CYBERSPACE OPERATIONS: THE UTILIZATION OF OUR RESERVE FORCE

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
Strategic Studies

by

RACHEL I. MARTIN, LIEUTENANT COMMANDER, U.S. NAVY
Bachelors of Science, State University of New York at Oneonta, Oneonta, NY, 2001

Fort Leavenworth, Kansas
2018

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
15-06-2018	Master's Thesis	AUG 2017 – JUN 2018

4. TITLE AND SUBTITLE

Cyberspace Operations: The Utilization of Our Reserve Force

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Rachel I. Martin, Lieutenant Commander, U.S. Navy

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

Cyberspace operations are essential to achieving objectives of our National Security Strategy. That is, without cyberspace operations, our nation's security interests would never be met. For instance, the U.S. military employs cyberspace operations as a way in which to achieve homeland defense. The significance of understanding cyberspace operations, specifically, the capabilities and gaps throughout our services is essential to ensuring the stability and protection of our social, political and economic infrastructure. This paper seeks to understand the role and employment of the military reservist in cyberspace operations. Do reserve units provide the best opportunities for cyberspace professionals, by allowing reservists to practice their cyber skills in the civilian world? Should the U.S. military add more reserve billets to U.S. Cyber Command (USCYBERCOM) over the next five years in order to increase our defensive and offensive capabilities so that we reduce our risk of penetration? Through the analysis of Doctrine, Organization, Training, Leadership and Education, and Personnel conclusions and recommendations will be made.

15. SUBJECT TERMS
Cyberspace, Cyberspace Operations, Offensive Cyberspace Operations, Defensive Cyberspace Operations, Department of Defense Information Networks, Information Assurance, Cyberspace Superiority, Reserve

16. SECURITY CLASSIFICATION OF: UNCLASSIFIED (U)			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. PHONE NUMBER** *(include area code)*
(U)	(U)	(U)	(U)	74	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39.18

MASTER OF MILITARY ART AND SCIENCE
THESIS APPROVAL PAGE

Name of Candidate: LCDR Rachel I. Martin

Thesis Title: CYBERSPACE OPERATIONS: THE UTILIZATION OF OUR RESERVE FORCE

Approved by:

_____, Thesis Committee Chair
Jack D. Kem, Ph.D.

_____, Member
Brian J. Gerling., M.S.

_____, Member
Kurt P. VanderSteen, M.M.A.S

Accepted this 15th day of June 2018 by:

_____, Director, Graduate Degree Programs
Robert F. Baumann, 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

CYBERSPACE OPERATIONS: THE UTILIZATION OF OUR RESERVE FORCE by Lieutenant Commander Rachel I. Martin, 74 pages.

Cyberspace operations are essential to achieving objectives of our National Security Strategy. That is, without cyberspace operations, our nation's security interests would never be met. For instance, the U.S. military employs cyberspace operations as a way in which to achieve homeland defense. The significance of understanding cyberspace operations, specifically, the capabilities and gaps throughout our services is essential to ensuring the stability and protection of our social, political and economic infrastructure. This paper seeks to understand the role and employment of the military reservist in cyberspace operations. Do reserve units provide the best opportunities for cyberspace professionals, by allowing reservists to practice their cyber skills in the civilian world? Should the U.S. military add more reserve billets to U.S. Cyber Command (USCYBERCOM) over the next five years in order to increase our defensive and offensive capabilities so that we reduce our risk of penetration? Through the analysis of Doctrine, Organization, Training, Leadership and Education, and Personnel conclusions and recommendations will be made.

ACKNOWLEDGMENTS

I would like to dedicate this thesis to my husband Louis. Without his unwavering support, patience, and British charm the light from the lighthouse would not be as bright as it is! I love him so much, he is my everything, and I cannot imagine a world in Kansas or anywhere else in the world without him. His ability to encourage when it seemed like the end was not near has been a true blessing through this process. Without my Louis, this paper would have taken far longer than needed. I love you Louis dearly, now, always, and forever. He's my super human!

"Super human effort isn't worth a damn unless it achieves results."
– Ernest Shackelton

TABLE OF CONTENTS

ACRONYMS

ADCON	Administrative Control
CIA	Central Intelligence Agency
CMF	Cyber Mission Force
CNAP	Cybersecurity National Action Plan
DoD	Department of Defense
DOTMLPF-P	Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, Facilities, and Policy
FBI	Federal Bureau of Investigation
FM	Field Manual
JP	Joint Publication
MAGTF	Marine Air-Ground Task Force
MCIENT	Marine Corps Information Enterprise
MCIP	Marine Corps Interim Publication
MILCON	Military Construction
NASA	The National Aeronautics and Space Administration
NATO	The North Atlantic Treaty Organization
NWP	Navy Warfare Publication
O&M	Operations & Maintenance
OPCON	Operational Control
RDT&E	Research, Development, Testing, and Evaluation
USCYBERCOM	United States Cyber Command
USNORTHCOM	United States Northern Command
USSTRATCOM	United States Strategic Command

ILLUSTRATIONS

Page

TABLES

Page

CHAPTER 1

INTRODUCTION

Overview

> We face cyber threats from state-sponsored hackers, hackers for hire, global cyber syndicates, and terrorists. They seek our state secrets, our trade secrets, our technology, and our ideas – things of incredible value to all of us. They seek to strike our critical infrastructure and to harm our economy.
>
> —James Comey

Cyberspace operations are essential to achieving the objectives of our National Security Strategy. Without cyberspace operations, our nation's security interests would never be met. The U.S. military employs cyberspace operations as a way in which to achieve homeland defense. The significance of understanding cyberspace operations, specifically, the capabilities and gaps throughout our services is essential to ensuring the stability and protection of our social, political, and economic infrastructure.

Primary Research Question

This paper will attempt to answer "do reserve units provide the best opportunities for cyberspace professionals, by allowing reservist to practice their cyber skills in the civilian world?" By exploring the dynamics of our current state of cyberspace operations throughout our military services, the author can determine whether the U.S. military is adequately balanced as a structure, including reservists, to conduct cyberspace operations. By way of illustration, in August of 2017, we stood up to U.S. Cyber Command as a combatant command. This is important because "the elevation of United States Cyber Command demonstrates our increased resolve against cyberspace threats and will help reassure our allies and partners and deter our adversaries. Elevation will

also ensure that critical cyberspace operations are adequately funded" (Mehta and Shane 2017).

Secondary Research Questions

Drawing from the primary question, the researcher will also attempt to answer, "Should the U.S. military add more reserve billets to U.S. Cyber Command (USCYBERCOM) over the next five years, in order to increase our defensive and offensive capabilities, so that we reduce our risk of penetration?" Simply put, should more reserves be added to the fight to expand our knowledge base in cyberspace operations? To understand the answer to this question, one could consider adding 20 additional reserve billets a year to USCYBERCOM, to understand if we are better postured to protect our national security interests. This potential solution is primarily based on the dynamic range of skill sets the cyberspace operations reserve personnel can bring to the fight.

Having the skill sets to defend our Department of Defense (DoD) information networks comes from years of education and training. Cyberspace operations reserve personnel are recruited because they already possess the skill sets necessary to provide defense against attacks, deliver tactical advantages, and have the ability to develop innovative tools and techniques for the future. These cyberspace operations skill sets are learned from formal education, and basic day-day tasks at their civilian jobs. By adding more reserve billets to the fight, we increase our defensive and offensive systems, as well as expand our skill sets spectrum, which ultimately reduces the risk of penetration. This is important because if our political or economic infrastructure is penetrated via cyber, the U.S. risks defeat, or worse, collapse of our country. Understanding the history of

cyberattacks, and how they have advanced over the years will be important in defining where the U.S military needs to be in the future.

History of Cyber Breaches against the United States Government

In 1989, Robert Morris created what is now commonly acknowledged as the first computer worm. This self-propagating virus spread so rapidly that it succeeded in closing down much of the internet (Julian 2014). This is broadly known as the first cyber-attack on the world's cyber infrastructure. Due to the infancy of the internet at the time, the impact was nowhere near as devastating as it would be today. However, it laid the groundwork for the kinds of security issues that we have seen ever since (Julian 2014). In December of 2006, The National Aeronautics and Space Administration (NASA) was forced to block emails with attachments before shuttle launches out of fear they would be hacked (NATO 2017). Business Week reported that the plans for the latest U.S. space launch vehicles were obtained by unknown foreign intruders (NATO 2017). This is significant because unlike the first attack in 1988 where computers slowed or eventually failed, sensitive information in the NASA attack was taken and blocked from computer banks.

Furthermore, in 2006, the Naval War College in Rhode Island had to shut down all of its computer systems for two weeks following a cyber-attack (Lawfare 2015). The important take-away is that it was not until the attack occurred, that the Naval War College developed strategies for naval warfare, as well on cyberspace (Lawfare 2015). The U.S., as a country, is now at a point as a country are now at a point where cyber-attacks are ongoing and occurring any minute throughout the day.

During June of 2007, the U.S. Secretary of Defense's unclassified email account was hacked by unknown foreign intruders as part of a larger series of attacks to access and exploit the Pentagon's networks (NATO 2017). This was a direct attack on the government's political infrastructure. The cyber-attack illustrated an inability to protect our national interests. Furthermore, in 2007, spyware left the National Defense University's email systems vulnerable to attacks and the University ultimately had to take its systems offline, due to hacks by unknown foreign intruders (Lawfare 2015). The U.S. military's ability to protect our country from foreign intruders is a basis for not only our National Security Strategy, but our National Military Strategy as well.

Interestingly, in the summer of 2008, the databases of both Republican and Democratic presidential campaigns were hacked and downloaded by unknown foreign intruders (NATO 2017). Additionally, in 2008, U.S. Central Command took a hard hit from a cyber-attack (Barnes 2008). "This one was significant; this one got our attention," said one defense official (Barnes 2008). As stated in the prior comment, the U.S. military needs to strengthen its cyber warfare capabilities.

During a 2011 speech unveiling the Department of Defense's cyber strategy, the U.S. Deputy Secretary of Defense mentioned that a defense contractor was hacked and 24,000 files from the Department of Defense were stolen (NATO 2017); putting our nation's security at risk. On a smaller scale, during 2011, the Sergeant at Arms confirmed that the U.S. Senate's website had been hacked after files from the website were posted online, indicating that Lulz Security had broken into the Senate's computer network (Lawfare 2015). This year Lulz Security had successfully accomplished two other cyber-

attacks on the Central Intelligence Agency (CIA) and the Federal Bureau of Investigation (FBI) as well

Cyber defense took the stage at a NATO conference in 2013. During their first-ever meeting dedicated to cyber defense on Tuesday (June 4), NATO Defense Ministers agreed that the Alliance's cyber-defense capability should be fully operational by the autumn, extending protection to all the networks owned and operated by the Alliance (NATO 2017). Moreover, the ministers discussed the development of the role of NATO in assisting Allies under cyber-attack, including the possibility of deploying Rapid Reaction Teams (RRT) (CCDCOE 2016). The RRT is comparable to our U.S. Cyber Command Cyber Mission Force (CMF). Both teams are employed to quickly react to cyber threats, ultimately showing trends in the need of quick reaction forces throughout our services.

Finally, some of the U.S. most recent cyber threats or attack examples are attackers gaining personal sensitive information on approximately 140 million Americans from Equifax's company data, the Russian 2016 cyber warfare involvement in the U.S. presidential election, and WikiLeaks publishing CIA documents. It is in the U.S. national interest to attack those who seek to disrupt U.S. national security. That is, our military needs the most highly qualified and capable military personnel in cyber warfare to serve. A brief glance at U.S. history cyberattacks and defense shows the importance of understanding trends, vulnerabilities, as well as advances in cyber-attacks.

Assumptions

The following are assumptions in cyber warfare based on history from 1988 to the present:

1. The threats from cyber-attacks are likely to increase.
2. Additional funding for developments in U.S. cyber defense will not decrease through the next five years.
3. Cyber warfare qualified personnel will continue to receive higher pay for civilian roles than military roles, due to pressure on government spending.
4. Current reserve capabilities will not be robust enough to combat the expected increase in cyber threats of the future.

Definitions and Terms

The terms and definitions below will provide a common framework and understanding of concepts as they are presented to the reader throughout this thesis.

Cyberspace: A global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers (JP 3-12, 2017).

Cyberspace Operations: The employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace (JP 3-12, 2017).

Cyberspace Superiority: The degree of dominance in cyberspace by one force that permits the secure, reliable conduct of operations by that force, and its related land, air, maritime, and space forces at a given time and place without prohibitive interference by an adversary (JP 3-12, 2017).

Department of Defense Information Networks: Operations to design, build, configure, secure, operate, maintain, and sustain Department of Defense networks to

create and preserve information assurance on the Department of Defense information networks (JP 3-12, 2017).

Defensive Cyberspace Operations: Passive and active cyberspace operations intended to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities, and other designated systems (JP 3-12, 2017).

Information Assurance: Actions that protect and defend information systems by ensuring availability, integrity, authentication, confidentiality, and nonrepudiation. (JP 3-12, 2017).

Offensive Cyberspace Operations: Cyberspace operations intended to project power by the application of force in or through cyberspace (JP 3-12, 2017).

Limitations and Delimitations

The restrictions placed on this paper are the shortcomings that are beyond the researcher's control, and that will place restrictions on methodology or conclusions. Time to conduct research, and the ability to travel to USCYBERCOM will be some shortfalls in formulating the findings and recommendations of this study. Delimitations are the boundaries within which this paper will stay. For instance, this paper will only examine doctrine, organization, training, leadership and education, and personnel as evaluation criteria to answer the primary and secondary research questions.

Chapter Conclusion

Chapter 2, discusses how the literature informs answers to the following secondary research question: Should the U.S. military add more reserve billets to

USCYBERCOM over the next five years in order to increase our defensive and offensive capabilities so that we reduce our risk of penetration?

By answering the secondary research questions, staying within the parameters of the study, one will understand the conclusions and recommendations of the primary research question "Do reserve units provide the best opportunities for cyberspace professionals by allowing reservists to practice their cyber skills in the civilian world?"

CHAPTER 2

LITERATURE REVIEW

Chapter Introduction

The literature review will define the parameters in which information is sought to answer the primary question of, "Do reserve units provide the best opportunities for cyberspace professionals, by allowing reservists to practice their cyber skills in the civilian world?" It is critical to understand guiding strategic Department of Defense (DoD) cyber policies, National Defense Strategy 2018, and the Cybersecurity National Action Plan (CNAP) before diving into USCYBERCOM and Reserve Units capabilities and gaps. Furthermore, the literature review will explore service specific doctrine, organization, training, leadership, and current personnel systems. This is of significance because the strategies and systems lay the foundations for how the units or commands operate, and where the most significant gap could lie.

Department of Defense Cyber Strategies

The Department of Defense 2015 Cyber Strategy covers strategic goals, implementation of those objectives, and then managing that strategy. It further defines three cyber missions for DoD: (1) defend its own network and systems, and information (2) protect U.S. interests against cyberattacks or significant attacks (3) directed by the President or the Secretary of Defense, DoD must be able to provide integrated cyber capabilities to support military operations and contingency plans.

DoD then further lays out strategic goals for its cyber mission: (DoD Cyber Strategy 2015)

1. Build and maintain ready forces and capabilities to conduct cyberspace operations;
2. Defend the DoD information network, secure DoD data, and mitigate risks to DoD missions;
3. Be prepared to defend the U.S. homeland and U.S. vital interests from disruptive or destructive cyberattacks of significant consequence;
4. Build and maintain viable cyber options and plan to use those options to control conflict escalation and to shape the conflict environment at all stages;
5. Build and maintain robust international alliances and partnerships to deter shared threats and increase global security and stability.

To achieve these goals, implementation and funding is needed at all levels. Put differently, due to the race in the advancement of technology, a broad range of skill sets throughout our military and its respective cyber warfare commands is needed to meet these challenges.

National Defense Strategy (2018)

The National Defense Strategy (2018) speaks to how today, the U.S. is contested in every domain – air, land, sea, space, and cyberspace. This represents a change in our global security environment. However, "for decades, the United States has enjoyed uncontested or dominant superiority in every operating domain" (National Defense Strategy 2018). Furthermore, cyber hackers are now non-state actors that threaten our nation's security environment. Due to this increasing threat of space and cyberspace as warfighting domains, the National Defense Strategy (2018) provides the following guidance:

> The Department will prioritize investments in resilience, reconstitution, and operations to assure our space capabilities. We will also invest in cyber defense, resilience, and the continued integration of cyber capabilities into the full spectrum of military operations.

Which then defaults to an "increase in personnel and platforms to meet key capability and capacity needs" (National Defense Strategy, 2018).

U.S. Cyber Command (USCYBERCOM)

The mission of USCYBERCOM is in line with achieving the DoD Cyber defense strategies. USCYBERCOM plans, coordinates, integrates, synchronizes, and conducts activities to: direct the operations and defense of specified Department of Defense information networks and; prepare to, and when directed, conduct full-spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries (USSTRATCOM 2017). Approximately 1,100 people (military, civilians, and contractors) serve at USCYBERCOM, with a Congressionally-appropriated budget for Fiscal Year 2015 of approximately $509 million for Operations and Maintenance (O&M), Research, Development, Test and Evaluation (RDT&E), and military construction (MILCON) (Rogers 2015). USCYBERCOM works with both private and public sector to secure infrastructure that can affect our economic stability. Furthermore, in 2017 USCYBERCOM elevated from a Sub Unified Combatant Command to a Combatant Command.

USCYBERCOM gaps include the help in hiring personnel, filling cyber team seats, intelligence and planning staffs, facilities to train and employ them, and resources to equip properly. This is a reflection of USCYBERCOM being built from the ground up

by cutting manning to the bone, initially sacrificing vital support functions and institutional infrastructure to create mission capabilities as fast as possible (Rogers, 2015). Another example of a USCYBERCOM gap is the inability to find qualified personnel to fill their cyber teams. USCYBERCOM is working on forming Cyber Mission Forces (CMF) to turn strategy plans in to operational outcomes (Rogers 2015). USCYBERCOM is hard pressed to find qualified personnel to man their CMF rosters, to get cyberspace professionals cleared and trained and supported across all 133 teams (Rogers 2015). In conclusion, that due to lack of funding and qualified manpower at USCYBERCOM, we as a nation, risk our national security.

Cyber National Action Plan

The cyber national action plan is the capstone of more than seven years of determined effort by this Administration, building upon lessons learned from cybersecurity trends, threats, and intrusions (CNAP 2017). This plan directs the Federal Government to take new action now and fosters the conditions required for long-term improvements in the U.S. approach to cybersecurity across the Federal Government, the private sector, and our personal lives (CNAP 2017). Highlights of the CNAP include actions to:

1. Establish the "Commission on Enhancing National Cybersecurity."
2. Modernize Government IT and transform how the Government manages cybersecurity
3. Empower Americans to secure their online accounts by moving beyond just passwords and adding an extra layer of security.

4. Invest over $19 billion for cybersecurity as part of the President's Fiscal Year (FY) 2017 Budget (CNAP 2017)

Through these actions, additional new steps outlined below, and other policy efforts spread across the Federal Government, the Administration has charted a course to enhance our long-term security and reinforce American leadership in developing the technologies that power the digital world (FACT SHEET: Cybersecurity National Action Plan 2017).

Better securing our own digital infrastructure is only part of the solution. The U.S. must lead the international effort in adopting principles of responsible state behavior, even while we take steps to deter and disrupt malicious activity. The U.S. cannot pursue these goals alone – we must pursue them in concert with our allies and partners around the world (CNAP 2017). To implement these sweeping changes, the Federal Government will need to invest additional resources in its cybersecurity. That is why the 2017 Budget allocates more than $19 billion for cybersecurity – a more than 35 percent increase over the 2016 enacted level. These resources will enable agencies to raise their level of cybersecurity, help private sector organizations and individuals better protect themselves, disrupt and deter adversary activity, and respond more effectively to incidents (CNAP 2017).

Reserve and Active Cyber Units

Throughout the U.S. military respective services, we have reserve units, which support active duty cyber units. To rearticulate, every reserve unit is attached to an active duty command. For example, the Army has Army Reserve Cyber (signalmen), Navy has reserve Information Professionals, there are Cyber Warfare Operation professionals

within the Air Force Reserve, and the Marines have reserve Cyber Network Operators, all of which are attached to reserve units that support their respective active duty commands. The significance of our reserve cyberspace operations personnel is the diverse skill sets they bring to the fight that the active duty personnel may not have. In several areas, such as critical infrastructure, both USCYBERCOM and the Services have recognized that our Reserve Component brings us unique and valuable skills (Rogers 2015).

Interestingly, throughout the literature review, it has not been possible to categorically prove that existing cyber units cannot combat cyber threats in the future. However, it is fair to assume that with growing cyber threats from multiple actors, there will always be a demand for more and better cyber technicians. The problem U.S. military see's now is recruiting cyber professionals to fill active duty gaps, not reserve cyber gaps. Therefore, it is important to use the reserve cyberspace operations personnel currently available.

Doctrine, Organization, Training, Leadership and Education, and Personnel

While looking to answer the primary research question, "Do reserve units provide the best opportunities for cyberspace professionals by allowing reservists to practice their cyber skills in the civilian world?" this paper will explore Doctrine, Organization, Training, Leadership and Education, and Personnel. Service specific and joint doctrinal literature will be of significance; because it provides the most up to current literature our military has to offer regarding their cyber offensive and defensive approach using reserves. Below is a list of service specific and joint doctrine that will be explored in order to answer the primary research question, and the secondary and tertiary questions:

Navy – Navy Information Operations, NWP 3-13; Navy Strategic Plan 2015-2020

Marine Corps – Marine Corps Cyberspace Operations, MCIP 3-32Ei; Marine Corps Strategy for Assured Command and Control; Marine Corps Concept of Cyber Operations; Marine Corps Information Enterprise Strategy (MCIENT)

Air Force – Annex 3-12 Cyberspace Operations, 24th Air Force Commanders Strategic Vision

Army – Cyberspace and Electronic Warfare Operations (FM 3-12), United States Army Center of Cyber Excellence Strategic Plan;

Joint – Cyberspace Operations (JP 3-12, 2017); Cyber Mission Analysis, Mission Analysis for Cyber Operations of Department of Defense

Chapter Conclusion

Chapter 3 will outline the research methodology used to answer the following secondary research question: Should the U.S. military add more reserve billets to U.S. Cyber Command (USCYBERCOM) over the five years in order to increase our defensive and offensive capabilities so that we reduce our risk of exposure to cyberspace threats?

By answering the secondary research questions staying within the parameters of the research, one will understand the conclusions and recommendations of the primary research question, "Do reserve units provide the best opportunities for cyberspace professionals by allowing reservists to practice their cyber skills in the civilian world?"

CHAPTER 3

RESEARCH METHODOLOGY

Chapter Introduction

This chapter will explore whether current Doctrine, Organization, Training, Leadership and Education, and Personnel will need to change throughout both Reserve and Active duty and how it needs to be addressed in order to answer, "Do reserve units provide the best opportunities for cyberspace professionals, by allowing reservists to practice their cyber skills in the civilian world?" The applicability of this framework is due to its context during the acquisitions process. For example, when the military was looking at filling a capability gap of access to littorals, the process involved identifying what part of the doctrine, training, leadership and education, and personnel would need to be changed or not. In summary, exploring only one evaluation criteria would yield a biased result, and therefore, five criteria will be evaluated in order to avoid the bias.

Evaluation Criteria

The researcher must consider doctrine across all military services to answer the primary research question. The doctrine analysis examines the way the military fights its conflicts with emphasis on maneuver warfare and combined air-ground campaigns to see if there is a more accurate method that could be used to solve a capability gap (DOTMLPF-P Analysis 2017). For example, the Army has FM 3-12 (*Cyberspace and Electronic Warfare Operations*), the Air Force utilizes Air Force Doctrine Document 3-12, Marines reference Marine Corps Concept for Cyberspace Operations, and the Navy has an NWP 3-13, and jointly we use Joint Pub 3-12. This is important because one must

analyze existing doctrine that addresses or relates to the analysis and eventual acquisition. Is it Joint? Service? Agency? (DOTMLPF-P Analysis 2017). Are there operating procedures in place that are not being followed which contribute to the identified need (DOTMLPF-P Analysis 2017)? Therefore, because there is doctrine to be explored through each service, one must take this into consideration in order to answer the primary research question.

Organization must be considered as a part of the framework to answer the primary research question. An organizational analysis examines how the U.S. military are organized to fight; divisions, air wings, Marine-Air Ground Task Forces, and other (DOTMLPF-P Analysis 2017). Among the services, the following organizations exist; Army Cyber Command (2nd Army), Air Force Cyber Command (24th Air Force), Fleet Cyber Command (10th Fleet), Marine Forces Cyber, which are all components of USCYBERCOM. By examining the organization, one can look to see if there is a more improved organizational structure or capability that can be developed to solve a capability gap (DOTMLPF-P Analysis 2017). Where is the problem occurring? Which organizations is the problem occurring in? Is the organization properly staffed and funded to deal with the issue? (DOTMLPF-P Analysis 2017). In conclusion, organizations are in place throughout the services, which must be explored to answer the primary research question.

Additionally, this paper will explore cyberspace training throughout the services to answer the primary research question. This training analysis will examine how the U.S. military prepares our forces to fight tactically from basic training, advanced individual training, various types of unit training, joint exercises, and other ways to see if

improvement can be made to offset capability gaps (DOTMLPF-P Analysis 2017). All services have training pipelines in place for their cyberwarfare professionals. Therefore, this research will examine the longevity, the broadness of skill sets taught, and the validity of training. This will be key to understand if the issue is caused, at least in part, by a complete lack of or inadequate training, and does training exist which addresses the issue (DOTMLPF-P Analysis 2017)? Therefore, because training is in place throughout the services it must be explored to answer the primary research question.

Furthermore, the researcher will need to consider leadership and education as part of the framework for answering the primary research question. The leadership and education analysis examine how the U.S. military prepares our leaders to lead the fight from squad leader to 4-star general/admiral and their overall professional development (DOTMLPF-P Analysis 2017). All services have leadership and education development starting from initial enlistment or commission to 4-star level. Understanding the pipeline will help the researcher answer the following: Does leadership understand the scope of the problem, and does leadership have resources at its disposal to correct the issue (DOTMLPF-P Analysis 2017)?

Finally, the researcher will study cyber warfare personnel throughout our services to answer the primary research question. The personnel analysis will examine the availability of qualified people for peacetime, wartime, and various contingency operations to support a capability gap by restructuring (DOTMLPF-P Analysis 2017). Throughout the U.S. military services, we have cyber warfare professionals in both the enlisted and officer communities. While examining these communities, the researcher will specifically examine: Is the issue caused, at least in part, by the inability or decreased

the ability to place qualified and trained personnel in the correct occupational specialties, and are the right personnel in the right positions (skill set match) (DOTMLPF-P Analysis 2017)? Therefore, because personnel are in place throughout the services, one must examine this area to answer the primary research question.

Table 1. Evaluation Criteria (DOTLP)

	Army	**Navy**	**Air Force**	**Marine Corps**
Doctrine				
Organization				
Training				
Leadership and Education				
Personnel				

1 pt = Change / 0 pt = No Change

Source: Created by author.

Research Methodology

The researcher's approach to addressing the following steps 2-4will be to consider doctrine, organization, personnel, leadership, and training.

Step 1: Summary of Literature Review – The literature will explore doctrine, organization, training, leadership and education, and personnel from the Navy, Army, Air Force, Marines, and USCYBERCOM.

Step 2: Do reserve units provide the best opportunities for cyberspace professionals, by allowing reservists to practice their cyber skills in the civilian world?

Step 3: Should the U.S. military add more reserve billets to USCYBERCOM over the next five years?

Step 4: Should the U.S. military add more reserve billets to USCYBERCOM over the next five years IOT increase our defensive and offensive capabilities so that we reduce our risk of penetration?

Step 5: Aggregation of answers to Secondary Questions

Step 6: Conclusion(s) (Answer to Primary Question)

Threats to Validity and Biases

There will be threats to validity and biases throughout the research to answer the primary research question. One threat of this paper will be a bias based on a school of thought, such as, reservists make better soldiers, sailors, airmen, and marines based on their civilian experiences. Another bias throughout this research, is at times, documents appear to range from 1-10 years old from the current year, 2018, leaving the analysis to be based on ideas or facts that are outdated. Furthermore, this paper only reviews doctrine, organization, training, leadership and education, and personnel from the Navy, Army, Air Force, Marines, and USCYBERCOM. Additionally, a threat to validity is that the author is not a cyberspace operational professional; therefore, the author depends on the value of research. In conclusion, it will be important that the reader takes this into consideration when reading the conclusions and recommendations in Chapter 5.

Chapter Conclusion

Chapter 4 will outline the data and analysis and summarize the literature review to answer the following research questions:

1. Do reserve units provide the best opportunities for cyberspace professionals, by allowing reservists to practice their cyber skills in the civilian world?

2. Should the U.S. military add more reserve billets to USCYBERCOM over the next five years?
3. Should the U.S. military add more reserve billets to U.S. Cyber Command (USCYBERCOM) over the five years to increase our defensive and offensive capabilities so that we reduce our risk of penetration?

This research will fill the gaps by allowing for a comprehensive review that will yield explicit consideration to existing evidence, which is necessary for the identification and development of unanswered and answerable questions (Robinson, 2013). Finally, by answering the research questions, and staying within the parameters of the research, one will understand the conclusions and recommendations of the primary research question, "Do reserve units provide the best opportunities for cyberspace professionals by allowing reservists to practice their cyber skills in the civilian world?"

CHAPTER 4

DATA PRESENTATION AND ANALYSIS

Chapter Introduction

This chapter will present results of the literature review, analysis of Doctrine, Organization, Leadership and Education, Training, and Personnel considerations by service using criteria established in the methodology. Specifically, the analysis of service specific and joint Doctrine, Organization, Leadership and Education, and training will be applied while seeking to answer the primary research question, "Do reserve units provide the best opportunities for cyberspace professionals, by allowing reservists to practice their cyber skills in the civilian world?" Furthermore, the same analysis will be applied to answer the secondary and tertiary research questions, "Should the U.S. military add more reserve billets to USCYBERCOM over the next five years in order to increase our defensive and offensive capabilities so that we reduce our risk of penetration?" While seeking to analyze and applying the evaluation criteria set forth in Chapter 3, conclusions and recommendations will be made in order to answer the primary research question.

Step 1: Results of the Literature Review

The results of the literature review indicated that significant amounts of data exist that covers strategies, policies, capabilities, and gaps for challenges the U.S. military faces in the cyber domain. However, there is little if any research and analysis on adequately utilizing the existing workforce, or generating a more capable workforce. The weight of these findings is of importance when it involves answering the primary research question, "Do reserve units provide the best opportunities for cyberspace

professionals, by allowing reservists to practice their cyber skills in the civilian world?" understanding where the most significant gap lies. Furthermore, the service-specific literature covering doctrine, organization, training, personnel, and leadership is such that if we were adequately utilizing the existing workforce, strength-wise, the literature suggests that we as a country have a solid foundation of information and strategy on how to best fight the current cyber warfare fight.

Step 2: Answering the Primary Research Question

Step 2 will address the primary research question, "Do reserve units provide the best opportunities for cyberspace professionals, by allowing reservists to practice their cyber skills in the civilian world?" This section will explore Army, Navy, Air Force, and Marine Corps current doctrine, organization, personnel, training, and leadership as it applies to the primary research question, "Do reserve units provide the best opportunities for cyberspace professionals, by allowing reservists to practice their cyber skills in the civilian world?"

Doctrine

Army – FM 3-12 Cyber Space and Electronic Warfare Operations dated April 2017 is the current Army doctrine with topics such as Cyberspace and Electronic Warfare Operations, Fundamentals, Relationships with Cyberspace Operations and Electronic Warfare, Cyberspace Electromagnetic Activities within Operations, and Integration with unified action partners. These topics suggest that a holistic operational approach at the current cyberspace fight is covered assuming workforce availability and skill sets; which

means, it fails to address the gaps in skill sets that could be augmented by the reserve force. Therefore, it does not answer the primary research question.

Navy – Navy Warfare Publication (NWP) Navy Information Operations 3-13 is the current doctrine that the Navy is operating off ~~of~~. The doctrine covers topics such as Information Operations Fundamentals, Information Related Capabilities, Information Operations Organizational Relationships and Forces, and Information Operations and Planning. With regards to the Navy, the texts suggest that a holistic operational approach at the current cyberspace fight is covered assuming the workforce availability and skill sets; which means, it fails to address the gaps in skill sets that could be augmented by the reserve force. Therefore, the NWP 3-13 does not answer the primary research question.

Air Force – Annex 3-12 Cyberspace Operations is the current doctrine that the Air Force is operating. The doctrine covers topics such as Policy Related to Command and Organization of Cyberspace Forces, Organization of Cyberspace Forces, Command and Control of Cyberspace Forces, and Design of Cyberspace Operations. The topics suggest that a holistic operational approach and strategy at the current cyberspace fight is covered assuming the workforce availability and skill sets; which means, it fails to address the gaps in skill sets that could be augmented by the reserve force Therefore, Annex3-12 does not answer the primary research question.

Marine Corps – Marine Corps Cyberspace Operations MCIP 3-32Ei is the current doctrine that the Marine Corps is operating. The doctrine covers topics such as Fundamentals of Cyberspace, Fundamentals of Cyberspace Operations, National/Joint Concepts Policy, Command Authorities and Organizations, Marine Corps Roles and Responsibilities, Authorities, Legal Considerations, Planning Cyberspace Operations,

Integrating Cyberspace Operations into Marine Air-Ground Task Force (MAGTF) Operations, Cyber Mission Force, MAGTF Cyberspace and Electronic Warfare Coordination Cell, and Joint Informational Environment. The topics suggest that a holistic operational approach and strategy at the current cyberspace fight is covered assuming the workforce availability and skill sets; which means, it fails to address the gaps in skill sets that could be augmented by the reserve force. Therefore, MCIP 3-32Ei does not answer the primary research question.

Table 2. Doctrine (Primary Research Question)

	Army	**Navy**	**Air Force**	**Marine Corps**
Do reserve units provide the best opportunities for cyberspace professionals, by allowing reservists to practice their cyber skills in the civilian world?	1	1	1	1

1 point = Change / 0 point = No Change

Source: Created by author.

Organization

Among the services, the U.S. military have the following organizations: Army Cyber Command (2nd Army), Air Force Cyber Command (24th Air Force), Fleet Cyber Command (10th Fleet), Marine Forces Cyber, which are all components of USCYBERCOM. Each service has an overarching body that organizes their services in such a way to fight the battle in the cyber domain. However, the service-specific command structures do not accurately answer the primary research question, nor do they provide a specific breakdown of where reserve units can augment the gaps on a daily

basis. For example, if U.S. Northern Command (USNORTHCOM) needs a reservist planner, GovDelivery advertises the requirements through a mass email to reserve personnel, in order to seek a pool of applicants from which the most appropriate candidate can be selected. The problem with this is there is no organization to filter or guide the process of selection in order to fill the gap.

Table 3. Organization (Primary Research Question)

	Army	**Navy**	**Air Force**	**Marine Corps**
Do reserve units provide the best opportunities for cyberspace professionals, by allowing reservists to practice their cyber skills in the civilian world?	1	1	1	1

1 point = Change / 0 point = No Change

Source: Created by author.

Leadership and Education

All services have leadership and education development starting from initial enlistment or commission to 4-star level. Whether one comes into the service with prior cyberspace operational experience or not, there are pipelines within each service for ~~our~~ cyberspace professionals to take that will improve their leadership and education. This is implemented from the beginning of service due to professional wickets that must be met in order to make promotion. Due to these constraints (professional wickets) that are placed upon our active cyberspace personnel, it is more than likely that the cyberspace reservist has more time to expand his skill sets than that of the active duty personnel. Furthermore, ~~our~~ active cyberspace operations professionals are stove piped into specific

leadership skills and education that they will be provided, limiting their creativity. This is why there have been programs situated for active duty members to leave service, and re-enter active service after two or three years in civilian service so that they may broaden their skill sets. Alternatively, the reserve cyberspace professional working in civilian jobs (non-government) leadership and educational pipelines demand more flexibility, due to the broader skill sets that are needed. Furthermore, most cyber reservist has more time to expand their skill sets and creativity due to the nature of their jobs. In short, leadership and education are a supporting function to answering the primary research question.

Table 4. Leadership and Education (Primary Research Question)

	Army	**Navy**	**Air Force**	**Marine Corps**
Do reserve units provide the best opportunities for cyberspace professionals, by allowing reservists to practice their cyber skills in the civilian world?	1	1	1	1

1 point = Change / 0 point = No Change

Source: Created by author.

Training

All services prepare U.S. forces to fight tactically from basic training, advanced individual training, various types of unit training, joint exercises, and other ways to see if improvement can be made to offset capability gaps (DOTMLPF-P Analysis 2017). All services have training pipelines in place for their cyberwarfare professionals. While considering the different training pipelines for ~~our~~ cyberspace professionals, it is evident that the training is not lacking, and this is not where the gap lies, but rather the lack of

qualified personnel to fill the gap. Therefore, training does not need to change to answer the primary research question.

Table 5. Training (Primary Research Question)

	Army	**Navy**	**Air Force**	**Marine Corps**
Do reserve units provide the best opportunities for cyberspace professionals, by allowing reservists to practice their cyber skills in the civilian world?	0	0	0	0

1 point = Change / 0 point = No Change

Source: Created by author.

Personnel

All services currently have initiatives to increase their personnel size with skill sets specific to cyberspace operations. It is essential to have the availability of qualified people for peacetime, wartime, and various contingency operations to support the capability gap. While examining both officer and enlisted cyberspace communities, the issue caused, at least in part, is by our services inability to attract and place qualified and trained personnel into correct occupational specialties. Furthermore, our failure to adequately use our cyber reserve force is resulting in not putting the available staff in the right positions (skill set match). Therefore, in response to the primary research question, personnel doe need to change.

Table 6. Personnel (Primary Research Question)

	Army	Navy	Air Force	Marine Corps
Do reserve units provide the best opportunities for cyberspace professionals, by allowing reservists to practice their cyber skills in the civilian world?	1	1	1	1

1 point = Change / 0 point = No Change

Source: Created by author.

Step 3: Answering the First Secondary Question

Step 3 will address the second secondary question, "Should the U.S. military add more reserve billets to USCYBERCOM over the next five years? This section will explore USCYBERCOM current doctrine, organization, personnel, training, and leadership as it applies to the secondary research question, "Should the U.S. military add more reserve billets to USCYBERCOM over the next five years?"

Doctrine

USCYBERCOM utilizes Joint Publication 3-12 Cyberspace Operations to guide and control everyday procedures and functions at USCYBERCOM. This is essential to ensuring a standardization of processes and understanding of the respective service cyber missions USCYBERCOM personnel support on a day to day basis. Topics within the Joint Publication 3-12 Cyberspace Operations include: Integrating Cyberspace Operations; The Joint Force and Cyberspace; Military Operations In and Through Cyberspace; National Intelligence Operations In and Through Cyberspace; Department of Defense Ordinary Business Operations In and Through Cyberspace; The Joint functions

and Cyberspace Operations, Authorities; Roles, and Responsibilities; and Planning and Coordination; Joint Operation Planning Process and Cyberspace Operations; Cyberspace Operations Planning Considerations; Command and Control of Cyberspace Operations; Synchronization of Cyberspace Operations; Assessment of Cyberspace Operations; Interorganizational Considerations; Multinational Considerations. These topics are significant because they provide an unclassified approach and understanding to Cyberspace Operations. However, Joint Publication 3-12 does not take into consideration the reserve force, or potential utilization of them. Concluding in order to answer the secondary research question, doctrine must change.

Table 7. Doctrine (Secondary Research Question)

	Army	**Navy**	**Air Force**	**Marine Corps**
Should the U.S. military add more reserve billets to USCYBERCOM over the next five years?	1	1	1	1

1 point = Change / 0 point = No Change

Source: Created by author.

Organization

USCYBERCOM was recognized in 2017 as a Combat Command. Department of Defense has recognized the importance of cyber and its challenges resulting in its nomination, to enable cyber to be given the priority it needs. Therefore, no one today can exert or maintain national power without acute sensitivity to the digital networks that underpin the world's communications, prosperity, and security (Rogers, 2015).

Additionally, by USCYBERCOM nature of being a Combat Command, it employs all sectors of the Department of Defense, Interagency, and also partners with private organizations to achieve its mission. Consequently, it may be evident that USCYBERCOM is employing the respective service's reservist. However, there is no suggestion that the unique opportunity is being correctly recognized or implemented.

Table 8. Organization (Secondary Research Question)

	Army	**Navy**	**Air Force**	**Marine Corps**
Should the U.S. military add more reserve billets to USCYBERCOM over the next five years?	1	1	1	1

1 point = Change / 0 point = No Change

Source: Created by author.

Leadership and Education

Much like the discussion in answering the primary research question regarding leadership and education, similarly, in this instance, our services have prepared our leaders for the fight who are attached to USCYBERCOM. That is, the Commander's staff at USCYBERCOM have the skills and expertise to help facilitate the mission and strategies set forth. Furthermore, because of the ever-changing and unstable cyber environment, leadership and education will continue to be essential to USCYBERCOM responsiveness. It is evident that while understanding the big picture of USCYBERCOM, leadership and education is not what is lacking within USCYBERCOM, rather the workforce with the skill sets needed that can hold the necessary clearance. Conversely,

though, it will take leadership and education to implement change and the new way of conducting business. Therefore, leadership and education will definitively have to change to answer the secondary research question.

Table 9. Leadership and Education (Secondary Research Question)

	Army	**Navy**	**Air Force**	**Marine Corps**
Should the U.S. military add more reserve billets to USCYBERCOM over the next five years?	1	1	1	1

1 point = Change / 0 point = No Change

Source: Created by author.

Training

Training is essential to the success of any mission. It is not about just understanding the specific function, one must understand the domains around them as well. For instance, when service specific teams get ready for deployments, on average, units can take up to six months prior to deployment to be fully ready to mobilize. This is significant because, without the proper training, and understanding of all the domains involved, a unit would likely not have mission success. USCYBERCOM's initiative to have cyber force teams is considered a crucial asset to both offensive and defensive cyber warfare. In order to deploy these cyber force teams, training effectively will be essential, resulting in, a workforce that has the necessary skill sets, understanding of the domains, and the agility to perform these missions. The following exert explains the focus and strategy of USCYBERCOM cyber mission force teams:

> The focus of USCYBERCOMs Cyber Mission Force teams aligns with the DoD Cyber Strategy's three primary missions: Defend DoD networks and ensure their data is held secure; support joint military commander objectives; and, when directed, defend U.S. critical infrastructure. Specifically, Cyber Mission Force teams support these mission sets through their respective assignments:
>
> -- Cyber National Mission Force teams defend the nation by seeing adversary activity, blocking attacks, and maneuvering to defeat them.
>
> -- Cyber Combat Mission Force teams conduct military cyber operations in support of combatant commands.
>
> -- Cyber Protection Force teams defend the DoD information networks, protect priority missions and prepare cyber forces for combat.
>
> -- Cyber Support teams provide analytic and planning support to National Mission and Combat Mission teams (USCYBERCOM News Release, 0ctober 24, 2018).

It is clear that the Commander of USCYBERCOM has recognized a gap in defense and offense, and therefore has created expeditionary and deployable cyber mission force teams. Therefore, training is not what needs to change based on data; instead it is the need for people to participate in the training. Thus, training does speak to the secondary question, as it is a subset of the secondary research question.

Table 10. Training (Secondary Research Question)

	Army	**Navy**	**Air Force**	**Marine Corps**
Should the U.S. military add more reserve billets to USCYBERCOM over the next five years?	0	0	0	0

1 point = Change / 0 point = No Change

Source: Created by author.

Personnel

USCYBERCOM does not have the availability of qualified people for peacetime, wartime, and various contingency operations to support the capability gap (Rodgers 2015). Additionally, our services do not have enough cyberspace professionals amongst both the enlisted and officer communities to defend themselves and USCYBERCOM demands. One must take this into consideration because USCYBERCOM lacks a sufficient workforce to succeed at daily strategic missions. Similarly, it is not just USCYBERCOM that is lacking personnel, but is a trend through all the services, attaining and retaining cyberspace professionals. Finally, the U.S. military cannot efficiently use our cyber reserve force that is resulting in not placing the available personnel in the right positions (skill set match). Therefore, personnel do need to change to answer the primary research question.

Table 11. Personnel (Secondary Research Question)

	Army	**Navy**	**Air Force**	**Marine Corps**
Should the U.S. military add more reserve billets to USCYBERCOM over the next five years?	1	1	1	1

1 point = Change / 0 point = No Change

Source: Created by author.

Step 4: Answering the Third Secondary Question

Step4 will address the third secondary question, "Should the U.S. military add more reserve billets to USCYBERCOM over the next five years IOT increase our

defensive and offensive capabilities so that we reduce our risk of penetration?" This section will explore Army, Navy, Air Force, and Marines current strategic cyber doctrine, organization, personnel, training, and leadership as it applies to the tertiary research question, "Should the U.S. military add more reserve billets to USCYBERCOM over the next five years IOT to increase our defensive and offensive capabilities so that we reduce our risk of penetration?"

Doctrine

Army – Army current strategic doctrine is United States Army Cyber Center of Excellence Strategic Plan.

> This document provides a strategy and framework to trans- form the Cyber CoE and Team Gordon (tenant organizations and community partners), develop concepts, doctrine, requirements, integrate cyberspace operations and train Soldiers and leaders. This strategy defines the Cyber CoE vision, mission, lines of effort, strategic imperatives, and objectives required to integrate capabilities across the Army to include the Army's signal, electronic warfare (EW), and military intelligence (MI) partners (see Figure 1) together with other Joint Service and Intelligence capabilities.

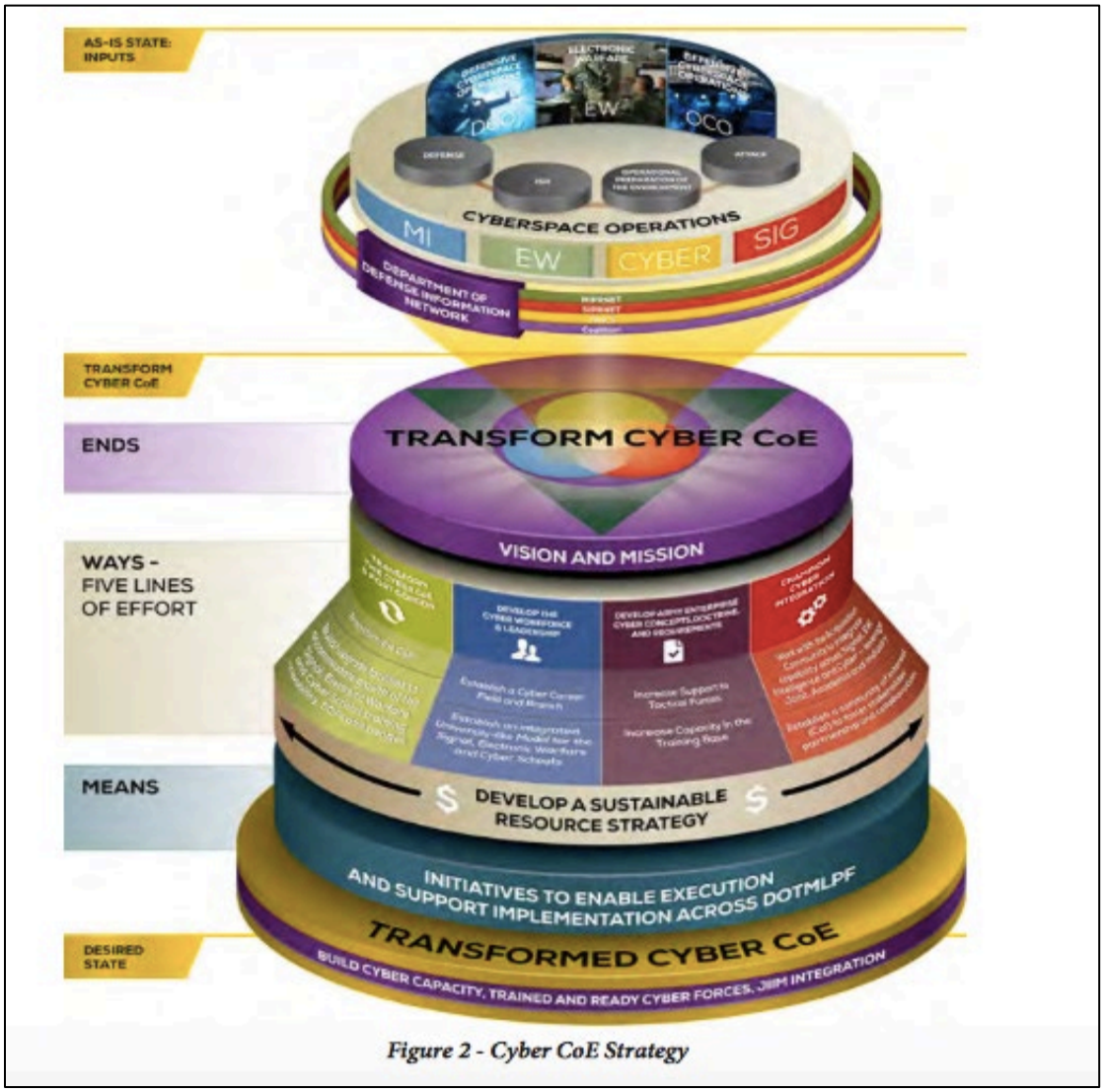

Figure 1. Cyber Center of Excellence Strategy

Source: U.S. Army Cyber Center of Excellence Strategy 2015

Moreover, there is a definitive strategy that the Army has considered addressing the current cyber problems that U.S. faces in today's multi-domain fight. This is substantial because a lack of understanding on how to address the issue can only lead to mission failure. Furthermore, the US Army Cyber strategy speaks explicitly to the

utilization and adaptability of all components (Active, Reserve, and Guard). In summary, the strategic vision speaks to reducing the risk of penetration. However, it does not explicitly address the ways and means in which they can utilize reserve, guard manpower to augment USCYBERCOM gaps. Additionally, the strategic vision merely speaks to being able to leverage Army, Joint, and CYBERCOM capabilities; however, it does not address the third secondary question.

Navy- Navy current Strategic Doctrine is U.S. Fleet Cyber Command / 10th Fleet Strategic Plan 2015-2020. This strategic plan covers five strategic goals. The strategic plan entirely speaks to the idea of reducing our penetration of risk over the next five years and does talk to utilizing our reserve component to augment the CMF teams, due to the civilian professional expertise and perspective they bring to the Navy Roles. The following are strategic goals from U.S. Fleet Cyber Command/Tenth Fleet Strategic Plan 2015-2020:

Strategic Goal 1: Operate the Network as a Warfighting Platform

Strategic Goal 2: Conduct Tailored Signals Intelligence

Strategic Goal 3: Delver Warfighting Effects Through Cyberspace

Strategic Goal 4: Create Shared Situational Awareness

Strategic Goal 5: Establish and Mature Navy's Cyber Mission Forces

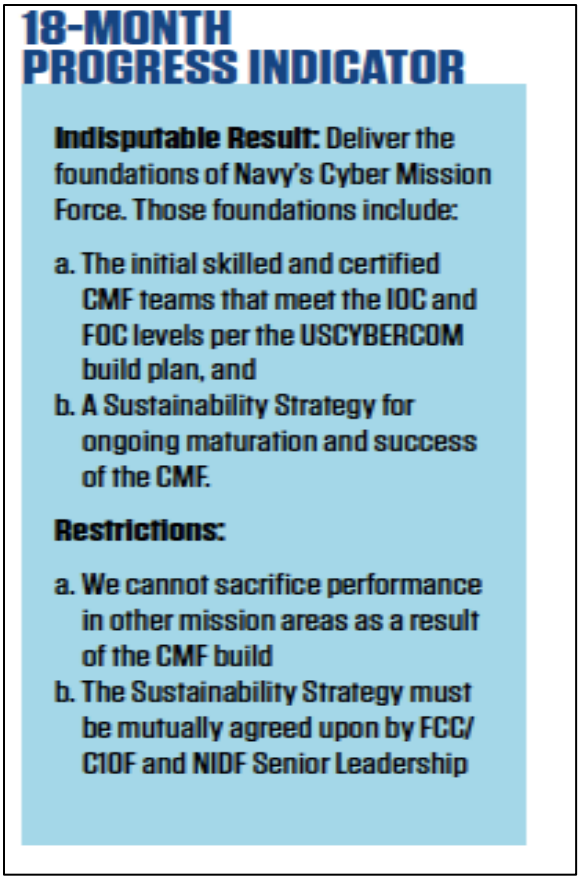

Figure 2. 18-Month Progress Indicator (NAVY)

Source: U.S. Fleet Cyber Command/Tenth Fleet Strategic Plan 2015-2020.

Conversely, like the Army Strategic Cyber plan, it explores ends ways and means in order to achieve cyber protection now and in the future. Furthermore, the Navy strategic plan speaks to how the Navy Strategic Cyber Plan aligns with USCYBERCOM Commander Vision and Guidance. Moreover, unlike the US Army Strategic plan it specifically speaks to how the Navy will address USCYBERCOM "U.S. Cyber Command specifically addresses that "USCYBERCOM has directed each of the services to establish the teams that will compose the Cyber Mission Force. FCC/C10F has been charged with the first stand up and development of 40 CMF teams on behalf of the Navy

(Navy Strategic Cyber Plan 2015-205).” Additionally, Navy current Strategic Doctrine is U.S. Fleet Cyber Command / 10th Fleet Strategic Plan 2015-2020 lays out an 18-month progress indicator (see Figure 03) to outline what the result will look like, including restrictions that shall be put in place as not to interrupt current Navy missions. Therefore, it can be inferred the Navy should add more reserve billets to USCYBERCOM

Air Force – Current strategic doctrine for Air Force Cyber is the Commander Strategic Vision. Air Force Strategic Priorities are the following:

1. Employ Multi-Domain and Integrated Cyberspace Capabilities in support of Combatant and Air Force Component Commanders
2. Develop and Empower Airman and Take Care of Their Families
3. Lead Through Teamwork and Partnerships
4. Inculcate a Strong Warfighting Culture into Cyberspace Operations
5. Equip the Force with Rapid, Innovative, Fielding of Cyber Capabilities.

This indicates that the pillars of Air Force cyber strategic priorities are what achieve the Air Force cyber mission “American Airmen Delivering Full-spectrum Global cyberspace capabilities and Effect for our Service, the Joint Force, and our Nation.”

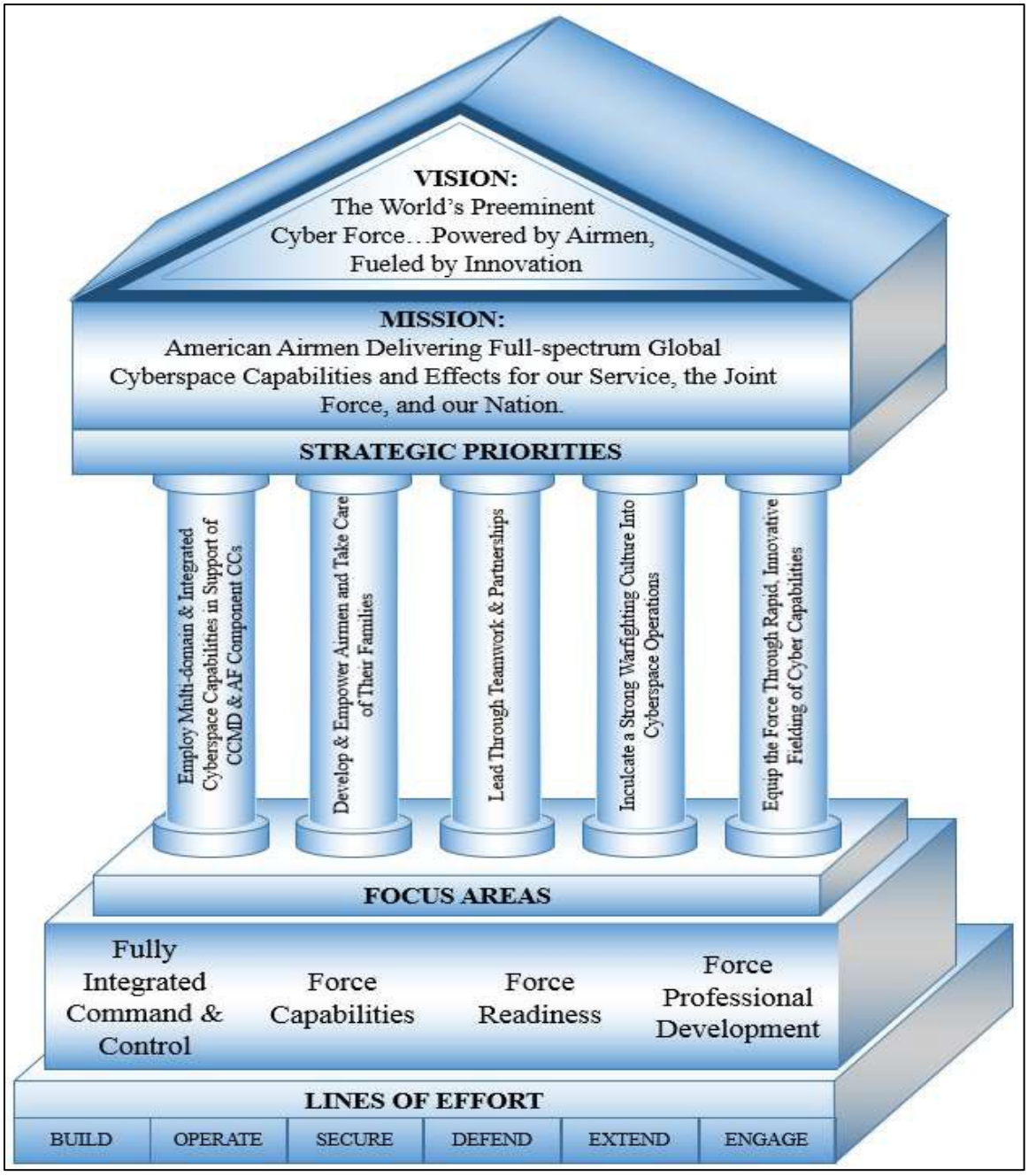

Figure 3. Cyber Strategic Vision (Air Force)

Source: Commander's Strategic Vision." 24th Air Force.

Besides, within the Commanders Strategic Mission, the doctrine speaks to the value of their reserve component. Similarly, our Total Force Airmen bring a unique blend

of experience and expertise to the full spectrum of cyber missions. Many cyberspace professionals work in prominent civilian positions within the Information Technology industry, which bolsters our mission effectiveness through their willingness to serve the nation. Reservists are often able to retain unique skillsets gained by investment in our cyber Airmen by supporting their continued service and dedication in the Air Reserve Component, which strengthens our overall mission capabilities (Air Force Commanders Vision, Cyber, 2008).

Therefore, the Air Force strategic vision speaks to the skills that are needed to increase our defense so that we reduce our risk of penetration. However, it does address whether the U.S. military add more reserve billets to USCYBERCOM over the next five years.

Marines – Current Marine Corps Strategic Doctrine for cyber is Marine Corps Concept of Cyber Operations. Topics covered are the future operating environment, military challenge, central and supporting ideas, required capabilities, and risks. This is significant because

It aims to inform the Marine Corps Capabilities Based Assessment process so that force developers can identify gaps and recommend appropriate doctrine, organization, training, materiel, leadership, and education, personnel, facilities and policy (DOTMLPF-P) solutions that will enable the Marine Corps to conduct globally integrated operations as part of a joint force (Marine Corps Concept of Cyber Operations, 2015)

Therefore, this doctrine speaks to what capabilities are needed to increase our defense so that we reduce our risk of penetration; however, it does not suggest that the U.S. military should add more reserve billets to USCYBERCOM over the next five years.

Table 12. Doctrine (Tertiary Research Question)

	Army	Navy	Air Force	Marine Corps
Should the U.S. military add more reserve billets to USCYBERCOM over the next five years IOT increase our defensive and offensive capabilities so that we reduce our risk of penetration?	1	0	1	1

1 point = Change / 0 point = No Change

Source: Created by author.

Organization

An organization must be considered as a part of the framework to answer the third secondary research question, whereas, each of the services employs their soldiers, sailors, and airmen within USCYBERCOM. The doctrine that best seems to answer the tertiary question holistically is, "Cyber Mission Analysis, Mission Analysis for Cyber Operations Department of Defense – August 2014." This mission analysis is significant because it discusses the following topics: our services cyber current state, current reserve and National Guard cyber units, way forward, and the Department of Defense assessment. Furthermore, understanding the utilization of reserves at USCYBERCOM will be essential to answering the primary research question, "Do reserve units provide the best opportunities for cyberspace professionals, by allowing reservists to practice their cyber skills in the civilian world?" Currently the following holds true:

> The Services' RCs already provide Headquarters support to USCYBERCOM. Currently, USCYBERCOM has 74 reservists from each of the four Services providing part-time support to USCYBERCOM's J-series directorates through the Joint Cyber Reserve Element (JCRE). The personnel are a mix of IMAs and unit-based personnel. The Services retain responsibilities for manning, training, and equipping assigned members, while the JCRE facilitates mission tasking, exercise augmentation, and joint administrative duties. (Cyber Mission Analysis, 2014)

Concluding that the mission analysis speaks to what USCYBERCOM currently has as far as Reserve capacity. However, it does not explicitly address the tertiary question, "Should the U.S. military add more reserve billets to USCYBERCOM over the next five years IOT increase our defensive and offensive capabilities so that we reduce our risk of penetration?"

Table 13. Organization (Tertiary Research Question)

	Army	**Navy**	**Air Force**	**Marine Corps**
Should the U.S. military add more reserve billets to USCYBERCOM over the next five years IOT increase our defensive and offensive capabilities so that we reduce our risk of penetration?	1	1	1	1

1 point = Change / 0 point = No Change

Source: Created by author.

Leadership and Education

Much like the discussion in answering the secondary research question regarding leadership and education, here, the researcher looks to add the perspective of reducing our risk to the penetration of cyberspace threats. Said otherwise, it will be necessary for our services to align their leaders to the fight today and in the future, by providing the

appropriate education. More importantly, due to the ever-changing cyber conflict, requiring our services reserve manpower to be broad ranging in their skill sets. For example, our fight is now a multi-domain fight demanding our leaders to be educated in a much more comprehensive range. It is evident that in accordance with the strategy of USCYBERCOM, one of its primary focus areas is to augment its CMF teams. The CMF is composed of three sets of forces aligned to achieve USCYBERCOM's three primary missions. Those mission sets are the Cyber National Mission Force, Cyber Combat Mission Force, and Cyber Protection Force. It will take leadership and education to implement change and the new way of conducting business in order to reduce the risk of penetration of cyberspace attacks. As services seek to employ their manpower in CMF teams, leadership and education will have to change. This is because each service is responsible for augmenting CMF teams at USCYBERCOM. This implies that services recognize the need to augment the CMF teams, however, the use of reserve personnel has not been resourced adequately. Therefore, the current doctrine (Cyber Mission Analysis, Mission Analysis for Cyber Operations Department of Defense – August 2014) to which was analyzed for this Leadership and Education section, does not speak to the tertiary research question.

Table 14. Leadership and Education (Tertiary Research Question)

	Army	Navy	Air Force	Marine Corps
Should the U.S. military add more reserve billets to USCYBERCOM over the next five years IOT increase our defensive and offensive capabilities so that we reduce our risk of penetration?	1	1	1	1

1 point = Change / 0 point = No Change

Source: Created by author.

Training

Similarly, as the researcher answered the primary and secondary research question, training is essential to the success of any mission. It is not just understanding the specific function, one must understand the domains around them as well. For USCYBERCOM to do this, "it currently provides the Services joint training for CMF personnel with the intent the Services will establish and implement long-term plans to train CMF personnel starting in FY 2017 (Cyber Mission Analysis, Mission Analysis for Cyber Operations Department of Defense – August 2014). Therefore, there is a definite way forward with emphasis on training personnel that will augment USCYBERCOM. Thus, training is not what needs to change based on data; preferably it is the need for people to participate in the training. As a result, the training does not speak to the to the tertiary research question.

Table 15. Training (Tertiary Research Question)

	Army	Navy	Air Force	Marine Corps
Should the U.S. military add more reserve billets to USCYBERCOM over the next five years IOT increase our defensive and offensive capabilities so that we reduce our risk of penetration?	0	0	0	0

1 point = Change / 0 point = No Change

Source: Created by author.

Personnel

USCYBERCOM does not have the availability of qualified people for peacetime, wartime, and various contingency operations to support the capability gap (Rodgers 2015). Due to lack of cyberspace professionals among both the enlisted and officer communities the U.S. military lacks some ability to augment USCYBERCOM demands. However, research and data prove that services are actively examining Recruitment, Retention, and Career Paths for Skilled Reserve Component Personnel that might augment this need. This is noteworthy because USCYBERCOM lacks a sufficient workforce to succeed at daily strategic missions. Moreover, the U.S. military currently cannot effectively recruit, retain, and strategize career paths for skilled reserve components that puts USCYBERCOM at a disadvantage with reserve manpower from the get-go. Therefore, personnel does need to change to answer the tertiary research question.

Table 16. Personnel (Tertiary Research Question)

	Army	Navy	Air Force	Marine Corps
Should the U.S. military add more reserve billets to USCYBERCOM over the next five years IOT increase our defensive and offensive capabilities so that we reduce our risk of penetration?	1	1	1	1

1 point = Change / 0 point = No Change

Source: Created by author.

Step 5: Aggregation of Secondary and Tertiary Research Question

Step 5 will summarize the aggregation of the secondary and tertiary question capability gaps in doctrine, organization, leadership, and education, training, and personnel. The researcher will venture to determine if there is continuity among the gaps that will need to be addressed when examining the primary research question, "Do reserve units provide the best opportunities for cyberspace professionals, by allowing reservists to practice their cyber skills in the civilian world?"

Doctrine

While exploring doctrine among the secondary research questions and tertiary question, it is evident that changes need to be made. However, the changes that need to be made are not within joint doctrine, but within the specific services doctrine (except navy). Current service particular doctrine does not appear to align with USCYBERCOM vision. For instance, services speak to the responsibility for filling the gaps within the CMF teams. However, they necessarily don't address the "how to" aspect with reservists, which begs the question if they believe reservists should be the answer. The only service

which seems to address the "how to" which answers the "should we" aspect is the US Navy, as they have put a measuring tool in place to ensure they are hitting the needs of USCYBERCOM. Therefore, single services will always act in their interest, and it is inconsequential what USCYBERCOM might ask for unless the Joint Chiefs are prepared to direct single services to use reserve manpower to augment the capability gaps.

Table 17. Doctrine (Aggregation of Secondary and Tertiary Research Question)

	Army	**Navy**	**Air Force**	**Marine Corps**
Should the U.S. military add more reserve billets to USCYBERCOM over the next five years?				
Doctrine (Join Doctrine 3-12, Cyberspace Operations)	1	1	1	1
Should the U.S. military add more reserve billets to USCYBERCOM over the next five years, IOT increase our defensive and offensive capabilities so that we reduce our risk of penetration?				
Doctrine (service specific Doctrine)	1	0	1	1

1 point = Change / 0 point = No Change

Source: Created by author.

Organization

The collection of data on service organizations and how they individually resource their reserve manpower to the USCYBERCOM fight resulted in a lack of utilization of reserve manpower. That is, it is evident that all services understand the uniqueness of the reserve skill set in the cyber domain. However, it is apparent through USCYBERCOM CDRs vision, and service-specific doctrine that are services are not necessarily employing their reservist to augment USCYBERCOM capability gaps. This is again being a direct result of our Joint Chiefs of Staff not directing services to recall

reservists to fill the capability gaps (manpower and skill sets) that our need at USCYBERCOM. Therefore, until the cyber fight is escalated to "wartime" campaigns, we may continue to see services push back on how they best see fit to utilize their reservists.

Table 18. Organization (Aggregation of Secondary and Tertiary Research Question)

	Army	**Navy**	**Air Force**	**Marine Corps**
Should the U.S. military add more reserve billets to USCYBERCOM over the next five years?				
Organization	1	1	1	1
Should the U.S. military add more reserve billets to USCYBERCOM over the next five years, IOT increase our defensive and offensive capabilities so that we reduce our risk of penetration?				
Organization	1	1	1	1

1 point = Change / 0 point = No Change

Source: Created by author.

Leadership and Education

The leadership and education analysis examined how leaders are prepared to lead the fight from squad leader to 4-star general/admiral and their overall professional development (DOTMLPF-P Analysis 2017). As the U.S. military augments capability gaps at USCYBERCOM with personnel with appropriate skill sets, leadership and education will need to change. This is because it will be necessary for our services to align their leaders to the fight today and in the future, by providing the education required to keep up with our ever so changing multi-domain fight. Furthermore, while exploring service specific doctrine and USCYBERCOM Commanders vision to answer the

secondary and tertiary research questions, it is evident that preparing leaders to fight with the proper education is not a capability gap. Instead, it is a subset of the employment of manpower within organizations where currently there is not a gap. However, should we need to change the organization over a period, then leadership and education amongst the ranks will result in needed change, as they are both directly linked?

Table 19. Leadership and Education (Aggregation of Secondary and Tertiary Research Question)

	Army	**Navy**	**Air Force**	**Marine Corps**
Should the U.S. military add more reserve billets to USCYBERCOM over the next five years?				
Leadership and Education	1	1	1	1
Should the U.S. military add more reserve billets to USCYBERCOM over the next five years, IOT increase our defensive and offensive capabilities so that we reduce our risk of penetration?				
Leadership and Education	1	1	1	1

1 point = Change / 0 point = No Change

Source: Created by author.

Training

While researching training to answer the secondary and tertiary question, it was evident that training was not necessarily what needed to change. Training pipelines, work ups, and service specific function school's necessary are all readily available to our service members whether Active, Guard, or Reserve. Understanding where to put our services time, energy, and the cost will better enable our leaders to focus resources on augmenting the capability gaps at USCYBERCOM. Therefore, training is not what needs to change based on data; rather it is the need for people to participate in the training.

Table 20. Training (Aggregation of Secondary and Tertiary Research Question)

	Army	Navy	Air Force	Marine Corps
Should the U.S. military add more reserve billets to USCYBERCOM over the next five years?				
Training	0	0	0	0
Should the U.S. military add more reserve billets to USCYBERCOM over the next five years, IOT increase our defensive and offensive capabilities so that we reduce our risk of penetration?				
Training	0	0	0	0

1 point = Change / 0 point = No Change

Source: Created by author.

Personnel

Personnel is an integral part of answering the secondary and tertiary question. A zero solution would be possible without the proper utilization of personnel; in order to answer the secondary and tertiary research question; the researcher must consider what personnel the U.S. military have to utilize. It is evident through reading service specific doctrine and USCYBERCOM Commanders Vision that what lacks are qualified personnel who can hold the necessary clearance to augment the CMF teams. Furthermore, although services seek to inflate their manpower within cyber communities, the doctrine and data suggest that they fall short at recognizing the real issue, which is maximizing the utilization of our reserve force. Concluding, the U.S. military currently cannot effectively recruit, retain, utilize, and strategize career paths for skilled reserve components that puts USCYBERCOM at a disadvantage with reserve manpower from the get-go.

Table 21. Personnel (Aggregation of Secondary and Tertiary Research Question)				
	Army	**Navy**	**Air Force**	**Marine Corps**
Should the U.S. military add more reserve billets to USCYBERCOM over the next five years?				
Training	1	1	1	1
Should the U.S. military add more reserve billets to USCYBERCOM over the next five years, IOT increase our defensive and offensive capabilities so that we reduce our risk of penetration?				
Training	1	1	1	1

1 point = Change / 0 point = No Change

Source: Created by author.

Step 6: Conclusion(s) (Answer to Primary Question)

As the analysis has shown, the answer to the primary research question, "Do reserve units provide the best opportunities for cyberspace professionals by allowing reservists to practice their cyber skills in the civilian world?" is affirmed. However, one must consider Doctrine, Organization, Leadership and Education, Personnel, and Training. After considering all of the above, and considering the secondary and tertiary questions, without a doubt, the most reasonable course of action is to inflate U.S. military cyber reserve force. Consequently, the services recognize there is a capability gap among each at recruiting, retaining, and formulating an aggressive career path for our cyberspace professionals. Therefore, to fill those gaps, would be more appropriate to use resources that are currently available. Drawing on prior information the utilization of reserve manpower, due to their broad-based knowledge sets, is recognized as a solution, however the willingness to use them, when to use them, and for what individually (joint or service specific) is the ongoing battle.

Chapter Conclusion

Chapter 5 will provide a conclusion and discuss a recommendation based on all data and research compiled throughout this review, to best answer the primary research question and build off literature review to answer the following primary research question, “Do reserve units provide the best opportunities for cyberspace professionals by allowing reservists to practice their cyber skills in the civilian world?

As this analysis has shown, the answer to the primary research question is affirmed. This confirms that staying within the parameters of the research, one will understand the conclusions and recommendations of the primary research question.

CHAPTER 5

CONCLUSIONS AND RECOMMENDATIONS

Chapter Introduction

As this analysis has revealed the answer to the primary research question, "Do reserve units provide the best opportunities for cyberspace professionals by allowing reservists to practice their cyber skills in the civilian world?" is affirmed. The research has also indicated that there is no current effort through doctrine, training, leadership and education, organization, and personnel; to exploit the expertise and depth of resources available to United States Military within the reserve community. This is of importance because the military appears to have the necessary tools to fight offensive and defensive cyber operations; however, we are not maximizing the use of them. To optimize the use of our reserve personnel the following would need to change:

Table 22. Summary of Primary Research Question (DOTLP):

	Army	**Navy**	**Air Force**	**Marines**
Doctrine	1pt	1pt	1pt	1pt
Organization	1pt	1pt	1pt	1pt
Training	0pt	0pt	0pt	0pt
Leadership and Education	1pt	1pt	1pt	1pt
Personnel	1pt	1pt	1pt	1pt

1 point = Change / 0 point = No Change

Source: Created by author.

To maximize the use of our reserve personnel at USCYBERCOM so that the U.S. military reduces our risk of penetration the following would need to change:

Table 23. Summary of Secondary and Tertiary Research Questions (DOTLP)				
	Army	**Navy**	**Air Force**	**Marines**
Doctrine	2pt	1pt	2pt	2pt
Organization	2pt	2pt	2pt	2pt
Training	0pt	0pt	0pt	0pt
Leadership and Education	2pt	2pt	2pt	2pt
Personnel	2pt	2pt	2pt	2pt

Total Points to Secondary Research Questions
1 - 2 points = Change / 0 point = No Change

Source: Created by author.

After reviewing both Table 1 and 2, the congruency is Training; the only aspect that does not need to change whether the reader is trying to answer the primary or secondary research questions. In fact, training is what the U.S. military has the most to offer. What needs to change is everything surrounding it (Doctrine, Organization, Leadership and Education, and Personnel).

Conclusions

This study sought to understand, "Do reserve units provide the best opportunities for cyberspace professionals by allowing reservists to practice their cyber skills in the civilian world?" While seeking to understand this question, it became apparent early in the study that yes, reserve units provide the best opportunities for cyberspace professionals by allowing reservists to practice their cyber skills in the civilian world. This was echoed consistently throughout several service leadership strategies, the importance of the reserves and its reservist. Furthermore, the research has also indicated that there is no current effort through doctrine, training, leadership and education,

organization, and personnel; to exploit the expertise and depth of resources available to United States Military within the reserve community. It will be of significant importance to utilize this sooner than later, considering the change in the threat towards the United States of America, posed by current and potential adversaries.

Concluding, regardless of service, leadership recognizes the cyber reservist as a significant asset to their service, but they also acknowledge that the reservist should not be the primary effort. What is critical now is the recognition of what the cyber reservist can offer to the priority Active duty element, by raising standards, increasing resources, and giving more detailed direction on how to maximize the community.

Recommendations

The following are recommendations that decision makers should be currently taking into consideration:

When considering how to best utilize and maximize the skills of the U.S. military reserve cyber operational force, regardless of service, the reservist should no longer be in a volunteer status. In other words, the reserve cyber operational force SHALL augment a cyberspace operational billet, with the option to extend up to 660 days once every five years.

An all-reserve cyberspace operational force (separate uniform) should be developed. The U.S. government should now be considering the formation of a cyber and space specific all-encompassing service. We should not pull the majority of personnel for this service from current services at the beginning, but we should be prepared to phase all cyber disciplines out of our respective services. What does he/she look like? What skills do they have? What pre-qualifiers are necessary to get into service? How long will

obligation to this service be? To do this, the U.S. DoD will first need to standardize training amongst all services, so regardless of where you are placed in the war fight, fundamental skill sets are all the same. Finally, U.S. government will need to increase funding for Cyber Space operations and the formation of this service.

Final Thoughts

The following final thoughts could possibly lead to a future study. As the nation becomes more technologically advanced, it will be important to explore organizational structures to enhance our advantage. Furthermore, strategies that are related to the formulation of a new organization should be considered.

Every military service has started at some stage in history as a result of emerging threats, crisis, and demand. Now is the time to recognize the cyber domain and risk in a way that justifies the requirement for a cyber operational force (separate service) similar to the Army, Navy, Air Force, and Marine Corps. The Air Force is the newest of the four services and was established in 1947 as a result of the emerging need and recognition of the demand for it. The time has now arrived where the U.S. must recognize the need for a service dedicated to the cyber domain.

A simple interim structure could be developed that encompasses the basic demands for command and control, operational management, training and doctrine, and management of materiel. Similarly, like our existing four services, there will be a need for cyber component commands within all existing Combat Commands. The newest Combatant Command, USCYBERCOM, might eventually become an interim headquarters for a new Department of Cyber, and would, therefore, form the basis of the new service under a four-star command. Furthermore, we would transition our cyber

personnel from the respective existing services over time into this newly formed cyberspace operational force (separate service). This would be a very similar transition much like in the historical development of the U.S. Air Force, emerging from the US Army. Below is a simple layout of what the command structure for the Cyber Force operational service may look like:

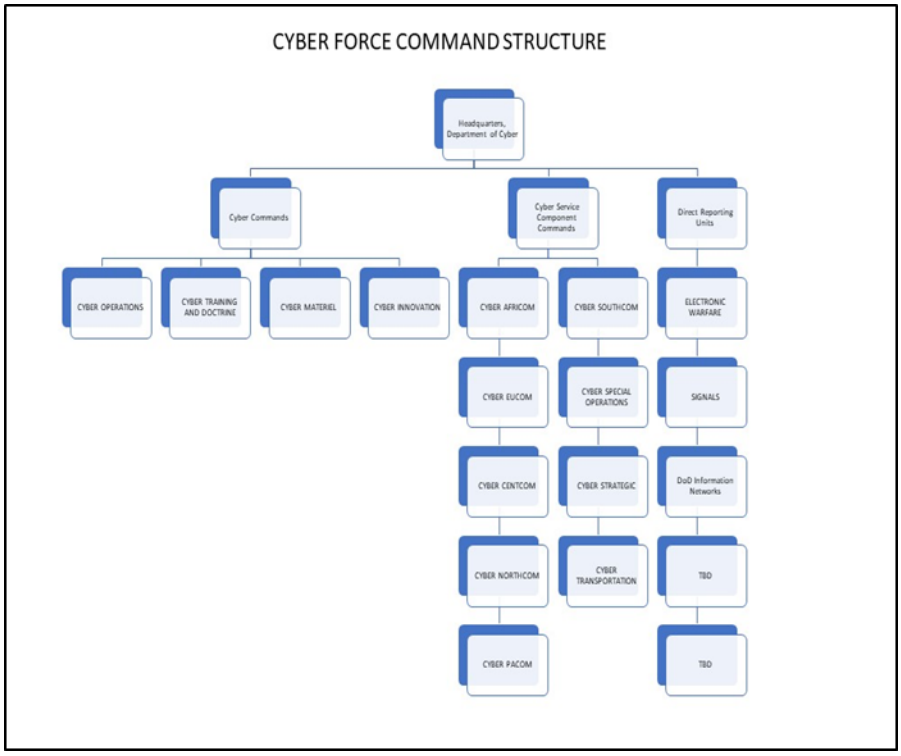

Figure 4. Proposed Cyber Force Command Structure

Source: Created by author.

Much like the Army, the Cyber Force service will have a similar structure. The Cyber Commands will consist of Cyber Operations, Cyber Training and Doctrine, and Cyber Materiel. Cyber Operations Command will be focused on providing forces capable of offensive and defensive cyberspace operations to combatant commanders. The Cyber

Training and Doctrine Command shall be focused on training and doctrine that aligns with the current and future cyber fight. Furthermore, the Cyber Materiel Command will focus on ensuring our cyberspace professionals are outfitted with the most up to date technology necessary to protect and sustain the advantage against our adversaries. Finally, the Cyber Innovation Command will be tasked with emerging new methods, ideas, and products to keep us ahead of our adversaries and leading our allies.

The Cyber Force service component commands will function similarly to service components of the Navy, Army, Air Force and Marines that exist now within the Combat Commands. Each command will be responsible for directing cyber operations throughout the respective combat command area of operations. The Direct Reporting units will be specific to the disciplines of cyber operations that are necessary for offensive and defensive cyberwar fight. For example, a unit that is specially designed for electronic warfare. This will be significant for military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy (JP 3-12, 2017). Additionally, because electronic warfare consists of three division (electronic attack, electronic protection, and electronic warfare support) subsets of the Electronic Warfare Command will be of equal importance.

This idea will undoubtedly be confronted by enormous challenges regarding justification and funding, and much debate over size, scope, and what responsibilities it has. There will also be inevitable resistance from the existing services which will be keen to protect their funding, as well as their cyberwarfare structures. However, unless the DoD makes revolutionary changes to the U.S. cyberspace operational approach to threats and requirements of cyber, we will continue to tackle this issue in a fragmented and

disjointed fashion, with the responsibilities of cyber, divided amongst the newly established combat command, and the existing four single services.

To make this a reality the U.S. either tackle this requirement head on, or we sit waiting for a cyber 9-11 to react. It seems counterintuitive to do this when the U.S. as a nation already know that something like this could likely occur in our immediate future.

REFERENCE LIST

AcqNotes. 2017. “DOTMLPF-P Analysis.” Accessed September 30, 2017. http://acqnotes.com/acqnote/acquisitions/dotmlpf-analysis.

Barnes, Julian E. 2008. “Pentagon Computer Networks Attacked.” *Los Angeles Times*, November 28. Accessed September 16, 2017. http://articles.latimes.com/2008/nov/28/nation/na-cyberattack28.

Comey, James. 2017. “BrainyQuote.” Accessed September 16, 2017. https://www.brainyquote.com/quotes/quotes/j/jamescomey727990.html?src=t_cyber.

Cooperative Cyber Defense Centre of Excellence. 2014.”NATO Defence Ministers’ Meeting on Cyber Defence.” October 16. Accessed September 16, 2017. https://ccdcoe.org/nato-defence-ministers-meeting-cyber-defence.html.

Department of the Army. 2017. Field Manual (FM) 3-12, *Cyberspace and Electronic Warfare Operations.* Washington, DC: Government Printing Office, April.

Department of Defense. 2014. *Mission Analysis for Cyber Operations of Department of Defense*. Washington, DC: Government Printing Office, August.

———. 2016. “All Cyber Mission Force Teams Achieve Initial Operating Capability.” U.S. Cyber Command News Release, October 24. Accessed 26 December 2017. https://www.defense.gov/News/Article/Article/984663/all-cyber-mission-force-teams-achieve-initial-operating-capability/.

Department of the Navy. 2014. Naval Warfare Publication 3-13, *Navy Information Operations.* Norfolk, VA: Government Printing Office.

Department of State. 2018. “Milestones: 1921-1936.” Accessed January 15, 2018. https://history.state.gov/milestones/1921-1936/great-depression.

Electronic Mapping System, Inc. 2017. “E-MAPS Home Page.” Accessed September 30, 2017. http://www.e-mapsys.com/.

Headquarters, U.S. Marine Corps. 2010. *Marine Corps Information Enterprise (MCIENT) Strategy*. Washington, DC: Government Printing Office, December.

———. 2016. MCIP 3-32 Ei, *Marine Corps Cyberspace Operations*. Washington, DC: Government Printing Office, 2 MAy.

Hollis, David. 2011. “A Reserve Component Initiative to Defend DoD and National Cyberspace.” *Small Wars Journal*, November 11. Accessed 26 December 2016, smallwarsjournal.com.

Joint Chiefs of Staff. 2013. Joint Publication (JP) 3-12 (R), *Cyber Operations*. Washington, DC: Government Printing Office. Accessed September 17, 2017. http://www.dtic.mil/doctrine/new_pubs/.

Kay, David J., Terry J. Pudas, and Brett Young. 2012. "Preparing the Pipeline: The U.S. Cyber Workforce for the Future." Defense Horizons, August.

Mehta, Aaron, and Leo Shane III. 2017. "Trump Elevates Cyber Command; Split with NSA Still an Option." *Marine Corps Times*, August 18. Accessed September 17, 2017. http://www.marinecorpstimes.com/dod/cybercom/2017/08/18/trump-elevates-cyber-command-split-with-nsa-still-an-option/.

North Atlantic Treaty Organization. 2013. "The History of Cyber Attacks-A Timeline." *NATO Review Magazine*. Accessed September 16, 2017. http://www.nato.int/docu/review/2013/ Cyber/timeline/EN/index.htm.

Office of the Press Secretary. 2016. "Fact Sheet: Cybersecurity National Action Plan." White House Archives. Accessed September 17, 2017. https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan.

Robinson, Karen. A., Oluwaseun Akinyede, Tania Dutta, Veronica Ivey Sawin, Tianjing Li, Merianne Rose Spencer, Charles M. Turkelson, and Christine Weston. 2013. *Framework for Determining Research Gaps During Systematic Review: Evaluation*. Rockville, MD: Agency for Healthcare Research and Quality.

Rosenzweig, Paul. 2012. "Significant Cyber Attacks on Federal Systems--2004-Present." Lawfare. May 7. Accessed September 16, 2017. https://www.lawfareblog.com/significant-cyber-attacks-federal-systems-2004-present.

U.S. Congress. Senate. 2015. *Statement of Admiral S. Rogers, Commander, United States Cyber Command Before the Senate Committee on Armed Services*. March 19. Accessed 26 December 2017. https://www.armed-services.senate.gov/imo/media/doc/Rogers_03-19-15.pdf.

U.S. Fleet Cyber Command/Tenth Fleet. n.d. *Strategic Plan 2015-2020*. Fort George Meade, MD: U.S. Navy.

United States Air Force. 2011. Annex 3-12, *Cyberspace Operations.* Maxwell AFB AL: Government Printing Office.

United States Army Cyber Center of Excellence. 2015. *Strategic Plan*. Washington, DC: Government Printing Office, September.

United States Marine Corps. 2015. *Marine Corps Concept for Cyberspace Operations*. Quantico, VA: Government Printing Office, October.

———. 2017. *Strategy for Assured Command and Control, Enabling C2 for Tomorrow's Marine Corps, Today*. Quantico, VA: Government Printing Office, March.

United States Strategic Command. 2017. "Fact Sheet." Accessed September 17, 2017. http://www.stratcom.mil/Media/Factsheets/Factsheet-View/Article/960492/us-cyber-command-uscybercom/.

Weggeman, Chris. 2017. *Commander's Strategic Vision*. 24th Air Force. Accessed 26 December 2017. www.afcyber.af.mil/Portals/11/documents/24%20AF%20Strategic%20Vision.pdf?ver=2017-03-08-112453-76.