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

This study, using historical data and precedence, presents information that indicates the U.S. Government is ineffective at defending its own cyber-network. Information provided in this study continues to argue that, similar to the creation of the Air Force from the existing Army Air Corps in the National Security Act of 1947, should create a new branch of the armed forces for cyber warfare. Throughout this study there are multiple examples of major breaches of secured network by nations as well as third party actors. The root of the government's inability to defend against such attacks comes from the inability to recruit and retain the most skilled "hackers" in the U.S. population. Discussed in this research is the reasoning behind the U.S.'s inability to attract the most skilled cyber professionals due to the current rigid military standards seen on existing branches of the armed forces, as well as an inability to compete monetarily against the private sector. This paper argues that with the creation of a new Cyber Force, the aforementioned issues will dissolve.

15. SUBJECT TERMS
Cyber Warefare, Hacker, Cyber Attack, DoD, Netowrk, Russia, China, Israel, DOTMLPF-P, National Security Act of 1947, Revolution in Military Affairs

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT (U)	**b. ABSTRACT** (U)	**c. THIS PAGE** (U)	(U)	68	**19b. PHONE NUMBER** *(include area code)*

MASTER OF MILITARY ART AND SCIENCE

THESIS APPROVAL PAGE

Name of Candidate: Major Anthony S. Caristi

Thesis Title: Ignoring a Revolution in Military Affairs: The need to Create a Separate Branch of the Armed Forces for Cyber Warfare

Approved by:

_______________________________________, Thesis Committee Chair
Eric M. Morrison, Ph.D.

_______________________________________, Member
LTC John E. Price, M.A.

_______________________________________, Member
Clay Easterling, M.A.

Accepted this 9th day of June 2017 by:

_______________________________________, Director, Graduate Degree Programs
Prisco R. Hernandez, Ph.D.

The opinions and conclusions expressed herein are those of the student author and do not necessarily represent the views of the U.S. Army Command and General Staff College or any other governmental agency. (References to this study should include the foregoing statement.)

ABSTRACT

IGNORING A REVOLUTION IN MILITARY AFFAIRS: THE NEED TO CREATE A SEPARATE BRANCH OF THE ARMED FORCES FOR CYBER WARFARE, by Major Anthony S. Caristi, 68 pages.

This study, using historical data and precedence, presents information that indicates the U.S. Government is ineffective at defending its own cyber-network. Information provided in this study continues to argue that, similar to the creation of the Air Force from the existing Army Air Corps in the National Security Act of 1947, should create a new branch of the armed forces for cyber warfare. Throughout this study there are multiple examples of major breaches of secured network by nations as well as third party actors. The root of the government's inability to defend against such attacks comes from the inability to recruit and retain the most skilled "hackers" in the U.S. population. Discussed in this research is the reasoning behind the U.S.'s inability to attract the most skilled cyber professionals due to the current rigid military standards seen on existing branches of the armed forces, as well as an inability to compete monetarily against the private sector. This paper argues that with the creation of a new Cyber Force, the aforementioned issues will dissolve.

ACKNOWLEDGMENTS

To begin, I would like to thank Dr. Eric Morrison, LTC John Price, and Mr. Clay Easterling for the guidance, insight, assistance, and time. Without them, this project would have never been possible. Gentlemen, thank you for maintaining interest in this topic long enough to see this through and for setting me up for success on more than one occasion. Additionally, thank you for dealing with dozens of emails attempting to coordinate and re-coordinate the defense. I only hope that this finished product can benefit others as much as I benefitted from you.

I would also like to thank the many family and friends who sent me articles and information pertaining to my research topic. Those articles kept the fires going when it seemed that I had found all I could find that was worth writing about.

Lastly, but definitely not least, I would like to thank my wife, Meg and the boys, Luca and Matteo. Through their patience alone was I able to continue to work through this project. Additional thanks are deserved to Meg when she “took one for the team” and read the paper when I thought I was done, even if she did tell me places I needed to write more. I love you, Meg and I couldn’t ask for a better partner.

TABLE OF CONTENTS

Page

MASTER OF MILITARY ART AND SCIENCE THESIS APPROVAL PAGE iii

ABSTRACT iv

ACKNOWLEDGMENTS v

TABLE OF CONTENTS vi

ACRONYMS viii

ILLUSTRATIONS ix

TABLES x

CHAPTER 1 INTRODUCTION 1

The Intangible Domain 1
Models 5
Problem 6
Limitations 9
Assumptions 10
Research Questions 10
Definitions 11
Significance of Study 14

CHAPTER 2 LITERATURE REVIEW 15

The National Security Act of 1947 15
Network Breaches 18
Talent Acquisition and Management 19
Summary 22

CHAPTER 3 RESEARCH METHODOLOGY 24

Doctrine 24
Organization 25
Training 25
Material 27
Leadership 28
Personnel 29
Facilities 30
Policy 31

CHAPTER 4 ANALYSIS 34

Background 34
Changes 36
Threats 37
Summary 44

CHAPTER 5 CONCLUSIONS AND RECOMMENDATIONS 45

Introduction 45
Summary of Findings 45
Interpretation of Information 47
A Way Forward 47
United States Cyber Military Academy at Silicon Valley 48
Broader Implications 51

BIBLIOGRAPHY 53

ACRONYMS

DoD	Department of Defense
DOTMLPF-P	Doctrine, Organization, Training, Material, Leadership, Personnel, Facilities-Policy
GAO	Government Accountability Office
IS	Islamic State
IT	Information and Technology
M.I.T.	Massachusetts Institute of Technology
OPM	Office of Personnel Management
PII	Personally Identifiable Information
U.S.	United States
USCYBERCOM	United States Cyber Command

ILLUSTRATIONS

Page

Figure 1. Incidents Reported by Federal Agencies, Fiscal Years 2006 through 2015 41

TABLES

Page

Table 1. Medical Services Bonus and Specialty Pay 28

Table 2. Projected Trend of Attacks on Government Networks Based off Current Trends 42

CHAPTER 1

INTRODUCTION

> True preparedness now means preparedness not alone in armaments and numbers of men, but preparedness in organization also. It means establishing in peacetime the kind of military organization which will be able to meet the test of sudden attack quickly and without having to improvise radical readjustment in structure and habits.
>
> — President Harry S. Truman, December 19, 1945,
> Special Message to the Congress

The Intangible Domain

In our world, there are enemy nation-states, activists, and hostile non-state actors that wish to do harm to the United States. All three of these organizations are utilizing the newest way to attack their targets; cyber-attacks. A cyber-attack can consist of identity and monetary theft, degrading or destroying of city power grids, illegal collection of intelligence, and even control of a country's nuclear weapon systems, just to name a few.[1] In essence, cyber-attacks are the newest and most effective method of espionage. The internet is so saturated with cyber-attackers that a researcher bought a server and put it online with the guise of a wireless toaster. Within 41 minutes, this "toaster" had been hacked.[2]

[1] Ted Koppel, *Lights Out* (New York: Penguin Random House, 2015).

[2] Andrew McGill, "We Built a Fake Web Toaster, and It Was Hacked in an Hour," *The Atlatic*, October 28, 2016, accessed October 29, 2016, https://www.theatlantic.com/technology/archive/2016/10/we-built-a-fake-web-toaster-and-it-was-hacked-in-an-hour/505571/.

To complicate matters, cyber-capable nations and “hackers” have the ability to make large amounts of money off the internet “black market.” A study conducted by the Rand Corporation found that illegal cyber activity in relation to the online black market is growing at an exponential rate and it will soon be “more profitable than the illegal drug trade.”[3] On this black market buyers can purchase government secrets stolen by hackers, or the code to do so themselves. Buyers can even purchase the services of hackers to conduct espionage on city infrastructure.[4]

These black markets are located all over the Dark Web. The Dark Web is just like the internet that any person can use on any given day, however it requires a piece of additional software downloaded from the regular internet. Developed by the United States (U.S.) Navy, Tor software allows your Internet Protocol (also known as IP, a unique identification number used to locate a user from any internet connected device) number to be hidden so that a user can navigate the Dark Web without being tracked by the authorities.[5] An individual transfers actual money from a bank account in to BitCoins which are digital forms of currency and completely legal. Once in the Dark Web, purchases are made by these BitCoins and are untraceable and can be used to purchase weapons, identities, drugs, trafficking of humans, and hacking software.[6]

[3] Lillian Ablon, Martin C. Libicki, and Andrea A. Golay, *Markets for Cybercrime Tools and Stolen Data* (Santa Monica, CA: Rand Corporation, 2014).

[4] Ibid.

[5] Brandon Gregg, “Online Black Markets and How They Work,” TechWorld, May 1, 2012, accessed April 1, 2017, http://www.techworld.com/security/online-black-markets-how-they-work-3355031/.

[6] Ibid.

The United States operates daily in an environment that is comprised of, at its basic level, ones and zeros, but affects the lives of billions. Since the early eighties government agencies of the world have engaged in operations using cyber platforms as their weapons.[7] The Secretary of Defense directs Cyber Operations in concert with National Intelligence Agencies and Department of Defense (DoD) organizations to conduct cyberspace defense of the network, cyberspace operational preparation of the environment, cyberspace intelligence, surveillance and reconnaissance, and cyberspace attack.[8] In 2009, as a result of an ever-growing threat, Secretary of Defense Robert Gates directed Strategic Command to create a sub-unified command which would be called United States Cyber Command (USCYBERCOM).[9] In December 2016, Congress signed legislation that if signed by the President, would elevate USCYBERCOM from a sub-unified command to a unified command.[10]

The USCYBERCOM's mission is to "plan, coordinate, integrate, synchronize and conduct activities to: direct the operations and defense of specified Department of Defense information networks and; prepare to, and when directed, conduct full spectrum

[7] Isaac R. Porche III, Jerry M Sollinger, and Shawn McKay, *A Cyberworm That Knows No Boundaries* (Santa Monica, CA: RAND, 2011).

[8] Brett T. Williams, "The Joint Force Commander's Guide to Cyberspace Operations," *Joint Forces Quarterly* 73 (2nd Quarter 2014): 12-19.

[9] U.S. Strategic Command, "Fact Sheet," March 2015, accessed November 5, 2016, https://www.stratcom.mil/factsheets/2/Cyber_Command/.

[10] Mark Pomerleau, "Congress Set to Elevate CYBERCOM to Unified Combatant Command," C4ISR Net, December 1, 2016, accessed December 12, 2016, http://www.c4isrnet.com/articles/congress-authorizes-elevating-cybercom-to-unified-combatant-command.

military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries."[11]

The USCYBERCOM is composed of service members, contractors, and DoD civilians from Army (ARCYBER), Navy (FLTCYBER), Air Force (AFCYBER), Marines (MARFORCYBER), and the 4th Estate,[12] USCYBERCOM headquarters is located at Ft. Meade, Maryland. It conducts cyber operations through Department of Defense Information Network Operations, Defensive Cyberspace Operations, and Offensive Cyberspace Operations.[13]

This complex environment has become a key component in operations for other nations as seen through recent events. During recent Russian aggression in Ukraine, the Russian Government, through use of their Cyber Force, nicknamed the Dukes,[14] shut down power through three distribution companies and then prevented Ukrainian citizens from reporting the outages by spamming the call centers.[15]

[11] U.S. Strategic Command, "Fact Sheet."

[12] OSD, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Defense Agencies, the DoD Field Activities, and all other organizational entities in the DoD that are not in the Military Departments or the Combatant Commands.

[13] Williams, 12-19.

[14] F-Secure, "The Dukes: 7 Years of Russian Cyberespionage," Whitepaper, September 17, 2015, accessed March 29, 2017, https://labsblog.f-secure.com/2015/09/17/the-dukes-7-years-of-russian-cyber-espionage/.

[15] Pavel Polityuk, "Ukraine Sees Russian Hand in Cyber Attacks on Power Grid," *Reuters*, February 12, 2016, accessed March 9, 2017, http://www.reuters.com/article/us-ukraine-cybersecurity-idUSKCN0VL18E.

In October 2016, an unconfirmed entity attacked Dyn, a New Hampshire-based network company that provides services to streamline websites.[16] All at once, thousands of internet-connected devices sent large amounts of data at the system which overloaded the network and consequently shut down hundreds of websites to include the New York Times, Twitter, and Amazon. While this attack focused on the American economy, future attacks could be focused on defense assets.[17]

Models

While the U.S. is still attempting to determine how to best construct their cyber community, other countries have recognized the looming threat that a weak Cyber capability poses and have responded appropriately. The Norwegian Defense Force established a Cyber Defense Force in 2012 which is a separate branch from their Armed Forces.[18] "The Norwegian Cyber Defense Force supports the Norwegian Armed Forces at home and abroad with the establishment, operation, further development and protection of their communications. The Cyber Defense Force also has an important role to play in the development of Network Based Defense."[19]

[16] Patrick Tucker and Caroline Houck, "Someone Weaponized the Internet of Things," Defense One, October 22, 2016, accessed October 23, 2016, http://www.defenseone.com/threats/2016/10/someone-weaponized-internet-things/132553/.

[17] Ibid.

[18] Norwegian Ministry of Defense, "Norwegian Defence 2013: Facts and Figures" (Information Report, Norwegian Ministry of Defense, Oslo, 2013), accessed September 25, 2016, https://forsvaret.no/en/organisation.

[19] Ibid.

The Israeli Defense Force requires conscription of their citizens and identifies at an early age, high school or even earlier, those with talent in the computer sciences. Upon graduation from high school, computer-proficient teenagers are selected for an elite cyber force and sent to intense cyber training.[20] While assigned to this organization, these cyber warriors are encouraged to act independently with little oversight to encourage creativity and problem solving as which results in highly capable hackers as well as internally developed software.

Problem

The DoD is ineffective in its defense of the nation's critical information and technology (IT) systems from both nations and independent actor threats as shown in the June 2015 Office of Personnel Management (OPM) breach that compromised over 21 million Americans' Personally Identifiable Information (PII).[21] In fact, a report from the Government Accountability Office (GAO) states that in Fiscal Year 2006 there were 5,503 information security incidents involving government systems.[22] Since then, the amount has steadily risen to the last report for Fiscal Year 2014 containing 67,168 incidents; an increase of 1,121 percent in eight years.[23]

[20] Richard Behar, "Inside Israel's Secret Startup Machine," *Forbes*, May 31, 2016, accessed January 1, 2017, https://www.forbes.com/sites/richardbehar/2016/05/11/inside-israels-secret-startup-machine/#1a5198de1a51.

[21] Gregory C. Wilshusen, *Cyber Threats and Data Breaches Illustrate Need for Stronger Controls across Federal Agencies* (Washington, DC: Government Accountability Office, 2015).

[22] Ibid.

[23] Ibid.

Members of the DoD recognize the deficiencies and are trying to improve capabilities. In March 2016, the Pentagon offered bounties to pre-approved, DoD-employed, amateur hackers to find vulnerabilities in the DoD network and offering a cash reward to individuals who find issues.[24] The Army published an additional "bug bounty" in November that same year citing similar concerns. Secretary of the Army Eric Fanning went as far to say, "We're not agile enough to keep up with a number of things that are happening in the tech world and in other places outside the Department of Defense."[25]

The DoD's ineffectiveness stems from the inability to attract and maintain the right skills and talent. USCYBERCOM is ineffective in its ability to recruit and retain quality talent due to the existing requirements for entry into the military and the gap in compensation provided by the private sector. The DoD published a comprehensive breakdown of the personnel make-up of USCYBERCOM with information through July, 2016.[26] As of the aforementioned date, USCYBERCOM consists of just over 36.5 thousand people and out of that, 34 percent of that force is comprised of Army Soldiers.[27]

[24] Andy Greenberg, "Pentagon Launches the Feds' First 'Bug Bounty' for Hackers," Wired, March 2, 2016, accessed April 1, 2017, https://www.wired.com/2016/03/pentagon-launches-feds-first-bug-bounty-hackers/.

[25] Lily Hay Newman, "The US Military Launches 'Hack the Army,' Its Most Ambitious Bug Bounty Yet," Wired, November 11, 2016, accessed March 28, 2017, https://www.wired.com/2016/11/us-military-launches-hack-army-ambitious-bug-bounty-yet/.

[26] Defense Civilian Personnel Advisory System, "Cyber One Stop," accessed August 30, 2016, https://www.cpms.osd.mil/Subpage/CyberOneStop/CyberHome.

[27] Ibid.

The next closest service is the Navy comprising 26 percent of the force.[28] As of 28 June 2016, the Army published its list of Military Occupational Specialty and Area of Concentration shortages listing Cyber enlisted strengths at 60.8 percent filled and officer cyber Area of Concentration shortages at 69.7 percent filled.[29]

Of the current USCYBERCOM force, 29 percent are eligible to retire in the next five years.[30] The largest percentage of USCYBERCOM personnel are part of the "Baby Boomer" generation ranging in age from 51 to 57 with the smallest percentage of personnel from the "Millennial" generation; arguably the group that is most capable of supporting the USCYBERCOM mission.[31] Over the past five years, USCYBERCOM has lost over 7,000 personnel to either retirement, transfers, resignations, or other losses.[32]

Looking at the numbers previously mentioned it is easy to see that USCYBERCOM not only has issues recruiting the talent it needs to fight the cyber war, but is also hemorrhaging talent. Those that work in the civilian sector within the cyber community believe that the DoD is hamstringing itself because of fitness, weight and drug standards on the military side of the house. Former cyber chief for the Department of Homeland Security, Mark Weatherford said "There are a lot of really smart, scary cybersecurity professionals out there who happen to have pink hair and tattoos, but you

[28] Ibid.

[29] Department of Army G1, *Department of the Army Manning Guidance* (Washington, DC: Government Printing Office, June 2016).

[30] Defense Civilian Personnel Advisory System.

[31] Ibid.

[32] Ibid.

won't find them at DHS, which also is averse to hiring cyber experts without a college degree."[33] In the 4th Estate, the drain is caused by pay discrepancies against the civilian sector.[34] National Security Agency human resource technical director stated that during exit interviews cyber agents state "I'm leaving to double my salary."[35]

Limitations

Title 10 and Title 50 are the documents that govern Cyber Operations in both the signal and intelligence communities as well as the DoD.[36] While these documents support each other, they are not mutually exclusive. Both Titles require each other to capture the whole picture of Cyber Security and Cyber Warfare. The current commander of USCYBERCOM is a Navy Admiral who oversees the National Security Agency's cyber operations as well as the DoD. Because of the compartmentalized nature of operations on both sides of USCYBERCOM, there are limitations and constraints on what information can be shared with the other side of the command.

This paper, while discussing a topic which is relatively classified in nature, will not discuss capabilities. This paper's focus will remain on force management within the

[33] Doina Chiacu, "Homeland Security Struggles to Tempt, Retain Cyber Talent," *Reuters*, April 26, 2014, accessed March 28, 2017, http://www.reuters.com/article/us-usa-cybersecurity-dhs-idUSBREA3P05O20140426.

[34] Jack Moore, "In Fierce Battle for Cyber Talent, Even NSA Struggles to Keep Elites on Staff," NextGov, April 14, 2014, accessed March 28, 2017, https://www.benton.org/headlines/fierce-battle-cyber-talent-even-nsa-struggles-keep-elites-staff.

[35] Ibid.

[36] Andru E. Wall, "Demystifying the Title 10-Title 50 Debate" (Paper, Harvard Law School, 2011), accessed November 5, 2016, http://harvardnsj.org/wp-content/uploads/2012/01/Vol-3-Wall.pdf.

Cyber Force and the U.S. Government and the possible need for a restructuring based off organizational capabilities as well as the current inability to attract and maintain the top talent within the cyber community compared to peer nations and non-state actors.

Assumptions

If a new organization is created, it will be governed by both Titles 10 and 50, or a new Title will need to be created to allow a cyber force to operate independently of U.S. intelligence agency integration.

While China has never openly taken responsibility for the 2015 cyber-attacks on OPM, China has been implicated by the U.S. Government and this thesis will continue that assumption.[37]

While Russia did not openly take responsibility for the cyber-attacks on Ukraine, Russia has been implicated by the U.S. Government and this thesis will continue that assumption.[38]

Research Questions

Primary research question: Should the DoD create a new service agency to defend the cyber domain similar to the creation of the Air Force in 1947?

Secondary research question: What should a new Cyber Service look like?

[37] Brendan J. Koerner, “Inside the Cyberattack That Shocked the US Government,” Wired, October 23, 2016, accessed March 26, 2017, https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/.

[38] Polityuk.

Definitions

The Department of Defense (DoD) defines Cyber Operations as actions that "enhance operational effectiveness and leverage various capabilities from physical domains to create effects, which may span multiple geographic combatant commanders' (GCCs') Areas of Responsibility (AORs)."[39] These effects can be obtained through three domains; the Cyber-Persona Layer, the Logical Network Layer, and the Physical Network Layer.[40]

Cyber-Persona Layer "is an individual's or groups' online identity(ies), holds important implications for joint forces in terms of positive target identification and affiliation, and activity attribution."[41]

Logical Network Layer "constitutes an abstraction of the physical network layer, depicting how nodes in the physical dimension of the information environment logically relate to one another to form entities in cyberspace. The logical network layer is the first point where the connection to the physical dimension of the information environment is lost."[42]

Physical Network Layer is defined as "the medium where the data travels. It includes wired (land and submarine cable) and wireless (radio, radio-relay, cellular,

[39] Department of Defense, Joint Publication (JP) 3-12 (R), *Doctrine for Joint Nuclear Operations* (Washington, DC: Government Printing Office, 2013).

[40] Ibid.

[41] Ibid.

[42] Ibid.

satellite) transmission means. It is the first point of reference for determining jurisdiction and application of authorities."[43]

The 4th Estate includes "28 Defense Department agencies that are not within combatant commands or military departments. These include the Defense Advanced Research Projects Agency, Defense Logistics Agency, Defense Security Cooperation Agency and the National Security Agency."[44]

Personally Identifiable Information is "information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc."[45]

Title 10 gives combatant commands statutory authorities and their commanders report directly to the Secretary of Defense.[46]

Title 50 establishes, defines and delineates authorities within the intelligence community, but it also clarifies that the Secretary of Defense controls those members of

[43] Ibid.

[44] June Edwards, "DoD's '4th Estate' Agencies to Procure Professional Services Via GSA's OASIS; Tiffany Hixson Comments," Executive Gov, June 17, 2016, accessed April 1, 2017, http://www.executivegov.com/2016/06/dods-4th-estate-agencies-to-procure-professional-services-via-gsas-oasis-contract-vehicles-tiffany-hixson-comments/.

[45] Clay Johnson III, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information," Whitehouse.Gov, May 22, 2007, accessed November 5, 2016, https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2007/m07-16.pdf.

[46] Wall.

the U.S. intelligence community, such as the National Security Agency and Defense Intelligence Agency, that are part of DoD.[47]

There are two major types of cyber operations that have affected the U.S. Government. The first is nation sponsored or government controlled where the country's government either conducts the cyber operations themselves or they pay a third party to do so.[48] The other side of cyber operations is conducted by "Hacktivists." A Hacktivist is a term that combines a hacker and an activist whose goal is to bring attention to their cause through disruptive cyber operations.[49] While Hacktivists do tend to have a political agenda, they are not typically tied to a nation-state as a basis for operations. There are other types of hacking incidents reported by the U.S. Government conducted by individuals who have an intent to gain monetarily but these are nominal and do not merit the restructuring of the DoD.

[47] Ibid.

[48] U.S. Congress, House, *Statement Admiral Michael S. Rogers, Commander, United States Cyber Command before the House Armed Services Committee, Subcommittee on Emerging Threats and Capabilities*, March 3, 2016, accessed March 28, 2017, http://docs.house.gov/meetings/AS/AS26/20160316/104553/HHRG-114-AS26-Wstate-RogersM-20160316.pdf.

[49] Dorothy Denning, "The Rise of Hactivism," *The Georgetown Journal of International Affairs* (September 8, 2015), accessed March 26, 2017, http://journal.georgetown.edu/the-rise-of-hacktivism/.

Significance of Study

While Admiral James Stavridis has made public statements professing the need for the U.S. to create its own cyber service,[50] this study is the first academic published research in this field to propose a new branch of the military to combat issues in the cyber domain, with the driving factor being the failure in talent recruitment and retention. Through research and recommendations in this thesis, changes could be made in the current organization that will lead to a more effective organization capable of defending against and defeating constant and complex enemy cyber-attacks. The information contained in this study should be sufficient in supporting the need to create a new branch of the armed forces that can support national strategy and defend critical network infrastructure and systems.

[50] David Weinstein and James Admiral Stavridis, "Time for a U.S. Cyber Force," *Proceedings Magazine* (January 2014), accessed March 29, 2017, https://www.usni.org/magazines/proceedings/2014-01/time-us-cyber-force.

CHAPTER 2

LITERATURE REVIEW

A study of DoD's structure for USCYBERCOM, ineffectiveness of protecting U.S. cyber networks and infrastructure, and its inability to attract and retain top cyber talent will provide a result in the display of the U.S.' cyber protection capabilities, or inability, and identify self-imposed limitations that prohibit the development of a talented and robust talent pool capable of defending and defeating cyber threats.

To provide a shared understanding through analysis, research will focus on how USCYBERCOM is organized, its leadership structure, and governing documents and how they draw parallels to the transition of the Army Air Corps to the Air Force. Research will also analyze USCYBERCOM's ineffectiveness in protecting the network and how its organization is a direct cause of it. Research will also be conducted on peer nations, as well as third party, non-state actors who have conducted cyber operations against the U.S. and its allies to provide insight in to the threat the U.S. faces as well as provide a framework for a successful independent cyber force. Finally, research will identify why the DoD has a problem recruiting and retaining talent that is competitive with national and international adversarial talent.

The National Security Act of 1947

The National Security Act of 1947 was enacted with the purpose "to promote the national security by providing for a Secretary of Defense; for a National Military Establishment; for a Department of the Army, a Department of the Navy, and a Department of the Air Force; and for the coordination of the activities of the National

Military Establishment with other departments and agencies of the government concerned with national security."[51]

Most relevant to this research was the creation of a separate Air Force. Prior to this Act, the DoD's combat air power existed as a branch of the Army called the Army Air Corps and later, the Army Air Force. Upon return from World War II, General Dwight D. Eisenhower championed the creation of a separate branch of service for the Air Force citing:

> [T]hat in his view 'no sane person' could any longer reject the idea of an independent United States Air Force. Based on the experience of World War II, the Army air arm deserved coequality with the land and naval forces. Eisenhower's advocacy was also based upon his conviction that unity of command had become absolutely essential and that a unified defense establishment would foster economy. In peacetime, the nation could no longer afford the brutal competition for resources.[52]

There are multiple parallels to be drawn from this example. Most importantly General Eisenhower mentions the competition for resources in a constrained environment. With the creation of a separate Air Force, the organization became better able to allocate a larger portion of resources and was run entirely by Air Force personnel trained in Air Force tactics and doctrine. The obvious benefit was a dedicated budget that those invested in the improvement of the Air Force would control and not have to compete with those who wished to allocate the preponderance of funds to ground forces.

[51] U.S. Congress, *The National Security Act of 1947*, July 26, 1947, accessed November 5, 2016, https://www.cia.gov/library/readingroom/docs/1947-07-26.pdf.

[52] Herman S. Wolk, *The Struggle for Air Force Independence 1943-1947* (Washington, DC: Air Force History and Museums Program, 1997).

Additionally, once separated the organization would have a voice with the Secretary of Defense and the President in how best utilize their forces for deployment.

Similarly, in 2016, the House of Representatives submitted bill H.R.6004 to modernize the government's technology capability citing a report that found "the Government has spent billions on failed and poorly performing IT investments due to a lack of effective oversight."[53] This lack effective oversight, like the Air Force, comes from an organization run by those who lack experience in the cyber field. On several instances the GAO noted the need to update the IT infrastructure due to the "holes" in its protection.[54] Much like the proponents for the implantation of a separate Air Force, the recommendations were ignored and vulnerabilities would soon be exploited.

Continuing to draw parallels, during the interwar periods of the 1920s and 1930s proponents for the U.S. Air Force like Brigadier General William Mitchell, argued that the Army did not know how to properly utilize air assets and were hampering the innovation and full power of what the Air Force could do. Proponents for change argued that because the Air Force was controlled by leaders who did not understand the service, its employment, and its capabilities, there was a need for leadership organic to the Air Force.[55]

[53] U.S. Congress, House, *Modernizing Government Technology Act of 2016*. H.R. 6004, 114th Cong. September 13, 2016, accessed September 26, 2016, https://congress.gov/bill/114th-congress/house-bill/6004.

[54] Government Accountability Office, *Agencies Need to Improve Controls over Selected High-Impact Systems* (Washington, DC: Government Accountability Office, 2016).

[55] Wolk.

Network Breaches

During 2015 OPM experienced two cyber-attacks that resulted in the compromising of 4.2 million personnel files of government employees and PII of 21.5 million individuals.[56] Additionally, 5.6 million people's fingerprint data had been exfiltrated in these attacks.[57] The significance of these breaches is greater than it appears at face value. Hackers obtained security clearance data on the 4.2 million that contains locations that personnel lived for the past several years, names and contact information for their friends and family as well as job history. Everything needed to steal identities.[58]

While the OPM breach in 2015 is the largest effect achieved within the U.S. by hackers, it is in no way the only one. "In recent data breaches, hackers took information from the United States Postal Service; the State Department; the Nuclear Regulatory Commission; the Internal Revenue Service; and even the White House."[59] These breaches are just a microcosm of issues that plague the U.S.' cyber security and can be seen in military organizations and the municipal sector as well.

To add insult to injury, the weaknesses in government cyber security were identified on numerous occasions by the GAO in their annual reports dating back to

[56] Wilshusen.

[57] OPM.Gov, "Statement by OPM Press Secretary Sam Schumach on Background Investigations Incident," September 23, 2015, accessed March 26, 2017, https://www.opm.gov/news/releases/2015/09/cyber-statement-923/.

[58] U.S. Congress, House, *Modernizing Government Technology Act of 2016*.

[59] Committee on Oversight and Government Reform, *The OPM Data Breach: How the Government Jeopardized Our National Security for More than a Generation* (Washington, DC: Committee on Oversight and Government Reform, 2016).

2005. Since then, both the Inspector General and the GAO have published reports to congress identifying vulnerabilities in multiple agencies, especially OPM. The breaches that followed were because “the agency failed to prioritize cybersecurity and adequately secure high value data.”[60] Moreover this failure to adapt IT security policies were a direct result of “the absence of an effective managerial structure to implement reliable IT security policies.”[61]

Talent Acquisition and Management

There are several factors to discuss with relation to the DoD’s ability to recruit and retain top talent. First it is important to understand that while USCYBERCOM consists of both military and 4th Estate personnel, they have separate challenges in either recruiting talent or maintaining it. The military is currently unable to attract Soldiers, Sailors, Airmen, and Marines to the cyber community because those recruits that are interested and proficient in cyber skills do not always meet the physical standards required for acceptance and retention and the armed forces such as minimum and maximum height and weight standards, as well as ability to pass a physical fitness test to the specific branch’s standards.

Senator Claire McCaskill, member of the Armed Services Committee and top-ranking Democrat on the Homeland Security and Governmental Affairs Committee stated “Having that physical capability is very, very important, but if you are part of an elite team that is working in a cyber space, where we are trying to go toe-to-toe with people

[60] U.S. Congress, House, *Modernizing Government Technology Act of 2016*.

[61] Ibid.

who have no constitutions . . . who have no rules they have to obey . . . we have to get the best and the brightest," she said. "I am not sure that's always the guy who can do the most sit-ups."[62]

Within the 4th Estate there are issues recruiting that are similar to the military.[63] This part of the organization however, has the added issue of retaining its workforce. While on the military side of the organization service members, on whole, serve for a high cause than money. But when a DoD civilian is hired, he or she receives training and job experience that parlays to a follow-on job in the civilian sector that can pay twice as much. Senior executive salary discrepancies between government IT employees and civilian sector range from 24 to 33 thousand dollars less a year for the Government Service civilian.[64] With less of a predilection towards a sense of duty and service to the country, as well as no minimum time of service contracts, the Government Service civilian can easily abandon his or her current position for "greener pastures." In fact, in both 2013 and 2014 the government lost more cyber-focused Government Service civilians than it hired.[65]

[62] Jesse Bogan, "Military Culture Must Change to Keep the Best Cyber Warriors: Senator," *St. Louis Post Dispatch*, August 30, 2016, accessed March 28, 2017, http://www.stltoday.com/news/local/govt-and-politics/military-culture-must-change-to-keep-the-best-cyber-warriors/article_201d0d86-fb55-551a-825e-615bf5e3560b.html.

[63] Defense Civilian Personnel Advisory System.

[64] Booz Allen Hamilton, *Cyber In-Security II* (Herndon, VA: Booz Allen Hamilton, April 2015).

[65] Ibid.

Other countries have realized that standards of fitness and appearance must be adjusted to attract and retain individuals skilled in cyber operations. The British Ministry of Defense has altered the requirements for its Cyber Warriors allowing for them not to take fitness tests, deploy abroad or bear arms and even allows them to grow their hair long and abstain from shaving. This has caused dissent within the Armed Forces in Great Britain as the standard Soldier feels it is represents poorly on the organization and that there is a feeling throughout the service that “the rules don’t apply to them.”[66] Though, these cyber warriors are integrated into the existing force and wear the same uniform as those required to maintain the existing standards.

There is a fear among service members and leaders, like the British have seen, and the U.S. anticipates, that allowing for avoidance of standards by cyber warriors would create a divide in the service that would hinder good order and discipline.

These divisions between service members and cyber warriors are anticipated if the U.S. were to allow separate standards like the British military did. However, with the creation of the Air Force in 1947 came the eventual creation of fitness standards different from that of its predecessor that came out of the Army.[67] As also seen in the Navy and Marine Corps each service has its own standards for acceptable criminal history and drug use, weight and body fat standards, and fitness standards. With the creation of a new

[66] Ben Farmer, “New Army Cyber Warriors Allowed Long Hair,” *The Telegraph*, March 26, 2016, accessed September 25, 2016, http://www.telegraph.co.uk/news/2016/03/26/new-army-cyber-warriors-allowed-long-hair/.

[67] Thomas E. Worden, “A Comparison of the Us Air Force Fitness Test and Sister Services’ Combat-Oriented Fitness Tests” (Thesis, Air Force Institute of Technology, Wright Patterson Air Force Base, March 2009).

cyber service, the standards could be tailored to be more appealing to those that fit in the top tier of talent without dissent amongst the standing branches.

Summary

The ineffectiveness of government cyber capabilities and talent management has been widely discussed and published. Stories in the national media;[68] reports from the GAO,[69] Booz Allen Hamilton,[70] and Rand;[71] testimonies from the USCYBERCOM Commander[72] as well as congressmen that sit on the intelligence, homeland security, and government modernization committees[73] have all conducted research and cited studies that address concerns about the government's ability to conduct cyber security and cyber operations. However, this is the first published document to combine the issues to recommend a change in DoD force structure on this magnitude.

There are however, top ranking officials within the DoD that identify the need for change. Lieutenant General Robert Brown, who was serving as the Commanding General of the U.S. Army's Combined Arms Center at Fort Leavenworth, is one of those

[68] Chiacu, "Homeland Security Struggles to Tempt, Retain Cyber Talent"; Bogan, "Military Culture Must Change to Keep the Best Cyber Warriors: Senator"; Koerner, "Inside the Cyberattack That Shocked the US Government."

[69] Office of Management and Budget, *Annual Report to Congress: Federal Information Security Modernization Act* (Washington, DC: Office of Management and Budget, 2016; Wilshusen, *Cyber Threats and Data Breaches Illustrate Need for Stronger Controls across Federal Agencies*.

[70] Booz Allen Hamilton.

[71] Porche, Sollinger, and McKay.

[72] U.S. Congress, House, *Statement Admiral Michael S. Rogers*.

[73] U.S. Congress, House, *Modernizing Government Technology Act of 2016*.

individuals. In reference to potential talented cyber recruits he said, “They grew up on Google and wear ponytails. We need to look at ways to bring them into the Army without necessarily going through the same training procedures as our combat troops.”[74]

Additionally, in a lecture given to the Command and General Staff Officer College in December 2016 Admiral (Ret) James Stavridis, former NATO Supreme Allied Commander in Europe, identified the cyber domain as one of the largest threats America faces today.[75] It is his belief that there should be the creation of a separate cyber service and that “they may have pink hair, and that’s o.k.”[76]

[74] Ben Farmer, “Fitness Tests Waived for MoD’s New Reservist Cyber Warriors,” *The Telegraph*, January 21, 2015, accessed September 25, 2016, http://www.telegraph.co.uk/news/uknews/defence/11360976/Fitness-tests-waived-for-MoDs-new-reservist-cyber-warriors.html.

[75] Admiral (Ret) James Stavridis, “Lecture to CGSOC Students” (Eisenhower Auditorium, Lewis and Clark Building, Ft. Leavenworth, December 6, 2016).

[76] Ibid.

CHAPTER 3

RESEARCH METHODOLOGY

This study began with identifying a series of attacks on U.S. internet infrastructure on both the government and private sector which resulted in compromised PII and degraded capabilities across the country. It reviewed definitions relevant to cyber operations and identified concerns with the current organization's ability to recruit and retain adequate talent. The literature review also highlighted USCYBERCOM's inability to recruit and retain talent capable of defending U.S. cyber systems.

This study considers major factors contributing to the inability for USCYBERCOM to conduct successful cyberspace operations and suggests a change in structure of the Armed Forces that could mitigate recruitment and retention issues. Part of this study is based off the identification of an immediate need seen in the current operational environment. In order to appropriately establish a Cyber Service this study applies the Doctrine, Organization, Training, Material, Leadership, Personnel, Facilities-Policy (DOTMLPF-P) lens for determining the what the service would look like.

Doctrine

A Cyber service would primarily be able to utilize existing USCYBERCOM doctrine. However, with a new organization comes the requirement for new governing regulations. Most importantly, the authorities that USCYBERCOM would require would need to be scrutinized. In order to conduct the full spectrum of operations, both Title 10 and Title 50 would have to apply.

Additionally, a difficulty in establishing doctrine for a force that operates an ethical gray area, would be the ability to publish doctrine on Cyber Offensive Operations. It is safe to assume that as most cyber capabilities and tactics are quarantined to the SECRET side of the government, the doctrine that governs it would have to remain there as well. This poses a challenge when developing young service members during training, as well as having those in charge of organizational oversight being able to view have access to the doctrine.

Organization

This aspect of the DOTMLPF-P lens is key to success of the creation of a new branch of service. Based off the current makeup of USCYBERCOM, there is a need for both military and civilian personnel. As in the transition in 1947 with the U.S. Air Force, current members of USCYBERCOM should be allowed to transfer to the new service in order to have organic leadership and expertise already in place. Conversely, the rest of the services would have to consider the release of their organic cyber-trained service members as with each branch would be supported by the new force.

Training

Part of the issues with recruitment have to do with the benefits. Arguably, the Massachusetts Institute of Technology (M.I.T.) is the premiere institution for computer science. M.I.T. graduates make, on average, $83,455 upon graduating from the institute[77]

[77] Massachusetts Institute of Technology, "MIT Facts, Alumni," accessed December 18, 2016, http://web.mit.edu/facts/alum.html.

whereas a starting Second Lieutenant in the military makes $32,862.40 annually.[78] There is no reasonable expectation for a person to forgo fifty thousand dollars when the annual cost of attending M.I.T. is over $62,000 a year.[79]

The key to overcoming this issue is the creation of a new cyber service academy. This academy could draw those top 2 percent away from M.I.T. with the promise of free tuition, a guaranteed job within the service and job experience that could parlay into a future position in the civilian sector, should they choose to leave the force after a mandatory active duty service obligation. This cyber service academy would operate in similar fashion to the sister services' academies; a four-year institution that is accredited and provides a bachelor's degree. This academy would offer fields of study specific to computer science and provide certification in programs like ethical hacking, cyber security, and programing.

As with the other military academies, upon completion of the school, graduates would be commissioned as a Second Lieutenant in the Cyber Force and be required to complete an initial service obligation of five years. If the academy is staffed with leaders in the field and has the latest technology available for training, the best and brightest of America's youth could be drawn away from premier institutions like M.I.T. with the promise of a "free education" and a job upon completion.

[78] Shala Munroe, "The Average Salary of a Second Lieutenant," Chron, accessed December 18, 2016, http://work.chron.com/average-salary-second-lieutenant-29294.html.

[79] Massachusetts Institute of Technology, "MIT Facts, Tuition and Financial Aid," accessed December 18, 2016, http://web.mit.edu/facts/tuition.html.

Material

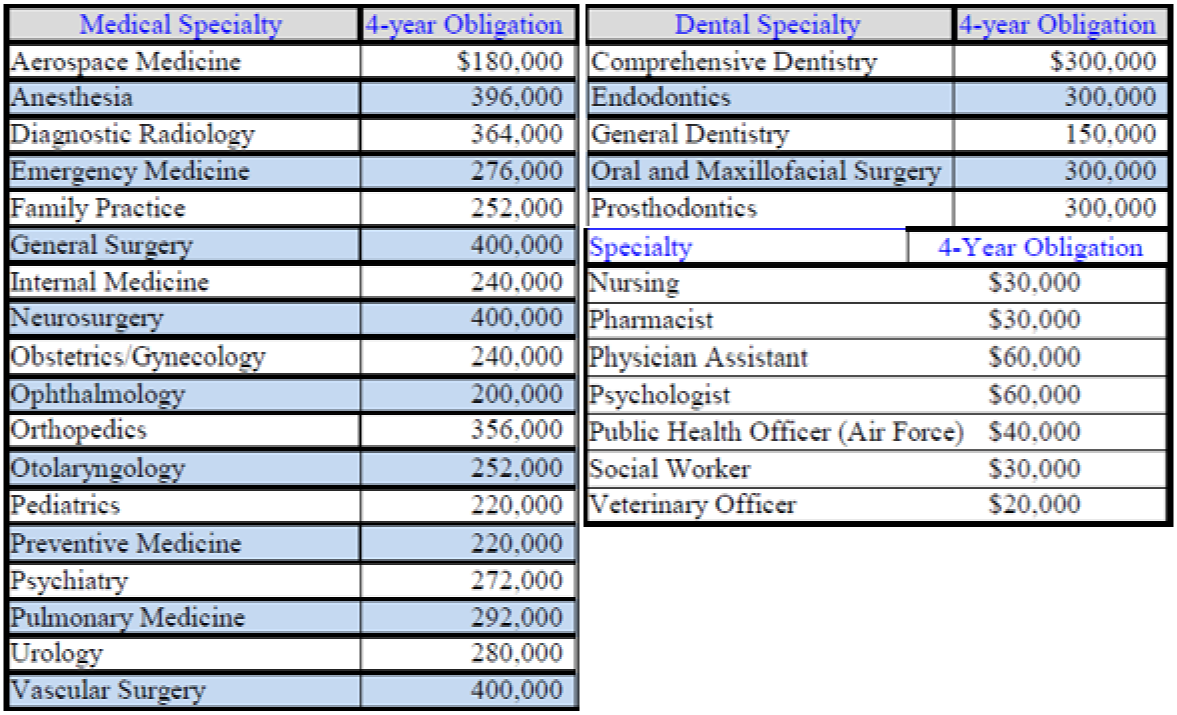
While there would be a requirement to provide new equipment to the organization and adjust current organizational tables, most of the materials needed would come from the existing structure of USCYBERCOM if there is no requirement to enlarge the force. The budget would be one of the greatest aspects affected by this transition. The need to create a new school is just one aspect of it. As mentioned before, one of the major issues with attracting and retaining civilian personnel is the inability to compete with the civilian sector salary and benefits packages.[80]

In order to ensure the attraction of the top cyber-capable talent, the U.S. government must be willing to provide bonus pay to cyber warriors in order to incentivize the high performing individuals away from the private sector. While on a smaller scale, the military already provides bonuses or incentives to health care professionals that range from $20,000 to $400,000 per person.[81] The government would have to allocate funds out of the budget for these bonuses to ensure the military remains competitive with private industry.

[80] Moore.

[81] Defense Finance and Accounting Service, "Military Pay Chart," January 1, 2017, accessed March 28, 2017, https://www.dfas.mil/militarymembers/payentitlements/military-pay-charts.html.

Table 1. Medical Services Bonus and Specialty Pay



Medical Specialty	4-year Obligation
Aerospace Medicine	$180,000
Anesthesia	396,000
Diagnostic Radiology	364,000
Emergency Medicine	276,000
Family Practice	252,000
General Surgery	400,000
Internal Medicine	240,000
Neurosurgery	400,000
Obstetrics/Gynecology	240,000
Ophthalmology	200,000
Orthopedics	356,000
Otolaryngology	252,000
Pediatrics	220,000
Preventive Medicine	220,000
Psychiatry	272,000
Pulmonary Medicine	292,000
Urology	280,000
Vascular Surgery	400,000

Dental Specialty	4-year Obligation
Comprehensive Dentistry	$300,000
Endodontics	300,000
General Dentistry	150,000
Oral and Maxillofacial Surgery	300,000
Prosthodontics	300,000

Specialty	4-Year Obligation
Nursing	$30,000
Pharmacist	$30,000
Physician Assistant	$60,000
Psychologist	$60,000
Public Health Officer (Air Force)	$40,000
Social Worker	$30,000
Veterinary Officer	$20,000

Source: Defense Finance and Accounting Service, “Fiscal Year 2017 Pay and Allowances Tables,” accessed March 30, 2017, www.dfas.mil.

Leadership

As mentioned, current USCYBERCOM leadership could move to the new service, but moving forward, development of leaders would require the continuation of developing partnerships with civilian counterparts to improve capabilities. The Art of Leadership in a newly created cyber force would be less critical than in the other services as the cyber force will not encounter actual combat. Leadership is necessary in any military organization to provide structure, orders, clarity, guidance, and intent with regards to missions. Leaders are also expected to develop, evaluate, and mentor those subordinates to them. However, unlike the other services where a Soldier, Sailor, Airman, and Marine can expect to come in contact with the enemy which could result in death, the Cyber service member would remain removed from hostile conflict. With this difference, the requirement for leaders to develop the Art of leadership would be diminished as a leader would not have to motivate his or her people to move under enemy fire with a threat of possible death.

Personnel

While the majority of a new force would come from existing USCYBERCOM, with an end state consisting of approximately 6,200 personnel,[82] looking at this aspect of DOTMLPF-P it is important to determine the size and type of people with which the organization will operate its mission. The simplest way to develop a plan for the size of the force is to compare it to other nations that have developed the capability to conduct offensive cyber operations.

Currently, there are "29 countries that have formal military or intelligence units dedicated to offensive cyber operations."[83] North Korea is estimated to have a cyber force of approximately 5,000 with the ability to develop their own malicious software (Malware) and conduct surveillance and destructive operations. Israel, with a population comparable to New York City, has an elite "Unit 8200" which has approximately 5,000

[82] Aliya Sternstein, "CYBERCOM to Congress: We Need a Bigger Budget," Next Gov, March 17, 2016, accessed March 26, 2017, http://www.nextgov.com/cybersecurity/2016/03/cybercom-appropriators-us-cant-efficiency-our-way-out-hacks/126740/.

[83] Jennifer Valentino-Devries and Danny Yadron, "Cataloging the World's Cyberforces," *The Wall Street Journal*, October 11, 2015, accessed March 26, 2017, https://www.wsj.com/articles/cataloging-the-worlds-cyberforces-1444610710.

people assigned.[84] There is difficulty in identifying sizes of cyber units in countries like Russia and China, however there are estimates from intelligence sources stating the Chinese cyber forces is approximately 100,000 Soldiers strong.[85] This, however, most likely takes into account the fact that China utilizes individual hackers as well as private IT companies to assist with cyber operations.

Facilities

Currently housed at Fort Meade, Maryland, there would be no need to move the organization. However, there are several benefits to relocating to locations that are mutually beneficial to engaging in and maintain partnerships with the civilian sector. Locations near Silicon Valley, California and Seattle, Washington offer the ability to work closely with technology giants like Apple and Microsoft. The question is how to array the Cyber Force with regards to support to the sister services. There could be an argument that contingencies should be co-located with large organizations. Wherever a Cyber Force entity is located, however, would be the requirement for state of the art facilities and the latest technology and network infrastructure.

Additionally, with the creation of a new force comes the requirement for basic training and Advanced Individual Training locations. However, it is important to note that since these individuals will not be expected to see combat, the requirements for weapons and combat training are non-existent, which negates the requirement for bases

[84] Behar.

[85] Steve Ranger, “The Impossible Task of Counting Up the World’s Cyber Armies,” ZD Net, May 6, 2015, accessed March 28, 2017, http://www.zdnet.com/article/counting-up-the-worlds-cyber-armies/.

to be large and open. The greatest requirement for these forces would be access to high speed internet and the latest computer technology.

Policy

It is in this aspect of force management where the government and the DoD would see a major shift and would be required to assume some risk. As mentioned before, part of the recruiting issue is that individuals who are capable of serving and excelling in the cyber domain may not be physically fit, willing to conform to a military appearance regulation, or might partake in recreational drug use. Changing how the other services' policies apply to the new cyber force would take a major shift in tradition and expectations from current governmental leadership.

While fitness is a requirement in all branches of the armed forces due to the potential of experiencing physically demanding tasks in combat situations, the new cyber warrior does not need to physically prove him or herself. If their only mission requires their ability to spend hours a day writing code and monitoring systems out away from any realistic threat, then the individuals involved do not need to be able run a specified distance in a limited time frame as other services are required. Part of incentivizing cyber-capable individuals would be the lack of requirement to be physically fit.

Leaders like Admiral Stavaridis,[86] Lieutenant General Brown,[87] and Senator McCaskill,[88] just to name a few have all publicly commented that the appearance of a

[86] Stavridis.

[87] Farmer, "Fitness Tests Waived."

[88] Bogan.

new cyber warrior should be allowed to differ from the traditional military member. Comments referring to hair color and length, tattoos, and weight have been made by forward thinkers, encouraging current leadership to consider relaxing current standards in order to attract more capable cyber warriors. This relaxing of standards, however, has consequences with morale within a force as seen in the British Army.[89] In addition to appearance, a major hurdle in policy change would be that of possible recreational drug use by the new cyber warrior.

While there is an inherent risk in allowing uniformed service members to partake in the use of narcotics, completely banning them can prohibit the growth and development of the cyber force. Federal Bureau of Investigation Director, James Comey stated in 2014 in reference to recruiting capable hackers, "I have to hire a great workforce to compete with those cyber criminals and some of those kids want to smoke weed on the way to the interview."[90] With states like Washington (a major hub for cyber capability) and Colorado already legalizing Marijuana, the government will have to consider adopting a more lenient policy towards drug use.

There is a major concern, however, in the ability to hire high school and college graduates proficient in hacking. The largest concern is the fact that if they are good at their job, there is the distinct possibility they have participated in illegal online operations. It could be as simple as pirating media, or it could be as complex as anything

[89] Farmer, "New Army Cyber Warriors Allowed Long Hair."

[90] Charles Levinson, "Comey: FBI 'Grappling' With Hiring Policy Concerning Marijuana," *Wall Street Journal*, May 20, 2014, accessed March 28, 2017, http://blogs.wsj.com/law/2014/05/20/director-comey-fbi-grappling-with-hiring-policy-concerning-marijuana/.

from illegally obtaining information from secured servers to stealing identities or credit information. Another major concern is the aforementioned drug use.[91] Current DoD policy directs doctors conducting initial military entrance physicals to evaluate applicants who use drugs for psychological disorders, and if so, disqualify them for service.[92]

Additionally, both a criminal past and history of drug use are non-starters during a security clearance interview process and would immediately result in a disqualification for a service that operates in the SECRET side of the government. If the government wants to recruit the top talent, there has to be changes to the recruiting and security process to allow for certain previous "indiscretions."

[91] Josephine Wolff, "Hire (Some of) the Hackers," *Slate*, September 9, 2015, accessed March 31, 2017, http://www.slate.com/articles/technology/future_tense/2015/09/the_u_s_government_needs_cybersecurity_experts_with_dodgy_pasts.html.

[92] Department of Defense, USMEPCOM Regulation 40-1, *Medical Qualification Program* (Washington, DC: Department of Defense, 2016).

CHAPTER 4

ANALYSIS

The primary purpose for this research was to determine the necessity and feasibility of creating a separate Cyber branch of the armed forces. This research looked through the DOTMLPF-P framework in order to identify the requirements for creation of this service and looked at the factors that are contributing to this concept. With the issues in retaining and recruiting talent, as well as the notable breaches of secured government networks, the previous chapters have introduced the main concerns the United States faces moving forward in a technologically dependent environment.

Background

Hacking had its first major demonstration of power in 1982.[93] The Russian Government used a Trojan Horse virus (a program designed to look like another program giving access to an unknown user) when they took control of Canadian natural gas pipeline which resulted in the "most monumental non-nuclear explosion ever seen from space."[94] In 1997, the U.S. Government conducted an exercise where they demonstrated their ability to, without provided permission or access, take control of an electrical power grid.[95]

[93] Porche, Sollinger, and McKay.

[94] Ibid.

[95] Ibid.

Hacktivism became prominent in the late 1980s with the primary intent being a goal of bringing attention to a hacker's cause through public displays.[96] Hacking tools later evolved in the mid-1990s in to denial of service attacks where the hacker would prevent a user from desired actions, which resulted in the birth of "spamming."[97] Publicly released information shows state actors, either developed at the national level or contracted by the government, have been conducting large scale cyber operations since the late 2000s. Currently on record there are 63 countries conducting these offensive operations against other nations with the minimum intent of conducting surveillance.[98]

Over the past 10 years, the U.S. Government has been the recipient of hundreds of thousands of cyber-attacks, a rise in over 1,000 percent, and those numbers do not even consider the similar amount seen on the private sector.[99] These attacks have included denial of service, intelligence collection, the public release of classified information, and the introduction of malicious code, just to name a few.[100] The largest amount of attacks came from other nations with the second most attacks coming from hacktivists. The severity of these attacks and damage done to the recipient are proportional to the amount of attacks conducted.[101]

[96] Denning.

[97] Ibid.

[98] Valentino-Devries and Yadron.

[99] Government Accountability Office.

[100] Ibid.

[101] Ibid.

With cyber-attacks on the rise over 1,000 percent in 10 years, it is obvious that the current model is not working. The government has recognized, through multiple reports to congress from the GAO, that changes are necessary to prevent catastrophic events from taking place as displayed in the Stuxnet attack of 2009. The Stuxnet virus, a type of "worm," laid dormant in the Iranian nuclear facility until activated by an unknown source resulting in damage to Iranian uranium enrichment centrifuges.[102] If an outside entity decided to conduct an attack, similar to Stuxnet on the U.S., the results could be catastrophic.

Changes

With the current cyber environment being as complex and threatening as it has been discussed so far, it is obvious that the U.S. Government needs to make drastic changes. The promotion of USCYBERCOM from a sub-unified combatant command, to a unified combatant command was a step in the right direction, but it is not enough. In the 1940s the U.S. identified the need to develop more capability in combat air power and determined that the Army Air Corps was not sufficient.[103]

Following World War II, leadership in the United States Government had a realization that with the creation of a separate branch of service for the Air Force, personnel, assets, and resources given to an individual branch would improve capabilities exponentially.[104] While there were proponents for the creation of the new Air Force,

[102] Porche, Sollinger, and McKay.

[103] Wolk.

[104] Ibid.

there were its opponents who felt a new service would not only take funding but personnel from the much-needed Army and Navy. By the time the National Security act of 1947 had been signed into law, creating the Air Force, the theory of independent air power had been around for thirty years with Army Air Corps pilot, Billy Mitchell touting a need for change.[105]

As mentioned earlier, there are several countries who have already recognized a need to bolster their militaries cyber capabilities by dedicating a branch of service. China, North Korea, Russia, Norway, and Israel have all placed a priority on cyber warfare and identified a separate branch of service to conduct defensive and offensive cyber capabilities. While it may not be completely necessary to create a new branch of service in the United States DoD, as seen in our close ally, the British Army, there is dissent among the ranks with the "waivers" authorized to cyber professionals which allow them to grow out their hair and not take fitness tests.[106] By simply creating a separate service, members of the existing services do not have to feel that there is a double standard. The differences can all be summed up in to simple service rivalries that already exist among the branches.

Threats

Unfortunately, there is not much information available on the structure, funding, and capabilities of Cyber Forces around the world. Most of the organizations, with exception of the Islamic State, operate clandestinely and do not claim ties to attacks.

[105] Ibid.

[106] Farmer, "New Army Cyber Warriors Allowed Long Hair."

China has gone on record as stating "China advocates the building of a peaceful, secure, open and cooperative cyberspace, and opposes militarization of cyberspace or cyber arms race. The Chinese government staunchly upholds cybersecurity, firmly opposes and combats all forms of cyberattacks in accordance with law."[107] But despites their propagandist response, as mentioned previously, the U.S. has linked multiple attacks, to include the attack on OPM, to China.[108]

Russian Government officials have also gone on record stating that they do not conduct offensive cyber operations saying, "Russia has never waged cyberwarfare against anyone. Russia believes that the cybersphere should be used exclusively for peaceful purposes. Ideally, our country would like to see the adoption of a legally binding international convention on global information security under U.N. auspices."[109] But, in a similar case as China, they have been linked to several cyber-attacks to include the large-scale shut down of the Ukrainian power grid in 2014.[110]

As the statement from the Russians alluded to, there is currently no international law governing information security and the act of cyber warfare. The United Nations has, however, passed UN Resolution 70/237 in December of 2015 stating that the issue was a rising concern and that a commission would look into a way forward. It additionally asked that all nations ensure their countries be cognizant of the threat and keep the flow

[107] Valentino-Devries and Yadron.

[108] U.S. Congress, House, *Modernizing Government Technology Act of 2016*.

[109] Valentino-Devries and Yadron.

[110] Polityuk.

of information free.[111] The reviewing United Nations committee is scheduled to meet in 2017 to discuss issues and recommend a way forward to the council.

New to the global threat is the introduction of the Islamic State (IS). The IS "is a Salafi-Jihadist militant organization in Syria and Iraq whose goal is the establishment and expansion of a caliphate (an Islamic state led by a supreme religious and political leader[112]) based on its extreme interpretation of Islam and Shariah."[113] And with a new organization comes the use of new forms of attack. The IS has been very successful in using cyber warfare against both the enemy it is fighting in Iraq and Syria as well as the western countries they believe are intruding in their region; namely the U.S. and Great Britain.

One such example of their abilities was displayed by Junaid Hussain, a former British citizen who committed hacking attacks against the United Kingdom and illegally listened in to secret conversations between them and their allies. Upon fleeing the country following his release from prison, Hussain went to Syria and began working with IS to recruit westerners and "activate" them to kill U.S. and United Kingdom military members. Hussain managed to accomplish this by hacking military servers and finding the PII for service members and subsequently publishing their information online and

[111] United Nations General Assembly, UN Resolution 70/237, *Developments in the Field of Information and Telecommunications in the Context of International Security* (New York: United Nations, December 2015).

[112] Gregg Myre, "What is a Caliphate?" National Public Radio, June 30, 2014, accessed March 31 2017, http://www.npr.org/sections/parallels/2014/06/30/326916530/whats-a-caliphate.

[113] Stanford University, "Mapping Militant Organizations: The Islamic State," March 29, 2017, accessed March 31, 2017, http://web.stanford.edu/group/mappingmilitants/cgi-bin/groups/view/1.

requesting their assassinations. In several instances the Federal Bureau of Investigation had to dedicate 24-hour protection to individuals on Hussain's list in order to prevent attacks.[114]

Those that have threatened and attacked the U.S. have made the conscious decision to dedicate assets to conduct operations against their adversaries in cyberspace. The world has seen the disasters that cyber-attacks can cause as mentioned earlier in this study. Destruction of nuclear centrifuges[115] and natural gas pipelines,[116] shutting down entire city electrical grids,[117] and the collection of people's PII[118] are all minor offenses compared to what a hacking organization is capable of if they are well resourced and skilled. The real possibility looms that disaster is just a few key strokes away.

Over a 10-year span from 2005 through 2015, there have been 403,013 network security breaches reported on government networks.[119] Those are just the numbers identified and the trend is rising, not declining. Below in figure 1 is the GAO's 10-year

[114] Damian Paletta, Danny Yadron, and Margaret Coker, "U.S. Drone Strike Kills Islamic State Hacker," *Wall Street Journal*, August 26, 2015, accessed March 31, 2017, https://www.wsj.com/articles/u-s-drone-strike-kills-islamic-statehacker-1440643549.

[115] Porche, Sollinger, and McKay.

[116] Ibid.

[117] Polityuk.

[118] Wilshusen.

[119] Government Accountability Office.

analysis of network security breaches which depicts an average over the 10 years of 18 percent increase of incidents per year.[120]

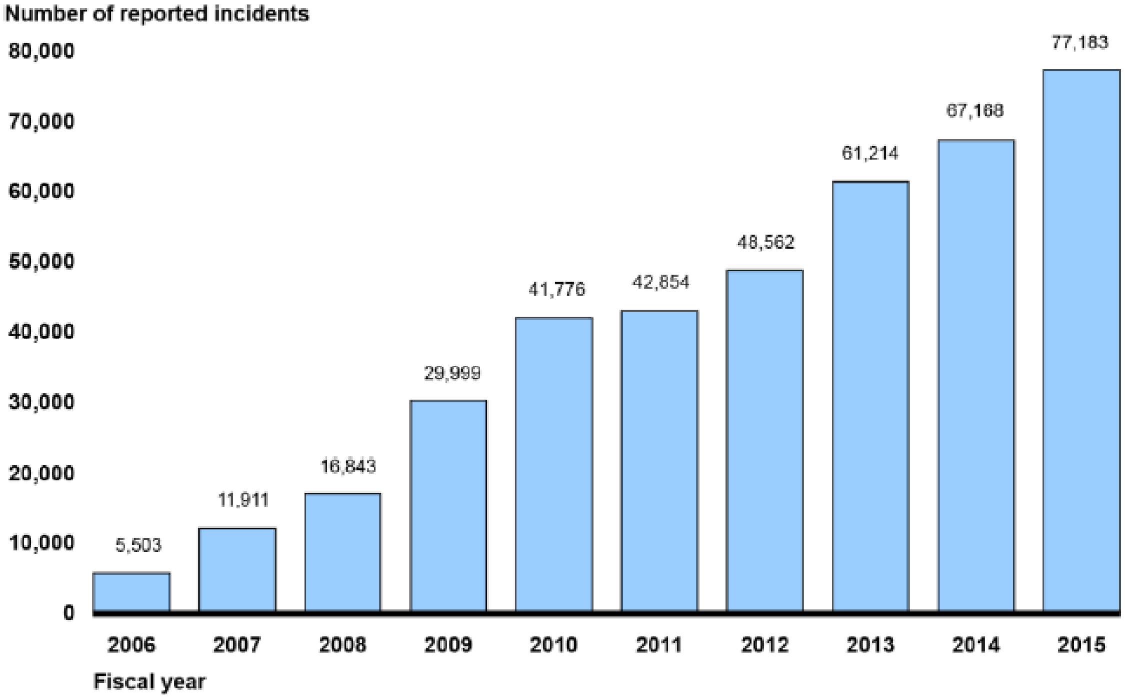
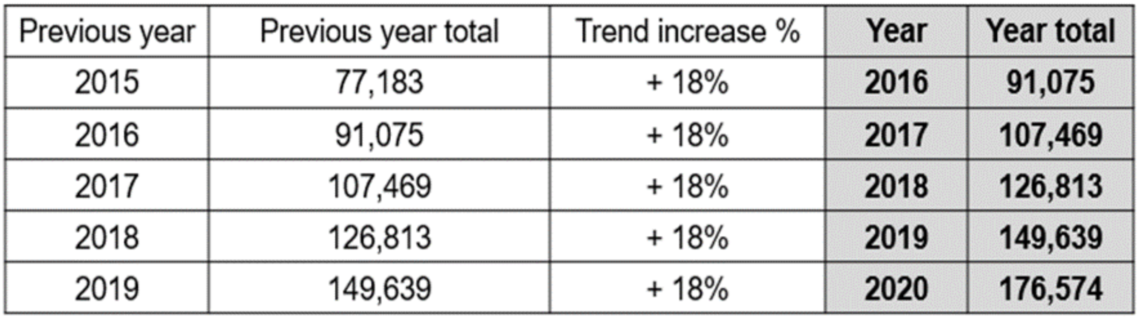


Figure 1. Incidents Reported by Federal Agencies, Fiscal Years 2006 through 2015

Source: Gregory C. Wilshusen, *Cyber Threats and Data Breaches Illustrate Need for Stronger Controls across Federal Agencies* (Washington, DC: Government Accountability Office, 2015).

[120] Ibid.

Table 2. Projected Trend of Attacks on Government Networks Based off Current Trends



Previous year	Previous year total	Trend increase %	Year	Year total
2015	77,183	+ 18%	**2016**	**91,075**
2016	91,075	+ 18%	**2017**	**107,469**
2017	107,469	+ 18%	**2018**	**126,813**
2018	126,813	+ 18%	**2019**	**149,639**
2019	149,639	+ 18%	**2020**	**176,574**

Source: Created by Author, using the model identified by GAO: Gregory C. Wilshusen, *Cyber Threats and Data Breaches Illustrate Need for Stronger Controls across Federal Agencies* (Washington, DC: Government Accountability Office, 2015).

Depicted in table 2 above is an extrapolation of the trend analysis pictured in figure 1 above. If trends are to continue in the same manor they have for the previous year, by the year 2020, the amount of attacks on government networks will have more than doubled with more than 176,000 attacks. This extrapolation, however is a fixed rate. If the change becomes exponential as technology becomes more and more prevalent and more readily available to developing nations, the results could number in the hundreds of thousands during a one year timeframe.

With trends like this, it is obvious that the threat is increasing and the current structure the government employs in USCYBERCOM is not sufficient to defend against nations and third-party actors who dedicate not only resources, but the recruit and retain the most skilled cyber warriors within their country to operate in their cyber organizations. And while the U.S. Government may be capable of providing large amounts of resources and funds into the current cyber organization, they have demonstrated that that they are incapable of recruiting and retaining the top talent in the cyber community.

In spring of 2016, the Pentagon created the bounty bug program, offering approved hackers outside the government identify flaws in the security systems of DoD sites and networks. The campaign, dubbed "Hack the Pentagon," resulted in hackers finding 138 flaws in less than a month.[121] These talented individuals were paid by the government a bounty if they found any flaws and out of the 1,500 hackers the participated 250 submitted vulnerability flaws.[122] That is 17 percent of the hackers that participated in the bug bounty were successful in identifying issues within the DoD network.

These 17 percent are the target population for individuals that the U.S. Government should be trying to recruit. However, as discussed earlier, these 17 percent are not interested in serving due to a multitude of reasons from fitness, appearance, criminal history, or just a lack of competitive pay. It is not, however, a lack of desire to serve their country. Their dedication or desire to serve their country was apparent when they offered to identifies flaws in the network in order to prevent further issues. The question the government has to ask themselves is not "why can we not recruit top-tier cyber talent?" but "what do we have to change to attract the interest of top-tier cyber talent?"

[121] Doug Olenick, "Pentagon Bug Bounty Program Finds 138 Vulnerabilities," *SC Media*, June 20, 2016, accessed March 29, 2017, https://www.scmagazine.com/pentagon-bug-bounty-program-finds-138-vulnerabilties/article/529564/.

[122] Ibid.

Summary

This chapter identified the precedence for the U.S. Government to create a new branch of the armed forces with the creation of the Air Force in the National Security Act of 1947.[123] This chapter also identified the potential size of the threat facing the U.S. if the current glide path is continued and the U.S. Government is unable to react proportionally to the aggressing actors. And lastly this chapter identified the ineffectiveness of the government in its ability to attract and maintain top cyber talent. Compiling all of the information presented in this chapter, it is a safe assessment to make that the U.S. is looking a revolution in military affairs in the face, and it is not identifying the need to change in order to survive.

[123] U.S. Congress, *The National Security Act of 1947*.

CHAPTER 5

CONCLUSIONS AND RECOMMENDATIONS

Introduction

This chapter plans to identify how the U.S. Government can best combat the increasingly lethal threat posed in cyber warfare. Through interpreting analysis provided in chapter 4, this chapter will draw conclusions about the state of USCYBERCOM's capabilities, the defining reasons on why the current structure needs to change, and ways to increase capability in a new organization. Wider implications for failure to adapt and change the organization will be presented before the conclusion of this chapter.

Summary of Findings

The world's cyber criminals, both state sponsored and independent are getting better and more aggressive. Attacks on the U.S. have increased and resulted in losses of PII and classified information. Attacks on other nations have resulted in the loss of power and commerce. Multiple nations to include North Korea, China, Russia, Israel, and Norway have all identified a need to create a new branch of the armed forces dedicated to the cyber mission.[124] With the dedication to the furthering of cyber capabilities through the cyber branch, these previously mentioned countries remain at the apex of cyber

[124] Valentino-Devries and Yadron, "Cataloging the World's Cyberforces"; F-Secure, "The Dukes: 7 Years of Russian Cyberespionage"; Behar, "Inside Israel's Secret Startup Machine"; Norwegian Ministry of Defense, "Norwegian Defence 2013: Facts and Figures."

warfare. One major difference in the countries mentioned versus the U.S. is the fact that the former all maintain conscription of their citizens.[125]

Since the U.S. has no discernable intentions to conduct conscription of its citizens, the government has a void to fill in recruiting top cyber talent to join the armed forces. Reason are armed forces policy prevents those with criminal histories and drug use from joining. This policy is also restrictive to the physically fit and healthy, and requires the maintenance of a specified grooming standard. The typical U.S. hacker is dissuaded or prevented from serving their country as a result of one of these previously mentioned criteria. Additionally, the private sector pays much more than the military does and does not require its employees to be placed in harm’s way. Compounding the issue of pay discrepancy is the fact that the top schools in the U.S. that award degrees applicable to cyber operations are expensive, which means graduates are less likely to take a lower paying job with massive student debt hanging over their heads.

Not only does the U.S. Government have trouble recruiting, but they are also incapable of retaining their talent. Governmentally trained and employed cyber warriors often leave the ranks of the government as soon as their initial contract is up. This is again, due to the fact that these employees can make much more in the private sector and are not required to maintain such rigid standards as found in the military.

It is through these issues the U.S. Government is facing a revolution in military affairs the same as it did post World War II with the need to create a separate branch of the military for the Air Force. It took years of debate and research before the U.S. made

[125] Charts Bin, “Military Conscription Policy by County,” 2011, accessed April 1, 2017, http://chartsbin.com/view/1887.

the decision in the National Security Act of 1947 to separate the Air Force from the Army and make it a branch of the armed forces by itself.[126] Research presented in this paper has identified the multiple causes for concern in both the security of the nation's network infrastructure as well as its ability to compete with peer nations.

While the government has created systems and organizations to combat the problem, they have not identified the best result. Organizations like the GAO and the House Committee to Modernize Technology, and the promotion of USCYBERCOM from a sub-unified command to a unified command are all positive steps forward but fall short of the needed outcome.

Interpretation of Information

The U.S. Government is incapable of recruiting and retaining talent necessary to protect critical and vital network infrastructure that leaves the U.S. and its citizens at risk of financial or physical crisis. The structure of the current cyber force within the U.S. Government is insufficient and must be changed to prevent possible catastrophe.

A Way Forward

The DoD must take a step further than they did with the promotion of USCYBERCOM to a unified command and create a new branch of the armed forces, the Cyber Force. The creation of this service will not only allocate additional funds to the service, allowing them to develop better capabilities, but it will also allow for the development of programs that will draw the top talent away from private industry. Just

[126] U.S. Congress, *The National Security Act of 1947*.

like the world has seen with the Israeli elite Unit 8200, the U.S. could develop systems capable of protecting DoD infrastructure, and even assist in protecting private industry.[127]

United States Cyber Military Academy at Silicon Valley

There are multiple benefits to the creation of a new service academy. Looking at the success of West Point, Annapolis, and the Air Force Academy is a perfect template for developing a concept of what the Cyber Academy should look like. Similar to the other academies, graduates would earn a bachelor's degree, however all degrees at this school would be focused on the computer sciences. As with most specialty schools, any school that is an "institute of technology" for example, experts in the field would be instructors and students would have access to technology and systems that standard state and private schools would not have equipped.

Like the other academies, students would be required to develop an understanding of the art of leadership and become familiar with military rank and structure, as well as doctrine, policy, and procedures. However, unlike the other academies, fitness, sports, and combat training will not be a requirement. As with any four-year university, sports will be a part of the school, however, like institutions like M.I.T., there will be limited offerings for varsity sports compared to Division 1 schools like West Point.[128]

The process to gain entry would be similar to the other service academy requirements, but changes would be necessary to maintain interest from the target

[127] Behar.

[128] Massachusetts Institute of Technology, "Activities and Clubs at MIT," accessed April 1, 2017, https://stuff.mit.edu/activities/sports.html.

audience. Instead of a fitness test, applicants would conduct testing on their ability to write or understand code, repair networks, and gain access to restrictive networks. Scoring well in the Science, Technology, Engineering, and Mathematics portions of early education would be the priority for these applicants. And like the other academies, a nomination from a member of congress or a senator would be required.

Just like the other academies, the Cyber Academy would require a mandatory service obligation of five years upon graduating. This would ensure that leadership within the organization, like other services, stay around longer than they currently are. Additionally, if necessary, the service could offer extension bonuses to those who stay in past their five years, as the Army saw in the late 2000s when the Army was having difficulty retaining captains.[129] The offer of a top-tier university that does not charge for tuition, room and board, and provides the graduate with a job the day of graduation will be hard to compete with.

The attraction of the best and the brightest who desire to work in the cyber industry and simultaneously serve their country will improve DoD cyber capabilities exponentially. Not only will the government have the best minds working to combat adversarial cyber operations, but the cyber warriors will be able to develop new software, technology, systems, and capabilities that the current USCYBERCOM members cannot fathom, similar to what is seen in the Israeli Unit 8200.[130] Additionally, with an influx of

[129] LTC Maura Gillen, “Captains Now Eligible for $25K Retention Bonus,” *Army Times*, September 13, 2007, accessed April 1, 2017, https://www.army.mil/article/4848/captains-now-eligible-for-25k-retention-bonus/.

[130] Behar.

talent comes competition, and with competition come the improvement of an organization and its capabilities.

Upon graduating and commissioning as Second Lieutenants, these junior cyber officers would be assigned to one of the few Cyber bases within the country. Locations are arguable, but co-location with strategic assets, as well as technology giants would best suit the performance of the Cyber Force. Locations like Washington DC, Seattle, Washington, Omaha, Nebraska, would provide regional support to organizations across the country while being co-located with assets capable of directing and assisting operations as needed. While the benefit of being located with strategic assets is obvious, the benefit of being located near technology giants like Microsoft and Apple allow for partnerships to develop and the ability to share and develop mutually beneficial security capabilities.

With the removal of USCYBERCOM for the creation of the Cyber Force, comes the requirement for the existing services to determine what happens to the service members currently in their forces who currently serve in the cyber realm. These services must understand that they are the “bill payers” and need to allow the service members to transfer over to the new cyber service in order to maintain continuity among the force and provide leadership to future cyber warriors. An added benefit to the loss of those individuals by the existing services is cost. With the creation of a new service, the budget of each service will have to be reduced. Proportionally, the loss of individuals and assets transferring over to the new service should absorb some of the sticker shock associated with the requisite budget cuts.

There is one concern that the DoD, as well as individual services, would have to prepare for and mitigate. The attempt of additional, non-cyber qualified individuals to transfer from their current services to the new Cyber Force. Policies must dictate expectations on requirements for entrance in to the new service. While there are, no doubt, individuals currently serving in non-cyber positions within all branches of the military, there will be those who are enticed to join the Cyber Force do to their lax regulations, increased pay, and lack of operational deployments, who have no cyber capabilities.

Broader Implications

This study has discussed the previous attacks in recent history executed by those wishing to do harm in cyber space. This study has also discussed the inability of the current U.S. cyber organization and the trends of attacks. What has yet to be said are the potential repercussions if nothing changes. Could the United States be staring a Black Swan event in the face? While IS has openly expressed their desire to attack western countries through the internet, intelligence officials do not believe they can cause massive destruction, yet.[131] However, as already mentioned, the Dark Web is easily accessible to IS and the type of software they could purchase that can lead to catastrophic results, lies there.[132]

While IS openly attacks our networks, the U.S. has implicated Russia and China on several occasions for attacks resulting in breaches of government secure networks. If

[131] Paletta, Yadron, and Coker.

[132] Gregg.

either of these, very capable countries, desire to conduct a major offensive cyber operation on the U.S. financial centers, power grids, energy plants, or weapon silos, the results would be catastrophic. A massive economic collapse or the detonation of nuclear weapons could easily become a reality if the U.S. does not do something to improve their cyber capabilities; and the creation of a new Cyber Force is the best way to do it.

BIBLIOGRAPHY

Ablon, Lillian, Martin C. Libicki, and Andrea A. Golay. *Markets for Cybercrime Tools and Stolen Data.* Santa Monica, CA: Rand Corporation, 2014.

Behar, Richard. “Inside Israel's Secret Startup Machine.” *Forbes*, May 31, 2016. Accessed January 1, 2017. https://www.forbes.com/sites/richardbehar/ 2016/05/11/inside-israels-secret-startup-machine/#1a5198de1a51.

Bogan, Jesse. “Military Culture Must Change to Keep the Best Cyber Warriors: Senator.” *St. Louis Post Dispatch*, August 30, 2016. Accessed March 28, 2017. http://www.stltoday.com/news/local/govt-and-politics/military-culture-must-change-to-keep-the-best-cyber-warriors/article_201d0d86-fb55-551a-825e-615bf5e3560b.html.

Booz Allen Hamilton. *Cyber In-Security II.* Herndon, VA: Booz Allen Hamilton, April 2015.

Charts Bin. “Military Conscription Policy by County.” 2011. Accessed April 1, 2017. http://chartsbin.com/view/1887.

Chiacu, Doina. “Homeland Security Struggles to Tempt, Retain Cyber Talent.” *Reuters*, April 26, 2014. Accessed March 28, 2017. http://www.reuters.com/article/us-usa-cybersecurity-dhs-idUSBREA3P05O20140426.

Committee on Oversight and Government Reform. *The OPM Data Breach: How the Government Jeopardized Our National Security for More than a Generation*. Washington, DC: Committee on Oversight and Government Reform, 2016.

Defense Civilian Personnel Advisory System. “Cyber One Stop.” Accessed August 30, 2016. https://www.cpms.osd.mil/Subpage/CyberOneStop/CyberHome.

Defense Finance and Accounting Service. “Fiscal Year 2017 Pay and Allowances Tables.” Accessed March 30, 2017. www.dfas.mil.

———. “Military Pay Chart.” January 1, 2017. Accessed March 28, 2017. https://www.dfas.mil/militarymembers/payentitlements/military-pay-charts.html.

Denning, Dorothy. “The Rise of Hactivism.” *The Georgetown Journal of International Affairs* (September 8, 2015). Accessed March 26, 2017. http://journal.georgetown.edu/the-rise-of-hacktivism/.

Department of Army G1. *Department of the Army Manning Guidance*. Washington, DC: Government Printing Office, June 2016.

Department of Defense. Joint Publication (JP) 3-12 (R), *Doctrine for Joint Nuclear Operations*. Washington, DC: Government Printing Office, 2013.

———. USMEPCOM Regulation 40-1, *Medical Qualification Program.* Washington, DC: Department of Defense, 2016.

Edwards, June. "DoD's '4th Estate' Agencies to Procure Professional Services Via GSA's OASIS; Tiffany Hixson Comments." Executive Gov, June 17, 2016. Accessed April 1, 2017. http://www.executivegov.com/2016/06/dods-4th-estate-agencies-to-procure-professional-services-via-gsas-oasis-contract-vehicles-tiffany-hixson-comments/.

Farmer, Ben. "Fitness Tests Waived for MoD's New Reservist Cyber Warriors." The Telegraph, January 21, 2015. Accessed September 25, 2016. http://www.telegraph.co.uk/news/uknews/defence/11360976/Fitness-tests-waived-for-MoDs-new-reservist-cyber-warriors.html.

———. "New Army Cyber Warriors Allowed Long Hair." *The Telegraph*, March 26, 2016. Accessed September 25, 2016. http://www.telegraph.co.uk/news/2016/03/26/new-army-cyber-warriors-allowed-long-hair/.

F-Secure. "The Dukes: 7 Years of Russian Cyberespionage." Whitepaper, September 17, 2015. Accessed March 29, 2017. https://labsblog.f-secure.com/2015/09/17/the-dukes-7-years-of-russian-cyber-espionage/.

Gillen, LTC Maura. "Captains Now Eligible for $25K Retention Bonus." *Army Times*, September 13, 2007. Accessed April 1, 2017. https://www.army.mil/article/4848/captains-now-eligible-for-25k-retention-bonus/.

Government Accountability Office. *Agencies Need to Improve Controls over Selected High-Impact Systems.* Washington, DC: Government Accountability Office, 2016.

Greenberg, Andy. "Pentagon Launches the Feds' First 'Bug Bounty' for Hackers." Wired, March 2, 2016. Accessed April 1, 2017. https://www.wired.com/2016/03/pentagon-launches-feds-first-bug-bounty-hackers/.

Gregg, Brandon. "Online Black Markets and How They Work." TechWorld, May 1, 2012. Accessed April 1, 2017. http://www.techworld.com/security/online-black-markets-how-they-work-3355031/.

Johnson III, Clay. "Safeguarding Against and Responding to the Breach of Personally Identifiable Information." Whitehouse.Gov. May 22, 2007. Accessed November 5, 2016. https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2007/m07-16.pdf.

Koerner, Brendan J. “Inside the Cyberattack That Shocked the US Government.” Wired, October 23, 2016. Accessed March 26, 2017. https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/.

Koppel, Ted. *Lights Out.* New York: Penguin Random House, 2015.

Levinson, Charles. “Comey: FBI ‘Grappling’ With Hiring Policy Concerning Marijuana.” *Wall Street Journal*, May 20, 2014. Accessed March 28, 2017. http://blogs.wsj.com/law/2014/05/20/director-comey-fbi-grappling-with-hiring-policy-concerning-marijuana/.

Massachusettes Institute of Technology. “Activities and Clubs at MIT.” Accessed April 1, 2017. https://stuff.mit.edu/activities/sports.html.

———. “MIT Facts, Alumni.” Accessed December 18, 2016. http://web.mit.edu/facts/alum.html.

———. “MIT Facts, Tuition and Financial Aid.”Accessed December 18, 2016. http://web.mit.edu/facts/tuition.html.

McGill, Andrew. “We Built a Fake Web Toaster, and It Was Hacked in an Hour.” *The Atlantic*, October 28, 2016. Accessed October 29, 2016. https://www.theatlantic.com/technology/archive/2016/10/we-built-a-fake-web-toaster-and-it-was-hacked-in-an-hour/505571/.

Moore, Jack. “In Fierce Battle for Cyber Talent, Even NSA Struggles to Keep Elites on Staff.” NextGov. April 14, 2014. Accessed March 28, 2017. https://www.benton.org/headlines/fierce-battle-cyber-talent-even-nsa-struggles-keep-elites-staff.

Munroe, Shala. “The Average Salary of a Second Lieutenant.” Chron. Accessed December 18, 2016. http://work.chron.com/average-salary-second-lieutenant-29294.html.

Myre, Gregg. “What is a Caliphate?” National Public Radio, June 30, 2014. Accessed March 31 2017. http://www.npr.org/sections/parallels/2014/06/30/326916530/whats-a-caliphate.

Newman, Lily Hay. “The US Military Launches ‘Hack the Army,’ Its Most Ambitious Bug Bounty Yet.” Wired, November 11, 2016. Accessed March 28, 2017. https://www.wired.com/2016/11/us-military-launches-hack-army-ambitious-bug-bounty-yet/.

Norwegian Ministry of Defense. “Norwegian Defence 2013: Facts and Figures.” Information Report, Norwegian Ministry of Defense, Oslo, 2013. Accessed September 25, 2016. https://forsvaret.no/en/organisation.

Office of Managment and Budget. *Annual Report to Congress: Federal Information Security Modernization Act.* Washington, DC: Office of Managment and Budget, 2016.

Olenick, Doug. “Pentagon Bug Bounty Program Finds 138 Vulnerabilties.” *SC Media*, June 20, 2016. Accessed March 29, 2017. https://www.scmagazine.com/pentagon-bug-bounty-program-finds-138-vulnerabilties/article/529564/.

OPM.Gov. “Statement by OPM Press Secretary Sam Schumach on Background Investigations Incident.” September 23, 2015. Accessed March 26, 2017. https://www.opm.gov/news/releases/2015/09/cyber-statement-923/.

Paletta, Damian, Danny Yadron, and Margaret Coker. “U.S. Drone Strike Kills Islamic State Hacker.” *Wall Street Journal*, August 26, 2015. Accessed March 31, 2017. https://www.wsj.com/articles/u-s-drone-strike-kills-islamic-statehacker-1440643549.

Polityuk, Pavel. “Ukraine Sees Russian Hand in Cyber Attacks on Power Grid.” *Reuters*, February 12, 2016. Accessed March 9, 2017. http://www.reuters.com/article/us-ukraine-cybersecurity-idUSKCN0VL18E.

Pomerleau, Mark. “Congress Set to Elevate CYBERCOM to Unified Combatant Command.” C4ISR Net, December 1, 2016. Accessed December 12, 2016. http://www.c4isrnet.com/articles/congress-authorizes-elevating-cybercom-to-unified-combatant-command.

Porche III, Isaac R., Jerry M Sollinger, and Shawn McKay. *A Cyberworm That Knows No Boundaries.* Santa Monica, CA: RAND, 2011.

Ranger, Steve. “The Impossible Task of Counting Up the World's Cyber Armies.” ZD Net, May 6, 2015. Accessed March 28, 2017. http://www.zdnet.com/article/counting-up-the-worlds-cyber-armies/.

Stanford University. “Mapping Militant Organizations: The Islamic State.” March 29, 2017. Accessed March 31, 2017. http://web.stanford.edu/group/mappingmilitants/cgi-bin/groups/view/1.

Stavridis, Admiral (Ret) James. “Lecture to CGSOC Students.” Eisenhower Auditorium, Lewis and Clark Building, Ft. Leavenworth, KS, December 6, 2016.

Sternstein, Aliya. “CYBERCOM to Congress: We Need a Bigger Budget.” Next Gov, March 17, 2016. Accessed March 26, 2017. http://www.nextgov.com/cybersecurity/2016/03/cybercom-appropriators-us-cant-efficiency-our-way-out-hacks/126740/.

Tucker, Patrick, and Caroline Houck. “Someone Weaponized the Internet of Things.” Defense One, October 22, 2016. Accessed October 23, 2016. http://www.defenseone.com/threats/2016/10/someone-weaponized-internet-things/132553/.

U.S. Congress. *The National Security Act of 1947*. July 26, 1947. Accessed November 5, 2016. https://www.cia.gov/library/readingroom/docs/1947-07-26.pdf.

U.S. Congress. House. *Modernizing Government Technology Act of 2016*. H.R. 6004, 114th Cong. September 13, 2016. Accessed September 26, 2016. https://congress.gov/bill/114th-congress/house-bill/6004.

———. *Statement Admiral Michael S. Rogers, Commander, United States Cyber Command before the House Armed Services Committee, Subcommittee on Emerging Threats and Capabilities*. March 3, 2016. Accessed March 28, 2017. http://docs.house.gov/meetings/AS/AS26/20160316/104553/HHRG-114-AS26-Wstate-RogersM-20160316.pdf.

U.S. Strategic Command. “Fact Sheet.” March 2015. Accessed November 5, 2016. https://www.stratcom.mil/factsheets/2/Cyber_Command/.

United Nations General Assembly. UN Resolution 70/237, *Developments in theField of Information and Telecommunications in the Context of International Security*. New York: United Nations, December 2015.

Valentino-Devries, Jennifer, and Danny Yadron. “Cataloging the World’s Cyberforces.” *The Wall Street Journal*, October 11, 2015. Accessed March 26, 2017. https://www.wsj.com/articles/cataloging-the-worlds-cyberforces-1444610710.

Wall, Andru E. “Demystifying the Title 10-Title 50 Debate.” Paper, Harvard Law School, 2011. Accessed November 5, 2016. http://harvardnsj.org/wp-content/uploads/2012/01/Vol-3-Wall.pdf.

Weinstein, David, and James Admiral Stavridis. “Time for a U.S. Cyber Force.” *Proceedings Magazine* (January 2014). Accessed March 29, 2017. https://www.usni.org/magazines/proceedings/2014-01/time-us-cyber-force.

Williams, Brett T. “The Joint Force Commander’s Guide to Cyberspace Operations.” *Joint Forces Quarterly* 73 (2nd Quarter 2014): 12-19.

Wilshusen, Gregory C. *Cyber Threats and Data Breaches Illustrate Need for Stronger Controls across Federal Agencies*. Washington, DC: Government Accountability Office, 2015.

Wolff, Josephine. “Hire (Some of) the Hackers.” *Slate*, September 9, 2015. Accessed March 31, 2017. http://www.slate.com/articles/technology/future_tense/2015/09/the_u_s_government_needs_cybersecurity_experts_with_dodgy_pasts.html.

Wolk, Herman S. *The Struggle for Air Force Independence 1943-1947*. Washington, DC: Air Force History and Museums Program, 1997.

Worden, Thomas E. “A Comparison of the Us Air Force Fitness Test and Sister Services’ Combat-Oriented Fitness Tests.” Thesis, Air Force Institue of Technology, Wright Patterson Air Force Base, March 2009.