REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
05/10/2019	Master's of Military Studies	SEP 2018 - APR 2019

4. TITLE AND SUBTITLE

Cyber as a Service: Organizing the DoD for the Fifth Domain

5a. CONTRACT NUMBER
N/A

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
N/A

6. AUTHOR(S)

Decker, Christina, L., Major, USAF

5d. PROJECT NUMBER
N/A

5e. TASK NUMBER
N/A

5f. WORK UNIT NUMBER
N/A

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
USMC Command and Staff College
Marine Corps University
2076 South Street
Quantico, VA 22134-5068

8. PERFORMING ORGANIZATION REPORT NUMBER
N/A

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)
Dr. Matthew J. Flynn

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
N/A

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Cyberspace and cyber capabilities present a new frontier for the US Department of Defense (DoD) and challenge for how the DoD should structure its forces and missions to employ, protect, and control an arguably new fifth or cyber domain. Using current DoD doctrine to create a definition for this new domain, the cyber domain is defined as exploiting the electromagnetic spectrum (EMS) through technology to create an operational space or cyberspace. Reorganizing cyber as its own service will create unity of effort in a domain the United States must dominate to gain the advantage in an increasingly automated conflict across multiple regions and domains.

15. SUBJECT TERMS

Cyber; DoD, Cyber Service Branch, Cyber Force, Cyber Capabilities; Cyber Domain; Cyber Definition; Cyber as the 5th Domain; Cyber Organization; Cyber Power; China; Separate Service; Cyberspace; EMS, electromagnetic spectrum; multi-domain; joint; mothership; Cyber Service; Cyber Structure

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			USMC Command and Staff College
					19b. TELEPHONE NUMBER *(Include area code)*
Unclass	Unclass	Unclass	UU	38	(703) 784-3330 (Admin Office)

United States Marine Corps
Command and Staff College
Marine Corps University
2076 South Street
Marine Corps Combat Development Command
Quantico, Virginia 22134-5068

MASTER OF MILITARY STUDIES

CYBER AS A SERVICE: ORGANIZING THE DoD FOR THE 5TH DOMAIN

SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF MILITARY STUDIES

MAJOR DECKER. CHRISTINA, USAF

AY 2018-19

Mentor and Oral Defense Committee Member: _____
Approved: _____
Date: _____

Oral Defense Committee Member: David Pinion
Approved: _____
Date: 3 May 2019

Executive Summary

Title: Cyber as a Service: Organizing the DoD for the Fifth Domain

Author: Major Christina Decker, United States Air Force

Thesis: Reorganizing cyber as its own service will create unity of effort in a domain the United States must dominate to gain the advantage in an increasingly automated conflict across multiple regions and domains.

Discussion: Cyberspace and cyber capabilities present a new frontier for the US Department of Defense (DoD) and challenge for how the DoD should structure its forces and missions to employ, protect, and control an arguably new fifth or cyber domain. Using current DoD doctrine to create a definition for this new domain, the cyber domain is defined as exploiting the electromagnetic spectrum (EMS) through technology to create an operational space or cyberspace. The need to reorganize cyber forces begins with recognizing the inherent relationship of cyberspace and the EMS as the cyber domain. China has made moves to recognized this relationship by reorganizing its cyber, space, and electronic warfare (EW) forces into a new Strategic Support Forces. With other states, like China, who are seeking superiority in this new operational environment, the United States should adapt but not in the same way.

The DoD should create a separate cyber service and clarify the roles and responsibilities between the service, agencies, and US Cyber Command. Currently there are organizational challenges with how cyber is disaggregated across the DoD and lacks a strong advocate to unify effort on the cyber and other domains. Existing domain-based services are grappling with how to gain advantages with and from cyber power. The risk with continuing results in duplication of effort, unintegrated capabilities, and delayed deployment of new capabilities. The creation of a cyber service branch has the potential to solve these issues and unify how the DoD conducts cyber operations within and across the other four domains.

The Chairman of the Joint Chiefs of Staff, General Joseph F. Dunford, characterized the evolution of conflict and the threats in the military environment as transregional, multi-domain, and multi-functional.[1] Cyberspace is both transregional and multi-domain since it is created by the EMS, which reaches across the globe and domains. By creating a cyber service, cyber power presents an interesting stepping stone to how the DoD could evolve pass domain-based services into a more agile joint force that is readily able to assemble and meet threats in a range of operational environments.

Conclusion: The United States must seek opportunities to gain military advantages and remain ahead of competitors. Creating a new Cyber Service Branch would help unify the DoD's disaggregated cyber capabilities and missions, and help provide the needed integration and resources to ensure the DoD is able to dominate in a new and vital cyber domain.

DISCLAIMER

Illustrations

Page

Tables

Page

Acknowledgments

Thank you to my MMS mentor, Dr. Matthew Flynn, for his direction and positive feedback throughout this process. Also, thanks to my mentor and Lieutenant Colonel Winston Gould, USAF (Retired), Lieutenant Colonel David Pinion, and Dr. Anne Louise Antonoff for helping me explore through history and journey to settle with the direction of this paper with cyber as a separate service. Lastly, I would like to thank my husband for supporting me and our family while I worked on this project.

To the readers, when starting this project, I did not want to advocate for an independent cyber service branch but instead how the DoD could be better organized to grow the US cyber capability. Through the process, however, the reality is that services have utility to promote and grow an idea and provide the resources, as the National Security Act of 1945 did with creating an independent Air Force. The caution with services it that while they help promote the development of a capability, they can also build barriers between holistically approaching the multi-domain conflicts. All future conflicts will encompass more than single domain for operations, but domain centric Services (to include cyber) are a stepping stone to building the next integration of functional based force that can fight within and across domains. The DoD should seek to evolve past the service construct so that all the part and pieces of the US military machine can be agile and assembled seamlessly for dynamic battlespace.

Table of Contents

Introduction

Cyberspace the new frontier and the US Department of Defense's (DoD) new challenge for organizing missions and forces. The need to reorganize missions and forces begins with recognizing the inherent relationship of cyberspace and the EMS as the fifth domain. The fifth domain or cyber domain is where cyberspace exists, a space poised to exploit the electromagnetic spectrum (EMS). However, while it is discussed as a domain, US doctrine does not recognize cyber as such. The definition of cyberspace according to the DoD is limited to the computer technology and the interconnectedness of that technology. There is no mention of how the EMS is utilized by that technology to create cyberspace. However, the cyber domain is a physical domain just like air, land, sea, and space that has always existed. The EMS is physical and the operational medium where cyber power effects its own and other domains. US military doctrine also treats cyberspace as part of the information environment. Both doctrinal approaches fall short in recognizing that *cyber is a domain* using the EMS as its operational medium. This domain dispute nevertheless causes confusion and duplicated effort amongst the services and agencies leveraging and operating the cyber domain on how to approach this new frontier. Hence, what the DoD is really faced with regardless of its doctrine definitions, but influenced by them, is how the US military should reorganize its forces and create a new cyber service to unify and optimize the advantage cyber power brings.

Recognizing cyber as a domain and updating cyberspace's definition to include the EMS as its operational medium is vital to evolving capabilities and developing the force structure needed. The advantage and lethality cyber possesses is an essential asset for global powers to have in their arsenal. Cyber capabilities can ease daily life or wreak havoc in modern society. To put it simply, capabilities are made up of resources and processes. Within a cyber context, cyber

capabilities range from the technology, hardware, software, infrastructure, systems, and networks (like global terrestrial and space-based communications and the internet) people leverage to do a range of activities from economic transactions, run industrial systems, operate electronics, compute algorithms, house big data, preform machine learning, build artificial intelligence, create and share media, etc. Such capabilities are essential to both civilian and military sectors and are vital in national strategies and policies.

The strategic importance of cyber capabilities for a state is the ability to employ, protect, and control domestic and military access to worldwide networks, and the defense or exploitation of those resources and processes within a state's borders. The technology to capitalize this new cyber domain is rapidly evolving. With cyberspace and cyber capabilities rapidly growing, there is urgency for the US to remain ahead of other states like China, Russia, Iran, and North Korea who are seeking superiority in this new operational environment. Out of these, China is a good example of how the state is reorganizing its forces to better exploit cyber and its effects on other domains like space. China recently stood up a new force that combined its space, electronic warfare (EW) and cyber together to better support its space capabilities. China's reorganization points directly at recognizing the inherent relationship of EW (which leverages or denies use of the EMS) and cyber as a medium in need of protection in order to control and employ China's space assets.

Within the DoD, each military service is responsible for a warfighting domain along with combatant commands and support agencies. However, with cyber, the existing land, maritime, and air services are grappling with how to build their own cyber force to employ, protect, and control cyber power affecting that domain. These existing services do not focus on cyber power as its own effort in the cyber domain, but instead see cyber power as supporting capabilities for

their domain (i.e. using computers to help navigate). The combatant commands and support agencies are also grappling with who is responsible for what missions pertaining to the cyber domain. The disparate distribution of cyber forces and missions across the DoD create confusion and lack an integrated approach. Each US military service branch should have its own cyber capabilities, but there should be a unified cyber force in one service providing support and conducting its own effort in its domain. Currently, the trouble with each service's cyber capabilities is that they are being constructed in service silos. Cyber is too important to have duplication of efforts, unintegrated capabilities, and delayed deployments of new capabilities. To improve management of the cyber domain, the stand up of an independent cyber service will increase and maintain the US dominance in this newly exploited domain like it did for airpower.

The Chairman of the Joint Chiefs of Staff, General Joseph F. Dunford, has recently described the evolution of conflict and the threats in the military environment as a steady trend toward the transregional, multi-domain, and multi-functional character of modern war.[2] The days of Napoleonic land warfare and Trafalgar sea battles have long since passed. The increasingly complex intersection of domains started with the rise of airpower 100 years ago during the First World War. Military forces have long imagined the ability to exploit the air but lacked the means to do so. Twentieth century technology finally enabled airpower and brought a new complexity to the fight. The age-old land and maritime domains now contended with the possibility of a strike emanating from the sky. Air and space have always existed, even though airpower is relatively new and a significant factor in changing the character of war. The EMS, like air, has always existed but only recently have people invented the technology to exploit this cyber domain. In this way, cyber capabilities are to the EMS as aircraft are to air: together, they have created a new dimension and change in warfare. Like aircraft and air, moreover, cyber

capabilities and the EMS impact all the other domains. Unlike the standup of the Air Force, however, a new cyber service branch should be fully integrated with the other services as much as its own line of effort to fully unify the capability. The seamless and joint application to leverage cyberspace across the other warfighting domains and its own will provide the greatest agility to an unknown battlespace. The US military needs to have advantage in the complex transnational, multi-domain, and multi-functional charter of conflict. Reorganizing cyber forces as its own service will create unity of effort in a fifth domain that the US must dominate to gain advantages in an increasingly automated conflict across multiple regions and domains.

Defining the Fifth Domain as Cyber

To define the fifth domain or cyber domain, the definition must capture the full range of characteristics of the EMS, cyberspace, and EW and how they fit with the operational and information environments. To begin, there is an initial exploration of how the DoD defines these characteristics in order to put together how the various definitions support acknowledging a new cyber domain. The purpose of defining the cyber domain through existing doctrine is because it already captures and defines the characteristics that comprise the domain. Nonetheless, the shortfall in doctrine is that it does not acknowledge how all the activities occurring in cyberspace and EW are enabled by technology exploiting the EMS. Technology has now provided the means to exploit the EMS by opening up a previously limited way for conducting operations by accessing and controlling the actual physical space where it exists.

While there is no official recognition of a fifth or cyber domain in the DoD, joint doctrine acknowledges the EMS, cyberspace, and EW as part of the operational environment. According to joint doctrine, the operational environment consists of four domains: air, land, maritime, and space. In addition to the domains, the operational environment consists of “the information

environment (which includes cyberspace); as well as the EMS, and involve conventional, special operations, ballistic missile, EW, information, strike, cyberspace, and space capabilities."[3] Next is to explore the EMS, cyberspace, and EW definitions, and how there is an inherent relationship between all that lead to defining the new cyber domain.

First, the DoD defines the EMS as, "The range of frequencies of electromagnetic radiation from zero to infinity."[4] This EMS definition provides the foundation for exploitation of the EMS by information and communication technology through leveraging various wave frequencies to transmit, receive, and control data and information. The use of this technology feeds into the current definition of cyberspace.

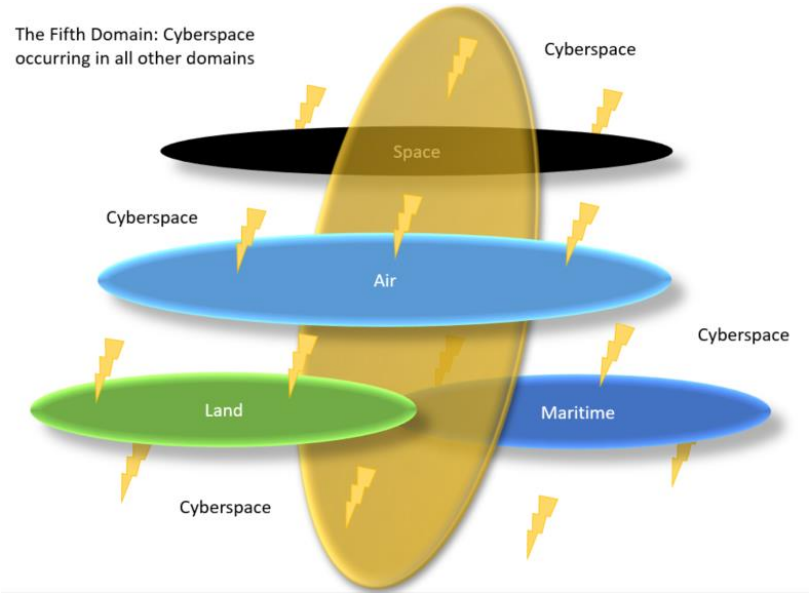
Second, Joint Publication 3-12 *Cyberspace Operations* defines cyberspace as, "A global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[5] The publication goes on to state that, "activities in the physical domains can create effects in and through cyberspace by affecting the EMS or the physical infrastructure."[6]

Third, the *DoD Dictionar*y describes EW as a military action involving the use of electromagnetic and directed energy to control the EMS or to attack the enemy.[7]

The definitions presented show that cyberspace is a way of *exploiting* the EMS through technology and where military actions are conducted. The network, computers, and devices that access cyberspace facilitate humanity's utilization this domain to process information at the speed of light. One example of this is how fiber optics transmit data as light and wireless technology transmits data as microwaves. Both light and microwaves are different frequencies along the EMS. The fifth domain then is the EMS as utilized by and benefiting from activities in

cyberspace, to include EW creating a cyber domain (see figure 1). Synergizing the joint doctrine definitions, this analysis defines cyber domain as follows: "The range of frequencies of electromagnetic radiation from zero to infinity utilizing directed energy to control the interdependent networks of information technology infrastructures, computer systems, processors, and controllers, telecommunications networks, and resident data." Additionally, the definition of capability in the Information Technology (IT) Infrastructure Library (an internationally used framework) is the "ability of an organization, person, process, application, IT service or other configuration item to carry out an activity." Therefore, a cyber capability is the ability of resources (organizations, people, applications, IT service, configurable items of computer technology and systems, infrastructure, electronics, etc.) and processes to act in cyberspace. Thus, this domain's name will use cyber as defined here as the fifth domain, which acknowledges the fact that the domain is the EMS as exploited by cyber capabilities creating the operational medium of cyberspace. Going forward in this paper, the fifth domain or *cyber domain* references this definition.

Figure 1.



Cyber capabilities are a new way for employing, protecting, and controlling electromagnetic radiation, data, and information. Before cyberspace, data and information just

used different means and ways to reach the desired end, much like mail versus email. Like air and space, the domain has always been there, but science and technology have enabled exploitation of the domain to both civilian and military advantage. Globally, states are recognizing the expanse and reach of cyber power and see how it is an essential capability as organizations, individuals, and economic firms transact throughout cyberspace exchanging information through various communications systems. US joint doctrine highlights how the relationship between space and cyberspace is unique in that virtually all space operations depend on cyberspace and a critical portion of cyberspace bandwidth is only provided via space operations resulting in a key global connectivity option for cyber operations (CO).[8] For these reasons, cyberspace is strategically vital for global powers and helps explain why China has started reorganizing its military forces to account for this strategic reality.

The Need for Change in US Approach to Cyber Power

In China, the People's Liberation Army (PLA) reorganized its space, cyber, and EW forces into one service named the Strategic Support Force (SSF) in 2016. This move brought together forces and unified critical capabilities, recognizing the inherent relationship between these operational environments and how cyberspace is essential to space power. The PLA's focus for the SSF is to enhance the Chinese space capability.[9] Former Second Artillery Officer Song Zhongping argues that the stand-up of the SSF better addresses this new warfighting domain. Song asserts that, "the SSF is an independent service 'unique in the world'" and argues that the concept of the SSF puts the PLA ahead of the US military in organizing its information-warfare forces."[10] Organizing space, cyber, and EW together ensures that a state can protect the freedom of use of its space assets by making sure data is transmitted to earth and the state is able to communicate and exchange information about the data. Song contends, "[T]he US military

inefficiently disperses its information-warfare forces among the services, the SSF concentrates the PLA's information-warfare forces under one command."[11] The structure of the SSF has potential to create synergy in securing its ability to leverage both space and cyber capabilities in conflict. Moreover, it strengthens China's control within the domain behind the "great firewall," the state's effort to block unwanted Internet traffic.

Both the United States and China see cyberspace as an operational domain, but take different views on employing, protecting, and controlling access the internet. Each nation's strategy emphasizes global competition within the domain and the need to develop, protect, and defend that space since it is critical for economic success. China's recognition of cyber as "a new domain of national security" defines cyberspace as part of its sovereignty and exercises control of access to and use of cyberspace.[12] Conversely, in the 2018 National Cyber Strategy (NCS), the Untied States' position for the domain is to retain "an open, interoperable, reliable, and secure Internet… expand communication, commerce, and free exchange of ideas" to support "America's vision of a shared and open cyberspace for the mutual benefit of all."[13] This free and open view opposes the restrictive perspective held by China. Cyber, like airpower, is changing the character of war and should not be so disjoined in its development as a warfighting capability given this domain "is so integral to the basic infrastructure of the United States and the larger global economy that actions to deny, degrade, or destroy parts of it have the potential to create intolerable security problems."[14] No matter the divergence, both national strategies address the development of their respective cyber capabilities and forces to project power within the domain.

The intent behind China's strategy presents a long-standing approach of "acupuncture warfare," a term describing how China seeks to zero-in on weak links in command, control, communication, and computers to severely weaken the opponent.[15] This refers to targeted

operations to pinpoint attacks that will have a large impact on the adversary. One way to weaken an opponent is through using offensive cyber capabilities. An example is the espionage virus Flame, which is an offensive cyber capability designed to produce a pervasive cyber power effect.[16] Flame exploits Windows software to allow gathering of user data that can translate into user names and passwords to gain access into a system and steal information or conduct other malicious activities.

On May 19, 2014, the United States charged five Chinese Military hackers with stealing intellectual property from American entities to benefit Chinese competitors including state-own enterprises.[17]This was the first time that the United States publicly sought legal action against Chinese cyber espionage. In response, a year later on September 25, 2015, President Barack Obama and Chinese party leader Xi Jinping pledged that "neither of their governments would conduct or condone economic espionage in cyberspace."[18] While only a verbal agreement, it did deter some economic espionage. However, China continued its effort and targeted military assets and arguably still some economic hacking. In an acupuncture attack in June 2018, the Chinese military targeted a contractor working for the Naval Undersea Warfare Center, stealing sensitive data on signal, sensor, cryptographic system, and the Navy submarine development unit's electronic warfare library.[19]

In the NCS, the United States views the other state actors in cyberspace as competitors. The Chinese government in its "China's Military Strategy" also shares the competitive view in cyberspace as more states are putting effort into developing their cyber capabilities.[20] However, viewing China as a competitor could place the United States in a struggle against a state whose motivation to compete for military dominance is the objective of survival.[21] To reference game theory, the United States may find itself playing a finite game against a state playing an infinite

game. A finite game is where there are known players, fixed rules, and a fixed objective. An infinite game involves known and unknown players, the rules are changeable, and the objective is to continue the game.[22] Accordingly, the United States could find itself in a confrontation with China playing a game of survival while the United States seeks only to win; in that dynamic, the United States risks running out of will and resources to keep playing.[23]

When evaluating the US cyber force structure against China's force structure, the better way is to address what needs to be done to operate under the premise of an infinite game and as an enduring rival vice a fixed game competitor. By viewing China as a rival, the United States can determine areas of continual improvement to keep playing the game so that it is "preserving overmatch." Recognizing that the United States has its cyber force capability spread amongst services and agencies makes forces disaggregate. China's move of cyber forces to the SSF is part of an overall realization of how its previous cyber force structure was not meeting its strategy to expand and support space. China's SSF reorganization should be used as a catalyst for the United States to evaluate its own force structure for weaknesses in meeting its strategy.

China's New Force and Cyber

Unlike warfare of the past, conflicts are increasingly fought in joint environments. Most likely there will never be a land or naval battle where the Army or Navy do not employ air and space power to provide support. As the past 100 years of US warfare has demonstrated, the United States prefers to go to the fight rather than stay home waiting to be attacked. To go to the fight involves complex joint operations. To conduct complex operations, a large amount of information and communication needs to happen and the best way to do just that is through cyberspace. When there is not a physical connection, the best way to pass information and communicate is through space. To transmit to space, an actor must be able to send signals along

the electromagnetic spectrum. The United States has an advanced capability to do this. Thus, it is logical to see why the PLA created the SSF to gain comparable capabilities to match the United States. However, no longer is modern warfare contained to a single domain. The United States recognizes the need for interchange through Joint Doctrine and the Goldwater Nichols Act, but still organizes by domain bound services.

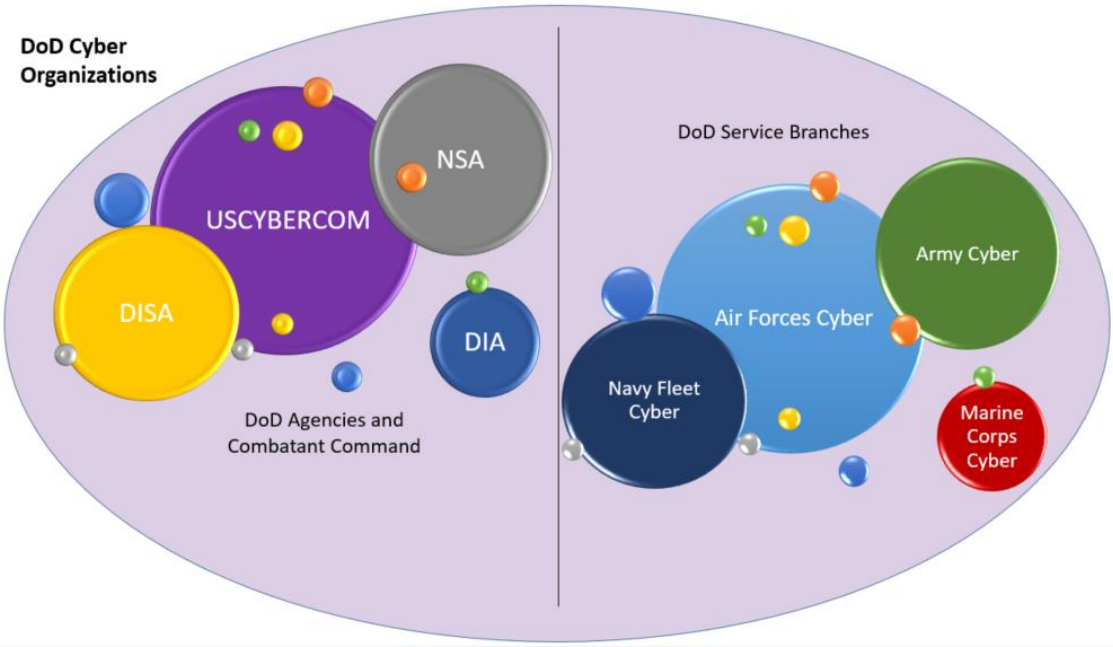
If the United States were to view China as a rival, as it once did with the Soviet Union, then the United States would use the SSF to evaluate its own organizational structure to meet its strategy. The United States has begun to do so domestically within the Department of Homeland Security with increased partnering with private industry and centralization of its operations center. The Chairman of the Joint Chiefs of Staff recently hinted the US military may be looking at evaluating its structure to be able to meet defense and security strategies.

Cyber capabilities are stitching together a complex battlefield where all domains are engaged in conflict simultaneously, adding a new dynamic to the character of war. To conduct complex modern warfare, a state must be able to see, communicate, and operate across a multi-domain battlespace. The United States does this very well. Nevertheless, if another state is rapidly mobilizing and innovating itself to meet the US dominance, as implied in organizing itself for this next revolution in warfare, the United States must continue to evolve. The system-to-system warfare through multi-domain interaction results in a virtual fight between the dragon and eagle. Based on China centralizing its cyber force, the United States should evaluate its cyber force structure and its capability to meet its strategy to preserve "overmatch in and through cyberspace."[24] While the SSF is an important move for the PLA, the DoD should also adapt – but not in the same way.

Cyber Organizations within the DoD

Figure 2 represents DoD cyber organizations. The DoD spreads its cyber capability (large lavender oval) amongst the various services and agencies (large labeled dots) with disparate pockets of smaller efforts separate but also contributing to cyber activities (small dots). Each service branch in the DoD has or is standing up cyber organizations to manage the expanding needs of modern warfare. There is also a unified functional combatant command in US Cyber Command (USCYBERCOM).

Figure 2:



Furthermore, there are three main agencies responsible for cyber missions: Defense Information Systems Agency (DISA), National Security Agency (NSA), and Defense Intelligence Agency (DIA). Cyber operations are complex and do need multiple stakeholders to employ, protect, and control them. However, the difficulty with cyber organically growing in several areas creates disaggregate efforts and challenges to joint operations from interoperability issues and ensuring leading edge capabilities are available to all mission sets. The diverging and converging efforts make the reevaluation of how to organize cyber a behemoth task.

The closest existing structure for a unified cyber force in the DoD is USCYBERCOM, but it is caught between competing visions of unity of command and separation of resources. There is the need for unity of command for centralized release authorities but also the ability for decentralized execution of cyber capabilities, which is complicated by the disaggregated missions, training, equipping, and organization among existing services and commands. The benefit from the traditional Service construct is centralization of resources – and therefore responsibility for readiness and interoperability – currently dispersed among other services and agencies. Its function is central to all other Services and commands,

In May 2018, USCYBERCOM became a combatant command apart from its sub-unified status under US Strategic Command. While USCYBERCOM seeks to be a unifying organization for US military cyber capability, it lacks the ability of a Service to be responsible for the organizing, training, and equipping of forces. USCYBERCOM, like other combatant commands, is reliant on each Service to provide its forces with a specialized foundation so that forces assigned to the combatant command are ready for use. USCYBERCOM leaders discussed at the 2018 Cyberspace Strategy Symposium their view that the Services "must integrate the concepts of cyberspace operations into how they organize, train, and equip the force."[25] Yet the United States does not have the authority to warranty that each cyber effort in each Service will comply with CYBERCOM's requirement to have Services to build their cyber forces and capabilities to be in sync and interoperable with one another. As retired Admiral James Stavridis and David Wienstein wrote, "Each component, although technically subordinate to [US]CYBERCOM, supports service and joint missions. In other words, Fleet Cyber Command answers to both the Chief of Naval Operations and the [US]CYBERCOM commander. When push comes to shove, though, the Navy dictates the criterion by which the 10th Fleet manages its cyber sailors. After

all, the Navy, not [US]CYBERCOM, is footing the bill."[26] Having siloed cyber development in each service poses threat to readiness. The goal in exploiting cyberspace is to control, relay, sense, manipulate, analyze, and process data and information faster to better respond than the adversary. If the US military cannot exchange data and information among its forces and ensure cooperation among those elements designated to command cyber forces, then it will lose to an adversary that can. The dilemma facing USCYBERCOM therefore questions whether there should be a separate Service for cyber forces, like airpower advocates argued in among various nations in the early interwar period, or each service retain its own cyber force. There is also then the question of who is responsible for what cyber missions, which also has been in need of deconfliction and clarification of roles and responsibilities of the organizations performing them.

A number of stakeholders are working within the DoD to deconflict missions. DISA and USCYBERCOM are one example of duplication in mission and need for deconfliction. In 2001, the Security of Defense combined the cyber defense and attack missions and assigned to a Joint Task Force (JTF) responsibility for combined global network operations (GNO). However, until the mission transferred from DISA to USCYBERCOM in 2010, there was duplication of effort. While DISA led the JTF-GNO mission, USCYBERCOM was also performing a joint network warfare mission allowing for duplication of cyber defense and attack missions until USCYBERCOM fully assumed the JTF-GNO mission with DISA as a supporting agency in 2010. While recorded as a success by DISA, USCYBERCOM's history details the overlap with the network warfare and JTF-GNO missions combining efforts starting in 2008.[27] This step created an organizational body, like a functional combatant command, dedicated to focus on the cyber mission and resulted in streamlining to counter inefficiencies.

The lack of a dedicated executive agent for cyber power leaves a gap of who oversees what capabilities are needed, who is managing cyberspace, and who is posturing the cyber force. Recently, the US government accountability office published a study in 2017 that found "weaknesses in DOD's approach to tracking its Executive Agents," which are used to facilitate collaboration to achieve critical department objectives.[28] Table 1 provides a sample of how various cyber capabilities are spread amongst the services and agencies within the DoD (table 1).[29]

Table 1: List of Service Executive Agents Assignment for Cyber Matters

Service Department Responsibility	DOD executive Agent Assignment
Army	Cyber Training Ranges
Air Force	Common Data Link Research and Development
Air Force	Defense Cyber Crime Center
Air Force	Digital and Multimedia Forensics
Navy	Printed Circuit Board and Interconnect Technology
DISA	Information Technology Standards
Department of Defense Test Resource Management Center	Cyber Test Ranges

There are also DoD agencies that supply and operate portions of the cyber capability. Two agencies responsible are Defense Information Systems Agency (DISA) and Defense Intelligence Agency (DIA). DISA's focus is on being the trusted provider in order for forces to conduct network operations and enabled lethality across all warfighting domains.[30] However, DISA is not the only provider of a network platform. As cyberspace has developed, the DIA has established its own platform for the intelligence community creating duplication with DISA. While there should be distribution of mission sets amongst the services and agencies, so as to ensure timeliness of response in combat support roles, the DoD is still in need of adapting its

structure to accommodate cyberspace operations within cyberspace and clarify roles and responsibilities.

The United States organization of its cyber forces is becoming more robust and has been taking forward steps. However, looking at the SSF forces, the United States must also seek better ways to organize for the digital age. By the United States having cyber forces in each branch of service and different capabilities in different agencies it is not hard to see how the current structure is very stove-piped.

One Cyber Force to Rule them All?

Conflict has never been isolated to one domain. In the evolution of warfare, it is worth considering how cyber can be best organized since it touches all and operates in all other domains. The principal cyber mission as it stands now is a part of the Air Force Mission to "Fly, fight, and win in air, space and cyberspace." However, because of cyber's integral role, every service has created its own cyber force. The Army, Navy, Marines, and the Air Force all need cyber capabilities in order to protect computer enabled weapon systems and command and control structures. Cyber's nature as a transregional and multi-domain capability makes it valuable, if used to its fullest capacity, on *multiple battlefields.* [31] The force development is needed, but each service is approaching how these forces are organized, trained, and equipped as enablers to the main domain mission instead of additionally approaching how cyber capabilities operate in the cyber domain. Command and control and weapon systems technology leverages cyberspace to do more, but the risk treating cyber as a supporting effort fails to capitalize on what fires cyber itself offers in the cyber domain.

Cyberspace is included within Title 10 wherein the law calls for integrated cyber and electronic warfare on the battlefield when addressing EW and managing the electromagnetic

environment. This section of Title 10 further reinforces this idea of the fifth domain in that it states under the guidance for EW and joint EMS operations, the need for an integration between cyber and EW.

Currently the US armed forces are organized based on domains in three service departments of the Army (land), Navy (sea), and Air Force (air and space). Based on that reasoning, a cyber force of some kind would also need to be its own service to adequately cover the domain. Even if the US military were to create such a force, however, USCYBERCOM would need to remain a functional coordinator of warfighting capabilities and requirements across the other services, as well as the interagency coordinator with other civil and government entities. However, taking the expanded definition of cyberspace, USCYBERCOM would include the EMS or EW as part of its mission.

The cyber domain is also a main means of C2 in modern warfare. Creating a leader to oversee this domain generates the advantage of a hub to deal with a complex and new way of conducting war. The idea of creating a separate service for cyber is the same as creating a separate Air Force and needing air mindedness. Just as Brigadier General William "Billy" Mitchell identified back in 1925 with the realization of a new warfighting domain that was changing the character of war, the DoD needs cyber minded people to focus and build expertise in the cyber domain. As early airpower advocates like Mitchell pointed out, the capability to launch operations from a new domain yields unforeseen advantages in battle. Cyber power is no guarantee of victory, but can wield great power to disrupt the adversary's ability to conduct war and change the speed at which a military force can operate. Nonetheless, cyber capabilities provide greater time and space to the power that can control, maneuver, exploit, strike, and

dominate cyberspace. The DoD needs to gain the advantage with cyber capabilities in a similar way it did with creating the Air Force.

Cyberspace is an operational space on the EMS. To really gain the advantage in the cyber domain, dedicated forces need to be organized, trained, and equipped to perform the necessary operations to achieve dominance and superiority within cyberspace and the fifth domain. This is not to discount that the fifth domain is still vital to the information environment, but the DoD must distinguish between the manipulation of information as substance and the exploitation of the medium or domain itself, integral to virtually all other operations, and one that allows a new paradigm of how conflict is conducted. As stated previously, most states and non-state actors are cognitive of this change and are adapting national policy, strategy, and doctrine. Thus, if cyberspace is a new domain vital to state interest and in need of defense, then the DoD should follow suit to create a new service in order to provide the unity of effort for securing American interests in the domain. Services are the main means of how capabilities are secure appropriations from the US Congress in the budgeting process. By creating a new service, the DoD would be leveraging the current budgeting paradigm to support the need for cyber capabilities and have one executive agent responsible for unifying and integrating efforts across all cyber operations within and on other domains. This would free USCYBERCOM to focus more of its efforts on warfighting functions by having a service ensuring the readiness of the forces and seamless operation of cyber capabilities across the expanse of cyberspace.

Cyberspace touches on both the transregional and multi-domain of how the character of war has evolved. Cyber is transregional in the sense that action in cyberspace can travel through the worldwide networks and affect a target on the opposite side of the globe, thousands of miles away, across all terrain. Cyber is also multi-domain as it operates in all the physical domains in

which humans can operate as well as in its own domain along the EMS. What Chairman Dunford has so aptly identified as the next evolution of warfare means the impossibility of confining oneself to old modes of warfighting.

The cyber domain is an interesting case to examine how to restructure the US force structure to address the new charter of conflict in a multi-domain, transregional, and multi-functional environment. While the advocacy for a new force is needed to unify and integrate efforts, a cyber service maybe a stepping stone to looking at the DoD as a whole and whether domain focused services make sense in the transregional, multi-domain, and multi-functional character of war the Chairman has described. It may be time to look at why congress must ensure the Chairman's characterization of war through the Gold-Water Nicholas Act. Instead, cyber might be the catalyst for creating a DoD that is functionally based and leverage the construct of the Joint Task Force to assemble a tailored force for a given battlespace, like Legos being put together to build whatever the required structure is for the problem set. However, to strive towards a new DoD organizational model away from services, cyber forces need the dedication of funds and equal power that being a service provides. This is a critical stepping stone to posture a more interoperable military force with the agility to project the need force in a dynamic range of conflicts.

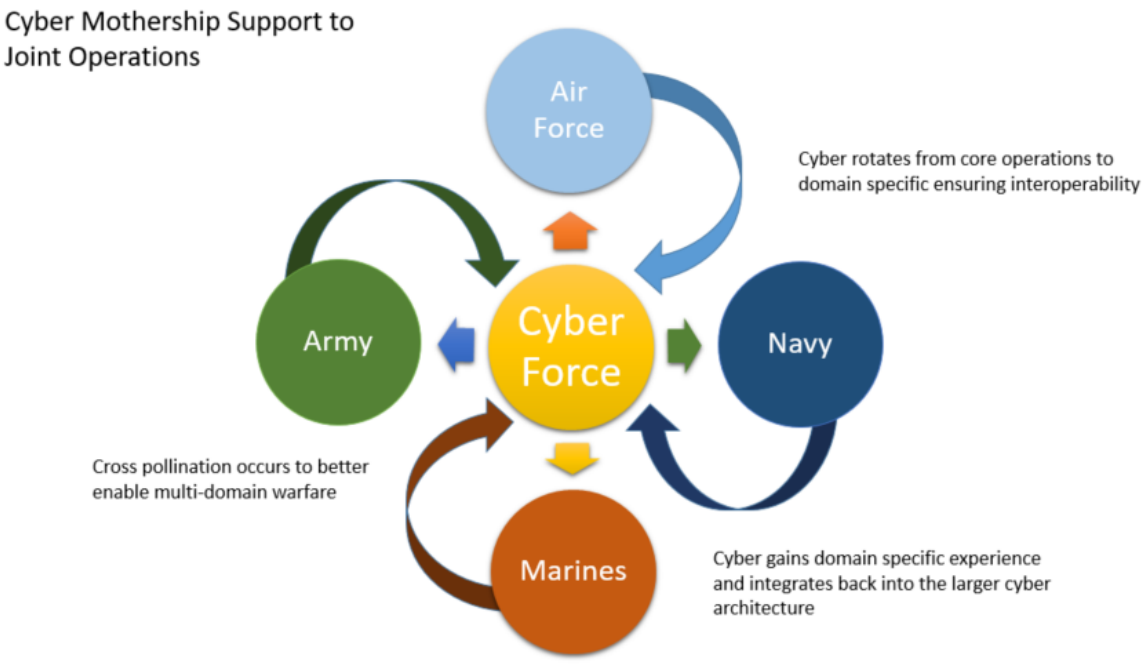
In contrast to China, the US Department of Defense's cyber, space, and EW forces are disaggregated among services and agencies. This separation causes parallel lines of effort duplicating and curtailing strides made due to lack of cohesion and communication across the various components. To properly address this emerging domain, a specific force responsible for cyberspace and EW, defined earlier as the fifth domain, should be a unified component in the DoD and a model for other mission sets that span other warfighting domains. With cyber

capabilities being developed within each service and with no single lead for cyber, having cyber capabilities becomes a means for securing funding amongst the services to fill the demands for meeting the cyber needs for defense. In some ways the Air Force is the lead or is supposed to own the cyber mission. However, just as not all air assets were moved into the Air Force, so too with cyber. Airpower is still grappling with its multi-domain charter with air assets within all three DoD service branches. Both the army and the navy retain airpower capability. Cyber power is undergoing much the same development.

Pursuing the airpower analogy, one might note that with different services there is no consistency in C2 for airpower operations. Joint doctrine must ensure that the Marines, Navy, Army, and Air Force are able to operate and communicate. However, interoperability in joint operations is still not a seamless process and is riddled with challenges. Why should we go down this same path for cyber? Instead, one can observe the success the IT industry has in creating a governing body of international standards in order to ensure the technology being put onto the market would be compatible with preexisting and future standards. Technology has evolved from floppies to CDs to thumb drives. However, these evolutions are adopted as the new industry standards after a mutual agreement among various bodies. With the DoD, while there are some governing bodies, like DoD CIO, there is no existential penalty for not complying with standards. With industry, not complying with interoperability standards means that company's product will not be usable with other products, so no one buys the product, and then the company folds or adopts the standard to survive. Instead in the DoD, each service procures siloed cyber capabilities. The siloed capability then needs to be made interoperable versus building it that way from the onset. The other option the service had is to retire or upgrade the capability, but the capability has too many sunk costs that deter or have become cost prohibitive to do so.

The new cyber service would help in setting the criteria for cyber capabilities and should absorb all the cyber operations within the services to ensure unity of efforts within the cyber domain and use of cyber by others. To fulfill other service needs for cyber, the cyber forces would be imbedded within each service. The construct is similar to how Combat Control or Special Operations Weather teams from the Air Force imbed with Army or Marine or other units to creating synergy between services in joint environment but also serve the large unit needs as

Figure 3.



well. The construct for cyber can be thought as a mothership type of rotation for the cyber force (figure 3). Think of the core of cyber being the main network operation or DoD Information Network (DODIN). Tours within the cyber service would rotate from working the core cyber operations to rotating out to be embedded in other services to fulfill their particular cyber needs. The difference is that the large CO and DODIN part of cyber would always be controlled by the cyber service and act as the "mothership" mission: cyber personnel would rotate in and out of it, all the while building expertise in each sister service. USCYBERCOM lacks the means and

influence over the other service branches priorities in order to fully achieve establishing universal standards across the DoD and overcoming inefficiencies associated with disparate personnel, resources, and priorities.[32]

The purpose of the cyber mothership rotation is to not discredit the particular needs for each operational platform and weapon systems and operational environment needs; rather, it is to achieve integration in the highest strategic and policy bodies of the United States. A problem with cyber that is actively being worked on today is the disaggregate way that cyber capabilities have organically grown within out of decades of rapid growth of technology improvement and adoption across all aspects of DoD missions. Cyber capabilities have achieved great strides in advancing the DoD's ability in communication, logistics, data and information exchange, medical, supply, control system, etc. What cyber capabilities has not done for the DoD is grown together. Many cyber capabilities have grown and been developed in isolated colonies and communities that have not learned how to relate and interact with other communities. Nor has cyber been developed from a holistic point of view, since every entity in the DoD has touted the need for it. However, the DoD itself has been slow and has struggled to cultivate cyber power and cyber mindedness in a comprehensive way; hence, the recent attention governing bodies have given to it in the last decade. However, when you are fighting against service kingdoms, it is a hard task to create and have the kingdoms accept a new emperor.

Cyberspace is the most permeable battlespace to conduct military operations. It is critical to the national security of the United States to anticipate the next military advancement. There has always been a desire to develop new and better military strategies that are more effective and efficient. Cyberspace, as a new field of battle operations, is vital to the future military success of this country and a key component of maintaining superiority over other competing global forces.

As a set of capabilities, cyberspace is a relatively new medium for conducting military operations; however, the increased capacity of nation states such as China, Russian, North Korea, and Iran in the area of cyber power makes it essential for the US military to strengthen cyber operations.

The Trump administration and OSD have crafted a new vision and set of policies concerning the military's cyberspace operations and control. Cyberspace is increasingly used for military operations on a daily basis, yet our capabilities are not at a level to fully leverage the potential of cyberspace. The reliance on technology for satellite surveillance, imagery, communications, GPS, and weather dominates how the US conducts campaigns in current theaters such as Afghanistan and Iraq. Without the use of cyberspace, the US military would be unable to use UAVs, laser guided ammunitions, and GPS to name a few space and cyberspace dependent capabilities utilizations.

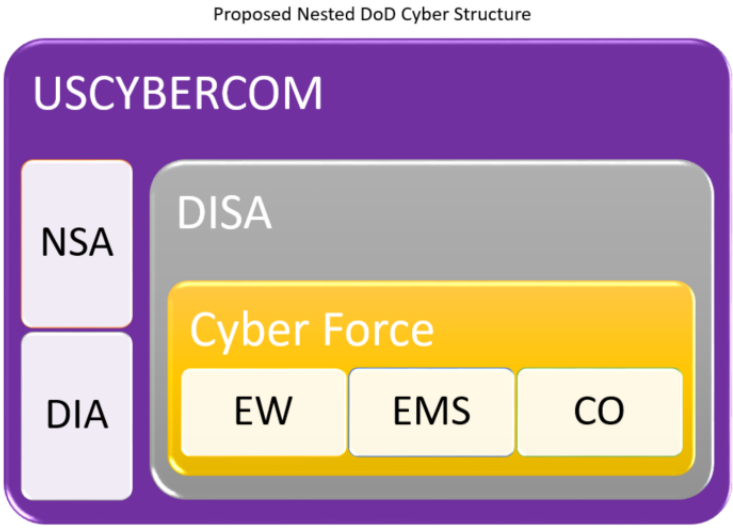
The military cyberspace is largely connected through commercial industries. This dependency could compromise our ability to fully control and develop our military resources. America's superior airpower has given the US military battlefield superiority. Airpower superiority is demonstrated by our global mobility, ability to focus precision attacks, and capacity to quickly transport resources from one region to another. By expanding and developing cyber capabilities within the proper organizational structure, we can expand our global mobility, increase our own precision attack capability, and maximize shifting regional deployments. We can shorten our response time to cyber attacks and go anywhere on the globe within minutes, yet never leave our borders. Cyberspace increases this strategic advantage exponentially by the size of the new area that could be controlled due to the transregional and multi-domain nature of cyberspace.

The DoD should not only stand up a separate cyber service, but also reorganize its cyber forces and missions into a nested structure (figure 4). In this nested structure, the focus is on the joint fight, making USCYBERCOM the predominate organization and warfighting component as a combatant command and also the main coordinating body to external DoD partners, like DHS who is responsible for domestic mission of cyberspace. Next, NSA and DIA are responsible for intelligence support to cyberspace instead of being a quasi-service provider as in today's construct. DISA is then the platform provider for cyberspace, as Verizon is in the commercial sector. Then an independent cyber service would take on organizing, training, and equipping forces encompassing the fifth domain characteristics of EW, EMS, and CO as earlier defined and adopt the fifth domain definition of cyberspace in this paper.

Cyber Service and Military Potential

Cyber has the real potential to be a unifying force across all the services. While there is no telling precisely what the next battlespace will comprise, the US military needs the agility to put for the combination of forces necessary to contest and dominate that complex environment. Setting up a cyber service is a stepping stone to getting to a more integrated force amongst the domain services. The next battlefield or even the one after can be very different in terms of what combination of forces is needed to conduct and support operations. While the cyber

Figure 4:



service is creating another bureaucratic entity within the DoD, cyber by its nature operates across all other domains. The mothership rotation of force development seeks to create a force that is joint. Understanding how cyber interacts in everything from a maritime environment to a space environment will create the necessary skill set to know how to work with domain specific military competencies and specializations to execute tactical, operational, and strategic mission sets.

In modern warfare, the cyber domain is becoming ubiquitous across the range of military operations. However, since cyber has grown in service silos, most of the technology lacks the ability to interoperate and integration is a massive task. Creating a cyber service force capable of being embedded in joint tactics and operations would be the first step to a more joint force, and would result in a Cyber Executive Agent invested in looking only at cyber and focused on integration and interoperability. Just as in industry, the cyber service would be responsible for establishing the set of standards and procedures needed to achieve this vision. USCYBERCOM is not the organization to do this. USCYBERCOM as a combatant command, needs to be focused on the application and coordination of cyber in conflict, i.e. the warfighting unit, and should have a service at its disposal making sure there is a cyber-minded force being organized, trained, and equipped for CO.

As a functionally aligned service designed to fight in a multi-domain battlespace, cyber service members will moreover be embedded in other services more specifically oriented to one domain – land, sea and undersea, littorals, and air – and, in this way, start to pave the way for breaking the DoD into more specialized functions, units of which could be arranged as needed for any given battlespace. Such units would function as the equivalent of Lego pieces from which the DoD could assemble the specific force needed for a specific conflict. This is the

baseline idea behind the Joint Task Force; however, lack of interoperability and service competition get in the way of the necessary flexibility. Because of how interwoven it is into everything every service does, cyber power is a good starting point towards a more unified and joint force needing with the growing complexity of how domains interact in conflict. Creating a cyber service as an independent, functional service branch would constitute the first step toward that goal.

Conclusion

Based on this examination, the United States should evaluate how to reorganize its forces to better meet threats. The United States has enjoyed a period without being significantly contested in the space and cyber domains, but China seeks to reposition itself as a great power. China's offensive cyber capabilities demonstrate ample ability and intent to take short cuts in economic and military development to improve its global position. China is already an offensive cyber threat leveraging the capability to further its state interest and has reorganized to do so even more by seeking improved integration between its space, cyber, and EW capabilities in the SSF to fight in a multi-domain battlespace.

The United States cannot afford to miss opportunities to maintain its military superiority. Creating an independent cyber service is the next step to ensure that end. While the status quo of cyber forces within each service and the agencies are working to improve capabilities and clarify roles and responsibilities, it is vital for the United States to continue to be an innovative leader in military advances. America faces strong competitors for cyberspace superiority. The world governance structures were not designed with cyberspace as a military delivery avenue. It will require a vision, strong leadership, and a dedication of adequate resources over time to realize the possibilities of an infinite battleground. The mission to defend and protect the United States

is more important than any dispute over resources and how they should be commended and deployed.

[1] Joseph F. Dunford, “Chairman’s Foreword,” National Military Strategy of the United States (Washington D.C.,

2018).
[2] Dunford.
[3] Joint Chiefs of Staff, "Joint Publication 3-0: Joint Operations," January 17, 2017.
[4] "DOD Dictionary of Military and Associated Terms," 2019, 76.
[5] Joint Chiefs of Staff, "Joint Publication 3-12: Cyberspace Operations," June 8, 2018, I-2.
[6] Joint Chiefs of Staff, I-2.
[7] "DOD Dictionary of Military and Associated Terms," 78.
[8] Joint Chiefs of Staff, "Joint Publication 3-12: Cyberspace Operations," I-2.
[9] Kevin Pollpeter, Michael Chase, and Eric Heginbotham, *The Creation of the PLA Strategic Support Force and Its Implications for Chinese Military Space Operations* (RAND Corporation, 2017), 2, https://doi.org/10.7249/RR2058.
[10] Pollpeter, Chase, and Heginbotham, 16.
[11] Pollpeter, Chase, and Heginbotham, 16.
[12] Ministry of National Defense of the People's Republic of China, "China's Military Strategy," May 26, 2015.
[13] The White House, "National Cyber Strategy of the United States of America" (Washington, DC, 2018), 1, https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.
[14] "The Joint Force in a Contested and Disordered World," 2016, 34, https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joe_2035_july16.pdf?ver=2017-12-28-162059-917.
[15] Gurmeet Kanwal, "China's Emerging Cyber War Doctrine," *Journal of Defence Studies* 3, no. 3 (2009): 17, https://idsa.in/system/files/jds_3_3_gkanwal_0.pdf.
[16] Kallie D. Fink, John D. Jordan, and James E. Wells, "Considerations for Offensive Cyberspace Operations," *Military Review* 35, no. 2 (May 2014): 10.
[17] US Department of Justice, "U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage," May 19, 2014, https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.
[18] Ellen Nakashima and Paul Sonne, "China Hacked a Navy Contractor and Secured a Trove of Highly Sensitive Data on Submarine Warfare," *The Washington Post*, June 8, 2018, https://www.washingtonpost.com/world/national-security/china-hacked-a-navy-contractor-and-secured-a-trove-of-highly-sensitive-data-on-submarine-warfare/2018/06/08/6cc396fa-68e6-11e8-bea7-c8eb28bc52b1_story.html?utm_term=.be83d1b9dda9.
[19] Nakashima and Sonne.
[20] Ministry of National Defense of the People's Republic of China, "China's Military Strategy," Section I.
[21] Francis C. Domingo, "Conquering a New Domain: Explaining Great Power Competition in Cyberspace," *Comparative Strategy* 35, no. 2 (2016): 156.
[22] Simon Sinek, "What Game Theory Teaches Us about War," *TED Archive*, November 8, 2016, https://www.youtube.com/watch?v=0bFs6ZiynSU.
[23] Simon Sinek, "Lecture to United States Marine Corps Univeristy on Know What Game You Are Playing" (Quantico, VA, 2018).
[24] The White House, "National Cyber Strategy of the United States of America," 20.
[25] US Cyber Command, "2018 Cyberspace Strategy Symposium Proceedings," 2018, https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM Cyberspace Strategy Symposium Proceedings 2018.pdf?ver=2018-07-11-092344-427.
[26] James Stavridis and David Weinstein, "Time for a U.S. Cyber Force," *U.S. Naval Institute Proceedings* 140, no. 1 (2014), https://www.usni.org/magazines/proceedings/2014/january/time-us-cyber-force.
[27] "Command History," accessed January 22, 2019, https://www.cybercom.mil/About/History/; "DISA - Our History, 1947-1960," accessed January 19, 2019, https://www.disa.mil/About/Our-History.
[28] "Defense Management: Needs to Improve Its Oversight of Executive Agents," 2017, https://www.gao.gov/assets/690/688430.pdf.
[29] "Defense Management: Needs to Improve Its Oversight of Executive Agents."
[30] Defense Information Systems Agency, "About DISA," DISA.MIL, accessed March 18, 2019, https://disa.mil/About.
[31] Leah Tanner, "Examining Cyber Command Structures," 2015, https://apps.dtic.mil/docs/citations/ADA620750.
[32] Stavridis and Weinstein, "Time for a U.S. Cyber Force."

Bibliography

"Command History." Accessed January 22, 2019. https://www.cybercom.mil/About/History/.

Command, US Cyber. "2018 Cyberspace Strategy Symposium Proceedings," 2018. https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM Cyberspace Strategy Symposium Proceedings 2018.pdf?ver=2018-07-11-092344-427.

Cyber Workforce." Accessed November 4, 2018. https://dodcio.defense.gov/Cyber-Workforce.aspx.

Defense Information Systems Agency. "About DISA." DISA.MIL. Accessed March 18, 2019. https://disa.mil/About.

Defense Management: Needs to Improve Its Oversight of Executive Agents," 2017. https://www.gao.gov/assets/690/688430.pdf.

DISA - Our History, 1947-1960." Accessed January 19, 2019. https://www.disa.mil/About/Our-History.

"DOD Dictionary of Military and Associated Terms," 2019.

Domingo, Francis C. "Conquering a New Domain: Explaining Great Power Competition in Cyberspace." *Comparative Strategy* 35, no. 2 (2016): 154–68.

Dunford, Gen Joseph F. "Chairman's Foreword." National Military Strategy of the United States. Washington D.C., 2018.

Fink, Kallie D., John D. Jordan, and James E. Wells. "Considerations for Offensive Cyberspace Operations." *Military Review* 35, no. 2 (May 2014): 4–11.

Giles, Keir, and William Hagestad. "Divided by a Common Language: Cyber Definitions in Chinese, Russian and English." In *2013 5th International Conference on Cyber Conflict (CYCON 2013)*. Tallinn, Estonia: IEEE, 2013. https://ieeexplore.ieee.org/abstract/document/6568390.

Staff, Joint Chiefs of. "Joint Publication 3-0: Joint Operations." January 17, 2017.

Joint Chiefs of Staff. "Joint Publication 3-12: Cyberspace Operations." June 8, 2018.

Joint Chiefs of Staff. "Joint Publication 6-01: Joint Electromagnetic Spectrum Management Operations," March 20, 2012.

Joint Chiefs of Staff. "The Joint Force in a Contested and Disordered World." *Joint Operating Environment*. July 14, 2016. https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joe_2035_july16.pdf?ver=2017-12-28-162059-917.

Kanwal, Gurmeet. "China's Emerging Cyber War Doctrine." *Journal of Defence Studies* 3, no. 3 (2009): 14–22. https://idsa.in/system/files/jds_3_3_gkanwal_0.pdf.

Lemay Center for Doctrine. *Air Force Basic Doctrine*, 2015. https://www.doctrine.af.mil/Portals/61/documents/Volume_1/V1-D01-Introduction.pdf.

Ministry of National Defense of the People's Republic of China. "China's Military Strategy." May 26, 2015.

Mitchell, William. *Winged Defense: The Development and Possibilities of Modern Air Power--Economic and Military*. University of Alabama Press, 2009.

Nakashima, Ellen, and Paul Sonne. "China Hacked a Navy Contractor and Secured a Trove of Highly Sensitive Data on Submarine Warfare." *The Washington Post*. June 8, 2018. https://www.washingtonpost.com/world/national-security/china-hacked-a-navy-contractor-and-secured-a-trove-of-highly-sensitive-data-on-submarine-warfare/2018/06/08/6cc396fa-68e6-11e8-bea7-c8eb28bc52b1_story.html?utm_term=.be83d1b9dda9.

Pollpeter, Kevin, Michael Chase, and Eric Heginbotham. *The Creation of the PLA Strategic Support Force and Its Implications for Chinese Military Space Operations*. RAND Corporation, 2017. https://doi.org/10.7249/RR2058.

"Radiation Basics." United States Nuclear Regulatory Commission, 2017. https://www.nrc.gov/about-nrc/radiation/health-effects/radiation-basics.html.

Sinek, Simon. "Lecture to United States Marine Corps Univeristy on Know What Game You Are Playing." Quantico, VA, 2018.

Sinek, Simon. "What Game Theory Teaches Us about War." *TED Archive*. November 8, 2016. https://www.youtube.com/watch?v=0bFs6ZiynSU.

Staff, Joint Chiefs of. "Joint Publication 3-0: Joint Operations." January 17, 2017.

Stavridis, James, and David Weinstein. "Time for a US Cyber Force." *US Naval Institute Proceedings* 140, no. 1 (2014). https://www.usni.org/magazines/proceedings/2014/january/time-us-cyber-force.

Tanner, Leah. "Examining Cyber Command Structures," 2015. https://apps.dtic.mil/docs/citations/ADA620750.

"The Joint Force in a Contested and Disordered World," 2016. https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joe_2035_july16.pdf?ver=2017-12-28-162059-917.

The White House. "National Cyber Strategy of the United States of America." Washington, DC, 2018. https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

US Department of Justice. "US Charges Five Chinese Military Hackers for Cyber Espionage Against US Corporations and a Labor Organization for Commercial Advantage." May 19, 2014. https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.

Welch, Larry. "Cyberspace-The Fifth Operational Domain: The Problem Cyberspace as a Domain-Similarities and Differences," 2011. www.ida.org.

Whittington, Michael C. "A Separate Space Force An 80-Year-Old Argument," 2000. http://research.maxwell.af.mil.