REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
04-05-2018	Master's of Military Studies	SEP 2017 - APR 2018

4. TITLE AND SUBTITLE

Warfighting in Cyberspace: Military Domains Demand Uniformed Services

5a. CONTRACT NUMBER
N/A

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
N/A

6. AUTHOR(S)

Grabowsky, Steve. C, Maj, USMCR

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. Lon Strauss

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

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

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The nation needs a branch of service to focus solely and distinctly on conducting warfare in and through cyberspace. Principle to this argument is the notion that cyberspace is a warfighting domain and not a warfighting function. This distinction serves as the basis for the claim to establish a uniformed service dedicated to the execution of all warfighting functions in cyberspace. Furthermore, this paper examines the statutory requirements of the nation ' s current military departments and associated branches and claims that the same requirements exist in cyberspace and therefore justifies a dedicated organization. Cyberspace organization, training, and equipping is different than other domains and deserves its own focus. The current military departments resource cyberspace to suit their primary domain and in doing so suffocate cyberspace warfighting potential. It also identifies the changing nature of cyberspace and why a service branch is best postured to perform capability development for a warfighting domain especially one as dynamic as cyberspace. Lastly, the paper examines how creating a service branch for cyberspace mimics command and control for other domains and allows Geographic Combatant Commands (GCC) the ability to integrate all warfighting domains within their assigned region.

15. SUBJECT TERMS

Cyber Service Branch, Cyber Force; USCYBERCOM; USSOCOM; Command and Control, C2; Title 10; Cyberspace; DoD

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
Unclass	Unclass	Unclass	UU	37	**19b. TELEPHONE NUMBER** *(include area code)* (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

TITLE: WARFIGHTING IN CYBERSPACE: MILITARY DOMAINS DEMAND UNIFORMED SERVICES

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

AUTHOR: Maj Steve Grabowsky

AY 2017-18

Mentor and Oral Defense Committee Member: Dr. Lon Strauss
Approved: [signature]
Date: 26 April 18

Oral Defense Committee Member: Dr. Brendan Valoriano
Approved: [signature]
Date: 4-26-18

Oral Defense Committee Member: LtCol Mark Howard
Approved: [signature]
Date: 26 Apr 18

Executive Summary

Title: Warfighting in Cyberspace: Military Domains Demand Uniformed Services

Author: Major Steve Grabowsky, United States Marine Corps

Thesis: Warfighting in cyberspace will only reach its full potential with the creation of a service branch that satisfies statutory responsibilities for domain cognizance, focuses on keeping pace with the changing nature of cyberspace, and mimics other operational domains for command and control.

Discussion: The nation needs a branch of service to focus solely and distinctly on conducting warfare in and through cyberspace. Principle to this argument is the notion that cyberspace is a warfighting domain and not a warfighting function. This distinction serves as the basis for the claim to establish a uniformed service dedicated to the execution of all warfighting functions in cyberspace. Furthermore, this paper examines the statutory requirements of the nation's current military departments and associated branches and claims that the same requirements exist in cyberspace and therefore justifies a dedicated organization. Cyberspace organization, training, and equipping is different than other domains and deserves its own focus. The current military departments resource cyberspace to suit their primary domain and in doing so suffocate cyberspace warfighting potential. It also identifies the changing nature of cyberspace and why a service branch is best postured to perform capability development for a warfighting domain especially one as dynamic as cyberspace. Lastly, the paper examines how creating a service branch for cyberspace mimics command and control for other domains and allows Geographic Combatant Commands (GCC) the ability to integrate all warfighting domains within their assigned region.

Conclusion: Current organization for cyberspace is limiting the DoD's warfighting potential. First, there is no singular organization responsible for domain cognizance in cyberspace. Cyberspace, like other recognized domains of warfare is unique and as such requires a single entity to determine the correct organization, training, and equipping necessary to move, maneuver, and project power in cyberspace. Furthermore, capability development in cyberspace requires expertise, speed, and agility; none of which COCOMs exhibit in developing capability for warfighting domains. Despite the DoD's claim to treat cyberspace as an operational domain, the current organization applies a function model to a warfighting domain and hinders its ability to effectively integrate cyberspace operations and project power in the manner currently afforded in other domains. USCYBERCOM is destined to repeat the same errors of USSPACECOM and likely arrive at the same conclusion for cyberspace that those in congress are now demanding for the space domain- the establishment of a service dedicated to cyberspace. The USSOCOM model approach to cyberspace does not adequately address the differences between warfighting in cyberspace and special operations.

DISCLAIMER

THE OPINIONS AND CONCLUSIONS EXPRESSED HEREIN ARE THOSE OF THE INDIVIDUAL STUDENT AUTHOR AND DO NOT NECESSARILY REPRESENT THE VIEWS OF EITHER THE MARINE CORPS COMMAND AND STAFF COLLEGE OR ANY OTHER GOVERNMENTAL AGENCY. REFERENCES TO THIS STUDY SHOULD INCLUDE THE FOREGOING STATEMENT.

TABLE OF CONTENTS

PAGE

Executive Summary ..... **i**

DISCLAIMER ..... **ii**

List of Tables and Figures ..... **iv**

Preface ..... **v**

Acknowledgements ..... **v**

INTRODUCTION **1**

CYBERSPACE ORGANIZATION **3**

CAPABILITY DEVELOPMENT AT THE SPEED OF CYBER **11**

COMMAND AND CONTROL FOR CYBERSPACE **18**

COUNTERING THE USSOCOM APPROACH **23**

CONCLUSION **29**

Bibliography **30**

List of Tables and Figures

Page
Table 1: Executive Order 9877 4
Table 2: USSOCOM vs USCYBERCOM Authorities 23

Figure 1: The Three Layers of Cyberspace 12
Figure 2: Internet Connected Devices and Addresses 13
Figure 3: USAF Total Aircraft Inventory 1950-59 17
Figure 4: Joint Task Force-Haiti Command and Control Organization 19
Figure 5: Army CH-47 Helicopter to SOCOM MH-47 Helicopter 27

Preface

I embarked on this project because of the challenges I faced in previous assignments with USCYBERCOM affiliated commands. There is an intense emphasis for planners assigned to the command to generate relevant options for commanders and for commanders to think about and employ cyberspace capabilities. Despite this emphasis, though there is a struggle to produce meaningful results. In my estimation, the struggle is based on our organizational approach. Commanders and planners are unable to fully integrate cyberspace with other domains because we do not treat it like other domains. Instead service departments are foraging paths within their own institutions, sometimes at the expense of proven combat capability, to support their assigned warfighting domain. This somewhat independent exploration into warfighting in cyberspace leads to a general unawareness of cyberspace capabilities and processes to leverage them. However, cross-service coordination is something planners and commanders have immense experience with and know very well. With that in mind, expecting the services to embrace and explore a new warfighting domain while preparing for 21st-century multi-polar great power competition is not a recipe for success. Instead a better approach would be to give the services back their own domains by creating a service to focus on cyberspace and rely on commanders and planners to do what they know- joint planning.

Acknowledgements

I would like to thank all that assisted in this effort. First, LtCol Tom Jarman, who provided levity during the busy times, and planted this seed during one late-night slide making adventure. Also, I would like to thank the staff and students at Command and Staff College of Marine Corps University for indulging my sometimes-passionate appeal to persuade others on this topic. Specifically, to Dr. Strauss, thank you for mentoring me along the during this project. My thanks extend to LtCol Howard and Dr. Valeriano for their input and insight to help shape this argument. Additionally, I must thank Andrea Hamlen and the rest of her team at the Marine Corps University Research Library. Your feedback and assistance on this and other projects along the way was extremely helpful and I sincerely appreciate it. Lastly, thanks to my wife, Lindsay and children, Sadie, and Levi. I know it was not always a fun dinner topic, but thanks for listening and know that your input helped shape this all the way to submission.

INTRODUCTION

"The U.S. military's dependence on cyberspace for its operations led the Secretary of Defense in 2011 to declare cyberspace as an operational domain for purposes of organizing, training, and equipping U.S. military forces."

-The Department of Defense Cyber Strategy
April, 2015

"Today, the president announced his decision to elevate U.S. Cyber Command as a unified combatant command. It reflects two factors: first, the maturity of Cyber Command itself, and second, the Department of Defense's long-term commitment to cyberspace as a warfighting domain."

-Mr. Kenneth P. Rapuano,
Assistant Secretary of Defense for Homeland Defense and Global Security.

President Trump penned a memo to the Secretary of Defense on the 18th day of August 2017 and with his signature authorized the elevation of United States Cyber Command (USCYBERCOM) to be the newest Combatant Command in the country. The President assigned USCYBERCOM "the responsibilities of Joint Force Provider and Joint Force Trainer," which are unique authorities for Unified Combatant Commands (UCC) and previously only belonged to United States Special Operations Command (USSOCOM).[1] Modeling USCYBERCOM after USSOCOM acknowledges that cyberspace is unique but implements a Functional Combatant Command where there should be a service branch. A function differs from a domain in both characterization and the way the Department of Defense (DoD) organizes its forces. The DoD organizes commands to execute functions and uniformed services to operate in domains. Warfighting in cyberspace will only reach its full potential with the creation of a service branch that satisfies statutory responsibilities for domain cognizance, focuses on keeping pace with the changing nature of cyberspace, and mimics other operational domains for command and control.

[1] Donald J. Trump, "Presidential Memorandum for the Secretary of Defense," The White House, August 18, 2017, 1, accessed January 19, 2018, https://www.whitehouse.gov/presidential-actions/presidential-memorandum-secretary-defense/.

This paper makes a case for the establishment of a separate branch of service dedicated to cyberspace rather than a joint command. Principle to this argument is the notion that cyberspace is a warfighting domain and not a warfighting function.[2] This distinction serves as the basis for the claim to establish a uniformed service dedicated to the execution of all warfighting functions in cyberspace. Furthermore, the paper examines the statutory requirements of the nation's current military departments and associated branches and claims that the same requirements exist in cyberspace and therefore justifies a dedicated organization. It also identifies the changing nature of cyberspace and why a service branch is best postured to perform capability development for a warfighting domain especially one as dynamic as cyberspace. Lastly, the paper examines how creating a service branch for cyberspace mimics command and control for other domains and allows Geographic Combatant Commands (GCC) the ability to integrate all warfighting domains within their assigned region. The DoD approach to organizing for warfighting in cyberspace is evolutionary and would benefit from a look at the legal responsibilities of the nation's current armed forces.

[2] US Department of Defense, *Department of Defense Strategy for Operating in Cyberspace*, July 2011, 5, accessed January 19, 2018, https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf.

CYBERSPACE ORGANIZATION

"In cyber, what we are going to do is reorganize. I told you we're reorganizing the department to a degree. You're going to see reorganization of the fundamental organizations."
-Jim Mattis, Secretary of Defense

The DoD's characterization of cyberspace as a domain places it on par with other traditional well-known domains and therefore should warrant a similar approach. The fundamental organizing construct for the DoD is military service departments. Each of the service departments specializes in warfighting domains to serve a unique role in the nation's military capability. Domains of warfare have either military branches or departments dedicated to organization, training, and equipping for the individuality of that domain. Based on that primary organizational principle, creating a single entity with the responsibility to organize, train, and equip in cyberspace is a logical approach. Today, however, that organization does not exist and services expand their roles to include the cyberspace domain. As retired United States Navy admiral and the current dean of the Fletcher School of Law and Diplomacy at Tufts University, James Stavridis points out the problem "is that no one service specializes in cyberspace operations."[3] Since no one service specializes in cyberspace, all services expand beyond their assigned domains to include organization, training and equipping for cyberspace. When President Truman signed Executive Order 9877, he cemented the roles of the Armed Forces and articulated specific domains for which each service shall organize train and equip the military.[4] Table 1 shows the roles prescribed for each service.

[3] James Stavridis and D. Weinstein, "Time for a U.S. Cyber Force." Proceedings- United States Naval Institute 140, no. 1 (2014): 40-45.
[4] Harry S. Truman: "Executive Order 9877—Functions of the Armed Forces," July 26, 1947. Online by Gerhard Peters and John T. Woolley, The American Presidency Project. http://www.presidency.ucsb.edu/ws/?pid=12717.

Table 1: Executive Order 9877

ARMY	AIR FORCE	NAVY	MARINE CORPS
1. To organize, train and equip land forces for:	1. To organize, train and equip air forces for:	1. To organize, train and equip naval forces for:	4. To maintain the U.S. Marine Corps:
a. Operations on land, including joint operations. b. The seizure or defense of land areas, including airborne and joint amphibious operations. c. The occupation of land areas.	a. Air operations including joint operations. b. Gaining and maintaining general air supremacy. c. Establishing local air superiority where and as required. d. The strategic air force of the United States and strategic air reconnaissance. e. Air lift and support for airborne operations. f. Air support to land forces and naval forces, including support of occupation forces. g. Air transport for the armed forces, except as provided by the Navy in accordance with paragraph r f, of Section III.	a. Operations at sea, including joint operations. b. The control of vital sea areas, the protection of vital sea lanes, and the suppression of enemy sea commerce. c. The support of occupation forces as required. d. The seizure of minor enemy shore 'positions capable of reduction by such landing forces as may be comprised within the fleet organization. e. Naval reconnaissance, antisubmarine warfare, and protection of shipping. The air aspects of those functions shall be coordinated with the Air Force, including the development and procurement of aircraft, and air installations located on shore, and use shall be made of Air Force personnel, equipment and facilities in all cases where economy and effectiveness will thereby be increased. Subject to the above provision, the Navy will not be restricted as to types of aircraft maintained and operated for these purposes. f. The air transport necessary for essential internal administration and for air transport over routes of sole interest to naval forces where the requirements cannot be met by normal air transport facilities.	a. To provide Marine Forces together with supporting air components, for service with the Fleet in the seizure or defense of advanced naval bases and for the conduct of limited land operations in connection therewith. b. To develop, in coordination with the Army and the Air Force those phases of amphibious operations which pertain to the tactics, technique and equipment employed by landing forces. c. To provide detachments and organizations for service on armed vessels of the Navy. d. To provide security detachments for protection of naval property at naval stations and bases. e. To provide, as directed by proper authority, such missions and detachments for service in foreign countries as may be required to support the national policies and interests of the United States.
2. To develop weapons, tactics, technique, organization and equipment of Army combat and service elements, coordinating with the Navy and the Air Force in all aspects of joint concern, including those which pertain to amphibious and airborne operations.	2. To develop weapons, tactics, technique, organization and equipment of Air Force combat and service elements, coordinating with the Army and Navy on all aspects of joint concern, including those which pertain to amphibious and airborne operations.		
3. To provide, as directed by proper authority, such missions and detachments for service in foreign countries as may be required to support the national policies and interests of the United States.	3. To provide, as directed by proper authority, such missions and detachments for service in foreign countries as may be required to support the national policies and interests of the United States.	2. To develop weapons, tactics, technique, organization and equipment of naval combat and service elements, coordinating with the Army and the Air Force in all aspects of joint concern, including those which pertain to amphibious operations.	
4. To assist the Navy and Air Forces in the accomplishment of their missions, including the provision of common services and supplies as determined by proper authority.	4. To provide the means for coordination of air defense among all services.		
	5. To assist the Army and Navy in accomplishment of their missions, including the provision of common services and supplies as determined by proper authority.	3. To provide, as directed by proper authority, such missions and detachments for service in foreign countries as may be required to support the national policies and interests of the United States.	5. To assist the Army and the Air Force in the accomplishment of their missions, including the provision of common services and supplies as determined by proper authority.

Source: Harry S. Truman: "Executive Order 9877—Functions of the Armed Forces," July 26, 1947. Online by Gerhard Peters and John T. Woolley, The American Presidency Project. http://www.presidency.ucsb.edu/ws/?pid=12717.

Today's language, codified in Title 10 of United States Code, captures the same essence of President Truman's order. The Army

> includes land combat and service forces and such aviation and water transport as may be organic therein. It shall be organized, trained, and equipped primarily for prompt and sustained combat incident to operations on land. It is responsible for the preparation of land forces necessary for the effective prosecution of war except as otherwise assigned and, in accordance with integrated joint mobilization plans, for the expansion of the peacetime components of the Army to meet the needs of war.[5]

Clearly legislators intend for the Army to specialize and prepare for warfare centered on *terra firma.* The language includes provisions for forces like aviation and water transport outside of pure land forces but only so as to support land combat.

[5] Armed Forces, 10 U.S.C § 3062 (2018), http://uscode.house.gov/browse/prelim@title10&edition=prelim.

The Department of the Navy is a bit unique in that it contains two separate military services in one department, the Navy, and the Marine Corps. Similar to the responsibilities of the Army and in the same legal reference, a separate section states that the Navy

> shall be organized, trained, and equipped primarily for prompt and sustained combat incident to operations at sea. It is responsible for the preparation of naval forces necessary for the effective prosecution of war except as otherwise assigned and, in accordance with integrated joint mobilization plans, for the expansion of the peacetime components of the Navy to meet the needs of war.[6]

The second service, the

> Marine Corps, within the Department of the Navy, shall … be organized, trained, and equipped to provide fleet marine forces of combined arms, together with supporting air components, for service with the fleet in the seizure or defense of advanced naval bases and for the conduct of such land operations as may be essential to the prosecution of a naval campaign.[7]

Legislators emphasize these services to operate in, on, and from the sea specifically at the seam of the land and sea domains. The Naval force, including both the Navy and Marine Corps, finds its niche in the maritime domain with the specific addition of skills to project power ashore through amphibious operations.

The last department, the Department of the Air Force,

> includes aviation forces both combat and service not otherwise assigned. It shall be organized, trained, and equipped primarily for prompt and sustained offensive and defensive air operations. It is responsible for the preparation of the air forces necessary for the effective prosecution of war except as otherwise assigned and, in accordance with integrated joint mobilization plans, for the expansion of the peacetime components of the Air Force to meet the needs of war.[8]

At first glance it appears that the United States Air Force essentially gets the remaining aviation elements leftover from the other services. That holds true up front, but the key attribute of the responsibility outlined in title 10 United States Code (USC) is for "prompt and sustained

[6] Armed Forces, 10 U.S.C § 5062 (2018), http://uscode.house.gov/browse/prelim@title10&edition=prelim.
[7] Ibid.
[8] Armed Forces, 10 U.S.C § 8062 (2018), http://uscode.house.gov/browse/prelim@title10&edition=prelim.

offensive and defensive air operations."[9] Said differently, all air forces belonging to the Air Force exist to prosecute offensive and defensive air operations of any duration. This distinction means that Air Force assets are in stark contrast to the aviation assets of other services in that they do not exist to support other domains, but solely for the purpose of air warfare. Along with the distinction comes the responsibility of the service department to organize, train, and equip purely for offensive and defensive air operations.

There is no question that the Army, Navy, and Air Force have the responsibility for land, sea, and air respectively. However, despite the speech from Deputy Secretary of Defense Lynn stating "the Defense Department has formally recognized cyberspace for what it is - a new domain of warfare. Like land, sea, air, and space, cyberspace is a domain that we must operate effectively within," no organization exists with the responsibility for the "effective prosecution of war" in cyberspace.[10]

Without an organization responsible for domain cognizance in cyberspace the DoD requires a coalition of the willing. USCYBERCOM has the tough task of creating organizational and domain institutional knowledge three-years at a time based on the personnel assignments to their command. Henri Lipmanowicz, organizational expert, and author of *Liberating Structures* accounts for the challenge facing USCYBERCOM and the DoD as the tension between buy-in and ownership. Lipmanowicz defines ownership as sharing "the ownership of an idea, a decision, or an action plan; it means that you have participated in its development and that [one] chose[s]… to endorse it."[11] He further elaborates that it "means that [one is] both willing and

[9] Ibid.
[10] William J. Lynn, "Remarks at USSTRATCOM Cyber Symposium," United States Department of Defense, 1, accessed January 19, 2018, http://archive.defense.gov/speeches/speech.aspx?speechid=1477.
[11] Henri Lipmanowicz and Keith McCandless, The Surprising Power of Liberating Structures: Simple Rules to Unleash a Culture of Innovation (Seattle, WA: Liberating Structures Press, 2016).

ready to implement it."[12] Conversely Lipmanowicz defines buy-in as the exact opposite, noting that "someone else or some group of people has done the development, the thinking, … and now they have to convince [another] to come along and implement their ideas/plans."[13] Without a service or branch for cyberspace warfighting the DoD is attempting to elicit buy-in from the other services, who already exhibit ownership to another domain, on a rotational basis depending on their assignment to USCYBERCOM. Statutorily requiring a single organization to focus on warfighting in cyberspace creates ownership up front and allows an unbiased approach to organization, training, and equipping for the domain.

Furthermore, a dedicated service for cyberspace with ownership of the domain would be able to dictate its organization. For instance, a separate service would create the opportunity to recruit and retain personnel with aptitudes and propensity for performance in cyberspace. The pool of personnel available to a cyberspace force may not be subject to the same physical standards that the Army or the Marine Corps currently requires. Instead of identifying where current services can apply talent to cyberspace, the DoD could directly identify, attract, and retain personnel who can execute warfighting functions in cyberspace. Creating a separate service or branch does two things for the DoD: First, it eliminates redundancy and reduces overhead. Services that are currently building cyberspace warfighting organizations can reduce or potentially consolidate those efforts. Services would still have the requirement for cyberspace elements to support their primary missions, but they would be Marines, Soldiers, or Sailors first rather than Cyber-Marines, Cyber-Soldiers, or Cyber-Sailors. Second, it refocuses the services on their assigned domain reducing the manpower pressure facing the services. Current pressures to retain and promote personnel in the cyber field are mounting. Services must wrestle with

[12] Ibid
[13] Ibid.

managing and in some cases inventing what the Fiscal Year 15 National Defense Authorization Act (NDAA) calls "non-traditional management approaches … for a portion of the cyber workforce, allowing the development and mastery of their tradecraft. The Department may require special considerations to ensure the Services can recruit, train, and retain top personnel."[14] Rather than creating nontraditional organizational constructs for personnel, the DoD can use its most traditional organizing principle and create a service that can recruit, retain, and promote personnel to suit warfighting in cyberspace.

Hand in hand with recruiting and retaining personnel is the ability to train. Creating a separate dedicated service or branch for cyberspace allows that service to focus explicitly on the skills unique to that domain. Each service trains for operations in cyberspace in a unique manner but none with the focus solely on the cyberspace domain. Currently the Army is training personnel to "merge cyber and electromagnetic activity (CEMA) into traditional and tactical military formations" while the Marine Corps approach is through a Marine Expeditionary Force (MEF) Information Group (MIG) designed to "bring together cyberspace, electronic warfare, information operations, command and control and intelligence functions all together to best support the" Marine Air-Ground Task Force (MAGTF).[15] The efforts from the services do their best to train cyber personnel in support of their service primary responsibility. The piece missing that a separate cyber service could fill is the specific technical skills required for cyber forces to operate against high-end competition in cyberspace. According to USCYBERCOM one of their mission imperatives is to defend the nation against "[s]tates, groups, and individuals … using and developing sophisticated capabilities to conduct cyber coercion, cyber attacks, and cyber

[14] *National Defense Authorization Act of 2015*, HR 3979 114th Cong., Congressional Record 291, (December 19, 2014).
[15] Mark Pomerleau, "Here's How Cyber Service Component Mission Sets Differ from CYBERCOM," C4ISRNET, July 27, 2017, accessed March 29, 2018, https://www.c4isrnet.com/cyber/2017/07/27/heres-how-cyber-service-components-cybercom-mission-sets-differ/.

exploitation against the United States and our allies. The targets of their efforts extend well beyond government and into privately owned businesses."[16] Service training for cyberspace does not develop the skills necessary to perform that mission. Advanced cyber training is not a priority for service departments because they are training cyber personnel to support their assigned mission. As Stavridis contends, "Cyberspace operations … do not require any of the core competencies of the five services; in fact, the cyber domain requires precisely the core competencies that none of the other branches possesses."[17] Developing a service or branch focused on high-end cyberspace specific skills to match the nation's adversaries is the best organizational approach.

Equipping is another statutory requirement that a separate cyberspace service or branch would fill. Cyberspace equipment is notably different than equipment in other domains but requires a similar approach. Warfighting in cyberspace requires weapons and platforms as on land, in air, or at sea, but the weapons look more like computer code and the platforms require a lot more encryption. Weapons in cyberspace may be for general application, or very specific application as in the case of Stuxnet which was "a precision, military-grade cyber missile."[18] "Cyber missiles" as in the case of Stuxnet, and other cyber weapons systems to support military operations in cyberspace require dedicated focus and should benefit from long-term planning, not one-off mission specific development, though that may be a requirement. In any case the current uniformed services are not in position to develop those weapons systems or platforms. Lt. Gen. Edward C. Cardon, former commanding general, U.S. Army Cyber Command (Second

[16] Michael Rogers, "Beyond the Build Delivering Outcomes through Cyberspace: The Commander's Vision and Guidance for US Cyber Command," United States Cyber Command, (Ft. Meade, MD: June 3, 2015).
[17] James Stavridis and D. Weinstein, "Time for a U.S. Cyber Force." Proceedings- United States Naval Institute 140, no. 1 (2014): 40-45.
[18] Mark Clayton, "Stuxnet Malware Is 'Weapon' Out to Destroy . . . Iran's Bushehr Nuclear Plant?" Christian Science Monitor, 21 September 2010, https://www.csmonitor.com/USA/2010/0921/Stuxnet-malware-is-weapon-out-to-destroy-Iran-s-Bushehr-nuclear-plant.

Army), wrote about this deficiency in a 2016 article regarding Army cyber capabilities, stating that the Army "did not have the institutional framework to provide both training and capability development in a domain" like cyberspace.[19] Equipping for warfighting in cyberspace requires domain expertise. Expertise that only exists when a service can focus purely on cyberspace domain cognizance.

[19] Ed Cardon, "Maturing Cyber Capabilities Critical to Army Future," www.army.mil, accessed March 29, 2018, https://www.army.mil/article/175465/maturing_cyber_capabilities_critical_to_army_future.

CAPABILITY DEVELOPMENT AT THE SPEED OF CYBER

"Innovation is moving at a scarily fast pace."

-Bill Gates, Founder of Microsoft Corporation

In addition to expertise, equipping for warfighting in cyberspace requires speed and agility. Joint Publication 3-12 defines cyberspace in "three layers: physical network, logical network, and cyber-persona. Each of these represents a level on which CO maybe conducted."[20] The physical layer of cyberspace is defined as

> physical network component is comprised of the hardware, systems software, and infrastructure (wired, wireless, cabled links, EMS links, satellite, and optical) that supports the network and the physical connectors (wires, cables, radio frequency, routers, switches, servers, and computers).[21]

More devices connected to the internet create more opportunities to conduct cyberspace operations. The logical layer requires more imagination and includes

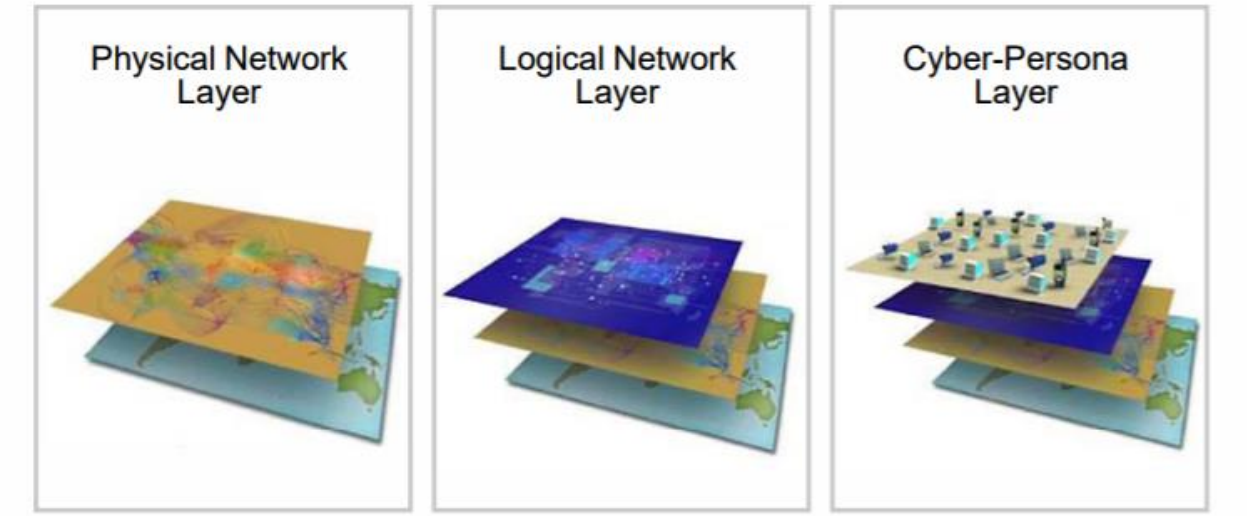
> those elements of the network that are related to one another in a way that is abstracted from the physical network, i.e., the form or relationships are not tied to an individual, specific path, or node. A simple example is any Web site that is hosted on servers in multiple physical locations where all content can be accessed through a single uniform resource locator (URL).[22]

Lastly, the cyber-persona layer "consists of the people actually on the network. Cyber-personas may relate fairly directly to an actual person or entity, incorporating some biographical or corporate data, e-mail and IP address(es), Web pages, phone numbers, etc."[23] Figure 1 depicts the three layers of cyberspace and what each includes.

---

[20] Joint Staff, *Cyberspace Operations*, JP 3-12, (Washington, DC: Joint Staff, 5 February 2013), http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12R.pdf
[21] Ibid.
[22] Ibid.
[23] Ibid.

Figure 1: The Three Layers of Cyberspace



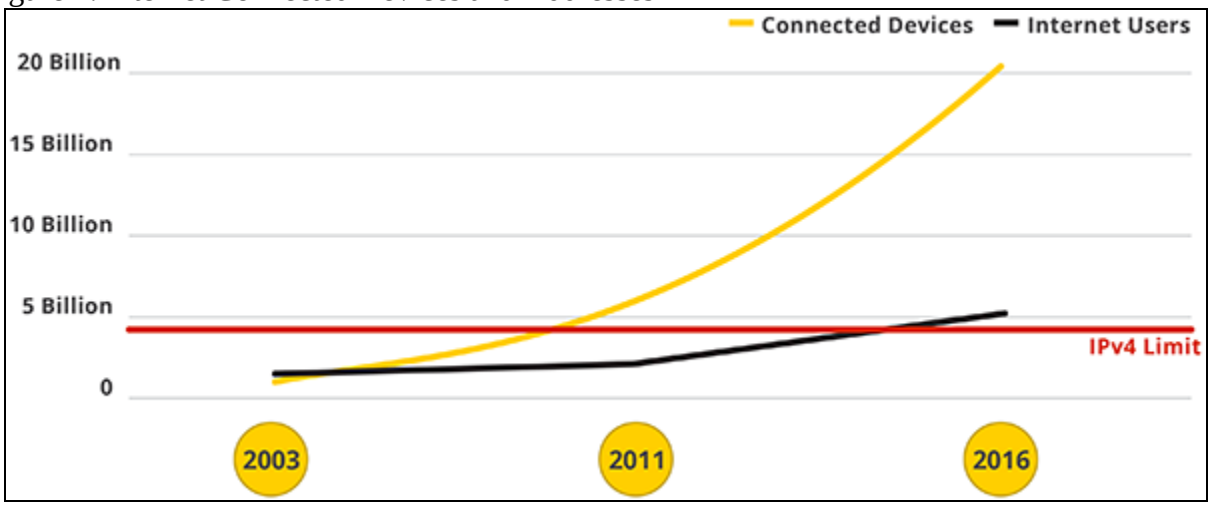
Source: Joint Staff, *Cyberspace Operations*, JP 3-12, (Washington, DC: Joint Staff, 5 February 2013), http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12R.pdf

Not only is cyberspace multidimensional but it is growing exponentially. According to Intel Corporation, the Internet of Things (IoT) "is growing at a breathtaking pace, from 2 billion objects in 2006 to a projected 200 billion by 2020."[24] Devices connected to the internet are proliferating so rapidly that the addressing system reached exhaustion. ICANN, the Internet Corporation for Assigned Numbers and Names, announced in February 2011 that "a critical point in the history of the Internet was reached today with the allocation of the last remaining IPv4 (Internet Protocol version 4) Internet addresses from a central pool. It means the future expansion of the Internet is now dependant [sic] on the successful global deployment of the next generation of Internet protocol, called IPv6."[25] Device connections outgrew the space and necessitated an entirely new addressing system to accommodate future connections. The capacity of addresses increased from $4.3x10^9$ to $3.4 x10^{38}$, to be clear that is an increase of over of $7.9x10^{28}$ times as many addresses. This is important because the addressing system serves as

[24] Intel, "A Guide to the Internet of Things Infographic," Intel, 1, accessed January 19, 2018, https://www.intel.com/content/www/us/en/internet-of-things/infographics/guide-to-iot.html.
[25] ICANN, "Available Pool of Unallocated IPv4 Internet Addresses Now Completely Emptied," February 3, 2011, 1, accessed January 19, 2018, https://www.icann.org/en/system/files/press-materials/release-03feb11-en.pdf.

one element of cyberspace terrain. Physical devices tied to cyber-personas through addresses creates opportunities for cyberspace operations. Figure 2 shows the rapid increase in devices and allocations for addressing. Now that the infrastructure is nearly limitless, exploitation of the terrain will continue at an exponential pace and capability development in cyberspace must keep pace.

Figure 2: Internet Connected Devices and Addresses



Source: Google IPv6, https://www.google.com/intl/en/ipv6/index.html

To keep pace with the growth in cyberspace, the department needs to reevaluate its capability development efforts. Cyberspace capability development will not be sufficient under the current organization because services develop capability based on their statutory requirements for their domain and no service exists to conduct capability development for the cyberspace domain. Stavridis points out that the current approach,

> not only … threaten[s] unity of command and foster[s] at times unhealthy competition among the services, but … CYBERCOM lacks sufficient influence over the services' priorities, and in the event that CYBERCOM and its components do not share mission interests, conflicts inevitably arise.[26]

[26] James Stavridis and D. Weinstein, "Time for a U.S. Cyber Force." Proceedings- United States Naval Institute 140, no. 1 (2014): 40-45.

Simply put, a standalone cyberspace force could develop capabilities unencumbered by the existing services competing priorities for capability development for their respective domains. The current arrangment forces prioritization decisions that pit cyberspace capabilities against capability development for the services' prescribed domain. Even when those cyberspace capabilities do win out, they often manifest in ways that support warfighting in other domains. Along those three layers of cyberspace, the Army may pursue physical capability development in cyberspace to support land warfare, while the Navy may pursue logical or persona layer capability development to support operations at sea.

Since the service departments are the organizations responsible for the preponderance of capability development, they have the most influence on what direction development takes. Prior to 2002, the DoD relied entirely on the services' ability to develop and procure capabilities. That changed after that year when the DoD tried to streamline its approach to capability development through the creation of the Joint Capability Integration Development System (JCIDS), "to replace the previous service-specific … system, which created redundancies in capabilities and failed to meet the combined needs of all US military services."[27] However, in 2008 the Government Accountability Office (GAO) "reviewed JCIDS documentation related to proposals for new capabilities and found that most--almost 70 percent--were sponsored by the military services, with little involvement from the joint community--including the combatant commands (COCOMs)."[28] The joint community and specifically the COCOMs are not in positions to create capabilities for warfighters. Even though COCOMs the warfighting, the best organization to create current capabilities are the service departments. The GAO report further

[27] U.S. Government Accountability Office, "Defense Acquisitions: DOD's Requirements Determination Process Has Not Been Effective in Prioritizing Joint Capabilities," U.S. Government Accountability Office (U.S. GAO), September 25, 2008, accessed March 29, 2018, https://www.gao.gov/products/GAO-08-1060.
[28] Ibid.

illuminated "that determining how best to integrate COCOM and service capability perspectives will be challenging because of differences in roles, missions, and time frames."[29] Service departments remain in the best position to create capabilities based on their assigned warfighting domain. Cyberspace will complicate the demands for capability development because of its dynamic nature, unique layers, and the speed at which warfighters need weapons systems delivered. The DoD needs to identify a service or branch with the responsibility and authority to pursue, test, and procure unique weapons systems and platforms to reach the full warfighting potential of cyberspace.

Current capability development efforts for cyberspace support warfighting in other domains. Cyberspace development now is very similar to early aviation capability developments that supported land and sea efforts during the interwar period because it exists to support other warfighting domains. Capability development for the United States Army Air Forces (USAAF) during the 1940s "took place at Air Materiel Command (AMC), but that organization was focused on the rapid acquisition of proven aviation technologies, not long-term [research and development] R&D."[30] Shortly after its independence, the Air Force "approved the creation of Air Research and Development Command (ARDC), which separated the R&D functions from Air Materiel Command. Along with ARDC, Fairchild approved the creation of a new Air Staff position, the deputy chief of staff, development (DCS/D)," which would oversee the link between technological development and unique skills of air force officers.[31] Air Force Flight Test Center chief historian, Dr. James Young, describes the circumstances surrounding the Army

[29] U.S. Government Accountability Office, "Defense Acquisitions: DOD's Requirements Determination Process Has Not Been Effective in Prioritizing Joint Capabilities," U.S. Government Accountability Office (U.S. GAO), September 25, 2008, accessed March 29, 2018, https://www.gao.gov/products/GAO-08-1060.
[30] Adam Grissom, Caitlin Lee, and Karl Mueller, "Innovation in the United States Air Force: Evidence from Six Cases," RAND Corporation, 2016, 9, accessed January 19, 2018, doi:10.7249/rr1207.
[31] Stephen B. Johnson, *The United States Air Force and the Culture of Innovation: 1945-1965*, (Washington, D.C.: Air Force History and Museums Program, 2002), 38.

Air Forces' challenges in the interwar period in developing the turbojet where "the procurement system under which they were forced to operate actually discouraged radical innovation."[32] Under previous organizational construct during the interwar period and prior to the establishment of ARDC, Air Force capability development efforts toiled. From 1946 to 1950 aircraft totals for the United States Army Air Forces (USAAF) and later the Air Force declined. At the end of 1946 there were 30,035 total aircraft but that fell to 17,686 by December of 1949.[33]

Once able to identify, develop, and procure weapons systems and platforms to suit the needs of the domain without subordination to land or sea the Air Force was able to radically change their aircraft inventory. In just a 10-year period from 1950-1959 the total number of aircraft in service jumped from 12,319 to 20,461. In nearly all categories of aircraft the inventory increased twofold or more. Figure 3 shows the totals including numbers for each of the following aircraft types: bombers, fighters, reconnaissance, tankers, and transports. A category like tankers for example increased by 1316.67%. A significant increase in tanker aircraft attests to the concepts that offensive and defensive airpower necessitated the requirement for aerial refueling and therefore prompted capability development. Conversely, during the 1950s "Naval Aviation … specialize[d] in missions as diverse as search and rescue, anti-submarine warfare, and electronic warfare," and their capability development efforts supported

[32] Jacob Neufeld, George M. Watson, and David Chenoweth, *Technology and the Air Force: A Retrospective Assessment*, (Washington, D.C.: Air Force History and Museums Program, U.S. Air Force, 1997), 12, accessed January 19, 2018, https://permanent.access.gpo.gov/airforcehistory/www.airforcehistory.hq.af.mil/Publications/fulltext/technology_and_the_af_a_retrospective_assessment.pdf.

[33] Headquarters United States Air Force, "UNITED STATES AIR FORCE STATISTICAL DIGEST JAN 1949-JUN 1950: FIFTH EDITION, (Washington, D.C.: Air Force Operations Statistics Division, U.S. Air Force 25 April 1951) https://media.defense.gov/2011/Apr/05/2001329940/-1/-1/0/AFD-110405-027.pdf.

those missions.[34] Much of the Navy's efforts centered around carrier-based operations whereas the Air Force development efforts during that time supported its strategic bombing missions.

Figure 3: USAF Total Aircraft Inventory 1950-59

	FY50	FY51	FY52	FY53	FY54	FY55	FY56	FY57	FY58	FY59
TOTAL										
Active	8,716	12,800	15,264	17,497	18,697	20,002	23,212	22,116	18,856	17,357
Reserve	949	144	7	370	485	632	754	753	659	779
ANG	2,654	583	961	1,340	1,728	1,908	2,138	2,170	2,429	2,325
Total	**12,319**	**13,527**	**16,232**	**19,207**	**20,910**	**22,542**	**26,104**	**25,039**	**21,944**	**20,461**
ICBMs	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**
BOMBERS										
Active	853	1,314	1,601	1,570	1,534	1,688	2,282	2,334	2,276	2,234
Reserve	89	0	1	9	12	23	79	3	0	0
ANG	198	8	20	32	62	0	89	52	46	39
Total	**1,140**	**1,322**	**1,622**	**1,611**	**1,608**	**1,711**	**2,450**	**2,389**	**2,322**	**2,273**
FIGHTERS/ATTACK										
Active	1,821	3,440	3,753	4,586	5,407	5,975	7,746	7,302	5,568	4,980
Reserve	1	0	0	100	109	170	165	114	0	0
ANG	1,802	388	541	694	1,021	1,311	1,442	1,460	1,774	1,680
Total	**3,624**	**3,828**	**4,294**	**5,380**	**6,537**	**7,456**	**9,353**	**8,876**	**7,342**	**6,660**
RECONNAISSANCE										
Active	255	430	557	630	778	1,001	1,267	1,117	944	887
Reserve	0	0	0	0	0	1	0	0	0	0
ANG	15	0	10	20	31	72	96	160	140	152
Total	**270**	**430**	**567**	**650**	**809**	**1,074**	**1,363**	**1,277**	**1,084**	**1,039**
TANKERS										
Active	84	172	265	476	638	745	907	932	1,023	1,190
Reserve	0	0	0	0	0	0	0	0	0	0
ANG	0	0	0	0	0	0	0	0	0	0
Total	**84**	**172**	**265**	**476**	**638**	**745**	**907**	**932**	**1,023**	**1,190**
TRANSPORTS										
Active	2,466	2,858	2,968	3,429	3,600	3,702	3,798	3,727	3,334	2,788
Reserve	50	5	1	116	181	249	305	488	599	721
ANG	181	91	88	86	95	96	168	170	181	183
Total	**2,697**	**2,954**	**3,057**	**3,631**	**3,876**	**4,047**	**4,271**	**4,385**	**4,114**	**3,692**

Source: Col. James C. Ruehrmund Jr. USAF (Ret.) and Dr. Christopher J. Bowie, *ARSENAL OF AIRPOWER: USAF Aircraft Inventory 1950-2016*, February 2018, The Mitchell Institute for Aerospace Studies, Air Force Association, Arlington, VA.

[34] United States. Department of the Navy. Naval Aviation Enterprise. 2010. *Naval Aviation Vision*. Washington, D.C.: U.S. Navy, Naval Aviation Enterprise, http://www.public.navy.mil/airfor/Documents/Vision%20Document.pdf

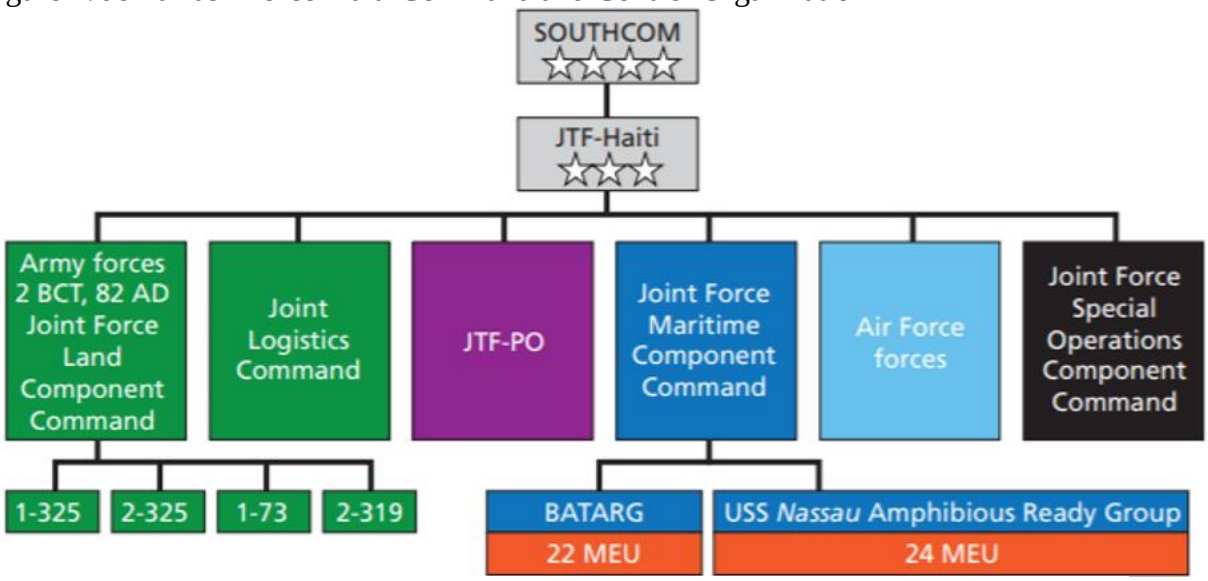
COMMAND AND CONTROL FOR CYBERSPACE

"The preeminent JFC [Joint Force Commander] requirement for freedom of maneuver in cyberspace is command and control (C2). It is impossible to fully employ today's joint force without leveraging cyberspace."

-Major General Brett T. Williams, USAF, former Director of Operations, J3, for U.S. Cyber Command

When the Air Force gained its independence from the Army in 1947 it was a major reorganization for the DoD. The DoD would not see another major reorganization of that scale until Congress passed the Goldwater-Nichols Act almost 40 years later. Redefining the interaction between the services and joint commands, the Goldwater-Nichols Act dictates the way the DoD operates today. The relationship between the service departments and the COCOM is one of provider and user. Services develop and provide forces to the joint commanders for execution in their respective areas. Additionally, the act created Geographic Combatant Commands (GCCs) as well as Functional Combatant Commands (FCCs). This system creates synergy in all warfighting domains under one GCC for a designated region. Under this construct GCC commanders can leverage their assigned service components to serve as subordinate commanders within their domain of cognizance as part of a joint force. The commanders can, and often do, depending on the situation, assign a component to execute air operations, land operations and operations at sea. Figure 4 illustrates one example of this concept for Joint Task Force Haiti during the earthquake relief efforts in 2010. It shows subordinate elements responsible for land, maritime, and air operations. In doing this, the JFC can synchronize the activities and effects in each domain to optimize mission accomplishment. This is one of the key differences between a GCC and a FCC. A FCC has global responsibility for that specific function and as such overlaps with a region that belongs to a GCC. The GCC must synchronize that function along with all other domain operations within its region.

Figure 4: Joint Task Force-Haiti Command and Control Organization



Source: Cecchine, Gary. 2013. *The U.S. Military Response to the 2010 Haiti Earthquake: Considerations for Army Leaders*. Santa Monica, CA: RAND. https://www.rand.org/content/dam/rand/pubs/research_reports/RR300/RR304/RAND_RR304.pdf.

Currently there are six Geographic Combatant Commands (GCCs) that exist "to promote the development of the region while cooperating to enhance security, deter aggression, respond with force when necessary and to provide humanitarian assistance."[35] Now with the Presidential memo from August 2017, the DoD has four Functional Combatant Commands (FCC) "whose mission is the worldwide performance of a warfighting function."[36] Inherent in the mission of FCCs is their execution of a function. Functions differ from domains according to the DoD. The difference between executing a function and where that function takes place is not just semantics. The former is what Joint Publication 3-0 (JP 3-0) identifies as "related capabilities and activities grouped together to help [Joint Force Commander's] JFCs integrate, synchronize,

[35] US Department of Defense, *USPACOM mission*, accessed January 19, 2018, https://www.defense.gov/About/Military-Departments/Unified-Combatant-Commands/.
[36] William C. Story, *Military Changes to the Unified Command Plan: Background and Issues for Congress*, CRS Report for Congress RL30245, (Washington DC: Congressional Research Service, June 21, 1999), 3, accessed January 19, 2018, http://www.congressionalresearch.com/rl30245/document.php?study=military%2bchanges%2bto%2bthe%2bunified%2bcommand%2bplan%2bbackground%2band%2bissues%2bfor%2bcongress.

and direct joint operations."[37] The latter is where those functions take place and not on its own a function. Since the DoD recognizes cyberspace as a warfighting domain and not a function, establishing a FCC for cyberspace runs counter to current doctrine and does not allow GCC commanders to effectively synchronize all warfighting domains in their regions. A service or branch dedicated to cyberspace operations would mimic other recognized domains and allow GCC commanders the option to organize subordinate commanders with domain cognizance for the execution of warfighting cyberspace. Furthermore, the GCC can then coordinate cyberspace activities with other warfighting domains to optimize for mission accomplishment.

It is also worth noting that Figure 4 also depicts a component under the JFC to coordinate the function of special operations. A JFC commander can choose to leverage a FCC in this manner for synchronization of specific functions with other domain activities, but normally FCCs are in a supporting role to the GCC for execution of the function like transportation for instance. United States Transportation Command (USTRANSCOM) provides global mobility in support of GCC mission execution. This becomes problematic, however, when the DoD builds FCCs around a warfighting domain instead of a function. This is the case with United States Space Command. In 1985 the DoD formally "consolidate[d] assets affecting US activities in space" as components under the United States Space Command (USSPACECOM) whose mission was "to conduct joint space operations in accordance with its Unified Command Plan's [UCP] assigned missions of Space Forces Support, Space Force Enhancement, Space Force Application and Space Force Control."[38] That mission and organization structure lasted until 2002 when USSPACECOM deactivated.

---

[37] Joint Staff, *Joint Operations*, JP 3-0, (Washington, DC: Joint Staff, 17 January 2017), http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_0_20170117.pdf, III-1.
[38] Air University, "Air University Space Reference Guide," AU Space Reference Guide, 18-1, accessed January 19, 2018, http://www.au.af.mil/au/awc/awcgate/srg/au-srg.htm.

USSCPACECOM was a casualty of competing national security interests and priorities in 2002. Nonetheless it remains that the DoD has done a poor job effectively integrating warfighting in the space domain. In the 17 years of its existence as a functional command USSPACECOM made little progress in its UCP assigned missions and therefore was an easy target for the Secretary of Defense to find efficiencies with respect to COCOMs. The years following produced more of the same result and prompted calls for change from congress. Congressman Wayne Allard outlined in a memo to Secretary of Defense Rumsfeld his frustration with DoD efforts in the space domain. Allard explained that "[d]espite this national security imperative [of warfighting in the space domain], it appears that the DoD has not been devoting sufficient attention to enhancing and defending our nation's space dominance. In fact, several recent management and organizational changes suggest that this trend is accelerating, much to the detriment of our nation's security."[39] Allard's frustration stemmed from the organizational decision to create a FCC for a place where warfighting functions occur.

Congress is still unhappy with the DoD efforts to further warfighting in the space domain and continues to press the DoD for change. Congressman Mike Rogers and Jim Cooper, both members of the House Armed Services Committee (HASC) introduced a measure in the Fiscal Year 2018 (FY18) National Defense Authorization Act (NDAA) to build a separate military branch focused on space. The HASC bill, H.R. 2810 proposed to

> authorize the creation of a Space Corps within the Department of the Air Force and require the Secretary of the Air Force to certify its establishment by January 1, 2019. The Space Corps would be led by the Chief of Staff of the Space Corps and would be composed of such offices and officials determined appropriate by the Secretary of the Air Force, in consultation with the Chief of Staff of the Space Corps. This section would further provide that the Chief of Staff of the Space Corps would be appointed for a term

[39] Space Daily, "Senator Opposes Pentagon Plan to Downgrade Space Command," Phys.org - News and Articles on Science and Technology, March 10, 2006, 1, accessed January 19, 2018, https://phys.org/news/2006-03-senator-opposes-pentagon-downgrade-space.html.

> of 6 years, be a member of the Joint Chiefs of Staff, and would report directly to the Secretary of the Air Force, as a co-equal of the Chief of Staff of the Air Force.[40]

The HASC is asking the DoD to recognize in organization what senior leaders in the Air Force and even the President say about space as a warfighting domain. The original approach to space as a FCC did not meet mission objectives because the DoD attempted to treat a warfighting domain as a function. Creating a space force is the logical DoD organizational application based on other warfighting domains. In recent speech, President Trump said his "new national strategy for space recognizes that space is a war-fighting domain, just like the land, air, and sea," and the United States "may even have a 'Space Force.' We have the Air Force; we'll have the Space Force."[41] Creating commands for functional execution does not allow GCC commanders to adequately command and control operations in the multi-domain joint environment where the DoD fights.

[40] FY18 National Defense Authorization Bill, HR 2810 (Draft), Subcommittee on Strategic Forces, 115th Cong. (June 22, 2017) HASC bill H.R. 2810, http://docs.house.gov/meetings/AS/AS29/20170622/106134/BILLS-115HR2810ih.pdf.

[41] Loren Grush, "Trump's "Space Force" Sounds a Lot like the Space Corps His Administration Didn't Want," The Verge, March 13, 2018, accessed March 29, 2018, https://www.theverge.com/2018/3/13/17117224/trump-space-force-air-force-corps-us-military.

COUNTERING THE USSOCOM APPROACH

"SOF and cyber forces differ in their core essences. Not only that but their essences are differentially unitary. These differences suggest something other than perfect correspondence in the analogy between SOF and cyber forces and indicate that alternative approaches to some of the contemporary challenges may be appropriate."

-Christopher Paul, Isaac R. Porche III, Elliot Axelband

The Other Quiet Professionals Lessons for Future Cyber Forces from the Evolution of Special Forces

The current solution to this challenge is to create a "service-like" COCOM for cyberspace operations in the same way structure used for USSOCOM. Table 2 compares the organization, training, and equipping authorities for USCYBERCOM and USSOCOM.

Table 2: USSOCOM vs USCYBERCOM Authorities

USSOCOM	USCYBERCOM
(2) Subject to the authority, direction, and control of the Assistant Secretary of Defense for Special Operations and Low Intensity Conflict, the commander of such command shall be responsible for, and shall have the authority to conduct, the following functions relating to special operations activities (whether or not relating to the special operations command): (A) Developing strategy, doctrine, and tactics. (B) Preparing and submitting to the Secretary of Defense program recommendations and budget proposals for special operations forces and for other forces assigned to the special operations command. (C) Exercising authority, direction, and control over the expenditure of funds— (i) for forces assigned to the special operations command; and (ii) for special operations forces assigned to unified combatant commands other than the special operations command, with respect to all matters covered by paragraph (4) and, with respect to a matter not covered by paragraph (4), to the extent directed by the Secretary of Defense. (D) Training assigned forces. (E) Conducting specialized courses of instruction for commissioned and noncommissioned officers. (F) Validating requirements. (G) Establishing priorities for requirements. (H) Ensuring the interoperability of equipment and forces. (I) Formulating and submitting requirements for intelligence support. (J) Monitoring the promotions of special operations forces and coordinating with the military departments regarding the assignment, retention, training, professional military education, and special and incentive pays of special operations forces.	(2)(A) Subject to the authority, direction, and control of the Principal Cyber Advisor, the commander of such command shall be responsible for, and shall have the authority to conduct, the following functions relating to cyber operations activities (whether or not relating to the cyber command): (i) Developing strategy, doctrine, and tactics. (ii) Preparing and submitting to the Secretary of Defense program recommendations and budget proposals for cyber operations forces and for other forces assigned to the cyber command. (iii) Exercising authority, direction, and control over the expenditure of funds— (I) for forces assigned directly to the cyber command; and (II) for cyber operations forces assigned to unified combatant commands other than the cyber command, with respect to all matters covered by section 807 of the National Defense Authorization Act for Fiscal Year 2016 (Public Law 114–92; 129 Stat. 886; 10 U.S.C. 2224 note) and, with respect to a matter not covered by such section, to the extent directed by the Secretary of Defense. (iv) Training and certification of assigned joint forces. (v) Conducting specialized courses of instruction for commissioned and noncommissioned officers. (vi) Validating requirements. (vii) Establishing priorities for requirements. (viii) Ensuring the interoperability of equipment and forces. (ix) Formulating and submitting requirements for intelligence support. (x) Monitoring the promotion of cyber operation forces and coordinating with the military departments regarding the assignment, retention, training, professional military education, and special and incentive pays of cyber operation forces.

Source: Armed Forces, 10 U.S.C § 167 and 167b

The authorities granted to USCYBERCOM are nearly identical to the authorities that USSOCOM has in the execution of its duties. There is, however, one fundamental difference

worth noting. Where special operations are a listing or group of activities, cyberspace is not. Section 167 of Title 10 USC defines Special Operations activities as:

> (1) Direct action; (2) Strategic reconnaissance; (3) Unconventional warfare; (4) Foreign internal defense; (5) Civil affairs; (6) Military information support operations; (7) Counterterrorism; (8) Humanitarian assistance; (9) Theater search and rescue; (10) Such other activities as may be specified by the President or the Secretary of Defense.[42]

Cyberspace differs from special operations in that it is a place where these activities and others occur. There is a clear distinction here. Cyberspace it is not a set of activities. USCYBERCOM is a command with the responsibility to prescribe training for operations in cyberspace but does not move beyond that. It fails to acknowledge cyberspace as a domain, instead attempting to treat it as a function. It makes sense for USSOCOM to conduct specialized training in those areas listed as special operations activities since they build upon the foundational skills drawn from conventional forces. In contrast though, listing activities associated with cyberspace would not only be self-limiting, but futile as the domain demands all warfare activities (i.e., not just special reconnaissance or reconnaissance, but both).

Nevertheless, under this approach, it will be USCYBERCOM's responsibility to dictate the training and certification for assigned cyber forces that belong to another service. This model works for USSOCOM because there is a finite list of activities that fall into the special operations category. USSOCOM does very well at setting the training requirements for specific actions and builds upon the entry-level training from each of the services. That process, however, does not translate to a domain by the very nature of special operations. Special operations skills rely on foundational knowledge from existing services as a foundation. USSOCOM then identifies the knowledge skills and abilities to conduct the 10 statutorily defined special operations activities. There may be a requirement for special operations in

[42] Armed Forces, 10 U.S.C § 167 (2018), http://uscode.house.gov/browse/prelim@title10&edition=prelim.

cyberspace in the future, but first a baseline for general purpose cyberspace forces needs attention before going down that path. Cyberspace is not special operations. According to the DoD, it is a domain and as such warrants creating, at a minimum, a branch of service within a military department, not simply a combatant command.

Additionally, the population of cyberspace forces relative to special operations forces suggests problems applying this model. Special operations personnel assigned to USSOCOM upon receiving their Special Operations Force (SOF) designation usually do not return to the general-purpose force based on authorities in table 2. The number of SOF positions relative to conventional authorizations allows the services to manage this loan of personnel. According to a 2015 Government Accountability Office report, SOF authorizations totaled "approximately 62,800 in fiscal year 2014."[43] Cyber personnel assigned to USSCYBERCOM and subject to career management outside the service process total much greater numbers and therefore likely not as tolerable for the services as special operations forces. The Cyber Mission Force (CMF), USCYBERCOM's effort to resource teams in cyberspace, constitutes more than 6100 personnel from across the services, but that does not include the total cyber workforce.[44] The cyber workforce includes operations and maintenance personnel, totaling more than 135,000 at last count, which could be subject to USCYBERCOM's influence in the management of personnel under authorities listed in Table 2.[45] Furthermore, those forces are critical to each service in the

[43] United States. Government Accountability Office, *"Special Operations Forces: Opportunities Exist to Improve Transparency of Funding and Assess Potential to Lessen Some Deployments,"* (Washington, DC: United States Government Accountability Office, 2015), https://www.gao.gov/assets/680/671462.pdf.
[44] Jim Garamone, "Cyber Command Deputy Details Formation of Cyber Mission Force," U.S. DEPARTMENT OF DEFENSE, June 22, 2016, 1, accessed February 22, 2018, https://www.defense.gov/News/Article/Article/809904/cyber-command-deputy-details-formation-of-cyber-mission-force/.
[45] "*Cyber Operations Personnel Report*," (Washington, DC: Department of Defense, 2012), http://www.nsci-va.org/CyberReferenceLib/2011-04-Cyber%20Ops%20Personnel.pdf.

conduct of its assigned missions. Career management is not the only opportunity cost facing the services under the current construct, they also face decisions about capability development.

USSOCOM by most accounts sets the example for fielding new capabilities because its rapid acquisition process consists of the Special Operations Forces Capabilities Integration and Development System-Urgent (SOFCIDS-U). SOFCIDS is essentially a replica of the Joint and Service capability development systems. But the reason that SOFCIDS works for special operations is that it has the "authority for the development and acquisition of Special Operations (SO)-peculiar equipment."[46] SO-peculiar equipment is an important distinction because JP 1-02 defines it as "equipment, material, supplies, and services required for special operations missions for which there is no Service-common requirement."[47] Another author describes this difference, stating "USSOCOM depends upon the DOD military services to provide the platforms, such as helicopters, aircraft, armored vehicles, and watercraft, while SOF AT&L acquires unique systems to modify those platforms for SOF missions."[48] GAO report 07-620 provides the following as an example of USSOCOM modifying a service specific platform:

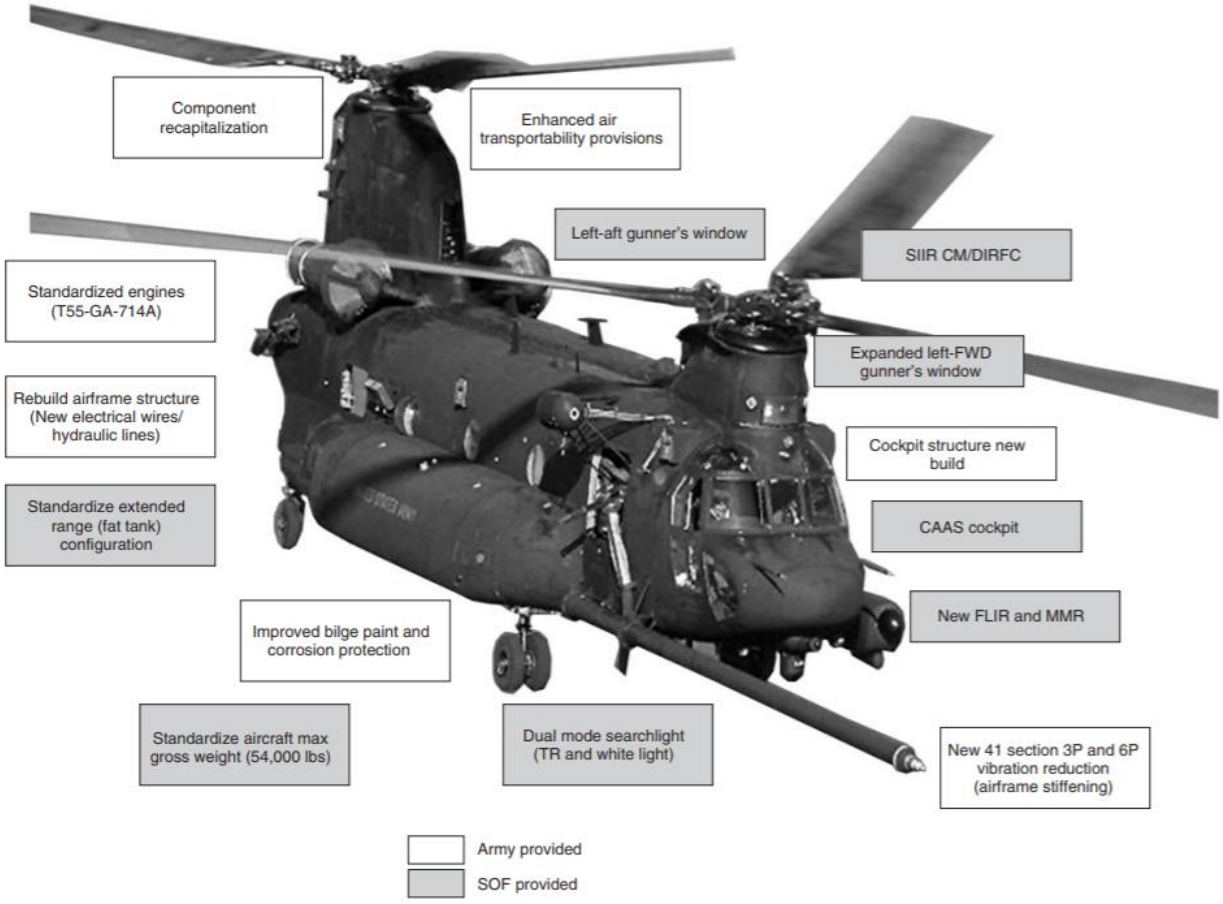
> SOCOM has … a program underway, estimated to cost about $200 million, which modifies the Army's service-common CH-47 helicopter to meet its SOF-peculiar requirements. Several features on the aircraft are SOCOM-peculiar such as the long aerial refueling probe on the front of the aircraft, the standardized extended range fuel tank, and the common aviation architecture systems cockpit. The CH-47 helicopter, when modified by SOCOM, becomes a MH-47G helicopter that provides SOCOM with a heavy assault helicopter with the latest avionics, sensors, aircraft survivability features, and weapons systems.[49]

---

[46] Armed Forces, 10 U.S.C § 167 (2018), http://uscode.house.gov/browse/prelim@title10&edition=prelim.
[47] Joint Staff, *Department of Defense Dictionary of Military and Associated Terms,* JP 1-02, (Washington, DC: Joint Staff, February 2018), http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf?ver=2018-02-21-153603-643, 215.
[48] Lt Col Christian G. Elenbaum, "Organizational Design for USSOCOM Rapid Acquisition," Master's thesis, Joint Advanced Warfighting School, 2017, 2, Defense Technical Information Center, http://www.dtic.mil/dtic/tr/fulltext/u2/1032272.pdf.
[49] United States. Government Accountability Office. *Defense Acquisitions: An Analysis of the Special Operations Command's Management of Weapon System Programs: Report to the Subcommittee on Emerging Threats and Capabilities, Committee on Armed Services, U.S. Senate*. (Washington, D.C.: U.S. Govt. Accountability Office, 2007), https://www.gao.gov/assets/270/262964.pdf.

Figure 5 illustrates the elements that SOCOM adds to the Army platform that are special operations unique. Without a service or branch dedicated to developing baseline platforms in cyberspace then adding "service like" authority to USCYBERCOM does not produce an advantage for capability development in cyberspace. Modeling USCYBERCOM after USSOCOM will likely result in cyberspace development that predicates on the existing service's cyberspace capabilities, which naturally would be subordinate to their statutory requirements for their respective domains of warfare producing suboptimal results for cyberspace.

Figure 5: Army CH-47 Helicopter to SOCOM MH-47 Helicopter



Source: Provided by USSOCOM for United States Government Accountability Office. *Defense Acquisitions: An Analysis of the Special Operations Command's Management of Weapon System Programs: Report to the Subcommittee on Emerging Threats and Capabilities, Committee on Armed Services, U.S. Senate*. (Washington, D.C.: U.S. Govt. Accountability Office, 2007), https://www.gao.gov/assets/270/262964.pdf.

As General Alexander stood up USCYBERCOM he envisioned an approach similar to USSOCOM. He later commented that

> In 2007, we laid out in a document, what's the right thing to do evolve Cyber Command. We looked at a sub-unified, a unified, a functional command and a separate service. It was my opinion that we go to a unified-functional, similar to SOCOM [US Special Operations Command]. I was not in synch on taking it to a separate service for a couple of reasons. First, I thought that the forces needed to be embedded in tactical configurations, and if they needed to do that, the services should be involved. So the second part is this is a new area, there is no need to jump. Let's take a step to the unified and functional, see how it is.[50]

If USCYBERCOM is to be an evolutionary command then it would be wise to learn from the perils of USSPACECOM early to skip the frustration that comes along with creating a FCC around a domain.

[50] Joe Gould, "Former NSA Chief: Follow SOCOM Model for Cyber," Defense News, August 08, 2017, accessed March 29, 2018, https://www.defensenews.com/opinion/intercepts/2015/04/17/former-nsa-chief-follow-socom-model-for-cyber/.

CONCLUSION

I would argue that it is also time to strongly consider whether or not we want to create a dedicated cyber force. It is time we at least began a conversation about a US Cyber Force. The idea will be vehemently opposed by the services, just as the Army and Navy fought the idea of an Air Force. But sooner or later, common sense tells us we will end up with a specialized force in this zone of combat.

-Admiral James Stavridis, USN (Ret)
Testimony Before Senate Armed Services Committee Cyber Security, 22 May 2017

Current organization for cyberspace is limiting the DoD's warfighting potential. First, there is no singular organization responsible for domain cognizance in cyberspace. Cyberspace, like other recognized domains of warfare, is unique and as such requires a single entity to determine the correct organization, training, and equipping necessary to move, maneuver, and project power in cyberspace. Furthermore, capability development in cyberspace requires expertise, speed, and agility; none of which COCOMs exhibit in developing capability for warfighting domains. Despite the DoD's claim to treat cyberspace as an operational domain, the current organization applies a function model to a warfighting domain and hinders its ability to effectively integrate cyberspace operations and project power in the manner currently afforded in other domains. USCYBERCOM is destined to repeat the same errors of USSPACECOM and likely arrive at the same conclusion for cyberspace that those in congress are now demanding for the space domain- the establishment of a service dedicated to cyberspace. The USSOCOM model approach to cyberspace does not adequately address the differences between warfighting in cyberspace and special operations.

Bibliography

Air University. n.d. "Air University Space Reference Guide 18-1." *AU Space Reference Guide.* Accessed January 19, 2018. http://www.au.af.mil/au/awc/awcgate/srg/au-srg.htm.

Cardon, Ed. 2016. *Maturing Cyber Capabilities Critical to Army Future.* September 21. Accessed March 29, 2018. https://www.army.mil/article/175465/maturing_cyber_capabilities_critical_to_army_future.

Clayton, Mark. 2010. *Stuxnet Malware Is 'Weapon' Out to Destroy . . . Iran's Bushehr Nuclear Plant?* September 21. Accessed March 29, 2018. https://www.csmonitor.com/USA/2010/0921/Stuxnet-malware-is-weapon-out-to-destroy-Iran-s-Bushehr-nuclear-plant.

Department of Defense. 2018. *About Unified Combatant Commands.* January 19. Accessed Janaury 19, 2018. https://www.defense.gov/About/Military-Departments/Unified-Combatant-Commands/.

Department of Defense. 2012. *Cyber Operations Personnel Report.* Personnel Report, Washington, D.C.: Department of Defense. http://www.nsci-va.org/CyberReferenceLib/2011-04-Cyber%20Ops%20Personnel.pdf.

—. 2011. "Department of Defense Strategy for Operating in Cyberspace." *Strategy for Cyberspace* . Washington, D.C.: Department of Defense, July 5. https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf.

Elenbaum, Christian G. 2017. *Organizational Design for USSOCOM Rapid Acquisition.* Master's thesis, Joint Advanced Warfighting School, Defense Technical Information Center. http://www.dtic.mil/dtic/tr/fulltext/u2/1032272.pdf.

Garamone, Jim. 2016. "Cyber Command Deputy Details Formation of Cyber Mission Force." *U.S. DEPARTMENT OF DEFENSE.* June 22. Accessed February 22, 2018. https://www.defense.gov/News/Article/Article/809904/cyber-command-deputy-details-formation-of-cyber-mission-force/.

Gould, Joe. 2017. "Former NSA Chief: Follow SOCOM Model for Cyber." *Defense News.* August 8. Accessed March 29, 2018. https://www.defensenews.com/opinion/intercepts/2015/04/17/former-nsa-chief-follow-socom-model-for-cyber/.

Government Accountability Office. 2007. *Defense Acquisitions: An Analysis of the Special Operations Command's Management of Weapon System Programs: Report to the Subcommittee on Emerging Threats and Capabilities, Committee on Armed Services, U.S. Senate.* Washington, D.C.: Government Accountability Office. https://www.gao.gov/assets/270/262964.pdf.

Government Accountability Office. 2008. *Defense Acquisitions: DOD's Requirements Determination Process Has Not Been Effective in Prioritizing Joint Capabilities.* Audit, Washington, D.C.: Government Accountability Office. https://www.gao.gov/products/GAO-08-1060.

Government Accountability Office. 2015. *Special Operations Forces: Opportunities Exist to Improve Transparency of Funding and Assess Potential to Lessen Some Deployments.* Audit, Washington, D.C.: Government Accountability Office.

Grissom, Adam, Caitlin Lee, and Karl Mueller. 2016. *Innovation in the United States Air Force: Evidence from Six Cases.* Research, San Antonio, TX: RAND Corporation.

Grush, Loren. 2018. "Trump's "Space Force" Sounds a Lot like the Space Corps His Administration Didn't Want." *The Verge.* March 13. Accessed March 29, 2018. https://www.theverge.com/2018/3/13/17117224/trump-space-force-air-force-corps-us-military.

Headquarters United States Air Force. 1951. "UNITED STATES AIR FORCE STATISTICAL DIGEST JAN 1949-JUN 1950: FIFTH EDITION." Statistical Digest, Air Force Operations Statistics Division, Washington, D.C. Accessed March 29, 2018. https://media.defense.gov/2011/Apr/05/2001329940.

Headquarters United States Navy. 2010. "Naval Aviation Vision. Washington, D.C.: U.S. Navy, Naval Aviation Enterprise, ." *Naval Aviation Enterprise.* January 1. Accessed March 29, 2018. http://www.public.navy.mil/airfor/Documents/Vision%20Document.pdf.

ICANN. 2011. "Available Pool of Unallocated IPv4 Internet Addresses Now Completely Emptied." *icann.com.* February 3. Accessed January 19, 2018. https://www.icann.org/en/system/files/press-materials/release-03feb11-en.pdf.

Intel. 2017. *A Guide to the Internet of Things Infographic," Intel, 1, accessed January 19, 2018, .* December 15. Accessed January 19, 2018. https://www.intel.com/content/www/us/en/internet-of-things/infographics/guide-to-iot.html.

Johnson, Stephen B. 2002. *The United States Air Force and the Culture of Innovation: 1945-1965.* Washington, D.C: Air Force History and Museums Program.

Joint Staff. 2013. *Cyberspace Operations, JP 3-12.* Washington, DC: Joint Staff. http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12R.pdf.

—. 2018. *Department of Defense Dictionary of Military and Associated Terms, JP 1-02.* Washington, D.C.: Joint Staff. http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf?ver=2018-02-21-153603-643, 215.

—. 2017. *Joint Operations, JP 3-0.* Washington, D.C.: Joint Staff. http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_0_20170117.pdf.

Lipmanowicz , Henri, and Keith McCandless. 2016. *The Surprising Power of Liberating Structures: Simple Rules to Unleash a Culture of Innovation.* Seattle, WA: Liberating Structures Press.

Lynn, William J. 2010. "Remarks at USSTRATCOM Cyber Symposium United States Department of Defense." *United States Department of Defense.* May 26. Accessed January 19, 2018. http://archive.defense.gov/speeches/speech.aspx?speechid=1477.

Neufeld, Jacob , George M. Watson, and David Chenowe. 1997. *Technology and the Air Force: A Retrospective Assessment.* Washington, D.C.: Air Force History and Museums Program.

Pomerleau, Mark. 2017. *Here's How Cyber Service Component Mission Sets Differ from CYBERCOM.* July 17. Accessed March 29, 2018. https://www.c4isrnet.com/cyber/2017/07/27/heres-how-cyber-service-components-cybercom-mission-sets-differ/.

Rogers, Michael. 2015. *Beyond the Build Delivering Outcomes through Cyberspace: The Commander's Vision and Guidance for US Cyber Command.* Commander's Vision, Ft. Meade, MD: United States Cyberspace Command.

Space Daily. 2006. "Senator Opposes Pentagon Plan to Downgrade Space Command ." *Phys.org - News and Articles on Science and Technology.* March 10. Accessed January 19, 2018. https://phys.org/news/2006-03-senator-opposes-pentagon-downgrade-space.html.

Stavridis, James, and David Weinstein. 2014. "Time for a U.S. Cyber Force." *Proceedings* (United States Naval Institute) 140 (1): 40-45.

Story, William C. 1999. *Military Changes to the Unified Command Plan: Background and Issues for Congress* . Report for Congress RL30245, Washington, D.C.: Congressional Research Service.

Truman, Harry S. 1947. "Executive Order 9877—Functions of the Armed Forces July 26, 1947." *The American Presidency Project Online by Gerhard Peters and John T. Woolley.* July 26. Accessed January 19, 2018. http://www.presidency.ucsb.edu/ws/?pid=12717.

Trump, Donald. 2017. "Presidential Memorandum for the Secretary of Defense." *Presidential Memorandum.* Washington, D.C.: The White House, August 18.