REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
27-04-2015	Master of Military Studies Research Paper	September 2014 - April 2015

4. TITLE AND SUBTITLE

USCYBERCOM's LACK OF COCOM AUTHORITY: EXAMINING COMMAND AUTHORITY AND C2 STRUCTURE WITHIN THE DODIN

5a. CONTRACT NUMBER
N/A

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
N/A

6. AUTHOR(S)

Phillips Atiim O., Major, USMC

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)

N/A

10. SPONSOR/MONITOR'S ACRONYM(S)
N/A

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

12. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES

N/A

14. ABSTRACT

Upon establishing USCYBERCOM, the Secretary of Defense and senior military leaders violated the doctrinal tenets of establishing a joint force command and command and control (C2). CDRUSCYBERCOM, as a joint force commander, was not delegated or assigned any combatant command (COCOM) authorities over the federal agencies and Services which own portions of the DODIN. The Defense Information Systems Agency (DISA) owns and operates the DODIN's backbone while the Service Chiefs own their respective portions of the network which is extended from garrison to the tactical environment through DISA in support of the geographic combatant commands (GCC). USCYBERCOM needs to be elevated to a full unified combatant command (CCMD) with specific COCOM authorities. Title 10 must be amended providing CDRUSCYBERCOM with the overall authority, direction, and control over DoD cyberspace operations along with acquisition authorities similar to US Special Operations Command. That commander should have a direct relationship with the DoD Chief Information Officer (CIO) and provide dedicated support in exercising the DoD CIO's Title 40 and 44 authorities for information technology acquisition and information resource management. Lastly, DISA should no longer report directly to the DoD CIO and be under CDRUSCYBERCOM's COCOM authority.

15. SUBJECT TERMS

USCYBERCOM, DISA, C2, command authority, DODIN, cyber, cyberspace operations, DoD CIO

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			Marine Corps University/Command a
Unclass	Unclass	Unclass	UU	32	**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:
USCYBERCOM'S LACK OF COCOM AUTHORITY: EXAMINING COMMAND AUTHORITY AND C2 STRUCTURE WITHIN THE DODIN

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

AUTHOR:
MAJOR ATIIM O. PHILLIPS, USMC

AY 14-15

Mentor and Oral Defense Committee Member: _____ 4/16/15
Approved: M. Flynn
Date: _____

Oral Defense Committee Member: J.W. Gordon
Approved: _____
Date: 4/14/15

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.

Preface

I had the pleasure of working at the Defense Information Systems Agency (DISA) from 2004 to 2007 as an Internet Protocol (IP) Engineer/ Project Manager on the classified and unclassified networks. During that time, I worked on multiple projects and working groups which gave me an unparalleled understanding of IP technologies, the immense scope of the Department of Defense (DoD) as a global service provider, the strategy and policy innerworkings between the DoD Chief Information Office (CIO), federal agencies, and the Services, and the authorities of the then-Commanding General, Joint Task Force-Global Network Operations. I chose this topic of command authorities to address with my MMS because I believed that there was a significant issue with DISA's implementation of the Joint Information Environment standards in concert with United States Cyber Command. That thought process grew into the following study which seeks to understand the command authorities and control processes within the DoD Information Network.

I would like to thank the following individuals in chronological order. First, my wife, Joy, and kids, Kweli and Amira, for continuing to love me while sacrificing weekends and holiday breaks as I pushed for another masters degree. Second, Mr. Bruce Bennett and Mrs. Kathryn Sonderegger, my bosses at DISA, for sending me to every training opportunity I asked for and assigning me to those projects. The technologies I learned almost ten years ago are still groundbreaking today. Last, a special thanks to LtCols Kevin Glathar and Haakon Waroe and Drs. Lynn Tesser, Richard DiNardo, and Matthew Flynn for showing me that there is a necessity for the academic study of history to go along with my passion for cyberspace operations.

Executive Summary

Title: USCYBERCOM's Lack of COCOM Authority: Examining Command Authority and C2 Structure within the DODIN

Author: Major Atiim O. Phillips, United States Marine Corps

Thesis: The requirement to elevate USCYBERCOM to a unified combatant command with the requisite command authorities and a new C2 structure are necessary to properly operate and defend the DODIN.

Discussion: Within the past 15 years, the DoD has made strides to define and adequately operate in cyberspace. Currently, Commander, United States (US) Strategic Command (CDRUSSTRATCOM) has retained the responsibility of the DoD's cyberspace mission in accordance with the Unified Command Plan. In 2009, CDRUSSTRATCOM consolidated three sub-component commands and established US Cyber Command (USCYBERCOM) to demonstrate unity of command and effort within the DoD's portion of cyberspace. CDRUSCYBERCOM, as a sub-unified combatant command reporting to CDRUSSTRATCOM, was assigned the epic mission to operate and defend the DoD information network (DODIN) and when directed, conduct full spectrum military cyberspace operations.

Upon establishing USCYBERCOM, the Secretary of Defense and senior military leaders violated the doctrinal tenets of establishing a joint force command and command and control (C2). CDRUSCYBERCOM, as a joint force commander, was not delegated or assigned any combatant command (COCOM) authorities over the federal agencies and Services which own portions of the DODIN. CDRUSCYBERCOM has coordination and synchronization responsibilities within a global network which supports the geographic combatant commanders (CCDRs) and is owned by the Service Chiefs via their Title 10, US Code (Title 10) authorities and the Defense Information Systems Agency (DISA) via the DoD Chief Information Officer's (DoD CIO) Title 40 and 44, USC (Title 40 and 44) authorities. As of early 2015, USCYBERCOM has made strides to focus on its assigned mission areas by standing up three subordinate joint force headquarters to support defending the nation, supporting geographic combatant commands (GCC), and securing, operating, and defending the DODIN.

This paper asserts that CDRUSCYBERCOM does not possess the necessary command authorities over the DODIN. DISA owns and operates the DODIN's backbone while the Service Chiefs own their respective portions of the network which is extended from garrison to the tactical environment through DISA in support of the GCCs.

Conclusion: USCYBERCOM needs to be elevated to a full unified CCMD with specific COCOM authorities. Title 10 must be amended providing CDRUSCYBERCOM with the overall authority, direction, and control over DoD cyberspace operations along with acquisition authorities similar to US Special Operations Command. That commander should have a direct relationship with the DoD Chief Information Officer (CIO) and provide dedicated support in exercising the DoD CIO's Title 40 and 44 authorities for information technology acquisition and

information resource management. Lastly, DISA should no longer report directly to the DoD CIO and be under CDRUSCYBERCOM's COCOM authority.

Table of Contents

INTRODUCTION

Since 1998, the Department of Defense (DoD) has played "hot potato" with assigning missions and responsibilities with regard to cyberspace planning and operations. Within the past 15 years, the DoD has made strides to define and adequately operate in cyberspace. United States (US) Space Command (USSPACECOM) was first assigned the mission to protect DoD networks in 1998.[1] United States Strategic Command (USSTRATCOM) assumed the cyberspace mission as part of its merger with USSPACECOM in 2002.[2] While USSTRATCOM has retained responsibility of the DoD's cyberspace mission, that unified combatant command (CCMD) has also created three different sub-component commands (two joint task forces and a joint force component command) enroute to the creation of United States Cyber Command (USCYBERCOM). USCYBERCOM's activation in 2009 was supposed to be an opportunity to demonstrate unity of command and effort within the DoD's portion of cyberspace while offloading USSTRATCOM's responsibility to synchronize planning of cyberspace operations. USCYBERCOM's establishment was found to be more of a consolidation effort within USSTRATCOM.

USCYBERCOM has the epic mission of operating and defending the DoD information network (DODIN) and when directed, conducting full spectrum military cyberspace operations.[3] More clearly, USCYBERCOM must operate, defend, and conduct offensive operations in support of the DODIN. The commander of USCYBERCOM (CDRUSCYBERCOM) only has the organic forces of USCYBERCOM's headquarters staff and the National Security Agency/ Central Security Service (NSA) to accomplish this three-part mission. The Defense Information Systems Agency (DISA) plays a vital role in DoD cyberspace operations, but are outside of USCYBERCOM's command and control (C2) structure.

Most warfighters are more interested in the DoD's offensive versus defensive cyberspace capabilities and the requisite authorities required to conduct a cyber attack. However, the unclassified and classified networks remain indefensible due to a host of reasons. To start, CDRUSCYBERCOM does not have the needed command authority to execute the mission. Additionally, CDRUSCYBERCOM does not have an adequate C2 structure to conduct the mission. This paper recommends elevating USCYBERCOM to a unified CCMD with the requisite command authorities and an updated C2 structure necessary to properly operate and defend the DODIN. This paper will analyze the history of the DoD's cyberspace authorities and C2 structure from past to present. Then, it will identify issues that reside from USCYBERCOM's current initiatives. Lastly, it proposes a set of combatant command (COCOM) authorities and an updated C2 structure that will enable USCYBERCOM to properly operate and defend the DODIN.

LITEARATURE REVIEW

This study rests on key literature discussing USCYBERCOM's creation from three subordinate organizations within USSTRATCOM to the most current cyber C2 framework. Specifically, sources include documents from USSTRATCOM's history, key leader Congressional testimonies and hearings, joint publications, published and unpublished papers, and the operating procedures of Joint Task Force-Global Network Operations and Joint Force Headquarters-DODIN (JFHQ-DODIN). This key literature is the aggregate of the following data points: my experience working for the DISA from 2004-2007, USSTRATCOM's Joint Concept of Operations (CONOPS) for Global Information Grid (GIG) Network Operations (NetOps) from 2005, Secretary of Defense (SECDEF) memorandums, David Hollis' 2010 Joint Force Quarterly article, General (Gen) Alexander's Congressional testimony in 2014, the Chairman of

the Joint Chiefs of Staff's (CJCS) two execute orders (EXORD), and JFHQ-DODIN's operation and defense C2 framework.

The literature strings together a narrative that CDRUSCYBERCOM has put the command in position to plan, operate, and act strategically, operationally, and tactically. David Hollis is a well-respected author and has decades of experience within the Office of the Secretary of Defense as a civilian and within USSTRATCOM as an officer in the U.S. Army. Hollis asserted that USCYBERCOM would need approximately five years to develop into a full unified CCMD and that the DoD needed to proper face the current threat with immediate action; that time is now. Strategically, USCYBERCOM is institutionally ready to serve as a full unified combatant command which, per Gen Alexander, should take its orders directly from the president and SECDEF for the speed of decision-making in cyberspace operations. Operationally and tactically, USCYBERCOM has implemented an updated cyber C2 framework, per the CJCS EXORDs, which is an adaptation of the 2005 Joint CONOPS for GIG NetOps.

The new cyber C2 framework along with the CJCS EXORDs attempted to answer an overarching issue: command authorities. The modification to the first EXORD created a newly titled authority, directive authority for cyberspace operations (DACO), which was delegated from the SECDEF to CDRUSCYBERCOM through CDRUSSTRATCOM. In the JFHQ-DODIN operating procedure document, DACO was equated to the tactical control authority over the DOD's components, e.g. CCMDs, Services, and agencies. DACO exacerbates the problem within the DoD, wherein there is not a single command with authority over all cyberspace operations. The authorities for the DODIN operations and defense are spread between the Services and DISA.

Those few who disagree on elevating USCYBERCOM to a full unified CCMD to then achieve these authorities anchor their opposition in the division of cyberspace authorities, responsibilities, and funding. First, a SECDEF memorandum stated that a Cost Assessment and Program Evaluation memorandum reversed his tentative approval to transfer DoDIN operations and defense from the Assistant SECDEF for Networks Integration and Information and DISA to USCYBERCOM. Duly, the SECDEF also cancelled the option to transfer operational control of DISA to USCYBERCOM due to a number of significant policy, operational, and practical concerns.

Second, Hollis' article makes a short reference to the legislative authorities within cybersecurity e.g. Titles 10, 40, and 44 U.S. Code. Additionally, via interview, he related the power struggle amongst senior leaders regarding the cost, timing, funding, and control of the network. The current fiscal constraints being placed upon the DoD represent bad timing to ask Congress for additional resources to establish a new CCMD; however, cyber-related initiatives have received additional funding during the fiscal downturn. Additionally, USSTRATCOM seeks to maintain authority, responsibility, and control of USCYBERCOM because of the aforementioned additional funding. No CCMDs want to lose more money in this fiscally constrained environment. Furthermore, the geographic combatant commanders (CCDRs) seek to maintain authority and control of all warfighting assets within their region. Those CCDRs view USCYBERCOM as reducing their control over part of their warfighting platform. Finally, the Service Chiefs do not want USCYBERCOM to be elevated because it would put the ownership of their network in jeopardy. The combination of these points presents a collection of reasons USCYBERCOM is not a full unified CCMD.

Four interviews also support this analysis. The interviewees all speak to background information on opposition to USCYBERCOM elevation, Service versus geographic CCMD (GCC), and understanding the legacy versus current cyber C2 framework. Lieutenant Colonel (LtCol) Limbert was Regional Command (SouthWest) (RC(SW)) C-6 Operations Officer as part of the US deployment to Afghanistan in 2010-2011. He related U.S. Central Command's (USCENTCOM) request vice requirement that a sub-component command change from their service to the GCC's domain name. Although RC(SW) was under CDRUSCENTCOM's COCOM authority, they did not have authority over RC(SW)'s network; that authority resided with the Marine Corps under Title 10.

Todd Beckman has over ten years of experience working for DISA. Specifically, he has multiple years with DISA-Europe as the Technical Advisor for Enterprise Operations Center-Europe (EOC-EUR). EOC-EUR was the first operational EOC under the regional DODIN commands as part of the current cyber C2 framework. Additionally, Mr. Beckman had years of experience working with and operating under the previous cyber C2 framework. He related that under the JTF-GNO C2 construct customers/users would routinely be confused on whether directives were coming from DISA or JTF-GNO due to the dual-hat status and lack of true authority over the network.

Colonel Patricia Rinaldi is the current JFHQ-DODIN J5 and former Director, Joint Operations Center, USCYBERCOM. She provides the most recent knowledge and understanding of USCYBERCOM's authorities and new cyber C2 framework. She states that the SECDEF's creation and delegation of DACO authority is the first true authority which no entity has had in the past. However, the true issue is that DACO is not well-defined or

understood by all those it will encompass. She asserts that DACO may evolve into that all-encompassing authority in the future.

David Hollis is the Chief of Staff, USCYBERCOM National Capital Region. As mentioned, he has decades of experience within USSTRATCOM and USCYBERCOM as a civilian and as a Colonel in the US Army Reserve. He provided up-to-date insight on the differing opinions of senior military leaders who oppose the elevation of USCYBERCOM. Additionally, as a published author in multiple professional journals, he provided reference to articles in favor of elevating USCYBERCOM and giving it some specialized authorities.

Overall, the sources show that USCYBERCOM is prepared to be elevated to a full unified CCMD and the current cyber C2 framework is a step in the right direction. Unfortunately, the sources also show that the overarching problem, lack of a single authority over DoD cyberspace operations with proper command authorities, continues to exist. This paper seeks to call attention to that omission in the hopes of getting this key point addressed.

UNDERSTANDING C2 OF A GLOBAL NETWORK

Prior to delving into the history of the DoD's cyber C2 authorities, a solid understanding of C2 must be established. Additionally, one must understand what C2 of a global network entails. The term C2 is often misunderstood as a simple organizational or C2 diagram with solid and dotted lines. While never as authoritative as those lines suggested, there is order. In contrast, the DoD's definition and understanding of C2 within cyberspace has been a moving target and thus leads to the current problem of an adequate control process without the command authorities to execute C2 of a global network. In 2006, the National Military Strategy for Cyberspace Operations (NMS-CO) outlined six fundamental ways to achieve the strategic goal of military superiority in cyberspace: network operations, information operations, kinetic actions,

law enforcement and counterintelligence, and themes and messages.[4] The closest 'way' to better C2 was network operations (NetOps). Col Robert Barker, US Army, stated that NetOps "is the command and control structure for the forces, people, procedures, and equipment operating and defending the information networks and infrastructure that comprise cyberspace."[5] The joint definition of NetOps is "activities conducted to operate and defend the Global Information Grid."[6] From the beginning, C2 of the DODIN was not a clear method to achieve military superiority in cyberspace. Military C2 is understood and executed well within the air, land, and sea domains. The application of C2 within cyberspace operations, and specifically the DODIN, applies the same as the other warfighting domains. Military planners must remember that C2 is actually two separate terms, command and control, which make up a compound term. This confusion is troublesome since the C2 of a global network adds a unique level of difficulty on top of an already complex structure.

Joint doctrine states effective command and control of joint operations begins by establishing unity of command through the designation of a Joint Force Commander (JFC) with the requisite authority to accomplish assigned tasks using an uncomplicated chain of command.[7] This makes sense when establishing a joint force from nothing. The DODIN has grown from the Services' small, independent networks to the Defense Information Systems Agency's (DISA) backbone network interconnecting the combatant command (CCMD), Service, and DoD agencies' networks. Each institution had already created and upgraded their methods of network C2. The Secretary of Defense (SECDEF) was late to the game in 2004 by authorizing Joint Task Force-Global Network Operations (JTF-GNO), under USSTRATCOM, to direct the operation and defense of the DODIN.[8] Even today, C2 of the DoD's network continues to be reactive vice proactive to the threats and vulnerabilities within the information environment.

COMMAND

Technically, command is the less difficult of the two terms. The joint definition of command is "the authority that a commander in the armed forces lawfully exercises over subordinates by virtue of rank or assignment."[9] Restated, command means a military commander (CDR) with lawful authority over subordinates. A CDR receives that lawful authority from one of four authorities: the President of the United States (POTUS), SECDEF, Title 10, and/or delegated authority from a senior CDR. In practice, the powers of command authority are vested in a CDR by POTUS or SECDEF. Those powers and duties are codified in Title 10. The Unified Command Plan (UCP) does not bestow command authority. The UCP "assigns missions; planning, training, and operational responsibilities; and geographic areas of responsibilities to [CCMDs]."[10] The UCP establishes CCMDs, wherein CCDRs receive their command authority from Title 10. Specifically, for the purposes of this paper, command authority is directly vested in unified CCDRs and Service Chiefs. CCDRs and Service Chiefs are authorized to delegate command authority to subordinate commanders, but they always retain overall responsibility.[11] Command authority, as given in Title 10, is more than designating who is ultimately in charge. There are a host of additional authorities that can be expressly vested within command.

CCDRs and Service Chiefs are empowered with additional, necessary authorities in order to carry out their assigned mission and duties. Service Chiefs have the organic authorities to man, train, and equip their forces for assignment and support of the CCDRs. CCDRs have the organic authorities for joint training, logistics, and military operations within their assigned geographic or functional area.[12] Per Title 10, the SECDEF is required to submit an annual budget proposal for the CCMDs.[13] CDR, US Special Operations Command (USSOCOM) is the

only CCDR with additional authorities similar to a Service Chief. CDRUSSOCOM has the unique authorities for the "development and acquisition of special operations-peculiar equipment" and "authority, direction, and control over the expenditure of funds... for special operations forces assigned to unified combatant commands other than the special operations command...."[14] The amount of authorities vested within a CDR may start to resemble the duties or responsibilities of the command. It is extremely important for CDRs and their staff to understand the inherent command authorities under a CCDR or Service Chief. Command authorities frame how much authority a CDR has over subordinate commands, responsibilities to senior CDRs, and how much organic resources they can control.

CONTROL

The joint definition of control can be misleading. Control is defined as the "authority that may be less than full command exercised by a commander over part of the activities of subordinate or other organizations."[15] Full command should be interpreted as COCOM which is bestowed in Title 10 and cannot be delegated or transferred.[16] Authorities less than COCOM should be interpreted as levels of authority or command relationships which are operational (OPCON), tactical (TACON), and administrative control (ADCON).[17] Control should not be analogous with command relationships. Command relationships is the "interrelated responsibilities between commanders, as well as the operational authority exercised by commanders in the chain of command."[18] Based on these definitions, control is subset of command authority. This is not only confusing but incorrect.

Control should be defined about the 'exercised by a commander' portion of the joint definition. Control is *how* a CDR uses assigned or attached forces to accomplish the mission. From a CCDR's perspective, the assigned forces are usually the headquarters element consisting

of the staff directorates and service component commands. Depending upon the responsibilities or command authority of the CCDR, the number of subordinate commands may increase in order to accomplish the full set of duties assigned. A CCDR exerts command authority by organizing his forces in a desired manner and delegating appropriate authorities to subordinate CDRs. Control occurs by those staff members and subordinate CDRs executing CCDR's intent, providing timely information for decision-making, and executing those decisions to accomplish the mission. Control is more of a supporting function of command.

COMMAND AND CONTROL (C2)

Based on the separate understanding of the terms command and control, the combined meaning of C2 makes sense. However, once again, this concept breaks down when considering with the joint definition of C2: "the exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission."[19] The definition is purely one sided and does not properly account for the disparate supporting functions conducted by subordinate CDRs and staff members. The all-inclusive definition of C2 should be: the exercise of authority and direction by a properly designated commander over assigned and attached forces via subordinate commanders and staff personnel to aid in decision-making and mission accomplishment. This definition affords an understanding of C2 as more than a diagram relating command relationships over subordinate commands. C2 is the business of CDRs. C2 is an iterative process which supports the CDR's decision-making process and the execution of assigned duties. Therefore, C2 requires consistent feedback between CDRs and subordinate forces.[20] The information contained in that feedback requires a C2 support structure or a C2 system to enhance the timeliness of decision-making. This understanding of C2 does not change with the advent of cyberspace. One must apply this level of understanding of C2 in order

to create a cyberspace C2 framework. If an information network is a support structure within the C2 process, is it possible to C2 a network?

KEY STAKEHOLDERS IN C2 OF A GLOBAL NETWORK

The DODIN is the DoD's portion of cyberspace. The term DODIN has changed over time, but the central understanding of its purpose has not. The DODIN was the Defense Information Systems Network (DISN) in the 1980s thru 2000. The DISN migrated to become the Global Information Grid (GIG) in early 2000 as part of a major bandwidth expansion project (GIG-BE) which introduced high speed optical transport as the backbone of the network. When USCYBERCOM activated in 2009, the term DODIN was introduced as part of defining cyberspace and the DoD's responsibilities within. The DODIN is the DoD's global network supporting the POTUS, SECDEF, CCDRs, Service Chiefs, and DoD agencies' C2. Therefore, the DODIN both serves as the C2 support structure for our senior national and military leaders and requires its own C2 framework as a global network.

The duality of the DODIN, as a C2 support structure supporting national and military CDR's C2 and requiring its own C2 framework, may be confusing but harkens back to the duality of operational versus administrative computers during the 1960s. In 1965, Representative Jack Brooks from Texas initiated the creation of the Brooks Act which mandated the purchase of federal, administrative computers and software through the General Services Administration with the exception of operational computers belonging to the Central Intelligence Agency and DoD intelligence, cryptography, and military C2.[21] In 1984, President Reagan's National Security Decision Directive (NSDD)- 145 abolished the difference between administrative and operational computing and telecommunications.[22] Therefore, the duality of the DODIN, as both an operational and administrative network, has stood the test of time.

Since C2 is the business of CDRs and the DODIN is a global network that supports all CDRs within the DoD, there must be a CCDR who is assigned the responsibility of this network. This is where the first tenet of C2, clearly defined authorities, roles, and relationships, is violated.[23] There are multiple commands that are major stakeholders within the DODIN.

The Office of the SECDEF (OSD) has the senior role within the DODIN. The SECDEF has command authority over all military operations. In regards to command authorities over the DODIN, the SECDEF has delegated Title 10 direction and control to the DoD Chief Information Officer (DoD CIO) as the information architect and executive, but retains authority over the network.[24] Additionally, the DoD CIO has Title 40 USC (Title 40) authorities as the senior CIO within the department to supervise and maintain the information technology (IT) acquisition and information resources management (IRM) practices within the federal agency.[25] Lastly, the DoD CIO also has Title 44 USC (Title 44), Paperwork Reduction Act, authorities which serve as an umbrella for multiple authorities to include dissemination of public information, privacy, IT acquisition, and IRM.[26] The DoD CIO is the senior stakeholder within the DODIN and is responsible for more than just the DODIN as a network. He is responsible for a large amount of the information which resides within the DODIN as the department's information executive. What follows is a short history of how the billet started, changed titles over the years, and ultimately arrived at its present state. The changes in the titles are not due to competition or authorities clash rather an evolution of authorities in accordance with legislation.

In 1970, OSD first established a staff member position of Assistant to the Secretary of Defense (Telecommunications) to preside over the defense department's communications network.[27] Throughout the 1970s to the early 1980s, the position was upgraded to an Assistant Secretary of Defense (ASD), downgraded to a Director's position, and re-established as ASD,

Command, Control, Computers, and Intelligence (ASD (C3I)) via DoD Directive (DoDD) 5137.1.[28] ASD (C3I) was formally mandated by law in the DoD Authorization Act of 1984. The law formalized the position's standing as the executive for the National Communications System, predecessor of the DODIN, and directed the Defense Information Systems Agency (DISA) to report to ASD (C3I).[29] ASD (C3I) became the command authority with the inherent responsibilities of direction and control of the DODIN. In 2003, OSD realigned the intelligence section away from ASD (C3I) and transitioned the authorities and title to ASD for Networks and Information Integration (ASD (NII)).[30] Finally, in 2012, OSD disestablished ASD (NII) and transferred those authorities to the DoD Chief Information Officer (DoD CIO).[31] DISA's reporting responsibility also transferred to the DoD CIO.

DISA, as a combat support agency, has been a key stakeholder in the C2 process of the DODIN since the inception of the network. In 1960, President Eisenhower directed his SECDEF, Charles Wilson, to survey military communications and report on possible duplications.[32] Based on that survey, the Defense Communications Agency (DCA) was established "with the primary mission of OPCON and management of the Defense Communications System (DCS)."[33] Rear Admiral Irvin was the first Director of DCA.[34] The DCS was the combination of the wire, radio, and radar systems implemented by the military services.[35]

DCA was established with OPCON of the DCS. OPCON was a well understood term within the then-joint doctrinal manual, Joint Action Armed Forces, with a valid definition in the joint dictionary, Dictionary of the United States Military Terms for Joint Usage.[36] At the time, OPCON was defined as:

> Those functions of command involving the composition of subordinate forces, the assignment of tasks, the designation of objectives[,] and the authoritative direction necessary to accomplish the mission. Operational control should be exercised by the use

> of the assigned normal organizational units through their responsible commanders or through the commanders of subordinate forces established by the commander exercising operational control.
>
> It does not include such matters as administration, discipline, internal organization and unit training, except when a subordinate commander requests assistance.[37]

However, the DoD Reorganization Act of 1958 introduced the term operational command (OPCOM) which created confusion with the difference between, at the time, unified and specific command and OPCON. Between the DoD Reorganization Act of 1958, the revised joint dictionary of 1962, and the UCP of 1963, OPCOM and OPCON were synonymous; however, OPCOM was "uniquely applied to the Operational Control exercised by the commanders of unified and specified commands over assigned forces… ."[38] The intent of OPCOM was to give CCDRs "unquestionable authority" over forces within their theater without burdening them with the "responsibilities and the large headquarters that would follow from an assignment of total or complete command authority" held by the Service Chiefs.[39] OPCON was understood as a level of command authority below unified, specified, and OPCOM. Therefore, the interpretation of the command authority that DCA had over the DCS was subordinate to the total command authority held by the Service Chiefs and the OPCOM held by the CCDRs. This understanding is key as it will continue to cause conflicts in C2 of the global network. This history sets a precedence of confusion in command authorities between CCDRs, Service Chiefs, and Director, DISA (DIRDISA) within the DODIN.

Over the decades, DCA would continually prove to be highly capable in improving operational efficiency and effectiveness with the responsibilities for communications systems transferred from the Services or created organically. In the 1960s, DCA was given the key responsibilities to establish "three common-user, defense-wide networks that would be known as the Automatic Voice Network (AUTOVON), the Automatic Digital Network (AUTODIN), and

the Automatic Secure Voice Communications Network (AUTOVOSECOM)."[40] During the Space Age, DCA would launch the Defense Satellite Communications System, which proved to be the workhorse of military satellite communications enabling high data rate, global communications.[41] During the Information Age, DCA improved the reliability and throughput of the classified and unclassified voice and organizational messaging networks while creating the Defense Data Network.[42] These improvements directly supported the GCC. As DCA expanded the disparate networks, they also set up field offices and network support centers within each GCC's AOR. In 1991, DCA underwent a major reorganization and was renamed DISA.[43] DISA continues to host a plethora of responsibilities to include creating and maintaining the standards to connect or extend DODIN services, network certification and accreditation, and operation and maintenance of core DODIN services. However, those responsibilities are not imposed by DISA's command authority over the DODIN, of which DISA has relatively none. Those responsibilities are imposed through the DoD CIO's command authority over DISA. Specifically, DISA provides dedicated support to the DoD CIO in the accomplishment of his Titles 40 and 44 authorities.[44] This close relationship may be the reason why the SECDEF has not realigned DISA under USCYBERCOM.

To identify if CDRUSSTRATCOM truly has any authority over the DODIN, one must understand how the cyberspace mission was created and delegated. As previously stated, DCA had created the DoD's data network and expanded the AUTOVON during the Information Age. Strategists understood that the network was the means by which information was stored and transported between CDRs and staff. Information warfare was the next stage of warfare. In 1997, a National Defense Panel outlined a transformational strategy which proposed "...giving USSPACECOM the mission of information support on a global scale...."[45] In 1998, during the

UCP review period, Gen Shelton, Chairman of the Joint Chiefs of Staff (CJCS), directed the Joint Staff to "work upon defensive information operations and, after an organization had been created, deal with offensive information operations."[46] Joint Task Force- Computer Network Defense (JTF-CND) was created, assigned its mission of protecting defense networks, aligned under USSPACECOM, and reached initial operational capability in December 1998 and full operational capability in June 1999.[47] JTF-CND's mission was expanded to include computer network attack; therefore, in April 2001, it was renamed to JTF- Computer Network Operations (JTF-CNO). JTF-CND and JTF-CNO's creation came with apparently no changes to DODIN command authorities. Then-ASD (C3I) retained command authority for the DODIN. The next transition of JTF-CNO was produced by the changes within the 2002 UCP.

The most notable portion of the 2002 UCP was the establishment of US Northern Command (USNORTHCOM); however, an ancillary part was the retention of USSTRATCOM. This is important because change 1 to the 2002 UCP merged USSPACECOM and USSTRATCOM under the command of USSTRATCOM.[48] Change 2 to the 2002 UCP assigned the responsibility for information operations to USSTRATCOM.[49] Under the merger, JTF-CNO transitioned under USSTRATCOM. Specifically, change 2 tasked USSTRATCOM with the responsibility for "integrating and coordinating DoD information operations (IO) [then] consisting of the core IO capabilities of computer network attack (CNA), computer network defense (CND)...."[50] Additionally, from a CND perspective, USSTRATCOM was tasked with identifying desired characteristics and capabilities, planning, and directing DoD-wide CND.[51] None of these tasks or responsibilities can be mis-interpreted to be command authority over IO or CND operations. At this point, USSTRATCOM was authorized to plan, integrate, and direct IO and CND operations.

In 2004, CDRUSSTRATCOM transitioned the CND portion of JTF-CNO to become JTF- Global Network Operations (JTF-GNO).[52] Duly, in 2005, he transitioned the remaining CNA portion of JTF-CNO to become Joint Functional Component Command- Network Warfare (JFCC-NW).[53] JTF-GNO would be responsible for "directing Global Information Grid operations and defense" as stated in the 2006 UCP.[54] The first actual delegation of command authority occurred in June 2004; the SECDEF assigned Director, DISA to be dual-hatted as CDRJTF-GNO and delegated authority of the GIG.[55] Although, the SECDEF is not authorized to unilaterally make changes to CCDR authorities established within Title 10, this delegation of authority finally empowered CDRJTF-GNO to do more than coordinate. CDRJTF-GNO's abilities were still in a quandary with this newfound authority. For the most part, CDRJTF-GNO gained the ability to preside over the backbone of the DODIN without having to get approval from the DoD CIO. The geographic CCDRs and Service Chiefs still retained command authority over their regional and service portions of the DODIN.

USSTRATCOM made the first attempt at codifying a then-GIG C2 framework as the Joint Concept of Operations (CONOPS) for GIG NetOps.[56] The JTF-GNO staff belonged to USSTRATCOM and was completely separate from DISA other than DIRDISA being dual-hatted as CDRJTF-GNO. For basic understanding which will be referenced later, USSTRATCOM's global NetOps C2 framework is as follows (see figure 1).[57]

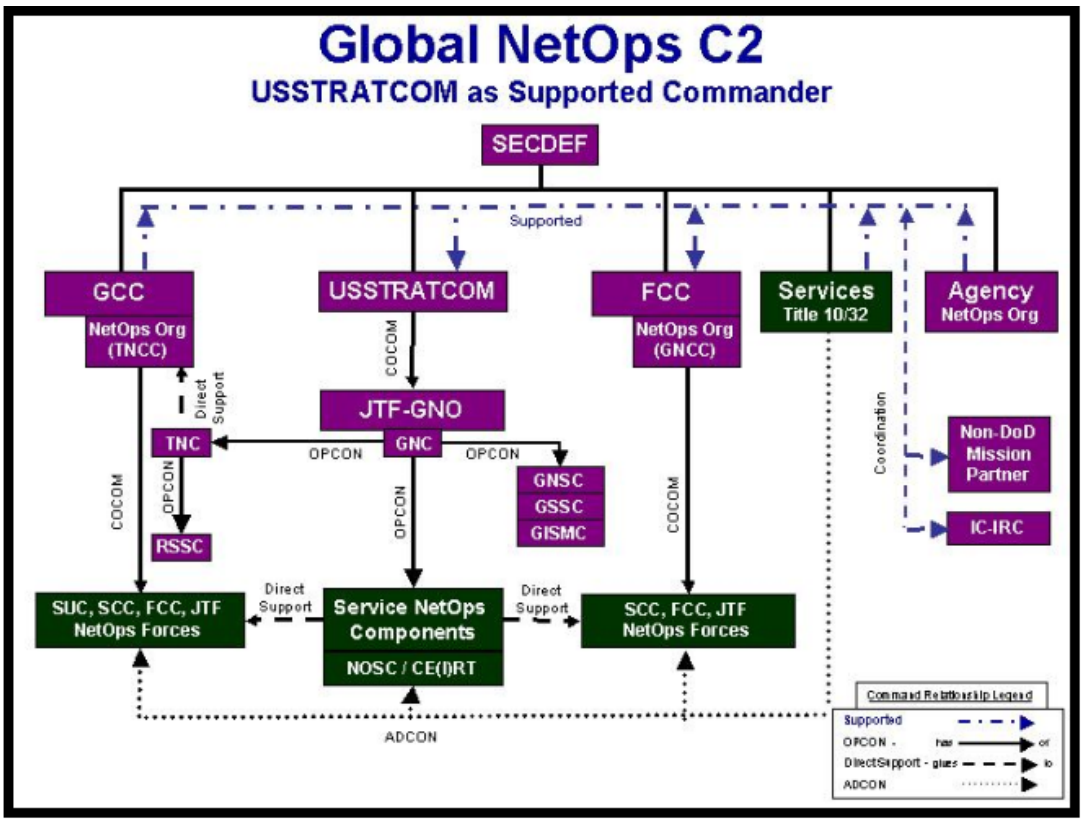

Figure 1

USSTRATCOM had COCOM authority over JTF-GNO and tasked CDRJTF-GNO to operate and defend the DODIN. JTF-GNO established a centralized Global NetOps Center (GNC) and regional Theater NetOps Centers (TNCs) aligned with the GCCs. The GNC and TNCs were OPCON to JTF-GNO. Additionally, under USSTRATCOM's COCOM authority, the Services' organic NetOps Centers were OPCON to JTF-GNO and ADCON to Service headquarters under their Title 10 authority. The TNCs which were regionally aligned with the GCCs were in direct support with the GCC's NetOps center, Theater NetOps Control Center (TNCC). JTF-GNO's TNCs worked closely with the GCCs' TNCCs to provide dedicated technical support, mitigate vulnerabilities, and relay real-time information about the health and readiness of the GCC's network. JTF-GNO had orders and directive authority based on the SECDEF delegation of authority letter, but many of their directives were implemented slow or the Service and/or GCC

were slow to react. While JTF-GNO was well-manned and structured regionally, the underlying Service networks were not. For example, the Air Force has a centralized Service Global NetOps Security Center (SGNOSC) and distributed Service Theater NOSCs (STNOSCs) aligned with the major GCCs.[58] However, the Marine Corps only has a centralized SGNOSC; the Marine Corps Enterprise Network (MCEN) is not regionally aligned with the GCCs and continues to undergo internal MCEN C2 evolutions.[59] There is a false understanding that Service networks are aligned with the hierarchical command structure and are nested or overlay onto the geographic configuration of the GCCs. As previously stated, the Service networks have grown and changed in accordance with the Service Chiefs' Title 10 requirements primarily. Aligning the network's control processes and hierarchy with a DoD-level C2 structure is secondary or even tertiary.

The activation of USCYBERCOM in 2009 was understood by senior military leaders and think tank personnel to be a major step in the right direction towards unity of command and effort within the DODIN.[60] JTF-GNO and JFCC-NW were disestablished with their roles and responsibilities rolled up into USCYBERCOM. CDRUSCYBERCOM was also dual-hatted as Director, NSA (DIRNSA). The offensive cyberspace operations (OCO) portion would reside within NSA while the defensive cyberspace operations (DCO) and DODIN operations portions would reside with USCYBERCOM. At the time of activation, it is unknown whether the delegation of authority from the SECDEF transitioned to CDRUSCYBERCOM. At this point it is immaterial whether the letter made the transition because the GCCs and Service Chiefs retained their command authorities over their sectors of the DODIN. The current state is a global network without unity of command due to DoD CIO/DISA, the GCCs, and Service Chiefs equally commanding their portions of the DODIN.

An example of the downfall of DODIN's lack of clear command with command authorities occurred in 2010 during I Marine Expeditionary Force (Forward)'s (I MEF (FWD)) deployment to Afghanistan as part of Operation ENDURING FREEDOM. I MEF (FWD) was redesignated as Regional Command (SouthWest) (RC(SW)), a coalition command. For network C2, RC(SW) coordinated through USCENTCOM's Joint Network Control Center (JNCC). International Security Assistance Force-Joint Command's (IJC) relayed USCENTCOM's desires. ADCON was retained by Headquarters US Marine Corps' (USMC) Network Operations and Security Center (MCNOSC).[61] RC(SW)'s network was a tactical extension of the MCEN primarily via DISA's gateway sites. RC(SW) did not rely on IJC nor USCENTCOM's JNCC for network services.

However, during the deployment, USCENTCOM attempted to coerce RC(SW) to make two major changes to its network. First, the JNCC wanted RC(SW) to migrate from its 'afg.usmc.mil' domain to the GCC's 'centcom.mil' domain. This change would have necessitated RC(SW) to rely on USCENTCOM and IJC, through the JNCC, for certain domain-level services. Changing domains does not decrease RC(SW)'s network threats nor vulnerabilities.

Secondly, USCENTCOM and multiple component commands wanted access to the routers within RC(SW)'s security boundary suites. The commands wanted to make modifications to the access control lists (ACLs) within those routers. Those ACLs are created by DISA based on attempted adversary intrusions at the internet access points connecting the DoDIN to the public internet. DISA sends those ACLs to all CCMDs/Services/agencies (CC/S/A) operating security boundaries. Changes to these ACLs would create a vulnerability within the DODIN defense-in-depth posture. Additionally, configuration management of

network devices was outside of the purview of USCENTCOM's authority. The MCNOSC retained configuration management over RC(SW)'s network. The JNCC supposedly would receive direct information from JTF-GNO regarding network intrusions externally targeting USCENTCOM networks. If the JNCC wanted to block a suspected method of intrusion they could not mandate any changes to ACLs or the security boundaries. USCENTCOM nor IJC could mandate either of the network changes due to a clear lack of command authorities within the DODIN.

This example demonstrates how the lack of command authorities within the DODIN C2 framework can lead to known vulnerabilities in the global network making it less secure for all. At that time, only the MCNOSC could mandate RC(SW) to upgrade its security boundary system because RC(SW) was operating as an extension of the Marine Corps' Title 10 MCEN. USSTRATCOM, USCENTCOM, nor IJC, as a JFC, could disrupt the Service's Title 10 authority. At times, blocking network vulnerabilities goes beyond simple changes at the keyboard. Sometimes, network security requires the procurement of an upgraded device across all security boundary systems. Each Service has to spread its Title 10 funding across all projects and programs to include weapon systems, training, and base infrastructure. Therefore, upgrades to network systems routinely occurs years after the technology was created. This is a pervasive problem which will continue to lead to a highly vulnerable DODIN.

CURRENT STATE OF CYBER C2 FRAMEWORK AND ITS FAULTS

Within the past two years USCYBERCOM and OSD have made some major changes. OSD, the Joint Staff, and USCYBERCOM have published joint doctrine for cyberspace operations, created a cyber C2 framework, and added forces to the DoD's cyber structure. Most

of these changes are heading in the right direction, but there remains major issues which are still unresolved.

In 2013, CDRUSCYBERCOM announced the creation of a Cyber Mission Force (CMF) to better support USCYBERCOM's three mission areas: defend the nation, CCMD support, and secure, operate, and defend the DODIN.[62] The makeup and mission area alignment of the CMF is as follows: National Mission Teams (NMT) will "defend the nation against national-level threats", Combat Mission Teams (CMT) will "be assigned to the [OPCON] of [CCMDs] to support their objectives", and Cyber Protection Teams (CPT) will "help operate and defend the DoD information environment."[63] The Services are building and providing initial training to the CMF prior to being transferred to USCYBERCOM for further tasking.[64]

The CMF is right on target. It is a great capability and provides the joint force an enhanced cyber capacity. Each of the teams within the CMF is a collection of cyber security, telecommunications, and intelligence specialties. USCYBERCOM J7, in coordination with DoD, has made substantive progress to overcome the lack of standardized cyber training across the Services. Currently, each Service has different job specialties that make up the cyber workforce where the CMF teams are created. Each Service also has disparate training pipelines for their cyber workforce which are tailored to support that Title 10 Service Chief's respective requirements. To overcome this issue, USCYBERCOM has created a layered policy and standards approach.

First, they created the USCYBERCOM Training and Readiness Manual (T&R Manual) which provides the tasks, conditions, and standards required to demonstrate individual and collective proficiency for CMF teams.[65] The T&R Manual will correlate the individual proficiency skills with the DoDD 8140 Cyberspace Workforce Management (DoDD 8140)

policy update.[66] DoDD 8140 will replace the DoDD 8570 Information Assurance (IA) Training, Certification, and Workforce Management policy which previously only applied to the IA workforce. DoDD 8140 will define cyber workforce roles based on the National Initiative for Cybersecurity Education (NICE) framework.[67]

Second, USCYBERCOM authored the Joint Cyberspace Training and Certification Standards (JCT&CS). The JCT&CS identifies the unique knowledge, skills, and abilities (KSAs) for each workforce role in the USCYBERCOM's cyber workforce and the CMF teams.[68]

Lastly, USCYBERCOM created a CMF Training Pipeline to outline the optimal path to achieve the KSAs which satisfy the JCT&CS. The pipeline is designed bridge the entry level or commercial training received from the Services and prepare CMF personnel to perform mission tasks.[69] These three products provide overall policy and standards for the Service cyber workforce along with specific training standards and certification criterion for designating the CMF teams are mission ready.

The next major change was the creation, and subsequent modification, of a cyberspace operations C2 framework in 2013. The previous DODIN C2 framework was the aforementioned Joint CONOPS for GIG NetOps under the charge of JTF-GNO in 2005.[70] This new cyber C2 framework seeks to implement unity of command and unity of effort across the DoD to execute full spectrum military cyberspace operations.[71] It also seeks to accomplish a requirement from the GCCs to enable them to conduct full spectrum military cyberspace operations.[72] The new cyber C2 framework consists of two main parts: overall C2 structure and detailed Joint Force Headquarters-DODIN (JFHQ-DODIN) C2 structure.

USCYBERCOM’s overall C2 structure enables full spectrum military cyberspace operations via focused componency across USCYBERCOM’s three mission areas (see figure

2).[73] Additionally, this new structure enables HQ, USCYBERCOM to focus on strategic and limited operational level operations while the JFHQs focus on operational operations.[74] Per the CJCS execution orders (EXORDs) and SECDEF approval, USCYBERCOM activated three subordinate headquarters (HQ) elements to align with its mission areas.[75] CDR National Mission Force (CNMF) HQ "will be aligned to the Strategic Defense against Offensive Cyber Attack (Defense of the Nation) mission area, with a national focus."[76] There will be four separate JFHQs-Cyber which are aligned "to [CCMD] support mission area for [OCO]."[77] Finally, JFHQ-DODIN "will be aligned to the Secure, Operate and Defend [the] DODIN mission area, with an operational focus across all CC/S/A."[78] Based on the operational focus of the JFHQs, the GCCs receive an offensive and defensive cyber capability thus enabling them to conduct full spectrum military cyberspace operations. Additionally, all three HQs are OPCON to USCYBERCOM, the JFHQ-Cyber will be in direct support of the respective GCC. Lastly, each GCC will have a Joint Cyber Center from USCYBERCOM embedded within the GCC's staff to provide dedicated, daily support in planning.

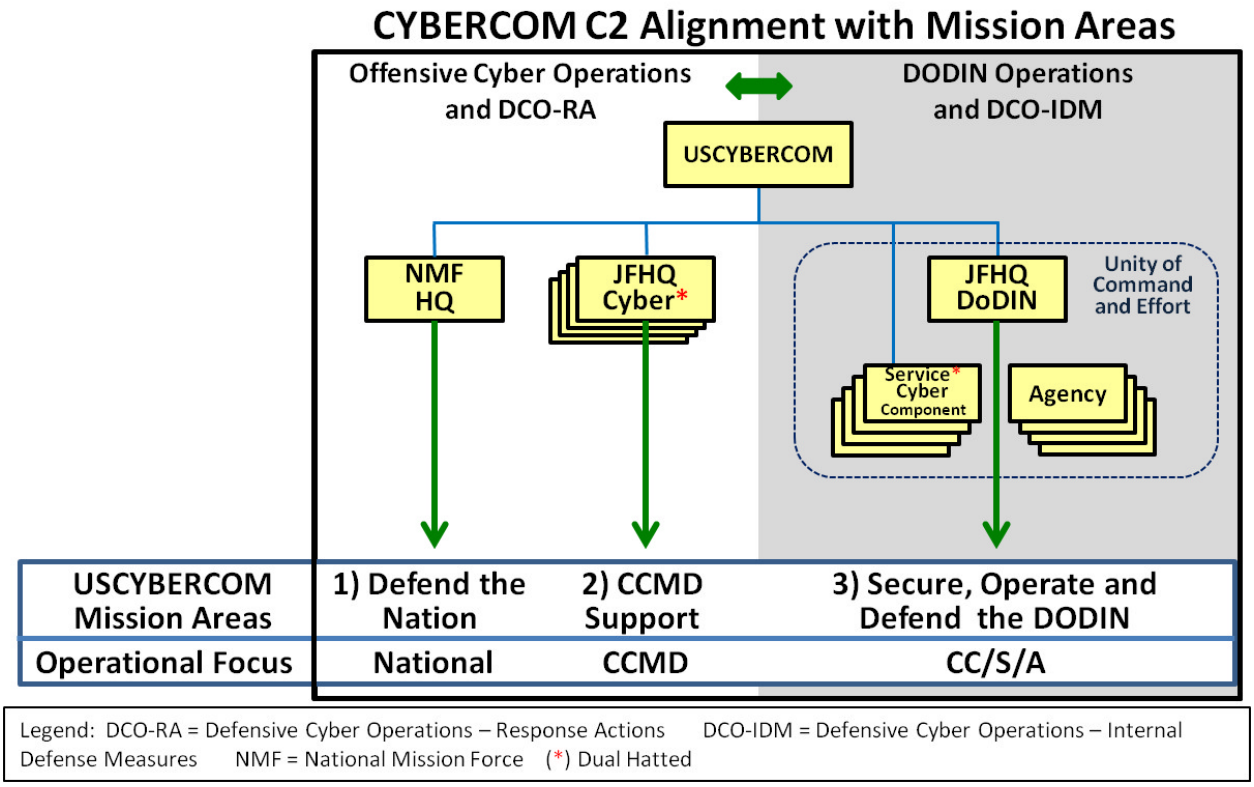

Figure 2

As previously stated, JFHQ-DODIN is tasked to secure, operate, and defend the DODIN. In the original directive, JFHQ-DODIN's commander and command authority were dictated in straight-forward, plain language. From a command perspective, DIRDISA is dual-hatted as CDRJFHQ-DODIN.[79] The SECDEF established "directive authority for cyberspace operations (DACO) for the purpose of issuing orders to DoD components in order to assure effective functioning and defense of the entire DODIN."[80] The DACO authority gave CDRJFHQ-DODIN authority to issue orders and directives to all DoD components to "compel unity of action" during the execution of his responsibilities.[81] The DoD components are the CC/S/As, in total. However, in the JFHQ-DODIN C2 framework, it described the DACO authority as being over "DISA and all other Agencies...a TACON equivalent authority...."[82] Within JFHQ-DODIN, the DACO authority is understood to be solely over the DoD's agencies which is the same TACON authority JFHQ-DODIN has over the Service cyber components.[83] JFHQ-DODIN J5 believes

that the DACO authority may evolve to a higher level authority as time passes.[84] Until then, the lack of command authority within JFHQ-DODIN, and by proxy USCYBERCOM, will continue to exacerbate the problem of no true DODIN commander and an inability to compel a Title 10 CDR to make the necessary changes to the network. The remaining elements of JFHQ-DODIN's C2 structure are simply retitled elements of JTF-GNO (see figure 3).[85]

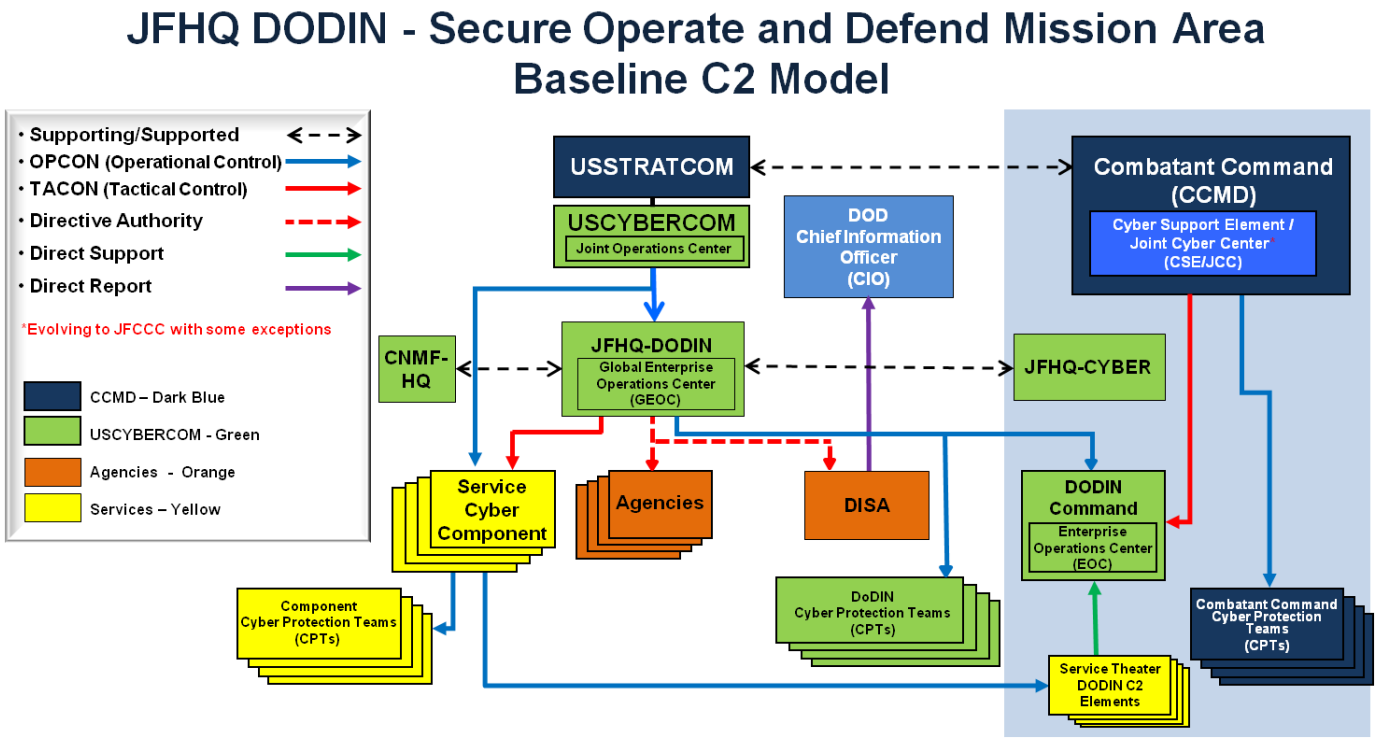

Figure 3

JFHQ-DODIN will centrally control its global responsibility to operate and defend the DODIN from its Global Enterprise Operations Center (GEOC).[86] The GEOC has the same function as JTF-GNO's GNC. From a regional perspective, there will be a DODIN Command supporting each GCC. Within each regional DODIN Command there will be an Enterprise Operations Center (EOC).[87] The difference between the DODIN Commands/EOCs versus TNCs is DODIN Commands are a fully functional commander with staff members (G-1/2/3/4, etc) with the EOC as a function within the G-3. TNCs were more focused on the network versus the

network and command functions.[88] As for command relationships subordinate to JFHQ-DODIN, the regional DODIN Commands/EOCs remain OPCON, the Service cyber components are TACON, and DoD agencies are DACO which is equivalent to TACON. The regional DODIN Commands/EOCs are TACON to the GCCs. I have no issues with this structure or command relationships. We will see what additional capability arises from the DODIN Command internal structure.

RECOMMENDATIONS

Based on the analysis above, there remains two major problems with the DoD's cyber C2 framework which will continue to impede the NMS-CO's goal of military cyberspace superiority. First, USCYBERCOM, as a subunified CCMD, does not have any delegated COCOM authorities to operate and defend the DODIN. It must become a full unified CCMD with additional COCOM authorities. Second, DISA should be under USCYBERCOM's COCOM authority and C2 structure instead of directly reporting to the DoD CIO. These two major changes, and the subsequent second order effects, will enable unity of command and effort within the DODIN. The first step appears to be on the verge of fruition, but without that second step, the change in structure will be largely ceremonial.

The compelling need for USCYBERCOM to be elevated to a full unified CCMD is due to the speed of decision-making required in the cyber domain. The classified network has been compromised. The unclassified network has multiple major and minor compromises each passing year. Elevating USCYBERCOM is not about making the DODIN more secure. It is about enabling and bestowing true decision-making power upon a commander and elevating the focus of cyberspace operations to then improve that security. General (GEN) Alexander stated in March 2014, that "over the next year we [will] have reached a tipping point where we are

going to need to shift to a unified command."[89] His main reason for making this recommendation was to attain the speed in "command and control from the President and the Secretary of Defense directly to that commander... as we add more teams and more complexity, [US]STRATCOM's ability to actually play in this will continue to go down."[90]

CCMDs are usually established or disestablished via the Unified Command Plan. It is of extreme importance that USCYBERCOM be established with enumerated authorities in Title 10, such as USSOCOM. This method would strengthen USCYBERCOM's stance and authorities because it would be at the approval of the POTUS and SECDEF and an act of Congress. It is always better to get the approval of two branches of government versus one. After elevating to a full unified CCMD, there are some specialized authorities that also need to be properly codified.

GEN Alexander and Hollis recognize that USCYBERCOM, as a full unified CCMD, needs to have acquisition authorities similar to USSOCOM.[91] The current DoD environment of fiscal constraint is causing a host of programs to be below the cut line that Title 10 CDRs need. Technology is not getting cheaper and our adversaries continue to increase their capabilities in cyber. Some Service Chiefs may delay spending on cyber technologies while others make the decision to spend on the same technology. Simple decisions of that nature can create major vulnerabilities and holes within our cyber defense perimeter. Title 10 needs to be updated to enable USCYBERCOM to have "authority to exercise the functions of the head of the agency under chapter 137... [The] staff of the commander shall include a command acquisition executive, who shall be responsible for the overall supervision of acquisition matters...."[92] Anything less than the verbiage that is identical to USSOCOM's would reduce CDRUSCYBERCOM's COCOM authority.

USCYBERCOM would also require specific verbiage in Title 10 declaring its COCOM authority over the entire DODIN which would be senior to the authority vested in the Service Chiefs. This clear wording would supersede the modification to the CJCS EXORD delegating DACO authority to CDRJFHQ-DODIN. It would also clarify that there is one overall commander of the DODIN, CDRUSCYBERCOM, who has enumerated COCOM authorities. Specifically, those COCOM authorities give him the authority, direction, and control over the CC/S/A's networking assets. That new section within Title 10 would also have to clarify the responsibilities of the Service Chiefs to coordinate their network operations, plans, and acquisitions with CDRUSCYBERCOM as the DoD's authority over network operations, defense, and acquisitions. This new Title 10 authority will enable USCYBERCOM the authority to achieve the Joint Information Environment (JIE). JIE will "consolidate and standardize the design and architecture of the [DODIN]."[93] This new Title 10 COCOM authority, paired with the previous acquisition authority, will declare CDRUSCYBERCOM as the overall commander of the DODIN with the responsibility and funding authority to standardize the DODIN architecture under the JIE standards.

There are additional authorities or sub-authorities which USCYBERCOM would need. I previously mentioned the DoD CIO's Title 40 and 44 authorities and the special relationship that DISA has in supporting the DoD CIO. I believe that USCYBERCOM's cyber C2 framework purposely distributed operational level operations onto the subordinate JFHQs to enable HQ, USCYBERCOM to be prepared to assume additional strategic authorities without burden. As a full unified CCMD, USCYBERCOM would be able to conduct unobstructed coordination and support for the DoD CIO's Title 40 and 44 authorities. HQ, USCYBERCOM as a primary, not

DISA, should provide administrative and operational support to the DoD CIO in order to gain cyberspace superiority through an enhanced understanding of the information environment.

The last recommendation is a logical conclusion based on the previous recommendations. Currently DISA directly reports to the DoD CIO. DISA needs to fall under USCYBERCOM's COCOM authority within the overall cyber C2 framework. As previously stated, DIRDISA is dual-hatted as CDRJFHQ-DODIN. JFHQ-DODIN is OPCON to USCYBERCOM and COCOM to USSTRATCOM. All of the military personnel within JFHQ-DODIN are service members who have been reassigned from DISA's manning document.[94] Therefore, when a subordinate DODIN CC/S/A receives a directive from JFHQ-DODIN or a regional DODIN Command there is always the age old question: Is this really from DISA or USCYBERCOM? This was the same problem when the DODIN was under the control of CDRJTF-GNO, who was dual hatted as DIRDISA.[95] DISA under CDRUSCYBERCOM's COCOM authority finally answers that question in the affirmative because there would be one clear command authority.

CONCLUSION

Since 1998, the protection of the DoD's computing assets has bounced around as a sub-component of a unified CCMD. The president and SECDEF are aware of the necessity to protect and defend our networks but have not placed the requisite emphasis on it. That lack of emphasis in part stems from how the Services understood the need to grow and extend their networks. As early as the presidency of Dwight D. Eisenhower, government officials recognized the need for centralized agency accounting for the growth of this conglomeration of technologies. DISA became the de facto CDR with OPCON of the global DoD network, but that command authority dwindled with the squabble between CCDR versus Service Chief command authority. USSTRATCOM made a fair attempt to demonstrate some command authority by

establishing JTF-GNO to conduct the COCOM's UCP responsibility to operate and defend the DODIN. Yet again, JTF-GNO's delegated SECDEF authority could not override Title 10 authority. Finally, after multiple studies, think tank recommendations, and compromises to our national security systems, USCYBERCOM was born with an expectation to unify and preside over the DODIN. Unfortunately, our national leaders were afraid to shoot directly for the NMS-CO's goal of military cyberspace superiority.

Now that USCYBERCOM has been operational for almost five years, there is finally the opportunity to correct the previous wrongs and learn from our mistakes. The SECDEF and Joint Staff finally agreed on a cyberspace operations C2 framework to implement unity of command and effort and enable full spectrum military cyberspace operations. Our senior leaders finally planned to do this in accordance with the same joint C2 framework that they signed years ago. In support of DODIN operations and DCO, they clearly designated and dual-hatted DIRDISA as CDRJFHQ-DODIN, the JFC of the defensive portion of the DODIN. They clearly bestowed that JFC with DACO authority over all DoD components, i.e. CCMDs, Services, and agencies. Again, a group broke the first clear directive for command and control. Due to the lack of a clear commander with very little authority, the JFHQ-DODIN C2 framework became the retitled Joint CONOPS for GIG NetOps of 2005. It has the same tenets of JTF-GNO's control structure, a central global network operations control center with regional network operations centers providing direct support to its respective GCC. The only worthy additions are the CMF teams and the Joint Cyber Center embedded within GCC's staff.

The time has come to break the cycle and elevate the focus of cyberspace operations. USCYBERCOM must become a full unified CCMD to support the speed of decision-making from the president through the SECDEF to the cyber CCDR. As a CCDR,

CDRUSCYBERCOM must have specialized COCOM authorities to enable the DoD to outpace its adversaries. Title 10 needs to be updated with poignant cyber-related acquisition language, identical to USSOCOM, so the Services are not deciding between funding an air, sea, land, space, or cyber weapon system. CDRUSCYBERCOM will oversee and acquire the necessary cyber systems that ensure the collective defense of the DoDIN in the garrison and combat environment. Title 10 must also designate CDRUSCYBERCOM as the overall commander of the DODIN and the Service Chiefs' Title 10 authority over their respective networks is subordinate to CDRUSCYBERCOM. These new COCOM authorities of command and fiscal responsibility will enable the implementation of the JIE standards. Additionally, CDRUSCYBERCOM should enjoy and shoulder the burden of the DoD CIO's Title 40 and 44 authorities vice DIRDISA. USCYBERCOM's updated cyber C2 framework was established to enable HQ, USCYBERCOM to focus on strategic level operations such as COCOM and Congressional authorities. Finally, DIRDISA will naturally fall under CDRUSCYBERCOM's COCOM authority as the clear command authority of full spectrum military cyberspace operations. When USCYBERCOM is elevated to a full unified CCMD with these COCOM authorities, there is no question that CDRUSCYBERCOM will be able to mount a concerted effort towards accomplishing its mission of operating and defending the DODIN.

Endnotes

[1] "History," *U.S. Strategic Command*, last modified August 2014, http://www.stratcom.mil/history/.

[2] Ibid.

[3] Headquarters Joint Staff, *Cyberspace Operations*, JP 3-12(R) (Washington, DC: Joint Staff, February 5, 2013), III-6.

[4] Headquarters Department of Defense, *National Military Strategy for Cyberspace Operations*, (Washington, DC: Department of Defense, December 11, 2006), ix.

[5] Robert Barker, "Command and Control of Network Operations," (master's thesis, U.S. Army War College, 2009), 2, http://www.dtic.mil/.

[6] Headquarters Joint Staff, *Department of Defense Dictionary of Military and Associated Terms*, JP 1-02 (Washington, DC: Joint Staff, December 15, 2014), 172.

[7] Headquarters Joint Staff, *Doctrine for the Armed Forces of the United States*, JP 1 (Washington, DC: Joint Staff, March 25, 2013), IV-15.

[8] Secretary of Defense Memorandum, "Assignment and Delegation of Authority to Director Defense Information Systems Agency," June 18, 2004.

[9] JP 1-02, 40.

[10] Andrew Feickert, *The Unified Command Plan and Combatant Commands: Background and Issues for Congress*, CRS Report for Congress R42077 (Washington, DC: Congressional Research Service, January 3, 2013), 1, http://fas.org/sgp/crs/natsec/R42077.pdf.

[11] JP 1, V-1.

[12] Feickert, 11.

[13] *Armed Forces*, U.S. Code, Title 10, Vol. III, sec 166 (2011).

[14] Ibid, section 167.

[15] JP 1-02, 50.

[16] JP 1, V-2.

[17] JP 1, V-2.

[18] JP 1-02, 42.

[19] JP 1-02, 40.

[20] Headquarters U.S. Marine Corps, *Command and Control*, MCDP 6-0 (Washington, DC: U.S. Marine Corps, October 4, 1996), 40.

[21] Michael Warner, "Notes on the Evolution of Computer Security Policy in the US Government, 1965-2003" (workshop presentation at Charles Babbage Institute supported by the National Science Foundation's Computer Security History Workshop, July 2014), 2.

[22] Warner, 5.

[23] JP 1, V-14.

[24] *Department of Defense Chief Information Officer Desk Reference, volume 1*, August 2006, http://dodcio.defense.gov/Portals/0/Documents/ciodesrefvolone.pdf, 151.

[25] DoD CIO desk ref, 2.

[26] DoD CIO desk ref, 24.

[27] Historical Office, Office of the Secretary of Defense, *Department of Defense Key Officials 1947-2014*, (Washington, DC: Department of Defense, June 2014), 66.

[28] DoD Key Officials, 68.

[29] DoD Key Officials, 68.

[30] DoD Key Officials, 68.

[31] Ashton Carter, Deputy Secretary of Defense, Disestablishment of Assistant Secretary of Defense for Networks and Information Integration (ASD(NII)) and Related Matters, Memorandum, 11 January 2012.

[32] "Our History: The Beginnings," *Defense Information Systems Agency*, last accessed January 19, 2015, http://www.disa.mil/about/our-history.

[33] DISA history, 1947-1960.

[34] DISA history, 1947-1960.

[35] DISA history, 1947-1960.

[36] Joint Chiefs of Staff, *Definition of Operational Command and Operational Control*. April 30, 1975, http://www.dod.mil/pubs/foi/joint_staff/jointStaff_jointOperations/265.pdf.

[37] OPCOM and OPCON, 9.

[38] OPCOM and OPCON, 12.

[39] OPCOM and OPCON, 4.

[40] DISA history, 1960s.

[41] DISA history, 1970s.

[42] DISA history, 1990s.

[43] DISA history, 1990s.

[44] U.S. Department of Defense, *Defense Information Systems Agency* (DISA), Directive 5105.19, 25 July 2006, 4.

[45] Ronald Cole, Edward Drea, et al., *History of the Unified Command Plan 1946-2012*, Officer of Chairman of Joint Chiefs of Staff, last modified 2013, http://dtic.mil/doctrine/doctrine/history/ucp.pdf, 75.

[46] History of UCP, 76.

[47] DISA history, 1990s.

[48] Casey, George, Director of Joint Staff. Promulgation of Unified Command Plan 2002 (with Change-1 and Change-2 incorporated), Memorandum, 4 February 2003, 2.

[49] UCP 2002, 2.

[50] UCP 2002, 15.

[51] UCP 2002, 15.

[52] STRATCOM history.

[53] STRATCOM history.

[54] UCP 2006, 29.

[55]Donald Rumsfeld, Secretary of Defense, Office of Secretary of Defense to Director of Defense Information Systems Agency, Assignment and Delegation of Authority to Director Defense Information Systems Agency, Memorandum, 18 June 2004.

[56] Headquarters, U.S. Strategic Command, *Joint Concept of Operations for Global Information Grid NetOps*, August 10, 2005, ii.

[57] GIG NetOps, 42.

[58] GIG NetOps, 34.

[59] S.M. Hoyle, "Network Operations Command and Control," (PowerPoint presentation. Plans, Policies, and Orders, Headquarters, Marine Corps, Arlington, VA, 12 June 2014).

[60] Scott Charney, James Langevin, et al. "Cybersecurity Two Years Later." Working Paper, Center for Strategic and International Studies, 2011, 10.

[61] Matthew Limbert, Lieutenant Colonel, USMC, formerly Regional Command (SouthWest) C-6 Operations Officer, email interview by author, March 4, 2015.

[62] *Statement of General Keith B. Alexander Commander United States Cyber Command: Hearing before the Senate Armed Services Subcommittee*. 113th Cong., 6, (2013).

[63] Gen Alexander, 6.

[64] Gen Alexander, 6.

[65] "Recommendations for Executive Action," U.S. Government Accountability Office, last modified 1 July 2014, http://www.gao.gov/products/GAO-11-421.

[66] GAO recommendations.

[67] Stephanie Keith, "Cyberspace Workforce," (PowerPoint presentation, AFCEA West, San Diego, CA, 31 January 2013).

[68] GAO recommendations.

[69] GAO recommendations.

[70] GIG NetOps, 1.

[71] Chairman, Joint Chiefs of Staff, *Modification to EXORD to Implement Cyberspace Operations Command and Control Framework*, Directive, November 14, 2014, 2.

[72] Government Accountability Office, *Department of Defense Cyber Efforts: More Detailed Guidance Needed to Ensure Military Services Develop Appropriate Cyberspace Capabilities.* (Washington, DC: Government Accountability Office, 2011), 16, http://www.gao.gov/products/GAO-11-421.

[73] Joint Force Headquarters-DODIN, *Executive Overview: DOD Information Network (DODIN) Operations and Defense C2 Framework and the Role of Joint Force Headquarters-DODIN*, January 5, 2015, 4.

[74] JFHQ-DODIN exec, 5.

[75] Chairman, Joint Chiefs of Staff. *Execute Order to Implement Cyberspace Operations Command and Control Framework*. Execute Order. June 21, 2013 and Mod to EXORD.

[76] JFHQ-DODIN exec, 4.

[77] JFHQ-DODIN exec, 4.

[78] JFHQ-DODIN exec, 4.

[79] Mod to EXORD, 2.

[80] Mod to EXORD, 3.

[81] Mod to EXORD, 3.

[82] JFHQ-DODIN exec, 9.

[83] Patricia Rinaldi, Colonel, USAF, Joint Force Headquarters-DODIN, J5, phone interview by author, February 6, 2015. Additionally, Col Rinaldi was previously assigned as the Director, Joint Operations Center, USCYBERCOM.

[84] Phone interview, Col Rinaldi.

[85] JFHQ-DODIN exec sum, 9.

[86] JFHQ-DODIN exec sum, 9.

[87] JFHQ-DODIN exec sum, 9.

[88] Todd Beckman, (Chief, Field Operations Support Branch, Operations Directorate, DISA) personal interview by author, January 16, 2015. Beckham was previously assigned as the Technical Advisor for Enterprise Operations Center-Europe (EOC-Europe). He was part of the initial operational capability of the first EOC.

[89] *Information Technology and Cyber Operations: Modernization and Policy Issues in a Changing National Security Environment: Hearing before the Senate Armed Services Subcommittee*. 113th Cong., 10 (2014) (Gen Keith B. Alexander, Commander, U.S. Cyber Command).

[90] Ibid, 10.

[91] Ibid, 10 and. Hollis, David M, "USCYBERCOM: The Need for a Combatant Command versus a Subunified Command," *Joint Force Quarterly* 58, (3rd quarter 2010), 51.

[92] Congress, Title 10, section 167, 112.

[93] U.S. Department of Defense, *The Department of Defense Strategy for Implementing the Joint Information Environment*, (Washington, DC: Office of the Department of Defense Chief Information Officer, September 2013), 1.

[94] Phone interview, Col Rinaldi.

[95] Personal interview, Todd Beckman.

Bibliography

Armed Forces. U.S. Code. Title 10, Vol. III, Sec 166 (2011).

Barker, Robert. "Command and Control of Network Operations." Master's Thesis, U.S. Army War College, 2009. http://www.dtic.mil/.

Beckham, Todd. Chief, Field Operations Support Branch, Operations Directorate, DISA. Personal interview by author. January 16, 2015.

Carter, Ashton. Deputy Secretary of Defense. Disestablishment of Assistant Secretary of Defense for Networks and Information Integration (ASD(NII)) and Related Matters. Memorandum, 11 January 2012.

Casey, George. Director of Joint Staff. Promulgation of Unified Command Plan 2002 (with Change-1 and Change-2 incorporated). Memorandum, 4 February 2003.

Chairman, Joint Chiefs of Staff. *Modification to EXORD to Implement Cyberspace Operations Command and Control Framework*. Execute Order. 14 November 2014.

Chairman, Joint Chiefs of Staff. *Execute Order to Implement Cyberspace Operations Command and Control Framework*. Execute Order. 21 June 2013.

Charney, Scott, Langevin, James, et al. "Cybersecurity Two Years Later." Working Paper, Center for Strategic and International Studies, 2011.

Cole, Ronald, Drea, Edward, et al. *History of the Unified Command Plan 1946-2012*. Officer of Chairman of Joint Chiefs of Staff. Last modified 2013, http://dtic.mil/doctrine/doctrine/history/ucp.pdf.

Department of Defense Chief Information Officer Desk Reference. Volume 1. August 2006. http://dodcio.defense.gov/Portals/0/Documents/ciodesrefvolone.pdf.

Feickert, Andrew. *The Unified Command Plan and Combatant Commands: Background and Issues for Congress*. CRS Report for Congress R42077. Washington, DC: Congressional Research Service, 3January 2013. http://fas.org/sgp/crs/natsec/R42077.pdf.

Headquarters Department of Defense. *National Military Strategy for Cyberspace Operations*. Washington, DC: Department of Defense, 11 December 2006.

Headquarters Joint Staff, *Cyberspace Operations*. JP 3-12(R). Washington, DC: Joint Staff, 5 February 2013.

Headquarters Joint Staff. *Department of Defense Dictionary of Military and Associated Terms*. JP 1-02. Washington, DC: Joint Staff, 15 December 2014.

Headquarters Joint Staff. *Doctrine for the Armed Forces of the United States*. JP 1. Washington, DC: Joint Staff, 25 March 2013.

Headquarters U.S. Marine Corps. *Command and Control*. MCDP 6-0 Washington, DC: U.S. Marine Corps, 4 October 1996.

Headquarters, U.S. Strategic Command. *Joint Concept of Operations for Global Information Grid NetOps,* 10 August 2005.

Historical Office, Office of the Secretary of Defense. *Department of Defense Key Officials 1947-2014*. Washington, DC: Department of Defense, June 2014.

"History." *U.S. Strategic Command*. Last modified August 2014. http://www.stratcom.mil/history/.

Hollis, David M. "USCYBERCOM: The Need for a Combatant Command versus a Subunified Command." *Joint Force Quarterly* 58 (3rd quarter 2010): 48-53.

Hollis, David M. USCYBERCOM National Capital Region, Chief of Staff. Phone interview by author. April 10, 2015.

Hoyle, S.M. “Network Operations Command and Control.” PowerPoint Presentation. Plans, Policies, and Orders, Headquarters, Marine Corps, Arlington, VA, 12 June 2014.

Joint Chiefs of Staff. *Definition of Operational Command and Operational Control*. Last modified, 30 April 1975. http://www.dod.mil/pubs/foi/joint_staff/jointStaff_jointOperations/265.pdf.

Joint Force Headquarters-DODIN. *Executive Overview: DOD Information Network (DODIN) Operations and Defense C2 Framework and the Role of Joint Force Headquarters-DODIN*. January 5, 2015.

Keith, Stephanie. “Cyberspace Workforce.” PowerPoint presentation. AFCEA West, San Diego, CA, 31 January 2013.

Limbert, Matthew, Lieutenant Colonel, USMC (formerly Regional Command (SouthWest) C-6 Operations Officer). Email interview by author. March 4, 2015.

“Our History: The Beginnings.” *Defense Information Systems Agency*. Last accessed January 19, 2015. http://www.disa.mil/about/our-history

“Recommendations for Executive Action.” U.S. Government Accountability Office. Last modified 1 July 2014. http://www.gao.gov/products/GAO-11-421.

Rinaldi, Patricia, Colonel, USAF, (Joint Force Headquarters-DODIN, J5). Phone interview by author. February 6, 2015.

Rumsfeld, Donald, Secretary of Defense. Office of Secretary of Defense to Director of Defense Information Systems Agency. Assignment and Delegation of Authority to Director Defense Information Systems Agency. Memorandum, 18 June 2004.

U.S. Congress. House. *Information Technology and Cyber Operations: Modernization and Policy Issues in a Changing National Security Environment: Hearing before the Senate Armed Services Subcommittee*. 113th Cong., 2014.

U.S. Congress. Senate. *Statement of General Keith B. Alexander Commander United States Cyber Command: Hearing before the Senate Armed Services Subcommittee*. 113th Cong., 2013.

U.S. Department of Defense. *Defense Information Systems Agency* (DISA). Directive 5105.19, 25 July 2006.

U.S. Department of Defense. *The Department of Defense Strategy for Implementing the Joint Information Environment*. Washington, DC: Office of the Department of Defense Chief Information Officer, September 2013.

U.S. Government Accountability Office. *Department of Defense Cyber Efforts: More Detailed Guidance Needed to Ensure Military Services Develop Appropriate Cyberspace Capabilities*. Washington, DC: Government Accountability Office, 2011. http://www.gao.gov/products/GAO-11-421

Warner, Michael. "Notes on the Evolution of Computer Security Policy in the US Government, 1965-2003." Paper presented at Charles Babbage Institute supported by the National Science Foundation's Computer Security History Workshop, July 2014.