NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

SPECIAL OPERATIONS FORCES UNILATERAL CONDUCT OF CYBERSPACE OPERATIONS

by

Anthony W. Bovino

December 2020

Thesis Advisor:	Ryan Maness
Co-Advisor:	Neil C. Rowe

THIS PAGE INTENTIONALLY LEFT BLANK

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

1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** December 2020	**3. REPORT TYPE AND DATES COVERED** Master's thesis

4. TITLE AND SUBTITLE SPECIAL OPERATIONS FORCES UNILATERAL CONDUCT OF CYBERSPACE OPERATIONS	**5. FUNDING NUMBERS**
6. AUTHOR(S) Anthony W. Bovino	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.	**12b. DISTRIBUTION CODE** A

13. ABSTRACT (maximum 200 words)

This thesis examines the use of cyberspace operations by special operations forces to address the threats the United States faces from adversaries. Special operations forces need to conduct cyberspace operations to sustain their battlefield advantage, compete with adversary capabilities, and protect their personnel. Special operations forces are not fully resourced to conduct tactical-level cyberspace operations. A questionnaire was created to assess how well special operations forces were equipped with the capabilities and authorities to conduct cyberspace operations on their own and with the Joint Service. The questionnaire was delivered to special operations units, United States Special Operations Command (USSOCOM) elements, United States Cyber Command (USCYBERCOM) elements, and other cyberspace-related organizations in the Department of Defense (DOD). Analysis of the questionnaire concluded that several resourcing problems impede special operations forces from conducting cyberspace operations, including doctrinal problems at the strategic, operational, and tactical levels. Recommendations are made to address the key policy and resourcing constraints.

14. SUBJECT TERMS special operations forces, cyberspace operations, cyberspace operations authorities	**15. NUMBER OF PAGES** 61
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89) Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

SPECIAL OPERATIONS FORCES UNILATERAL CONDUCT OF CYBERSPACE OPERATIONS

Anthony W. Bovino
Lieutenant Commander, United States Navy
BSB, Virginia Tech, 2004

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN CYBER SYSTEMS AND OPERATIONS

from the

NAVAL POSTGRADUATE SCHOOL
December 2020

Approved by: Ryan Maness
Advisor

Neil C. Rowe
Co-Advisor

Alex Bordetsky
Chair, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This thesis examines the use of cyberspace operations by special operations forces to address the threats the United States faces from adversaries. Special operations forces need to conduct cyberspace operations to sustain their battlefield advantage, compete with adversary capabilities, and protect their personnel. Special operations forces are not fully resourced to conduct tactical-level cyberspace operations. A questionnaire was created to assess how well special operations forces were equipped with the capabilities and authorities to conduct cyberspace operations on their own and with the Joint Service. The questionnaire was delivered to special operations units, United States Special Operations Command (USSOCOM) elements, United States Cyber Command (USCYBERCOM) elements, and other cyberspace-related organizations in the Department of Defense (DOD). Analysis of the questionnaire concluded that several resourcing problems impede special operations forces from conducting cyberspace operations, including doctrinal problems at the strategic, operational, and tactical levels. Recommendations are made to address the key policy and resourcing constraints.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF ACRONYMS AND ABBREVIATIONS

AFSOC	Air Force Special Operations Command
AISUM	Artificial Intelligence for Small Unit Maneuver
CCIR	Commanders Critical Information Requirements
CO-IPE	Cyberspace Operations Integrated Planning Element
CONOP	concept of operation
DOD	Department of Defense
DODIN	Department of Defense Information Network
DOTMLPF	doctrine, organization, training, materiel, leadership, personnel, facilities
FRAGO	fragmentation order
JCIDS	Joint Capability Integration and Development System
JIPOE	Joint Intelligence Preparation of the Operational Environment
JSOC	Joint Special Operations Command
MARFORCYBER	Marines Forces Cyber Command
MARSOC	Marine Special Operations Command
NAVSPEC-WARCOM	Naval Special Warfare Command
NITRD	Networking and Information Technology Research and Development
NSPM	National Security Presidential Memorandum
OPORD	operation order
PED	process, exploit, disseminate
PPD	Presidential Policy Directive
USAFRICOM	United States Africa Command
USASOC	United States Army Special Operations Command
USCENTCOM	United States Central Command
USCYBERCOM	United States Cyber Command
USPACOM	United States Pacific Command
USSOCOM	United States Special Operations Command
USSTRATCOM	United States Strategic Command

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

This work would not have been possible without the compassion and strength bestowed on me by my Lord and Savior Jesus Christ. “When you saw only one set of footprints in the sand, it was then that I carried you.”

I would like to thank my wife, my best friend, and my partner in all things, Samantha. Your unshakable work ethic was an inspiration to me throughout this process. You provided me encouragement at just the right times, a talent of yours for which I am forever grateful.

I would like to thank my mother and father, Ray and Sue. Thanks for believing in me, more than I believed in myself at times. You’ve provided me the inspiration to accomplish work on this scale.

I would like to thank my advisors, Dr. Rowe and Dr. Maness. I can’t thank you enough for the patience, support, and attention you have given me throughout. The process was just as beneficial as the end product. I am a better writer, researcher, and student as a direct result of your mentorship.

I would like to thank members of the special operations community that supported my research. Your inputs were the engine for this project. I hope it can benefit you as we all carry the mission forward.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

Special operations forces are part of the Joint Services for missions in hostile and politically sensitive environments as defined by Joint Publication 3-5, Special Operations (Joint Chiefs of Staff [JCS], 2014). Accordingly, special operations must have unconventional and technically advanced capabilities available for their missions to sustain their competitive edge over the adversary. Joint Publication 3-5 says that special operations should support theater and national objectives, and therefore must complement the capabilities of conventional forces assigned to the functional and geographic combatant commands. Special operations should not substitute for conventional military forces, but should enhance all kinds of warfare in a theater, including those in the cyberspace and information domains. Most cyberspace operations are performed by forces assigned to United States Cyber Command (USCYBERCOM). Appropriately resourced forces outside of USCYBERCOM are also authorized to conduct cyberspace operations. This includes force assigned to United States Special Operations Command (USSOCOM), and other military units operating at the tactical edge.

Cyberspace operations are a vital component today of a nation's information operations and political warfare. Cyberspace operations can be scoped to have operational effects at the tactical through strategic levels. Accordingly, special operations forces must integrate cyberspace operations into their normal repertoire of capabilities to sustain a competitive battlefield advantage. Compared to their conventional military counterparts, special operations complete their assigned tasks using tactically focused methods underpinned by small-unit operations, technical and cutting-edge capabilities, and other factors that enhance speed and lethality of the missions they execute. Special operations are typically high-risk, constrained by time, and can be clandestine and covert. To achieve their objectives, technical special operations tradecraft must be coupled with non-standard capabilities.

With the emergence of cyberspace as a warfare domain, special operations forces no longer have a technology advantage against their peer adversaries, since proximity to enemy combatants is unnecessary for the delivery of cyber effects. Although not officially

documented, there is a consensus within the Department of Defense (DOD) that special operations forces and other military units must unilaterally perform cyberspace operations to accomplish tactical objectives, promote unit security, and enhance DOD partner-agency missions. These forces lack the operational doctrine, equipment, or trained personnel for cyberspace operations by themselves. This thesis examines governing DOD cyberspace doctrine for support of unilateral special operations cyberspace operations, DOD partner agency support to special operations conduct of cyberspace operations, and USSOCOM support of cyberspace operations.

A. HYPOTHESIS

Special operations forces cannot perform their own unilateral cyberspace operations for several reasons. First, DOD organizations have debated what organizations should own the tools and authorities for cyberspace operations. Policy ambiguity by USCYBERCOM and the enterprise-level DOD must be overcome to allow special operations to meaningfully use cyberspace operations. Second, the special operations community needs to build cyberspace-operations capabilities. Recruitment and training of personnel familiar with both special operations and cyberspace operations is difficult due to the cultural differences between the two communities. Cyber tools designed to support special operations must be developed for their unique and low-density missions. Third, institutional knowledge is lacking on how special operations can integrate cyberspace operations into campaigns. Ground-force commanders are unaware how to request cyberspace operations, and how they can complement or enable tactical operations.

The hypothesis proposed in this thesis is that, if appropriately resourced, special operations forces can capitalize on cyberspace operations to achieve tactical and strategic objectives and enhance unit safety.

B. RESEARCH QUESTIONS

- How well does current DOD cyber-operations doctrine, partner agency support, and man, train, and equip resourcing allow special operations units to conduct cyber operations at the required operational pace? Are

appropriate technical mechanisms in place to get appropriate and properly vetted cyber targets?

C. PURPOSE AND SCOPE

This research assessed the adequacy of manning and technical capabilities in USSOCOM operational units that conduct cyberspace operations. It examined cyberspace-operation authorities and approval mechanisms for special operations. It examined the relationship between USCYBERCOM and USSOCOM, and assessed the level of operational support and capability development that USCYBERCOM dedicates to special operations. The research also examined doctrinal and resource challenges facing special operations units operating at the tactical edge of operations. Specific recommendations are made for the policy and resource changes required to modernize USSOCOM's cyber workforce so that USSOCOM units conducting cyberspace operations can assess the capability requirements, doctrinal amendments, and level of support needed from partner agencies in a modern cyber-warfare capability.

D. OUTLINE OF THE THESIS

This thesis begins with a literature review of cyberspace operations and special operations doctrine. This review identifies key institutional issues impeding unilateral cyberspace operations in special operations. It highlights USCYBERCOM responsibilities to conduct cyberspace operations for partner agencies, and to support cyber warfare capability development across the DOD. The literature review identifies previous academic work on cyberspace operations for special operations, and locates current gaps in governing and academic literature related to the topic.

We distributed a questionnaire to special operations units to identify operational impediments in the cyber warfare domain. An assessment was made on the manning, training, and equipment adequacy of special operations cyberspace operators to identify deficiencies. The questionnaire was used to guide interviews with special operations units, USCYBERCOM entities, and other tactical units on their ability to perform cyberspace operations. Its goal was to measure the effectiveness of current USSOCOM cyberspace operations and support to current special operations cyberspace operations, and we

recommend how to fix specific resource deficiencies. The reporting on these operations was also examined to determine if lessons are being learned and operational limitations are being resolved. We tried to identify if similar limitations exist for other units operating at the tactical edge of maritime, ground, and air domains.

Chapter II examines the applicability of cyberspace operations doctrine and case work for special operations. Chapter III interviews special operations units that conduct cyberspace operations for data about mission accomplishment. Chapter IV shows the results of the questionnaire and describes current practice. Chapter V gives conclusions and recommendations for future work.

II. RELATED WORK

Cyberspace is physical computing components that are logically connected through a networked medium. For the DOD, Cyberspace operations include “military, intelligence, and ordinary business operations in cyberspace” (JCS, 2018a, p. II-1). Military operations in cyberspace can aid a commander’s objective (JCS, 2018a). Examples of their effects include force projection against targets in the physical or logical domain, intelligence development, and defensive actions to preserve friendly-force networks. Special operations differ from conventional military operations, as they require “unique modes of employment, tactics, techniques, procedures, and equipment” (JCS, 2014, p. I-1). Core special operations activities include direct actions against enemy combatants, special-reconnaissance operations, unconventional warfare, hostage rescue and recovery, counter-insurgency operations, civil affairs operations, and humanitarian aid. An example of a special operations cyber operation could be the manipulation of an adversary surveillance system during a direct-action raid. The limited quantity of previous work on tactical cyberspace operations, and lack of special operations language in the governing cyber doctrine, make it difficult to research cyberspace operations by special operations units.

Cyberspace is a relatively new warfighting domain. Cyber doctrine, legislation, and tactics are dynamic entities, driven by evolving policy and technical considerations. Many open-source, academic, and government publications address cyber warfare from a strategic perspective. With tight budgets, DOD must address great-power competitions, safeguard critical infrastructure, and maintain operations in the cyber domain. Special operations cyberspace operations are a lower priority for Pentagon strategists as they are not routinely needed in a tactical environment. The lack of tactical-level cyber-operations doctrine and a lack of awareness of offensive cyberspace capabilities by warfare commanders contribute to this.

The special operations community has a unique opportunity to shape macro-level cyber operational doctrine. Some nations routinely commit cyber-enabled intellectual theft and political coercion without following rules of engagement in the cyber domain. Given the lack of domestic and international consensus on what is a cyberattack, tactical and

granular explorations of cyber warfare are limited. A United Nations consortium of experts on international cyber-operations law convened in 2013 to develop the Tallinn Manual (Schmitt, 2013). The Tallinn Manual is a working set of international norms and governance for cyber warfare. However, the laws are non-binding for members outside of the United Nations. Furthermore, as several case studies within it point out, member-nations routinely conduct cyberspace operations that do not rise to the level of force to avoid culpability under the laws. "A cyber-operation constitutes a use of force when its scale and effects are comparable to non-cyber operations that include a use of force" (Schmitt, 2013, p. 45). Tactical cyberspace operations in destabilizing information campaigns are not directly addressed in this work.

A. CYBER STRATEGY

The *Cyberspace Solarium Commission Report* indicates the United States lacks a unified strategy for combating public and private attacks in cyberspace (King et al., 2020). This deficiency is seen in the gaps related to tactical cyberspace-operations doctrine. Nation-state adversaries and violent extremist organizations use effective and low-cost cyberspace operations to match the United States technical and financial advantages in cyberspace. Due to their close physical placement to adversaries of these types, properly equipped special operations forces could combat these threats. The emergence of endpoint technologies such as internet-of-things devices, 5G cellular technology, and mesh networks suggest special operations forces could be the logical combatant for these targets. The report attributes disparate cyber-security strategies among USCYBERCOM, the Cybersecurity and Infrastructure Agency, the public and private sectors, and other organizations as a barrier to protecting American interests in cyberspace. It lists several factors contributing to why the United States government does not effectively collaborate with outside entities. The United States government does not have a declared public policy on cyber-attack responses. Exchanging information with the private sector is hampered by classification issues. Despite improved guidance from National Security Presidential Memorandum (NSPM) 13 that endorses a forward defense posture in cyberspace, many government institutions still struggle with securing all interests in cyberspace (White

House, 2018). These issues compound the unilateral conduct of cyberspace operations by special operations forces.

The report also says “Specifically, DOD should develop the capacity to provide decision makers with cyber options, including options to support crisis bargaining and response that are independent of and do not rely on existing cyber campaign plans and the forces already committed to them” (p. 112). This reaffirms that special operations forces must have cyber-warfare options available to accomplish their core activities. It also says “A prerequisite to keeping pace with them and anticipating their behavior, rather than simply reacting and responding to it, is gaining and maintaining access against defined targets and pursuing adversaries as they maneuver” (p. 112). The report also says that the National Security Agency’s role as a combat support agency should be supporting Title 10 and that cyberspace operations at the tactical and operational level should be assessed. These statements imply that expeditionary forces, including special operations forces, should be properly equipped with cyberspace capabilities.

B. CYBER OPERATIONS

In 2009, the DOD established USCYBERCOM to plan offensive and defensive cyber warfare. USCYBERCOM was created as a sub-unified combatant command subordinate to USSTRATCOM in June 2009, and was elevated to a full unified command in August 2018. The cyber domain is increasingly contested due to the ability of many nation-states to cheaply and remotely attack military, civilian, and financial infrastructure.

General DOD guidance calls for U.S. cyber forces to operate alongside land, sea, air, and space forces. Joint Publications governing cyberspace operations and special operations identify methods and terms for warfare (JCS, 2014). However, doctrine does not specifically identify how cyber will support special operations. Another publication says that cyberspace operations can support air, land, maritime, space, and special operations (JCS, 2018a). However, it does not explain how to request operational support or technical-capability development.

The U.S. DOD cyberspace operations doctrine is in Joint Publication 3-12 (JCS, 2018a). It describes military operations in the cyberspace domain and identifies DOD

combat forces, intelligence agencies, and support entities that plan, approve, and execute cyberspace operations. The organizations identified are members of the military intelligence community with large-scale operational technology that can be used in strategic operations. The doctrine discusses the integration and synchronization of cyberspace capabilities across a range of military operations, and identifies the roles and responsibilities of the other combatant commanders to ask for USCYBERCOM capabilities.

Joint Publication 3-12 highlights several issues necessary to fully integrate cyberspace operations into joint targeting. These include the need for centralized planning to synchronize cyberspace operations with kinetic operations and fires in the operational environment, de-confliction between government entities, and a thorough understanding of cyberspace-operations planning by commanders. If multiple agencies have the same target in cyberspace, uncoordinated actions could produce reduced effectiveness, lost intelligence, unintended detection, or complete compromise of the mission. Tactical actions in cyberspace rely on effects that are confined to a local area, but the risk of collateral effects is increased in cyberspace. A clearly articulated capability deficiency that outlines the need to conduct cyberspace operations below the combatant-command level could be entered into the Joint Capabilities Integration and Development System (JCIDS).

Cyberspace operations vary in their function and intent. Special operations could significantly help the Joint Targeting Cycle (JTC) with remote cyberspace operations. One publication calls for offensive maneuvers such as cyberspace attack to be synchronized and de-conflicted during targeting (JCS, 2018a). However, it says that USCYBERCOM is in charge of joint targeting in cyberspace, and does not address the similar capabilities of USSOCOM. This omission leaves a considerable gap in the chain of responsibility among Joint Services for cyberspace operations.

Cyberspace is part of the information environment that affects all parts of physical warfighting. Special operations forces can include cyberspace operations among their specialized capabilities to expand their commanders' offensive options, enhance unit security, and achieve both tactical and strategic cyber effects. Cyberspace operations can affect the physical and logical components of an adversarial computer system, or target

data in computer systems by modifying it. Effects can be logical or physical. An appropriate comparison between physical and logical effects are the 2014 Office of Personnel Management data breach versus the 2010 Stuxnet attacks. U.S. Government personnel data was stolen from the Office of Personnel Management on a massive scale by Chinese actors, and it had a logical effect (Office of Personnel Management, n.d.). The 2010 Stuxnet attacks targeted a Siemens programmable logic controller in an Iranian nuclear facility and the physical process of uranium refinement, so it had a physical effect (Hughes, 2018, Chapter 6, p. 80, para. 3).

The "cyber persona layer" of cyberspace is information that identifies a person by email addresses, online login credentials, and IP addresses. Exploitation of it can enable access to physical and logical components of an adversary computer system independent of the scale of the target. Operational cyber technology applied by special operations units could develop targets and enable cooperation with USCYBERCOM entities better equipped to handle larger-scale problems discovered at the tactical level.

Militaries can use cyberspace operations to influence the information environment in an integrated campaign. Since 2007, peer adversaries of the United States have conducted cyber operations and information wars to achieve their national interests. The 2007 Russian attacks against Estonia were the first known use of a cyber-capability to achieve a strategic effect, when the Russian government and civilian hackers temporarily hurt the Estonian government and the country's financial infrastructure (Conner and Vogler, 2017). In 2013, Russia combined cyber operations, electronic warfare, and information operations while invading Ukraine. They used an integrated information-operations campaign to target Ukrainian-soldier communications and Ukrainian military networks; denial of service, social-media manipulation, and interception of communications disrupted basic Ukrainian military operations (Brantly et al., 2017). Russia coupled their tactical information-operation efforts with wide-scale disinformation campaigns. They paid millions to troll-farms to post pro-Russian messages on social media sites, blogs, and forums that were critical of Russian actions (Duggan, 2015). These combined operations greatly overmatched their Ukrainian adversaries without provoking a Western military response.

Cyberspace operations by the Combatant Commanders and the Joint Services can also affect the logical and physical warfighting domains (JCS, 2018a). These operations include offensive cyberspace operations, defensive cyberspace operations, and DOD information-network operations (DODIN). Offensive cyberspace operations try to deny, degrade, or destroy physical or virtual infrastructure to achieve military objectives. A Title 10 military offensive cyberspace operation is defined as a mission, conducted outside of friendly-force cyberspace, which exhibits an intent other than defending that space against an imminent threat. It targets adversarial computing capabilities in the logical and physical domains. An offensive action can target a single electronic device or an entire military information system. The effect can range from denial of service against a wireless device to a complex network infiltration to sustain an undetected presence. The tactical environments of special operations forces suit small-scale cyberspace operations, but the forces could aid cyberspace target refinement and handoff for cyber operations that have strategic implications. The recent 2018 revocation of Presidential Policy Directive (PPD) 20 and its replacement with NSPM-13 could signal a change in United States cyber strategy. Recent overt cyber-operation actions by the United States against Russia (Balmforth, 2019) show a shift towards forward defense and persistent engagement, consistent with the updated 2018 DOD Cyber Strategy. Special operations forces could capitalize on this shift in policy that might aid tactical-level cyberspace operations.

Defensive cyberspace operations can defend military information systems from threats in cyberspace (JCS, 2018a). The USCYBERCOM Cyber Protection Force protects the DODIN and related cyberspace. The physical infrastructure and accompanying personnel required to defend a military network are beyond the scope of what special operations forces can do, so we will not discuss them.

The DOD and intelligence agencies also perform cyberspace operations for theater and national-intelligence priorities (JCS, 2018a). Intelligence functions in cyberspace are typically Title 50 operations and can be conducted by either military personnel or civilians. The National Security Agency provides intelligence support to cyberspace operations at the tactical and operational levels.

C. SPECIAL OPERATIONS AND CYBER OPERATIONS

Doctrine (JCS, 2018a) does not specifically identify how USCYBERCOM will support USSOCOM, the organization that mans, trains, and equips special operations forces and provides combat forces to the geographical combatant commanders. The responsibility of providing forces while manning, training, and equipping is unique to USSOCOM (JCS, 2014). USSOCOM also has its own cyberspace capabilities. Thus, support mechanisms between USCYBERCOM and USSOCOM must be specified.

Previous work identified a lack of organic cyberspace-operations manning and technical capabilities at the U.S. Army Special Operations Command (USASOC) (Rivera, 2019.) Special operations forces below the combatant-command level do not have a permanent cyber-workforce assigned to their force structure. The other branches of the Joint Service are experiencing the same deficiency, which will be discussed in Chapter III. Rivera identified that USCYBERCOM cannot dedicate resources to supporting tactical-cyberspace operations. There is a gap in the ability to conduct tactical-level cyberspace-operations despite the requirement to perform them.

Special operations forces must thoroughly understand what authorities govern cyberspace operations based on the intent of the requested operation. Beyond classification issues, cyberspace operations can use the same commands to accomplish Title 50 intelligence missions as they do for Title 10 offensive missions. Scanning, enumeration, sustaining a presence on a network, installing payloads, and other operations can straddle the line between Title 10 and Title 50 based on degree of intrusiveness, political sensitivity, risk of detection, collateral effects, and other considerations. Once a mission planner can determine the relevant authorities, the approval chains diverge for intelligence gathering versus offensive effects, and civilians cannot perform most offensive actions in cyberspace that rise to the level of force. Another issue is that Title 10 operations require an approved CONOP (concept of operation) to execute at the strategic and operational levels, but the authority for Title 10 cyberspace operations is held by Operational Orders (OPORD) and Fragmentary Orders (FRAGO) at the geographic combatant-command level. Depending on sensitivity of the offensive operation and its potential collateral effects, the CONOP

may require a higher approval level than that of a local commander. Hence, offensive cyberspace operations may be slow to execute.

Special operations missions can be amplified by cyberspace operations (Duggan & Oren, 2016). Targeting in the cyber domain can enhance the lethality of direct-action missions. Increased connectivity resulting from networked warfare at the tactical level can promote trust and interoperability with partner forces. Cyberspace operations can help special operations forces interpret events and recognize disinformation. These types of cyberspace operations require the unique access and placement of special operations forces.

All commanders now can consider requesting or conducting cyberspace operations to aid their missions. The Commander of USCYBERCOM is the coordinating authority for cyberspace operations that defend DOD networks and military cyberspace operations in adversarial cyberspace (JCS, 2018a). The National Security Agency is tasked with signals-intelligence and cyber-security support to USCYBERCOM. For theater-specific cyberspace operations, USCYBERCOM can be either the supporting or supported commander. This means that it must support commanders requiring cyberspace operations to achieve their objectives. Conversely, units at the tactical edge of operations must support USCYBERCOM if they can; their operations do routinely place them near adversarial cyber targets.

1. Administrative Obstacles

A challenge for integration of cyberspace and conventional operations is that personnel planning the technical details of a cyberspace operation may not understand its contribution to a larger military campaign, and commanders may not know how to request and integrate cyber effects into their campaigns. One article attributes this disconnect to weaknesses in professional military education on both sides (Bender, 2013). USCYBERCOM has the responsibility to educate their technical experts on how to integrate cyber maneuvers into the operational military culture and to develop a curriculum within professional military education.

Previous work examined how well USSOCOM's resources for special operations and cyber operations addressed the current operating environment (Tebedo, 2016). It concluded that special operations require additional internal or external capabilities, but could not determine if USCYBERCOM could provide them. It also investigated whether the core USSOCOM missions of precision strikes and special warfare could be improved through cyberspace operations. It concluded that they could, and made a case for using the asymmetric nature of cyberspace operations to strengthen the twelve kinds of surgical strikes to include direct action, special reconnaissance, counterinsurgency operations, and the remaining core activities. It also argued that cyber operations are ineffective unless they are coupled with action in the physical domain.

Another question examined by Tebedo was whether USCYBERCOM's support teams sufficed for cyber support to special operations, but the analysis was inconclusive. It does recommend that if USSOCOM needed an internal cyberspace-operations capability, reorganization of an existing special operations unit would be the best option, given budgetary constraints (Tebedo, 2016). They suggested reorganizing USASOC Civil Affairs Brigade into a USSOCOM cyber team. Clearly, barriers to special operations forces efficiently conducting cyberspace operations exist. DOD-wide policy limitations, disparate operational strategies, and lack of institutional knowledge are contributing factors. USCYBERCOM is focused on warfare against nation-state adversaries and its resources are committed to sustaining a competitive advantage in strategic operations. DOD doctrine incompletely specifies how special operations forces and other units operating at the tactical edge should perform cyberspace operations. A declared policy on how the United States should approach cyber security and cyberspace operations is lacking. Congress, the public sector, and private industry agree that a broad approach is needed to combat the diverse threats found in cyberspace.

2. Targeting Limitations

Targeting in the cyber domain is not a refined process within the DOD, since cyber munitions are not guaranteed to be reliable. Adversaries patch system vulnerabilities through periodic updates, and adapt to the tactics, techniques, and procedures used against

them, as the DOD and National Intelligence Community do in response to attacks. Given these considerations, sustaining a competitive advantage in the cyber domain is challenging on a small scale.

Geographic combatant commands and USCYBERCOM follow the Joint Targeting Cycle, which puts targets into the theater campaign plan. Targets are nominated based on the planning and intelligence considerations for the theater of operations. Intelligence functions such as the Joint Intelligence Preparation of the Operational Environment (JIPOE), country assessments, and threat assessments are used (JCS, 2018b). This information refines the Commander's Critical Information Requirements (CCIR), which support decision-making at all levels within the theater. The Combatant Commander then directs operations by subordinate commanders against the vetted targets.

Geographic Combatant Commanders nominate targets based on the intelligence, including those in the cyber domain. However, when the Combatant Commander does not unilaterally own the forces that can strike a cyber-target within their theater, a request must be generated for support from outside functional commanders like USCYBERCOM. Although the Geographic Combatant Commander may wish to fire against a target in their theater, they may not have complete authority to do so if using a cyber capability.

For example, the Combatant Commander can nominate a country's cellular infrastructure for targeting if it is used for enemy command and control and thus can be considered a legitimate target. A cellular infrastructure is a networked system containing transceiver stations, gateways, and potentially millions of user devices, all of which are potential targets. The infrastructure could be targeted on a large scale by destroying control centers and major relay points within the network using kinetic means such as a strike-warfare capability. The Combatant Commander could authorize this and conduct the operation with forces assigned to the theater. Alternatively, the infrastructure could be targeted by cyber means through its connection to the Internet; the connection could be interrupted, taking the system offline temporarily or permanently, or malicious code could be injected at the user level to propagate upstream to vital network nodes. The Combatant Commander must request support from outside entities to do this. This additional coordination may impede timely execution of a mission.

3. Collateral Limitations

Another challenge with targeting is that a target like the cellular network is used by enemy actors, but it is also part of a country's legitimate communications network used for commerce, government administration, emergency services, and other routine communications. The virtual battlespace is challenging to separate from innocent use by civilians. This differs from targeting in the physical domain, where military objectives can be more clearly isolated. Joint targeting doctrine requires that force be proportionate, timely, and minimize collateral effects against non-combatants. A carefully engineered cyber-munition is more likely to achieve this. Therefore, a cyber capability must be suitably complex for use in the intended target environment, and must balance legal considerations with effectiveness against the enemy.

4. Technical Limitations

The reliability of cyber capabilities must be factored into their use by special operations forces. Capabilities depend on hardware vulnerabilities, software vulnerabilities, and human vulnerabilities. Cyber operators exploit those found in network appliances, end-user devices, and internet-of-things devices. The degree of success in exploitation varies depending on how often users update operating systems and application software. The more actively is a networked managed, the lower the probability of success in its exploitation. If the network is actively managed, detection by the adversary is more likely. In a time-constrained environment, tactical forces would need capabilities that are suitable for the speed of special warfare. Cyberspace operations requiring a sustained network presence and time-consuming technical development are better suited for strategically aligned and equipped forces. USCYBERCOM is best postured to make the decision whether cyberspace operations can proceed, as it performs the bulk of DOD intelligence missions in cyberspace. Accurate cyber threat intelligence is required to understand enemy capabilities, courses of action, and behaviors in both the physical and logical domains (Dickinson, 2016, para. 3). This process shapes future offensive and defensive cyberspace operations (Dickinson, 2016, para. 4). Under USCYBERCOM, the Commanders of the Joint Forces Headquarters-Cyber refine intelligence requirements,

provide tactical courses of action, and integrate cyberspace operations into theater campaigns (JCS, 2018a). Joint Publication 3-12 directs the other combatant commands to integrate cyberspace capabilities into military operations by coordinating with USCYBERCOM. Absent narrow, theater-specific guidance, USCYBERCOM has the final say regarding the feasibility of cyberspace operations, even if the adversarial cyber-target exists in the physical space of a geographic combatant command. USSOCOM forces and the geographic combatant commands they are assigned to would have to seek legal advice from a Judge Advocacy Group to pursue operations not approved by USCYBERCOM. USSOCOM forces could propose alternative actions based on cyber threat intelligence produced by USCYBERCOM, and operational intelligence produced through other means.

III. INTERVIEW QUESTIONS AND RESULTS

A. QUESTIONNAIRE

A questionnaire was developed to examine how well special operations forces are formulating and executing cyberspace operations. The questions are broadly focused on the authorities, capabilities, and resourcing that special operations forces require to conduct cyberspace operations. The questions also address cyberspace-operations support by entities outside of USSOCOM.

Our distribution of the questionnaire to USSOCOM program offices, special operations units, USCYBERCOM, and combat support agencies such as the National Security Agency, identified factors that impede cyberspace operations by special operations forces. It identified USCYBERCOM entities responsible for providing cyberspace-operations support to special operations activities, and assessed the effectiveness of that support. The assessment also examined the level of reporting fidelity maintained for these operations, and tried to identify similar obstacles for other military units.

The questionnaire consisted of two parts and is provided in Appendix A and Appendix B. Ten questions focused on cyberspace operations that special operations forces perform; eight questions focused on cyberspace operations that USCYBERCOM performs for the special operations community. The questionnaire was sent to participants between April 2020 and May 2020, and responses were received between April 2020 and September 2020.

B. QUESTIONS FOR USCYBERCOM AND SUBORDINATE ELEMENTS

The questionnaire was delivered to the USCYBERCOM J2 Intelligence Division, and Marine Forces Cyber Command (MARFORCYBER). Although some responses to the questionnaire were unclassified, responses about specific operational metrics related to cyberspace operations and special operations are held at SECRET level enclaves in the Supplemental to this thesis. All responses from MARFORCYBER are held at the SECRET level.

1. USCYBERCOM J2 Intelligence Division Questionnaire Responses

The questionnaire was forwarded to the J2 Intelligence Division of USCYBERCOM at Fort Meade, Maryland. Mr. Dave Wilson of the J2 Intelligence Division fielded the request for information. The responses were provided on UNCLASSIFIED and SECRET enclaves, where appropriate. During an unclassified phone conversation, Mr. Wilson said USCYBERCOM performs computer network operations and computer network exploitation to shield deployed tactical units from operational risk (D. Wilson, personal communication, July 21, 2020). He said that USCYBCERCOM provides historical cyberspace-operations context to military customers to prepare them for deployment to an area of operations. Operational support and capability development for USSOCOM is provided by MARFORCYBER, the Marine Corps service component commander for USCYBERCOM.

2. Title 10 and Title 50 Authorities

Mr. Wilson reaffirmed that Title 10 and Title 50 of the U.S. Code are the primary governing mechanism for cyberspace operations. However, conflicts exist between Congressional committees that monitor Title 10 military operations and Title 50 intelligence operations (Wall, 2011). These conflicts contribute to the difficulties military units experience during the performance of cyberspace operations, as the governing U.S. codes do not differentiate well between military operations and intelligence activities in cyberspace.

Mr. Wilson explained the differences between Title 10 and Title 50 of the U.S. Code, as they pertain to oversight of cyberspace operations. Title 10 of the U.S. Code empowers the executive branch of government to review and approve military operations, but it can delegate approval authority to operational commanders. The Congressional Armed Forces Committee in the legislative branch receives reports on military operations and performs oversight of military operations. Title 50 of the U.S. Code governs the conduct of intelligence activities, and requires that congressional intelligence committees be kept well-informed of intelligence activities. Intelligence activities are done by the National Intelligence Program, which includes the Director of National Intelligence, the

Central Intelligence Agency, and any other program or department designated by the President of the United States. Congressional intelligence committees provide oversight of intelligence activities. Intelligence activities can also be done by DOD under the authority of the Secretary of Defense. The Congressional Armed Services Committee and the Congressional Intelligence Committee share oversight when DOD performs intelligence activities (Wall, 2011).

3. Title 10, Title 50, and Unconventional Warfare

Mr. Wilson provided a reference that further differentiated between Title 10 and Tile 50 of the U.S. Code. The document used a comparison between cyberspace operations and unconventional warfare. The distinction between Title 10 and Title 50 cyberspace operations is similar to the distinction between unconventional warfare and covert actions (Wall, 2011). Joint Publication 3-5 defines unconventional warfare as "operations or activities done by special operations forces, to enable a resistance movement or insurgency to coerce, disrupt, or overthrow a government or occupying power by operating through or with an underground, auxiliary, and guerilla force in a denied area." Title 50 of the U.S. Code defines a covert action as "an activity of the U.S. government to influence political, economic, or military conditions abroad, where it is intended that the role of the U.S. government not be apparent or openly acknowledged." Differences reflect the authority ordering the operation and whether the operation is acknowledged by the U.S. Government. If the operation is directed by a military commander, and is intended to be acknowledged by the United States Government, it is considered unconventional warfare and a military action. If the operation is directed by the Director of National Intelligence, and is not intended to be acknowledged by the United States Government, then it is a covert action. Congressional intelligence committees are concerned that DOD is labeling certain cyberspace operations as military activities to avoid more stringent oversight requirements. The DOD is not required to inform Congressional armed-services committees about military operations.

C. QUESTIONS FOR SPECIAL OPERATIONS UNITS

The special operations portion of the questionnaire was distributed to the USSOCOM J3 Cyber Division, and their subordinate operational commands. It contained questions on operational metrics, achieving operational objectives, requests for support from DOD cyberspace-operations agencies, and manning and equipment levels. As before, responses about specific operational metrics related to cyberspace operations and special operations are in the classified supplemental.

The questionnaire was also sent to the J3 Cyber Division of USSOCOM in Tampa Bay, Florida, the Air Force Special Operations Command (AFSOC) 361st Technical Directorate in Destin, Florida, the Joint Cyber Operations Group at Fort Meade, Maryland, and the Naval Special Warfare Special Reconnaissance Teams. The Joint Cyber Operations Group responses are in the classified supplemental. Operational metrics provided by the Special Reconnaissance Teams are in the classified supplemental.

1. USSOCOM J3 Cyber Division Questionnaire Responses

The questionnaire was forwarded to the USSOCOM J3 Cyber Division as a request for information. Although the USSOCOM J3 Cyber Division supports offensive, defensive, and routine DOD cyberspace operations, only questions related to offensive cyberspace operations were asked. The USSOCOM J3 Cyber Division provided the following responses, but due to need-to-know restrictions, questions about current and future operations were not answered.

a. Authorities

The first question asked, “Are cyber authorities granted in time to enable operations?” According to Lieutenant Commander Tyrone Pham of the USSOCOM J3 Cyber Division (personal communication, July 8, 2020), the required authorities are in place, but occasional operational permission roadblocks and interagency de-confliction issues have delayed cyberspace operations.

b. Support from the interagency

USSOCCOM also partially answered question three, “Was support requested and provided from outside agencies such as USSCYBERCOM and the National Security Agency?” USSOCOM could request support from USCYBERCOM and the National Security Agency for cyber capability development, technical expertise, and operational coordination. USCYBERCOM and the geographic and functional combatant commanders have installed coordination elements in their respective organizations. The Cyberspace Operations Integrated Planning Element (CO-IPE) is a USCYBERCOM support team embedded at combatant commands. The Joint Cyber Center is a combatant-commander-owned team embedded in their planning staff. USCYBERCOM CO-IPE teams were formed in September 2017, and should be fully capable by 2022 (Pomerleau, 2019, para. 8). Organizational relationships of the CO-IPE teams are described in Joint Publication 3-12, and relationships between the CO-IPE and USCYBERCOM subordinate commands are specified by USCYBERCOM orders. The CO-IPE teams coordinate cyberspace-operations planning between the combatant commander and USCYBERCOM during routine and contingency operations. They provide tailored technical advice to the combatant commanders, and act as a link to USCYBERCOM.

The flow of communication from the CO-IPE to USCYBERCOM occurs with the combatant-command Joint Cyber Center. The Joint Cyber Centers are cyberspace-operations advisors to the combatant command to integrate cyberspace operations into a theater campaign. Joint Publication 3-12 shows the administrative and operational placement of the Joint Cyber Centers, but does not specify their responsibilities to the combatant commander. According to (DOD Inspector General, 2014), the U.S. Central Command (USCENTCOM) uses their Joint Cyber Center for network defense actions, developing and integrating cyberspace operations, and identifying cyber-readiness requirements for its forces. The U.S. Pacific Command (USPACOM) uses their Joint Cyber Center for intelligence and operations functions for cyberspace operations.

According to Lieutenant Commander Pham (personal communication, July 21, 2020), the USSOCOM Joint Cyber Center has staff from multiple joint-forces codes such as the “J-2” intelligence staff, the “J-3” operations staff, and the “J-6” communications

staff. The CO-IPE staff also help Joint Cyber Center planning. Staff from the joint-force codes and the CO-IPE, DOD. The J6 communications department also integrates cyber operations into training events.

The interview results from the USSOCOM J3 Cyber Center confirm the relationship described in Joint Publication 3-12. The CO-IPE gives intelligence and recommendations on cyberspace-operation courses of action to the Joint Cyber Center during routine and contingency operations (personal communication, July 21, 2020). The Joint Cyber Center then provides the courses of action to the combatant commander for integration into the larger theater campaign. The Joint Cyber Centers and CO-IPEs have yet to standardize their relationships, likely due to their relative organizational immaturity compared to USCYBERCOM. The USSOCOM Joint Cyber Center relationships with CO-IPEs are the most mature among the combatant commanders due to the co-location of USCYBERCOM Cyber Protection Teams within the USSOCOM Joint Cyber Center, and the CO-IPE personnel distribution among the USSOCOM owned Joint Special Operations Command and Theater Special Operations Commands. USSOCOM is the only combatant commander with geographically embedded Theater Special Operations Commands that partition cyber planning within their force structure. For example, the USCENTCOM Theater Special Operations Command established direct communications through the USCENTCOM Joint Cyber Center using a liaison officer (T. Pham, personal communication, July 21, 2020). This is a unique relationship between Theater Special Operations Commands and Joint Cyber Centers. USCENTCOM relies heavily on special operations for their campaigns, so special operations cyberspace operations are well represented in larger USCENTCOM campaign plans. Special operations forces are considered as autonomous, and have defined their Joint Cyber Center role when lacking guidance.

c. Resourcing of cyber operations

The second response from the USSOCOM J3 Cyber Center addressed part of question 2, “Are cyber forces within USSOCOM and their respective sister service enterprises 100% resourced in Manning, Training, and Equipment?” According to

Lieutenant Commander Pham (personal communication, July 8, 2020), one obstacle is that research and development has been closely monitored by Congress for duplication across DOD. USSOCOM has succeeded in justifying its research and development funding, but the associated substantiating research and justifications have delayed new capabilities. The federal government uses the Networking and Information Technology Research and Development Program (NITRD) to recommend investments in cybersecurity, software engineering, and other information technology areas (Sargent, 2020). Current increasing investment trends in DOD information-technology research and development could support new cyberspace-operations capabilities for USSOCOM.

d. Artificial intelligence for special operations

Special operations forces can use organizations outside of USSOCOM to refine cyberspace-operations capabilities. The Joint Artificial Intelligence Center is the DOD center of excellence for artificial-intelligence delivery. Artificial intelligence can enhance tactical and operational level cyberspace operations for special operations forces.

The National Defense Industrial Association is an educational nonprofit organization that promotes innovation in technology and processes (National Defense Industrial Association, n.d.). It hosted a webinar about artificial intelligence in irregular warfare and low-intensity conflicts. Its Special Operations and Low Intensity Conflict division in particular is developing artificial intelligence solutions for tactical-unit maneuvers (Hudson, 2020). Artificial intelligence in special operations could reduce human effort to prepare the battlefield for conflict. It could reduce the cognitive load on analysts, cyber-operations personnel, and battlefield operators, allowing better-informed decisions during combat. It can also be used for cyberspace-operations planning. The artificial-intelligence initiative Artificial Intelligence for Small Unit Maneuver (AISUM) will improve access by special operations forces to targets (National Defense Industrial Association, 2020) by combining special operations and conventional warfighting capabilities. An AISUM future-capabilities video showed surface combatants, amphibious combatants, intelligence platforms, and special operations forces collaborating in an artificial-intelligence-enabled common operational picture. AISUM will allow special

operations forces to plan, train, and rehearse in a three-dimensional version of the operating environment, using unmanned aerial systems navigating to an objective without relying on Global Positioning System data. Object detection algorithms will be enhanced by video navigation and signals intelligence. AISUM can also provide a tactical maneuver element (Morris, 2020) and, for cyber-operations target development, persistent cyberspace operations in a denied or degraded communications environment could occur without human-analyst intervention. Also, autonomous intelligence assessment could be forwarded to the ground-force operator.

Artificial intelligence can be used in special operations for predictive maintenance (Hughes, 2020), but it can also enable small unit maneuvers, provide quicker decision making, and preserve the life of the force on the battlefield. However, requirements for artificial intelligence must be described clearly and appropriately in the Defense Acquisition System. These requirements include uniform data storage, system interoperability, and data security.

Artificial-intelligence-based cyberspace operations could contribute to special operations by automating the collection, processing, and fusion of cyberspace data (Breede, 2020). Reducing dependence on intelligence communications tethered to a remote processing station could not only speed decision making for the tactical operator, but could support communications in a difficult environment. The next generation of drones should possess artificial intelligence to classify objects and discriminate threats in real time (Babbitt, 2020). The Joint Artificial Intelligence Center is working to extend such warfighting capabilities (Joint Artificial Intelligence Center, n.d.). For example, the U.S. Army Special Operations Command (USASOC) is developing small aerial systems that can navigate autonomously indoors. The Center also created the Cyber National Mission Initiative (Joint Artificial Intelligence Center, 2019) which focuses on network mapping, anomaly detection, autonomous cyber defense, and other threat detection tasks difficult for human beings.

Data standardization will be important for artificial-intelligence integration in special operations. No DOD standard ontology for data collection and storage exists (Hughes, 2020) and this will be important for warfighting tools such as rifles, combat

vehicles, and battlefield equipment. A standard application interface could enable sharing of data in a unified database format, and the Joint Artificial Intelligence Center is working on this. Standardization also means that hardware and software must use open architectures and interfaces that allow system interoperability, and document their implementations thoroughly.

2. USAFSOC Questionnaire Responses

The questionnaire was also sent to the United States Air Force 361st Technical Directorate, a division of AFSOC. Its mission is to "organize, train, and equip to provide special operations forces mission partners with decision advantage through timely, accurate, and relevant situational awareness." It permits air commandos to do special operations intelligence, surveillance, and reconnaissance (ISR) for worldwide missions. It also provides cyberspace-operations support to the Air Force and Joint Forces attached to USSOCOM-aligned Theater Special Operations commands.

a. Authorities

The 361st Technical Directorate also supports Air Force and Joint Force elements attached to the Joint Special Operations Command (JSOC), a combatant command subordinate to USSOCOM. For the question "Are cyber authorities granted in time to enable operations?," they said that authorization of cyberspace operations is now more readily granted than in previous years (J. Copp and B. Shaffel, personal communication, July 29, 2020). Since 2018, AFSOC operational elements have become more familiar with procedures to gain approval, and USCYBERCOM appears to have become more comfortable with approving offensive cyberspace operations.

b. Resourcing of cyberspace operations

The next questions were, "Are cyber forces within USSOCOM and their respective sister service enterprises 100% resourced in manning?" and "Is a training program in place and accessible to educate special operations personnel on the conduct of cyberspace operations?" According to AFSOC, their special operations community has trouble getting personnel qualified to perform cyberspace operations because no billet requirements are in

the Program Objective Memorandum (J. Copp and B. Shaffel, personal communication, July 29, 2020). Commanders compensate by typically assigning cyberspace-operations responsibilities as a collateral duty to intelligence and signals intelligence subject-matter experts, as the fields are related to cyberspace operations.

c. Support from the interagency

For the question "Is support requested and provided from outside agencies such as USSCYBERCOM and the National Security Agency?," AFSOC said that SIGINT and cyberspace-operations partner agencies have increased operational and intelligence sharing since 2018 (J. Copp and B. Shaffel, personal communications, July 29, 2020). This is likely due to the shift in cyberspace-operations policy and more familiarity with tactical-cyberspace operations offered by USCYBERCOM. Tactical-level operations for operational-level and strategic-level goals have a well-defined process in Joint Publication 5-0, Joint Operations (JCS, 2017); USCYBERCOM can approve certain tactical-level cyberspace operations. AFSOC said that coordination between USCYBERCOM and tactical-level agencies appears to be improving. A Joint Priority Effects List does not exist for cyberspace operations. A Joint Priority Effects List could assign cyberspace operations to the appropriate tactical, operational, or strategic organization, and ease staffing constraints.

3. Naval Special Warfare Special Reconnaissance Team TWO Responses

The Naval Special Warfare Special Reconnaissance Teams perform combat and intelligence support for special operations forces. They prepare the environment, gather intelligence and reconnaissance, and provide combat support. For the question "Are cyber authorities granted in time to enable operations?" the Naval Special Warfare response was similar to that of AFSOC. Cyberspace-operation approvals were reported to be easier to get due to increased familiarity with tactical-level requests on behalf of the geographic combatant commanders, and due to improved staffing mechanisms between these commanders and USCYBERCOM (H. Gage, personal communication, July 31, 2020).

For the questions "Are cyber forces within USSOCOM and their respective sister service enterprises 100% resourced in manning?" and "Is a training program in place and

accessible to educate special operations personnel on the conduct of cyberspace operations?," no cyberspace-operations billets were reported to be codified. Commanders perform cyberspace operations by repurposing personnel into cyber roles. Training requirements and courses of instruction to qualify cyberspace-operations personnel are in development.

D. CONCLUSION

In summary, the interview responses indicated that cyberspace-operations permissions are becoming easier to get as approval authorities become more familiar with these operations. Permissions for offensive operations are also becoming easier to obtain due to revised executive-branch guidance. Nonetheless, lack of necessary manning and equipment in JCIDS is delaying capability development. At the moment, cyberspace-operations personnel are being taken from existing billets. Cyberspace-operations integration below the strategic level is inefficient due to new advisory capabilities at the combatant command level.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. FINDINGS

This chapter summarizes key impediments to special operations forces ability to conduct cyberspace operations that were discovered in the questionnaire. The DOD is adequately equipped to perform cyberspace operations at the strategic level using the operational forces of USCYBERCOM and the planning elements resident at the combatant commands. The DOD is authorized to conduct cyberspace operations below the strategic level, and has forces capable of performing such operations. The roles and responsibilities of these forces in cyberspace are unclear. This chapter provides justification for organizing the cyberspace-operational doctrine, resourcing, and structure of forces that operate below the strategic level.

A. CYBERSPACE OPERATIONS FOR SPECIAL OPERATIONS

Special operations forces must develop capabilities that address the scope of their operational environment, and that will be effective against the type of enemy they routinely encounter. Unique issues are associated with tactical-level cyberspace-operation capabilities. Unlike strategically-focused cyberspace operations, special operations forces often operate near the enemy, and this exposes their personnel to increased risk of injury or death. Their cyber capabilities should focus on providing advanced indications and warnings and increasing standoff distance from the enemy. This focus will also affect missions at the strategic level.

The DOD has not clearly defined the roles and responsibilities of cyber-operations personnel operating below the strategic level. A mature cyber force should have command and personnel alignments capable of a wide array of operations. Tactical commanders should be educated on how to use the unique capabilities of cyber operations to complement national security goals.

Complex operations that require long lead times and persistent engagement are not suitable for special operations. Special operations need not attack the adversary's entire network. Instead, they can target critical vulnerabilities associated with an operational center of gravity. A special operations cyberspace capability could develop intelligence

against and locally prosecute the single cyberspace nodes in tactical environments. Access to adversary technology such as cellular telephones, laptops, and tactical communication networks could enable discovery of enemy intentions or disable their communications. Russia used these tactics to great effect during their invasion of the Crimean Peninsula; they impeded the Ukrainian military's ability to mobilize their troops.

The targeting cycle could also push cyberspace operations from the strategic level to the tactical level. Violent extremist organizations now depend on the Internet for basic functionality; for instance, the Islamic State used social-media for recruiting and command-and-control. USCYBERCOM and the National Intelligence Community track violent extremist organizations movements through cyberspace, but lack forces to act in the physical domain. Such operations can be planned through cyberspace, and handed off to special operations forces or other tactical units for physical prosecution.

B. CYBERSPACE OPERATIONS BY JOINT SERVICES

Joint operations have several options for cyberspace operations. USCYBERCOM is the functional combatant command in charge of worldwide military cyberspace operations It provides intelligence support to military customers at the strategic, operational, and tactical levels of warfare. However, it delegates operational support of their mission to the Cyber Mission Forces and Cyber National Mission Forces. They indirectly support military customers by the CO-IPE, which advises the combatant command at the operational level and connects to strategic elements at USCYBERCOM.

The Joint Cyber Center is at the combatant command level. It is staffed and equipped by the combatant command and advises the Combatant Commander on the integration of cyberspace operations into theater operations. Neither the CO-IPE and the Joint Cyber Center directly interact with conventional forces or special operations forces assigned to an area of operations, so the Joint Cyber Center is important.

The Cyber Mission Forces and Cyber National Mission Forces within USCYBERCOM provide operational support to their assigned geographic and functional combatant commands. Service commands provide the personnel for them. MARFORCYBER is the Marine Corps component command supporting USSOCOM.

ARCYBER supports USCENTCOM and USAFRICOM. AIRFORCYBER supports the United States Northern Command (USNORTHCOM), the United States Strategic Command (USTRATCOM), and the United States Transportation Command (USTRANSCOM). Fleet Cyber Command (FLTCYBERCOM) and the Navy's 10th Fleet support the Pacific Command (USPACOM) and Southern Command (USSOUTHCOM).

MARFORCYBER has the fewest forces among the service component commands. The geographic and expeditionary similarities of the Marine Corps missions to special operations missions justify their support of USSOCOM. Additional questionnaire responses about MARFORCYBER support to special operations forces are provided in the Supplemental.

Special operations forces and conventional forces can perform some cyberspace operations according to theater guidance. At the tactical level, special operations relies more heavily on their unique warfighting capabilities than conventional forces do; for instance, they require more regional orientation and cultural expertise (JCS, 2014, p. ix). Because their work is time-sensitive, and is done in clandestine, covert, and low-visibility environments, special operations use signals-intelligence and cyberspace-operation capabilities often. Some conventional-force units have their own signals-intelligence capabilities, but special operations units rely on it more. Similarly, at the operational and strategic level of warfare, special operations forces have more organizations supporting cyberspace operations.

C. CYBERSPACE OPERATIONS BELOW THE STRATEGIC LEVEL

Cyberspace operations below the strategic level of warfare are managed in many ways. The Cyber Mission Forces and Cyber National Mission Forces are owned by USCYBERCOM, but act according to geographic and functional command alignments. The forces performing cyberspace operations for a combatant command are not directly controlled by the Geographic Combatant Commander. Control by USCYBERCOM rather than the geographic commander requires additional coordination when units at the tactical level need cyber support. This contrasts with the relationship USSOCOM has with geographic combatant commanders. The Theater Special Operations Command is a

subordinate command of USSOCOM (JCS, 2014, p. ix), and the Secretary of Defense assigns operational control of Theater Special Operations Commands and their tactical units to the geographic combatant command.

The CO-IPE and Joint Cyber Centers plan cyber operations, but below the geographic combatant command, no entity does. For warfare areas in the physical domain, a component commander exists. The Joint Forces Land Component Commander controls all military operations on land within the theater of operations; the Joint Forces Maritime Component Commander controls operations at sea; the Joint Forces Air Component Commander controls operations in the air. Component commanders perform cross-domain operations in the physical domain as part of combat operations. The transfer of forces from one physical warfighting domain to another is documented in Joint Publications. No Joint Forces Cyber Component Commander plans, synchronizes, and executes cyberspace operations with other component commanders in the theater. Despite being owned by USSOCOM, operational control of Theater Special Operations Commands remains with the geographic combatant command. These units have geographic focus and regional expertise on special operations within the theater, and include dedicated cyberspace operations planning personnel. They can use cyberspace operations at the tactical level, and can reach back to the USCYBERCOM support mechanisms at the combatant command. It is clear that a void in cyberspace-operations guidance occurs below the strategic level. The tactical-level units lack defined budgets that address the manning, training, and equipment to perform cyberspace operations due to no official requirement. Without a codified budget, operational and tactical-level units must use open-source and commercial tools to piece together a cyber capability (Mulder, 2016). The lack of coordination between Congressional oversight committees in monitoring Title 10 and Title 50 operations is another barrier to developing a unified cyberspace operations instruction. The governing codes do not differentiate well between military operations and intelligence activities in cyberspace.

V. RECOMMENDATIONS

It is clear that cyberspace operations could enhance special operations. The United States follows legal processes before conducting cyberspace operations. However, these legal processes could be accelerated, and ambiguous policy must be clarified. Conflicting cyberspace-operations policies come from many different parts of government, and they provide little guidance at the tactical level. As a result, the special operations community depends too much on strategic guidance that is inapplicable to tactical-level goals.

A. OPERATIONAL-LEVEL AND TACTICAL-LEVEL FORCE ALIGNMENT

We suggest that personnel from the CO-IPE or Joint Cyber Center be moved from the strategic level to operational level of the theater, and that a Joint Forces Cyber Component Commander be established to oversee the execution of both operational-level and tactical-level cyberspace operations. The Joint Forces Cyber Component Commander could plan operations with the Land, Sea, and Air Component Commanders and special operations task forces. They would interface with strategic-level USCYBERCOM elements for requested support. A redistribution of strategic-level personnel to theater planning would better help tactical units such as special operations forces.

We also suggest that USCYBERCOM Combat Mission Teams that serve missions for geographic combatant commands should be controlled by the Geographic Combatant Commander. As with the relationship of USSOCOM to geographic combatant commanders, USCYBERCOM could act as a force provider satisfying the military-service responsibilities to man, train, and equip forces. Operational-level and tactical-level cyberspace-operations priorities would be determined by the commander, and ranked appropriately within their theater campaign plan.

It would also help if the composition and mission of the Joint Cyber Center were defined in Joint Publication 5-0, Joint Planning, and reflected in Joint Publication 3-12, Cyberspace Operations. The billet structure should include offensive positions, defensive positions, intelligence personnel in “J-3 intelligence” roles, and personnel in “J-6 communication” roles. This structure would include capabilities from each cyberspace-

operations functional-mission area. If Joint Cyber Center missions are found to duplicate those at the CO-IPE, personnel should be reassigned to the operational and tactical level cyberspace-operations units. Special operations units should formulate a problem statement about cyberspace operations at the tactical-unit level that is endorsed by combatant commanders. It should list missions not accomplished due to capability deficiencies, and how appropriate resources would solve the issue. Capability requirements should be developed using the Doctrine, Organization, Training, Materiel, Leadership, Personnel, and Facilities (DOTMLPF) analytic process and should identify materiel and non-materiel solutions for JCIDS.

B. PROFESSIONAL MILITARY EDUCATION

Commanders of special operations forces need education on the operational use of cyberspace operations. They also need to become familiar with operational planning for the cyber domain and the technical and intelligence requirements to target in the cyber domain. This will allow realistic cyber-operation development, and appropriate scoping of missions. USCYBERCOM planning courses should be offered to commanders of special operations forces. The curriculum should address joint interoperability of cyber forces, conventional forces, and special operations forces. The curriculum should cover support mechanisms in to USCYBERCOM, possible cyberspace operations, and cyberspace-operations authorities.

The Goldwater-Nichols Act of 1986 instituted changes in the command and control structure and professionalization standards of the force including the Joint Professional Military Education program, and the cyberspace domain should be better represented in its curriculum.

C. CAPABILITY DEVELOPMENT

Special operations forces must be familiar with the full range of cyber operations and cyberwarfare including offensive, defensive, and DODIN operations, and open-source and commercial-off-the-shelf capabilities for cyberspace operations. They also need to understand defensive principles, network topology, traffic analysis, and threat-detection methods.

Knowledge of artificial intelligence should be included in this, as it can reduce workloads for cyberspace operations and apply analytic power to threat recognition. The Joint Artificial Intelligence Center can help commanders select technology for artificial-intelligence enhancement.

Identification of future cyberspace-operations requirements by the DOTMLPF process ensures properly written problem statements in JCIDS. Use of the DOTMLPF process to resource a special operations cyber-capability should emphasize doctrine, billeted positions, and technical capabilities. The formal medium to document a capability deficiency, and request remediation is JCIDS. Entering the problem into JCIDS ensures the capability requirement is transparent to the larger special operations community, that efforts aren't duplicated across the DOD, and that future defense-acquisition projects can rely on similar research previously addressed by the Defense Acquisition Process.

D. DOCTRINE

Tactical-level cyberspace-operations doctrine should reflect inputs from units below the strategic level. This means that special operations forces should contribute to Joint Publications on special operations targeting, and planning. The relationship between geographic and functional commands that can perform cyberspace operations beyond USCYBERCOM's Cyber Mission Forces and Cyber National Mission Forces is not currently explained. This does not enable intelligent development, targeting, and operational synchronization by commanders outside of USCYBERCOM. If operational-level and tactical-level force realignments occur, Joint Publication 3-12 should reflect them. Joint Publication 3-5 Special Operations should describe how cyberspace operations fit into special operations core activities such as reconnaissance, direct action, unconventional warfare, and civil affairs. Joint Publication 5-0 Joint Planning should mention planning and tracking considerations for operations that cross physical domains, logical domains, and multiple combatant commands. Amendments to joint-forces cyberspace-operations doctrine and the National Security Presidential Memorandums should address ambiguity in classifying cyberspace operations under Title 10 or Title 50 authorities. Technical terms for cyberspace operations should be based on the authorities found in Title 10 and Title 50.

E. CONCLUSION

Special operations forces need unilateral cyberspace operations. Better ability to do so will equalize competition with peer adversaries already operating in the cyber domain. DOD organizations that can do strategic cyber missions can better support the Joint Forces at the operational and tactical levels. This requires combining inputs from strategic and tactical commanders, the defense industry, the commercial sector, and DOD science and technology organizations.

The recommendations of this thesis can extend to other military units at the tactical edge of operations. U.S. Navy surface combatants, subsurface combatants, manned air platforms, and unmanned air platforms would benefit from an increased ability to include cyberspace operations. U.S. Air Force air platforms would also benefit.

An increased ability of expeditionary forces to conduct cyberspace operations also affects their vulnerabilities and centers of gravity, so defensive cyberspace technologies should also be examined. Unfortunately, the traditional centralized infrastructure and manning for network defense does not readily scale to the tactical level. Future tactical-level cyberspace capabilities should have other ways to obtain robust information-assurance measures, operational-security measures, and encryption engineered into hardware and software. Such defensive operating procedures for tactical-level cyberspace operations should be endorsed by USCYBERCOM and the National Security Agency to ensure best practices are used including artificial intelligence.

Resourcing a capability to meet threats in the cyber domain should be accomplished through the DOTMLPF process. Quantitative analysis must be done on the criticality of a special operations cyber capability versus competing lines of effort. An assessment must be made of the risk associated with not resourcing a special operations cyberspace capability. In a budget-constrained environment, special operations leadership must decide how to redistribute their budget if a cyber-capability is required but not fully funded. Alternatively, the special operations community must choose not to resource a cyber-capability and assume operational risk.

APPENDIX A. SPECIAL OPERATIONS INTERVIEW KICK-OFF QUESTIONNAIRE

1. How many special operations missions were planned to enable primary or follow-on cyberspace operations for the last three years?

2. Were the primary or follow-on cyberspace operations mission objectives achieved?

3. Were the requested cyber authorities granted in time to enable the operation?

4. Was support to the primary or follow-on cyberspace operations requested and provided from outside agencies such as the NSA, USCYBERCOM, etc.?

5. How many enhancing cyberspace operations were integrated into SOF missions for the last three calendar years?

6. Were the enhancing cyberspace operations mission objectives achieved?

7. Were the special operations mission objectives achieved? If they were not, were the cyberspace operations the limiting factor?

8. Was support to the enhancing cyberspace operations requested and provided from outside agencies such as the NSA, USCYBERCOM, etc.?

9. Were the requested enhancing cyber authorities granted in time to support the operation?

10. Are cyber forces within USSOCOM and their respective sister service enterprises 100% resourced in Manning, Training, and Equipment (MTE)? If not, what are the deficiency percentages for each category? Specifically, how many billets are gapped? Is funding secured to acquire SOF peculiar operational technologies? How many requests for SOF peculiar operational technologies went unfulfilled? Is a training program in place and accessible to educate SOF personnel on the conduct of cyberspace operations?

All UNCLASSIFIED and higher classification responses related to operational metrics are held on SECRET-level enclaves.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX B. SUPPORT AGENCY INTERVIEW KICK-OFF QUESTIONNAIRE

1. How many special operations forces missions requiring cyberspace operations were supported in the last three years?

2. Were the primary or follow-on cyberspace operations mission objectives achieved?

3. Were the requested cyber authorities requested and granted in time to enable the cyber component of the special operation?

4. How many enhancing cyberspace operations were integrated into special operations forces missions for the last three calendar years?

5. Were the enhancing cyberspace operations mission objectives achieved?

6. Were the requested enhancing cyber authorities granted in time to support the operation?

7. How many special operations forces initiated cyberspace operations requests were disapproved due to insufficient lead time in the last three years?

8. What level of Research and Development funding and support is directed to USSOCOM and its subordinate commands for cyber capability development?

All UNCLASSIFIED and higher classification responses related to operational metrics are held on SECRET-level enclaves.

THIS PAGE INTENTIONALLY LEFT BLANK

SUPPLEMENTAL

Additional information for Chapters III, IV, and V is in a classified supplemental to this thesis. The supplemental contains details about cyberspace-operations metrics, sources, and methods. This supplemental has a SECRET//NOFORN classification. Please email inquiries to rresources@nps.edu.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Babbitt, J. (Contributor). (2020, July 23). *Artificial intelligence for small unit maneuver* [Presentation]. SO/LIC July Webinar- AISUM Challenges in Support of Deploying Artificial Intelligence for SOF. https://www.ndia.org/events/2020/7/23/solic-webinar

Balmforth, T. (2019, June 17). Russia thwarts U.S. cyber attacks on its infrastructure: news agencies. *Reuters*. https://www.reuters.com/article/us-usa-russia-cyber-russia/russia-thwarts-u-s-cyber-attacks-on-its-infrastructure-news-agencies-idUSKCN1TI1U0

Bender, J. M. (2013, November) The cyberspace operations planner: Challenges to education and understanding of offensive cyberspace operations. *Small Wars Journal*. https://smallwarsjournal.com/jrnl/art/the-cyberspace-operations-planner

Brantly, A., Cal, N., Winkelstein, D. (2017). *Defending the borderland - Ukrainian military experiences with IO, cyber, and EW*. Army Cyber Institute at West Point.

Breede, D. (Contributor). (2020, July 23). *Artificial intelligence for small unit maneuver* [Presentation]. SO/LIC July Webinar- AISUM Challenges in Support of Deploying Artificial Intelligence for SOF. https://www.ndia.org/events/2020/7/23/solic-webinar

Conner, M., Vogler, S. (2017). *Russia's Approach to Cyber Warfare* (Contract number N00014-16-D-5003). CNA Analysis and Solutions. https://cle.nps.edu/access/content/group/b3000976-a9ef-4407-b4b6-e237588e5118/Units4-7-CountrySpecific/Russia/RussiaCyberWarfare_CNA.pdf

Copp, J., Shaffel, B. 361st Technical Directorate, AFSOC. Phone call. July 29, 2020.

Department of Defense. (2018). *Summary of the Department of Defense cyber strategy.* https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF

Department of Defense. (2018). *Summary of the 2018 Department of Defense artificial intelligence strategy.* https://media.defense.gov/2019/Feb/12/2002088963/-1/-1/1/SUMMARY-OF-DOD-AI-STRATEGY.PDF

Dickinson, J. (2016, December 4).*T-DCOIS: Maneuvering through cyber space.* United States Army. https://www.army.mil/article/179094/t_dcois_maneuvering_through_cyber_space

DOD Inspector General (2014, December 08). *Joint Cyber Centers cyberspace operations.* U.S. Department of Defense. https://media.defense.gov/2018/Aug/27/2001958644/-1/-1/1/DODIG-2015-048.PDF

DOD Joint Artificial Intelligence Center (2019, October 28). *Integrating AI and cyber into the DOD.* Retrieved August 3, 2020, from https://www.ai.mil/blog_10_25_19-integrating-ai-and-cyber-into-the-DOD.html

Duggan, M. (2015). Strategic development of special warfare in cyberspace. *Joint Force Quarterly, 79(4), 46-53).* https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-79/jfq-79_46-53_Duggan.pdf

Duggan, M., Oren, E. (2016). U.S. Special Operations Forces in cyberspace. *The Cyber Defense Review, 1(2), 73-79.* https://cyberdefensereview.army.mil/Portals/6/Documents/CDR%20Journal%20Articles/US_Special_Operations_Duggan_Oren.pdf?ver=2018-08-01-090209-853.

Gage, H. Special Reconnaissance Team TWO. Phone call. July 31, 2020.

Hudson, D. (Contributor). (2020, July 23). *Artificial intelligence for small unit maneuver* [Presentation]. SO/LIC July Webinar- AISUM Challenges in Support of Deploying Artificial Intelligence for SOF, online. https://www.ndia.org/events/2020/7/23/solic-webinar

Hughes, K. (Contributor). (2020, July 23). *Artificial intelligence for small unit maneuver* [Presentation]. SO/LIC July Webinar- AISUM Challenges in Support of Deploying Artificial Intelligence for SOF, online. https://www.ndia.org/events/2020/7/23/solic-webinar

Hughes, D. P. (2018). *Archer's stakes in cyberspace: Methods to analyze force advantage.* https://link.springer.com/chapter/10.1007%2F978-3-319-74107-9_6

Joint Artificial Intelligence Center (n.d.). *Joint warfighting operations.* Retrieved July 28, 2020, from https://www.ai.mil/mi_joint_warfighting_operations.html

Joint Artificial Intelligence Center. (2020, June 18). *A roadmap to getting "AI ready."* https://www.ai.mil/blog_06_18_20-a_roadmap_to_getting_ai_ready.html

Joint Chiefs of Staff. (2014). *Special operations* (JP 3-5). https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_05.pdf

Joint Chiefs of Staff. (2017). *Joint planning* (JP 5-0). https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp5_0_20171606.pdf

Joint Chiefs of Staff. (2018a). *Cyberspace operations* (JP 3-12). https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf

Joint Chiefs of Staff. (2018b). *Joint targeting* (JP 3-60). https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_60.pdf

King, A., Gallagher, M. (ed.) (2020). *Cyberspace Solarium Commission report*. https://www.solarium.gov

Mulder, G. D. (2016). *Tactical cyber capabilities*," [Master's thesis, Naval Postgraduate School]. NPS Archive: Calhoun.

Morris, B. (Contributor). (2020, July 23). *Artificial intelligence for small unit maneuver* [Presentation]. SO/LIC July Webinar- AISUM Challenges in Support of Deploying Artificial Intelligence for SOF, online. https://www.ndia.org/events/2020/7/23/solic-webinar

National Defense Industrial Association (n.d.). *About.* Retrieved July 28, 2020, from https://www.ndia.org/about

Office of Personnel Management. (n.d.). *Cybersecurity incidents.* https://www.opm.gov/cybersecurity/cybersecurity-incidents/

Pham, T. USSOCOM J3 Cyber Cell. Phone call. July 8, 2020.

Pomerleau, Mark (2017, October 11). *Cyber Command stands up planning cells at combatant commands.* C4ISRNet. https://www.c4isrnet.com/show-reporter/ausa/2017/10/11/cyber-command-stands-up-planning-cells-at-combatant-commands/

Pomerleau, Mark (2019, August 21). *How the Army is helping combatant commands with cyber planning.* CISRNet. https://www.fifthdomain.com/show-reporter/technet-augusta/2019/08/21/how-the-army-is-helping-combatant-commands-with-cyber-planning/

Rivera, R. (2018). *Absence of tactical level cyber capabilities for the U.S. Army special operations warfighters.* [Master's thesis, Utica College].

Sargent Jr., J. F. (2020). *Federal Research and Development (R&D) Funding: FY2020* (CRS Report No. R45715). Congressional Research Service. https://fas.org/sgp/crs/misc/R45715.pdf

Schmitt, M. (ed.). (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge University Press, 2017. https://cle.nps.edu

Secretary of Defense. (2018). *Summary of the Department of Defense Cyber Strategy*. https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF

Tebedo, J. C. (2016). *Special operations and cyber warfare* [Master's thesis, Naval Postgraduate School]. NPS Archive: Calhoun. https://calhoun.nps.edu/handle/10945/51622

White House. (2018). *National security presidential memorandum 13 - Cyberspace operations.* White House.

White House. (2019, February 11). *Maintaining Leadership in Artificial Intelligence* (Executive Order 13859). https://www.govinfo.gov/content/pkg/FR-2019-02-14/pdf/2019-02544.pdf

Wilson, D. USCYBERCOM J2 Intelligence Division. Phone call. July 21, 2020.

United States Cyber Command. (n.d.). *Mission and vision.* Retrieved April 22, 2020 from https://www.cybercom.mil/About/Mission-and-Vision/

Wall, H. (2011). Demystifying the Title 10 Title 50 debate: distinguishing military operations, intelligence activities, and covert action. *Harvard National Security Journal 3*, 85-142.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California