DEFENDING FORWARD: SEIZING THE INITIATIVE IN CYBERSPACE BELOW THE LEVEL OF ARMED CONFLICT

A thesis presented to the Faculty of the U.S. Army
Command and General Staff College in partial
fulfillment of the requirements for the
degree

MASTER OF MILITARY ART AND SCIENCE
Strategic Studies

by

DANIEL S. YOON, DEFENSE INTELLIGENCE AGENCY
B.A., University of Maryland, College Park, Maryland, 2010

Fort Leavenworth, Kansas
2019

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

1. REPORT DATE *(DD-MM-YYYY)* 14-06-2019	**2. REPORT TYPE** Master's Thesis	**3. DATES COVERED** *(From - To)* AUG 2018 – JUN 2019
4. TITLE AND SUBTITLE Defending Forward: Seizing the Initiative in Cyberspace below the Level of Armed Conflict		**5a. CONTRACT NUMBER** **5b. GRANT NUMBER** **5c. PROGRAM ELEMENT NUMBER**
6. AUTHOR(S) Mr. Daniel Yoon, DIA		**5d. PROJECT NUMBER** **5e. TASK NUMBER** **5f. WORK UNIT NUMBER**
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) U.S. Army Command and General Staff College ATTN: ATZL-SWD-GD Fort Leavenworth, KS 66027-2301		**8. PERFORMING ORG REPORT NUMBER**
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)		**10. SPONSOR/MONITOR'S ACRONYM(S)** **11. SPONSOR/MONITOR'S REPORT NUMBER(S)**

12. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for Public Release; Distribution is Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The United States recognizes the strategic and economic importance of the cyberspace domain for advancing and securing its national interests. Despite efforts to deter malicious cyberspace activities, the United States continues to face and suffer countless cyberspace attacks from state and nonstate actors at a threshold below the level of armed conflict often referred to as the "gray zone." This research study examines how the United States can build a whole of society approach to leverage interagency, the private sector, local government, academia, and coalition partners' cyberspace capabilities and authorities. The purpose of the whole of society approach is to proactively execute joint operations in order to compete and contest against adversaries in cyberspace across the conflict continuum. A qualitative analysis of existing joint interagency models lends to providing a solution for a cohesive unified action for countering malicious cyberspace activities below the level of armed conflict.

15. SUBJECT TERMS
Cyberspace, Cyberspace Operations, Deterrence, Global Commons, JIATF, USCYBERCOM

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. PHONE NUMBER** *(include area code)*
(U)	(U)	(U)	(U)	120	

MASTER OF MILITARY ART AND SCIENCE

THESIS APPROVAL PAGE

Name of Candidate: Daniel S. Yoon

Thesis Title: Defending Forward: Seizing the Initiative in Cyberspace Below the Level of Armed Conflict

Approved by:

____, Thesis Committee Chair
Richard A. Olsen, D.Min.

____, Member
Lieutenant Colonel Jordon T. Ewers, M.A., M.S.

____, Member
Lieutenant Colonel Justin M. Horgan, M.A.

Accepted this 14th day of June 2019 by:

____, Director, Graduate Degree Programs
Robert F. Baumann, Ph.D.

The opinions and conclusions expressed herein are those of the student author and do not necessarily represent the views of the U.S. Army Command and General Staff College or any other governmental agency. (References to this study should include the foregoing statement.)

ABSTRACT

DEFENDING FORWARD: SEIZING THE INITIATIVE IN CYBERSPACE BELOW THE LEVEL OF ARMED CONFLICT, by Daniel S. Yoon, 120 pages.

The United States recognizes the strategic and economic importance of the cyberspace domain for advancing and securing its national interests. Despite efforts to deter malicious cyberspace activities, the United States continues to face and suffer countless cyberspace attacks from state and nonstate actors at a threshold below the level of armed conflict often referred to as the "gray zone." This research study examines how the United States can build a whole of society approach to leverage interagency, the private sector, local government, academia, and coalition partners' cyberspace capabilities and authorities. The purpose of the whole of society approach is to proactively execute joint operations in order to compete and contest against adversaries in cyberspace across the conflict continuum. A qualitative analysis of existing joint interagency models lends to providing a solution for a cohesive unified action for countering malicious cyberspace activities below the level of armed conflict.

ACKNOWLEDGMENTS

First and foremost, I would like to thank my thesis committee, Dr. Rick Olsen, LTC Justin Horgan, LTC Jordon Ewers, and Dr. Eric Morrison for their guidance and mentorship throughout this academic year. I am incredibly blessed to have these individuals as my committee members. I am truly grateful for the committee's patience and encouragement as well as the candid discussions and genuine interests for the thesis topic. Without them, this research would not have come to fruition.

I also would like to send special thanks to my staff group advisor Mrs. Candy Smith and the entire staff group 16D. I am thankful for the staff group instructors for challenging me academically and allowing me to grow professionally. Thank you all for welcoming me as your own. I will cherish the experiences and the relationships I've gained at the United States Army Command and General Staff College for many years to come. Furthermore, I would like to thank my family and friends who have supported me throughout this academic year.

Last, but certainly not least, I would like to thank my girlfriend, Ji-Yeon Kim. You've helped me stay focused and motivated in completing this thesis. You've taught me that no obstacles or barriers are too challenging to overcome when I believed there was no end in sight. Thank you for your love and encouragement during this long journey.

TABLE OF CONTENTS

ACRONYMS

CIKR	Critical Infrastructure and Key Resources
DCO	Defensive Cyberspace Operations
DCO-RA	Defensive Cyberspace Operations – Response Action
DODIN	Department of Defense Information Network
DOTMLPF-P	Doctrine, Organization, Training, Materiel, Leadership, Personnel, Facilities, and Policies
FBI	Federal Bureau of Investigation
JIATF	Joint Interagency Task Force
JIIM	Joint, Interagency, Intergovernmental, and Multinational
JIIOC	Joint Interagency Intelligence Operations Center
JTF	Joint Task Force
LOE	Lines of Effort
NCIJTF	National Cyber Investigative Joint Task Force
NCCIC	National Cybersecurity and Communications Integration Center
NICCP	National Interdiction Command and Control Plan
NSA	National Security Agency
OCO	Offensive Cyberspace Operations
SecDef	Secretary of Defense
SWOT	Strength, Weaknesses, Opportunities, and Threats
USCYBERCOM	United States Cyber Command
USSOUTHCOM	United States Southern Command
USG	United States Government

ILLUSTRATIONS

TABLES

Page

CHAPTER 1

INTRODUCTION

Background

The United States recognizes the strategic and economic importance of the cyberspace domain for advancing and securing its national interests. The United States views the cyberspace domain as a global common and aims to secure and enforce international norms within the domain to pursue its strategic objectives (Trump 2017a, 41). Over the past decade, the United States faced cyberspace attacks from both state and non-state actors against U.S. critical infrastructure and key resources (CIKR) including, but not limited to, financial institutions, universities, government, and military services (CSIS 2018).

The cyberspace attacks have not only damaging impacts on the U.S. economy but also significant psychological effects on the American people. According to a September 2018 Marist Poll, approximately one out of every three American adults believed a foreign country would tamper with the 2018 midterm election's results (Marist Poll 2018). Moreover, these cyberspace attacks and exploitations do not meet the level of armed conflicts leaving policymakers uncertain on how to appropriately respond without increasing tensions in the cyberspace domain.

The United States recognizes a long-term strategic and cyberspace threat and risk to U.S. national interests from China and Russia with sophisticated cyber capabilities. Additionally, the United States acknowledges the growing threat of North Korea, Iran, and nonstate actors' use of malicious cyberspace activities, with moderate capabilities, against the United States (DOD 2018b, 1; Kramer, Butler, and Lotrionte 2017, 3). These foreign state and non-state actors' cyberspace attacks reportedly cost the United States between $57 billion and $109 billion, according to a February 2018 White House's Council of Economic Advisers report (Marks 2018; Trump 2018b, 1). In 2014, the Centers for Strategic International Studies (CSIS) estimated that cybercrime activities—including stealing data (e.g., intellectual property), financial theft, and ransomware—cost the global economy about $500 billion (Lewis 2018a, 4). The same CSIS study assessed an increasing number of malicious cyberspace activities daily. As an example, there are 80 billion malicious scans, 300,000 new malware, 33,000 phishing attempts, 4,000 ransomware, and 780,000 data exfiltration daily (Lewis 2018a, 4).

A group called "Guardian of Peace" with alleged North Korean assistance conducted a cyberspace attack against Sony Pictures Entertainment (SPE) and released sensitive internal data to the public and destroyed their servers in November 2014, costing SPE approximately $100 million in economic losses (Cieply and Brooks 2014; Richwine 2014). In response, SPE hired Mandiant, a private cybersecurity firm, to investigate the cyberspace attack to their servers. Many other private cybersecurity companies conducted investigations on the 2014 cyberspace attack against SPE. Following the investigations and technical analysis, private cybersecurity firms were the first to report credible attribution of SPE cyberspace attack to a North Korean actor known as "Dark Seoul" within weeks (DeSimone and Horton 2017, 7-8).

Thomas Bossert, a former U.S. Homeland Security Advisor, linked the malware attack known as WannaCry to North Korea in December 2017 (Bossert 2017). The WannaCry malware, malicious ransomware, spread to more than one hundred countries and cost the global economy eight billion dollars (Barlyn 2017). As of 2017, an average

U.S. private company experienced about 130 security breaches annually, with a single malicious cyberspace activity costing it roughly $21 million per incident as well as information loss, business disruption, revenue losses, and equipment damages (Trump 2018b, 7-9).

The state-sponsored actors will continue to conduct cyberspace operations below the level of armed conflict or the "gray zone" (see the "gray zone" in the *Definitions* section below) to avoid soliciting a retaliatory response from the United States. On malicious cyberspace activity's psychological impact, the U.S. intelligence community assessed "Russian President Vladimir Putin ordered an influence campaign in 2016 aimed at the U.S. presidential election" (DNI 2017, ii). In March 2016, General Staff Main Intelligence Directorate (GRU), a Russian intelligence agency, executed cyberspace operations (CO) to interfere and undermine the U.S. presidential election and democratic process (DNI 2017, 2; CNN 2018). Furthermore, Russia conducted information operations in cyberspace to sow dissent within the U.S. voting populace. In November 2016, a Russian-affiliated Facebook group called "Black Matters US" organized a demonstration against then-candidate Donald Trump. Approximately sixteen thousand Facebook users planned to attend the "Black Matters US"-led protests and as many as five to ten thousand protestors physically demonstrated in New York City (Breland 2017).

In support of the Russian influence campaign, the Internet Research Agency (IRA) created and disseminated false information and documents to sow discord and distrust between the U.S. populace, the candidates, and the political systems in early 2014 (Matishak 2018). Subsequently, the IRA conducted information operations on social media platforms, such as Facebook and Twitter, through fake accounts to influence and mislead U.S. voters and promulgate misinformation and false accusations of the 2016 presidential candidates (Matishak 2018). Moreover, the Russian intelligence hacked into the U.S. Democratic National Committee's (DNC) networks and servers to exfiltrate damaging emails and documents regarding presidential candidates to the Internet to incite conflict within the Democratic Party (Yourish 2018).

The United States used economic pressures (e.g., sanctions) and law enforcement actions (indictments) to respond to state-sponsored cyberspace attacks. However, there were no reported proportional U.S. actions in the cyberspace domain beyond defense, thus allowing malicious cyberspace actors to continue to exercise freedom of maneuver and action against U.S. networks. If uncontested in the cyberspace domain, adversaries will seek to find and hold key terrain in cyberspace to gain a marked strategic advantage in the event of a future conflict, such as a large-scale combat operation, with the United States. Key terrain in cyberspace is no different from other warfighting domains – it is an area that "affords any combatant a position of marked advantage" (JCS 2018a, I-6).

Following the North Korean cyberspace attack against SPE, the United States enforced sanctions against North Korean organizations responsible for the attack to deter future malign behavior in cyberspace (Meer 2015, 5). The economic sanctions did not stop North Korean malicious cyberspace actors' global WannaCry ransomware attack in May 2017 (Symantec 2017). Similarly, in December 2018, the Department of State (DOS) and the Treasury issued a joint sanction against Russian entities, including the IRA, for their involvement in the 2016 U.S. election hacking. To bolster the effects of the sanction, the Treasury Department designated GRU-affiliated individuals responsible for the 2016 U.S. election hacking (Bureau of Public Affairs 2018). Also, in July 2018, the Department of Justice indicted twelve Russian intelligence officers for conducting cyberspace operations to undermine the 2016 U.S. election (CSIS 2018). In addition to USG response, CrowdStrike, a private cybersecurity firm, analyzed the DNC networks and attributed the malicious cyberspace activity to the Russian government, specifically Russian hackers Cozy Bear and Fancy Bear (Marwan 2017).

Over the past several years, China conducted cyberspace exploitation against U.S. private and military networks to exfiltrate intellectual properties and technology information, likely to bolster its economy and defense sectors. In response, the U.S. Department of Justice indicted five Chinese People's Liberation Army officers for "economic espionage" in May 2014; however, Chinese malicious cyberspace activities against the United States continued to persist (Chang 2014). In July 2015, suspected Chinese cyberspace actors hacked the Office of Personnel Management (OPM) and compromised personally identifiable information (PII) of at least 22.1 million federal employees and contractors, likely to support their intelligence collection apparatus and national objectives (Nakashima 2015). Recently, in December 2018, Rob Joyce, a former White House cyber adviser, highlighted that "Chinese cyber activity in the United States had risen in recent months" targeting U.S. critical infrastructure and sectors including energy, financial, and transportation (Finkle and Bing 2018).

Despite economic and law enforcement response actions, adversary cyberspace forces will continue their malign activities in cyberspace against the United States as both state and non-state actors view cyberspace operations as relatively low cost with a high-reward payoff. Ann Cox, DHS' Cybersecurity Division Program Manager, explained that the barrier to entry for conducting malicious cyberspace activity is very low (Terdiman 2018). General Paul Nakasone, the Commander of United States Cyber Command (CDRUSCYBERCOM), also assessed that cyberspace threats against the United States continue to persist due to the low barrier to entry and "capabilities are rapidly available and can be easily repurposed" (JFQ 2019, 4).

In addition to the low barrier to entry, the clandestine nature of the cyberspace domain enables adversarial nation-state actors to claim plausible deniability of any wrongdoing, which degrades United States' ability to attribute and effectively deter malicious cyberspace activities (Chen 2017, 102). For cyber attribution, the process involves identifying the infrastructure for the intrusion against victim systems, perpetrator employing the intrusion, and the adversary responsible for the malicious cyberspace activity (Davis, Boudreaux, Welburn, Aguirre, Ogletree, McGovern, and Chase 2017, 9). Malicious cyberspace actors often exploit and compromise infrastructure belonging to unwitting Internet users globally to mask the origin of the cyberspace attack, enabling actors to claim plausible deniability. Cybersecurity experts assess that about 100 to 150 million devices are compromised worldwide to support cyberspace attacks and other illicit activities in the cyberspace domain (Mazanec 2015, 224).

With total disregard for the U.S. economic and diplomatic pressures, in December 2018, North Korea malicious cyberspace actors reportedly conducted cyberspace exploitation against U.S. universities for information on biomedical engineering since May 2018 (CSIS 2018). Cybersecurity researchers reported in November 2018 that Russian malicious cyberspace actors impersonated U.S. DOS officials with the intent to gain access to networks of the military, law enforcement agencies, and defense contractors (CSIS 2018). According to a joint FBI and DHS report, probable Russian cyberspace actors targeting U.S. energy companies, nuclear, water, aviation, and manufacturing facilities in October 2017 and March 2018 (CSIS 2018).

Limitations

The information regarding tactics, techniques, and procedures (TTP) for cyberspace operations as well as capabilities are classified and not releasable to the public. Additionally, specific U.S. military and interagency plans for cyberspace operations remain in classified channels. Therefore, this research study will only incorporate open source and unclassified information regarding U.S. policies, strategies, doctrine, and organizations as well as historical context for cyberspace operations. This research study will not include discussions of specific cyberspace operations tools and military plans. The research study intends to increase situational understanding for policymakers and commanders on devising systems or conditions to proactively compete, and contest malicious cyberspace actors below the level of armed conflict.

Assumptions

This research study assumes that the United States does not have a comprehensive whole of society approach to compete and contest malicious cyberspace actors at a threshold below the level of armed conflict. The United States has several organizations, such as DHS, FBI, and USCYBERCOM, that manages and operates cybersecurity issues. However, the various organizations have different policies and procedures for responding to cyberspace incidents often competing for the same resources. The *Cyber Security Policy Guidebook* cited that the most significant challenge for USCYBERCOM is the "long-standing 'stovepipe' mentality of military organizations" (Bayuk, Healy, Rohmeyer, Sachs, Schmidt, and Weiss 2012, 234).

In September 2017, the Commander of United States Central Command (USCENTCOM) General Joseph Votel opined that "historically, cyberspace operations have been stovepiped and executed independently" (Pomerleau 2017a). General Votel emphasized that normalizing the cyberspace as a warfighting domain requires "broader authorities that are more responsive than current bureaucratic processes" (Votel, Julazadeh and Lin 2018, 5). Similarly, Ambassador Gina Abercrombie-Winstanley, a former foreign policy advisor for USCYBERCOM, noted that Former Secretary of Defense (SecDef) Ash Carter expressed disappointment in the effectiveness of USCYBERCOM due to the "tensions brought on by other agencies not wanting CYBERCOM to use those [cyber capabilities]" (Abercrombie-Winstanley 2018).

Additionally, this research study assumes the existing joint interagency organizations for cybersecurity issues are under-resourced to pursue the concept of defending forward outlined in the *2018 DOD Cyber Strategy*. The current joint interagency organizations are the National Cyber Investigative Joint Task Force (NCIJTF) and the National Cybersecurity and Communications Integration Center (NCCIC) (FBI 2019c; DHS 2018b). The NCIJTF has over twenty interagency partners from law enforcement, the intelligence community, and the DOD to collectively accomplish the mission of coordinating, integrating, and sharing information to support investigations on cyberspace threats (FBI 2019c). NCCIC is "a national hub for cyber and communications information, technical expertise, and operational integration . . . and incident response center" (National Cybersecurity and Communications Integration

Center 2018). These above joint cyber organizations listed above effectively coordinate and share information regarding cybersecurity issues across the USG and private sectors as well as foreign partners. However, these joint interagency entities do not possess the capability or authorities to execute cyberspace operations to proactively compete and contest malicious cyberspace actors under the defending forward concept.

Another assumption of this research study is that the USG faces challenges in deterring state-sponsored and nonstate malicious cyberspace activities that fall below the level of armed conflict or the "gray zone." General Paul Nakasone emphasized that adversaries are adjusting and adapting their cyberspace operations to avoid provoking a U.S. military response (Nakasone 2019b, 12). Regarding malicious cyberspace activities in the "gray zone," Nakasone further highlighted that "adversaries still feel able to operate against the United States and its interests through cyberspace, and because historically there has been little cost imposed for doing so" (Nakasone 2019b, 12). Similarly, this research assumes that current USG measures against malicious cyberspace activities, such as sanctions and indictments, fail to stop cyberspace attacks and exploitations against U.S. national interests as cited in examples above. These assumptions form the basis for the research questions below.

Research Questions

The primary research question is "as deterrence in cyberspace fails, how can the United States develop a whole of society approach in the cyberspace domain to proactively compete and contest state-sponsored malicious cyberspace actors and activities against U.S. national interests in a state below the level of armed conflict?"

The secondary research questions, are what changes in policy or doctrine is necessary for enabling the United States to proactively compete and contest state-sponsored malicious cyberspace actors in a state below the level of armed conflict? What are the methods and means for the United States to compete and contest state-supported malicious cyberspace actors and activities against U.S. national interests other than deterrence? In support of U.S. national interests, how does the United States secure and defend the global commons and lines of communication in the cyberspace domain? What U.S. organization is responsible for integrating and executing the instruments of national power against state-sponsored malicious cyberspace actors and activities?

Definitions

The Department of Homeland Security (DHS) defines critical infrastructure as "those assets, systems, networks, and functions—physical or virtual—so vital to the United States that their incapacitation or destruction would have a debilitating impact on security, national economic security, public health or safety, or any combination of those matters" (FEMA 2008, 2). Also, DHS identifies Key Resources as "publicly or privately controlled resources essential to [the] minimal operation of the economy and the government" (FEMA 2008, 2).

Cyberspace is "the domain within the information environment that consists of the interdependent network of information technology (IT) infrastructures and resident data" according to U.S. joint doctrine on Cyberspace Operations (JCS 2018a, 21). The informational dimension is a logical layer where "information is stored, processed, disseminated, and protected . . . [including] content and flow of information" (JCS 2014, I-3). The Joint Staff defines Cyberspace Operations (CO) as the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace (JCS 2018a, 21).

Under CO, the three types of operations are Department of Defense Information Networks (DODIN) Operations, Defensive Cyberspace Operations (DCO), and Offensive Cyberspace Operations (OCO). DODIN operations are “operational actions taken to secure, configure, operate, extend, maintain, and sustain DOD cyberspace and to create and preserve the confidentiality, availability, and integrity of the DODIN” (JCS 2018a, 36). The purpose of DCO is to “defend the DODIN, or other cyberspace DOD cyberspace forces [which] have been ordered to defend, from active threats in cyberspace . . . by defeating on-going or imminent malicious cyberspace activity” (JCS 2018a, 36).

A type of DCO is DCO – Response Action (DCO-RA), which is an operation “taken external to the defended network or portion of cyberspace without the permission of the owner of the affected system” (JCS 2018a, 38). The joint doctrine further expands that “[s]ome DCO-RA missions may include actions that rise to the level of use of force, with physical damage or destruction of enemy systems” (JCS 2018a, 38). Offensive cyberspace operations are “CO missions intended to project power in and through foreign cyberspace through actions taken in support of [combatant commanders] or national objectives” (JCS 2018a, 39).

The United Nations (UN) defines the whole of society approach as the contribution of various entities, including intergovernmental organizations civil society, academia, and private sector and industry to support U.S. national interests and objectives (UN General Assembly 2012). The UN defines global commons as “those parts of the planet that fall outside national jurisdictions and to which all nations have access” (UN

2013, 5). The UN further notes that “the international law identifies four global commons, namely the High Seas, the Atmosphere, the Antarctica and the Outer Space” (UN 2013, 5).

The DOD Joint Publication 3-0 “Joint Operations” defines deterrence as “the prevention of action by the existence of a credible threat of unacceptable counteraction and/or belief that the cost of action outweighs the perceived benefits” (JCS 2017b, GL-8). In *Arms and Influence* (1966), Thomas Schelling defines deterrence as “to prevent from action by fear of consequences” (Schelling 1966, 71). The DOD defines Joint Interagency Task Forces (JIATF) as “formal organizations usually chartered by the DOD and one or more USG civilian department or agency, and guided by a MOA or other founding legal documents that define the roles, responsibilities, and relationships of the JIATF’s members” (JCS 2017a, 273). The joint doctrine on Interorganizational Cooperation also highlights that the JIATF is “typically formed for a specific task and purpose” (JCS 2017a, 273).

Gray zone conflicts are engagements that occur between conventional and irregular war as “they occur below the North Atlantic Treaty Organization’s (NATO) Article 5 threshold and below the level of violence necessary to prompt a UN Security Council Resolution” (Echevarria 2016, 12). The characteristics of a gray zone conflict are the gradual pursuit of political objectives through campaigns, use of nonmilitary and nonlethal capabilities (e.g., information operation), and intent to remain under the threshold for conventional conflict (Mazarr 2015, 58). Applicable to cyberspace operations, the principle of the law of armed conflict (LOAC) are a military necessity, proportionality, and distinction (Belk and Noyes 2012, 32).

Significance of the Study

The U.S. policymakers, military, and interagency partners need to recalibrate their approaches and efforts to malicious cyberspace activities and threats to U.S. national interests. State-sponsored malicious cyberspace actors, like Russia and China, continue to exploit U.S. vulnerabilities in the lack of measures for malign behavior in cyberspace domain short of war. The cyberspace domain enables adversaries to asymmetrically and cost-effectively compete and contest U.S. national interests and influence globally.

In the absence of such measures, malicious cyberspace activities severely impacting the U.S. economy, political systems, technological edge, and the American way of life will continue to persist without consequence. The national strategies on cyberspace, such as the *National Security Strategy*, provide ample purpose and ends for cybersecurity. However, the United States needs to devise a way to incorporate a whole of society approach to proactively compete and contest adversarial malicious cyberspace activities against the U.S. interests.

CHAPTER 2

LITERATURE REVIEW

The purpose of this chapter is to provide shared understanding and context on ends, ways, and means for U.S. cyberspace operations through a review of strategic to operational level documents and publications. First, this chapter reviews national strategies and policies to identify the purpose, strategic end states, and national interests for the cyberspace domain through the employment of the instruments of national power. Next, the literature review examines how U.S. joint and interagency policies and doctrine can shape and enhance existing ends, ways, and means for cyberspace operations, planning process, and organization to proactively compete and contest against malicious cyberspace activities against the United States.

Moreover, this review explores the concept of global commons and its application to the cyberspace domain. The last section of this chapter will review leading experts' and academia's understanding and analysis of cyberspace deterrence strategy. Chapter 4, "Analysis," addresses the gaps and applications of the strategic and operational level document to shape the future of cyberspace operations.

National Security Documents

National Security Strategy

The United States recognizes the importance of the cyberspace domain as a critical enabler for diplomatic, information, military, and economic capabilities to achieve its national interests. The cyberspace domain is interwoven into the fabric of society and impacts the lives of the global populace on a daily basis. In the *National*

Security Strategy of the United States of America, (hereafter, *National Security Strategy*) the USG identifies its "strategic vision for protecting the American people and preserving [American] way of life, promoting [economic] prosperity, preserving peace through strength, and advancing American influence in the world" (Trump 2017a, II). Within this strategic vision, the strategy underscores the importance of the cyberspace domain in achieving U.S. national interests. Dr. Michael Sulmeyer (hereafter, Sulmeyer), director of the Belfer Center's Cyber Project at the Harvard Kennedy School, assesses that the Trump administration understands "that cyberspace is a critical part to practically every aspect of national security" (Sulmeyer 2017a).

To protect the homeland, the *National Security Strategy* highlights a critical requirement for securing and defending U.S. CIKR against malicious cyberspace actors and activities (Trump 2017a, 4). The strategy further emphasizes the need to protect U.S. intellectual property and preserve research and technology industries to achieve economic prosperity and maintain a competitive advantage globally (Trump 2017a, 4). U.S.-based research and technology industries experience intellectual property theft in and through the cyberspace domain by state-sponsored malicious actors. Furthermore, the United States aims to develop robust capabilities, including in cyberspace, to compete, contest, and deter adversaries (Trump 2017a, 4).

The *National Security Strategy* identifies challenges and obstacles in the cyberspace domain to achieving U.S. strategic vision of protecting the homeland. The strategy acknowledges that cyberspace provides state and nonstate actors an asymmetric capability to negatively impact U.S. national interests "without ever physically crossing [the United States'] borders" (Trump 2017a, 12). Also, the strategy recognizes there are vulnerabilities within U.S. CIKR that state and nonstate cyberspace actors can exploit to disrupt security and economic sectors, such as financial institutions (Trump 2017a, 12). The strategy recommendations include, but are not limited to, prioritizing risks for CIKR, deterring and disrupting malicious cyberspace actors, and improving information sharing with private sectors on cyberspace attacks (Trump 2017a, 13).

In the *National Security Strategy*, the White House seeks to bolster and increase U.S. economic prosperity. The global economy and financial transactions are dependent on a free and secure cyberspace domain (Trump 2017a, 18). The strategy identifies the problem of intellectual property theft in and through cyberspace, which undermines U.S. economic prosperity, and provides an example of China's malicious activities of stealing "U.S. intellectual property valued at hundreds of billions of dollars" (Trump 2017a, 21). The *National Security Strategy* seeks ways to combat "cyber-enabled economic warfare" through counterintelligence and law enforcement activities as well as to protect data and networks to counter espionage in and through the cyberspace domain (Sulmeyer 2017a; Trump 2017a, 22).

Under the strategy, the United States identifies cyberspace as a common domain and aims to ensure the global commons are free through the employment of the instruments of national power (Trump 2017a, 41). Also, the *National Security Strategy* prioritizes protecting and securing a free and open Internet to support U.S. national interests as well as global goods and services (Trump 2017a, 41). The *National Security Strategy* signals the importance of the cyberspace domain to achieving U.S. strategic vision as well as highlights the vulnerabilities.

One of the aims of the U.S. strategic vision and national interest is to "preserve peace through strength" through the employment of the instruments of national power (Trump 2017a, 25). The *National Security Strategy* views "the revisionist powers of China and Russia, the rogue states of Iran and North Korea, and transnational threat organizations" as threats and competition against U.S. national interests (Trump 2017a, 25). Specifically, the strategy determines Russia's investment in military capabilities, including cyberspace operations, as the most significant threat to U.S. national interests (Trump 2017a, 25-26).

The *National Security Strategy* also discusses the issue of the proliferation of low-cost cyberspace capabilities globally. The strategy assesses that low-cost cyberspace capabilities enable state and nonstate actors to strategically threaten U.S. economic and security interests without using nuclear weapons (Trump 2017a, 27). Moreover, the strategy proposes that "[d]eterrence must be extended across all of these domains [including cyberspace] and must address all possible strategic attacks," including malicious cyberspace activities (Trump 2017a, 27). Also, the *National Security Strategy* assesses that adversaries are highly capable of competing and contesting U.S. national interests using asymmetric methods and hybrid warfare at a level below the threshold of armed conflict (Trump 2017a, 27). Furthermore, the strategy calls for joint U.S. military forces to develop and integrate full-spectrum capabilities to deter and defeat the "full range of threats to the United States" in a multi-domain conflict (Trump 2017a, 29).

Within the cyberspace policy section, the *National Security Strategy* determines not only that the cyberspace capabilities provide low-cost options to adversaries against U.S. national interests but also that the clandestine nature of cyberspace attacks provides plausible deniability to perpetrators (Trump 2017a, 31). Additionally, the cyberspace policy underscores the detrimental effects of cyberspace attacks in "[undermining] faith and confidence in democratic institutions and the global economic system" (Trump 2017a, 31). These cyberspace attacks directly impact the core values, virtues, and belief of the United States and the American people.

In response to the cyberspace threats, the *National Security Strategy* asserts that the "[United States] will deter, defend, and when necessary defeat" malicious cyberspace actors against U.S. national interests (Trump 2017a, 31-32). To achieve this goal, the United States will invest and improve cyberspace capabilities and forces (materiel and organization) to defend and secure CIKR and ultimately U.S. national interests (Trump 2017a, 32). Moreover, the U.S. policymakers will seek to "improve the integration of authorities and procedures across the [USG] so that cyber operations against adversaries can be conducted as required" (Trump 2017a, 32). Eric Jensen, Special Counsel to the General Counsel of the Department of the Defense, assesses that the *National Security Strategy* "view[s] a cyber violation of sovereignty as a 'risk' about which the government will be 'informed,' but not necessarily 'averse' to taking . . . to stop malicious activity" (Jensen 2017).

The *National Security Strategy* asserts the significance of the cyberspace domain and prioritizes actions to defend and secure the domain in support of U.S. national interests. However, some experts believe the *National Security Strategy* lacks substantive policy actions and goals regarding cybersecurity and the cyberspace domain. While Sulmeyer does note that the document identifies Russian cyberspace threats to the U.S.

democratic process, he also argues that the objectives for protecting U.S. election systems are largely absent from the strategic document (Sulmeyer 2017a; Trump 2017a, 35).

Tarah Wheeler, a New America Cybersecurity policy fellow, decries the *National Security Strategy*'s prioritized actions for outsourcing cybersecurity to private sectors. She reasons that this presents a vulnerability for the United States and an opportunity for state and non-state actors to conduct cyberspace attacks against U.S. national interests (Wheeler 2018). Additionally, Wheeler believes that the *National Security Strategy* is more hostile than previous strategies and fails to call for building international norms regarding cybersecurity (Pomerleau 2017b).

National Defense Strategy

The U.S. Department of Defense (DOD) similarly acknowledges that global malicious cyberspace activities and actors are serious threats to U.S. national interests and critical infrastructure in the *National Defense Strategy* (DOD 2018b, 3). As a response to cyberspace threats, the DOD prioritizes investment in cyberspace defense and capabilities to integrate and support military operations (DOD 2018b, 6). Additionally, DOD published the *Department of Defense (DOD) Cyber Strategy* to emphasize the significance of the strategic cyberspace threats to the United States and its allies and partners.

National Cyber Strategy

In September 2018, the White House established the *National Cyber Strategy* to support and pursue the four strategic objectives outlined in the *National Security Strategy.* The *National Cyber Strategy* focuses on securing both the government and private sectors, imposing a cost to deter malicious cyberspace activities, and ensuring an open and secure Internet for economic security and prosperity including strengthening relationships with allies and partners on cyberspace issues (Trump 2018a, 2-3). Regarding partnership, the strategy emphasizes that the United States will work to build a relationship with the coalition and foreign partners, private industries, civil societies, and academia to promote Internet governance, security, and freedom (Trump 2018a, 25). Similar to the *National Security Strategy*, the *National Cyber Strategy* overtly depicts Russia, China, Iran, and North Korea as state actors that operate and challenge the United States in cyberspace (Trump 2018a, 2).

To achieve objectives in the *National Cyber Strategy,* the United States recognizes the need to develop and enhance the federal cybersecurity workforce as well as build a coalition to deter malign behaviors in the cyberspace domain (Trump 2018a, 17-21). Additionally, the *National Cyber Strategy* identifies securing federal networks and information as a high priority. The strategy further recommends centralizing the management and oversight of federal cybersecurity as well as empowering DHS to secure and defend federal networks and information (Trump 2018a, 6). Moreover, the strategy calls for integrating and improving supply chain risk management into federal government organizations' procurement processes to identify and prevent "risk vendors, products, and services" (Trump 2018a, 7).

In protecting critical infrastructure from malicious cyberspace activities, the *National Cyber Strategy* seeks to pursue public-private cybersecurity partnership in developing a comprehensive risk management approach to address "threats, vulnerabilities, and consequences." The seven priority key areas to apply this comprehensive risk management approach are “national security, energy and power, banking and finance, health and safety, communications, information technology, and transportation” (Trump 2018a, 8). Also, the strategy highlights the need to improve and secure transportation and maritime cybersecurity citing the United States’ economy and national security reliance on global trade and transportation as well as open sea and air lines of communications (Trump 2018a, 9-10).

Department of Defense Cyberspace Strategy

To implement the *National Cyber Strategy,* the DOD devised the *DOD Cyber Strategy* to address the growing threat in the cyberspace domain from peer and near-peer adversaries. The *DOD Cyber Strategy* identifies China and Russia as states that pose the most significant long-term strategic risk and competition against U.S. national interests (DOD 2018b, 1). *DOD Cyber Strategy* also acknowledges that the United States’ reliance on the Internet and the information environment for every aspect of society presents a vulnerability that malicious cyberspace actors can exploit to harm U.S. national interests. Moreover, the *DOD Cyber Strategy* emphasizes the need for the military to work close with interagency, private industry, and international partners on issues and interests in the cyberspace domain (DOD 2018b, 1).

Under the *DOD Cyber Strategy,* the Secretary of Defense prioritizes three lines of effort (LOE) for competing and contesting nation-state and nonstate cyberspace actors against U.S. national interests. The first LOE focuses on the “U.S. military’s ability to fight and win wars” which includes the cyberspace domain (DOD 2018b, 2). In the first LOE, the DOD concentrates on defending U.S. critical infrastructure and defense industrial bases in the cyberspace domain (DOD 2018b, 2). Furthermore, the DOD promotes a concept of defending forward to deny adversarial cyberspace operations against U.S. national interests and critical infrastructure (DOD 2018b, 2).

The second LOE of the *DOD Cyber Strategy* aims to defend the homeland by defeating or deterring significant malicious cyberspace activities against U.S. critical infrastructure (DOD 2018b, 2). The second LOE's goal is to preemptively stop threats in key terrain in cyberspace outside of the United States. Similar to the first LOE, defending the homeland from malicious cyberspace activity will require coordination with interagency and private entities to achieve the stated goal in the *DOD Cyber Strategy* (DOD 2018b, 2). The third LOE is to ensure the United States partners and collaborates with coalition allies and partners to "strengthen cyber capacity, expand combined cyberspace operations, and increase bi-directional information sharing" to support U.S. national and strategic objectives as well as the mutual goals of partner nations (DOD 2018b, 2).

The *DOD Cyber Strategy*'s strategic approach highlights the need to leverage all instruments of national power to defend and protect U.S. national interests across the conflict continuum. This strategic approach enables the United States to proactively compete and contest against malicious cyberspace actors and threats to DOD systems and CIKR at a level below the threshold of armed conflicts (DOD 2018b, 4).

The United States will not only employ U.S. military capability for countering adversarial cyberspace threats but will also integrate and incorporate interagency, private sector, and foreign partners to bring a broad range of whole-of-society capabilities to bear. Furthermore, the *DOD Cyber Strategy* aims to reinforce "norms of responsible state behavior in cyberspace" to prevent and dissuade malicious cyberspace activities against critical civilian infrastructure during peacetime. The United States, the United Nations, and interagency partners will promote norms and behaviors in cyberspace similar to the treatment of global commons in the maritime domain (DOD 2018b, 5).

Regarding the *DOD Cyber Strategy*, Bobby Chesney, Associate Dean for Academic Affairs at the University of Texas School of Law, assesses that the concept of "defending forward" is the United States conducting cyberspace operations and activities outside of U.S. networks to prevent or disrupt malicious cyberspace activities (Chesney 2018a). Chesney further determines that "defending forward" is a concept for globally executing cyberspace operations in adversaries' networks or midpoint infrastructure (Chesney 2018a). Additionally, Chesney infers the administration made changes to Presidential Policy Directive 20 (PPD-20) to streamline the interagency vetting process and requirements for cyberspace operations outside of the United States under the "defending forward" concept (Chesney 2018a). Moreover, Chesney assesses that the "defending forward" approach may be limited to responding to adversarial cyberspace threats against the DODIN and not private and commercial networks (Chesney 2018a).

Similarly, Nina Kollars and Jacquelyn Schneider, professors at the Naval War College, assess the tone of the 2018 *DOD Cyber Strategy* as a stark contrast from its 2015 predecessor. Kollars and Schneider suggest that the 2018 *DOD Cyber Strategy* has a "more active and risk-acceptant tone" versus the reactive language found in the 2015 version. Both Kollars and Schneider believe that the "defend forward" concept is the most significant change from the 2015 *DOD Cyber Strategy* (Kollars and Schneider 2018). Like Chesney, Kollars and Schneider assess that this concept implies a more preemptive approach to responding to malicious cyberspace activity against U.S. interests below the level of armed conflicts (Kollars and Schneider 2018).

In addition to the preemptive approach, Ben Buchanan, an assistant teaching professor at Georgetown University, infers that the *DOD Cyber Strategy* frees U.S. Cyber Command to be more aggressive and execute operations outside U.S. networks but also noted implications and risks of escalating conflicts (Buchanan 2018). Buchanan also highlights that some concepts in the *DOD Cyber Strategy* are not novel and cited the National Security Agency's activities against China's People's Liberation Army and their malicious cyberspace activities against U.S. interests (Buchanan 2018). Gary Schmitt, a resident scholar at American Enterprise Institute, also judges that the key themes in the *DOD Cyber Strategy* are not new; however, he emphasized that the strategy explicitly mentions China and Russia as adversarial competitors with the United States in the cyberspace domain (Schmitt 2018).

In opposition to the 2018 *DOD Cyber Strategy*, some experts argue that the cybersecurity strategy is reckless and will do more to harm U.S. interests than to help. Josephine Wolff, an assistant professor at the Rochester Institute of Technology, posits that the defend forward concept of conducting offensive cyberspace operations for defensive purposes will not deter but embolden malicious cyberspace actors' intents against the United States (Wolff 2018). Wolff believes that the 2018 *DOD Cyber Strategy* will escalate cyber conflicts and divert resources away from cyberspace security and defenses. Wolff further argues that the strategy does not identify means or ways for "controlling the escalation of cyberspace conflicts" (Wolff 2018). Furthermore, Wolff argues that instead of the "defend forward" concept, the United States should focus its cyberspace strategy on security, defense, and target hardening of U.S. CIKR as a better approach to counter malicious cyberspace activities (Wolff 2018).

U.S. Cyberspace Security and Operations Authorities

There are a myriad of U.S. domestic laws and authorities that enable the USG to execute cyberspace operations and secure critical infrastructure in cyberspace from malicious cyberspace activities. The DOD Joint Publication 3-12 "Cyberspace Operations" informs that authorities for military cyberspace operations are derived primarily from Title 10*, Armed Forces*; Title 50, *War and National Defense*; and Title 32, *National Guard* (JCS 2018a, III-2). In addition to military-related authorities, Joint Publication 3-12 states that interagency partners play a significant role in the cyberspace domain through their respective authorities such as Title 6, *Domestic Security*; Title 18, *Crimes and Criminal Procedures*; and Title 28, *Judiciary and Judicial Procedures* (JCS 2018a, III-3).

Title 6, Domestic Security

The DHS is the principal organization for operating and maintaining the security of the cyberspace domain within U.S. territories under Title 6, *Domestic Security,* authority (JCS 2018a, III-3). Under Title 6, *Domestic Security*, Chapter 6 *Cybersecurity,* the Secretary of Homeland Security, in coordination with the SecDef, the Attorney General, and other relevant stakeholders, is responsible for supporting cybersecurity efforts for U.S. critical infrastructure in response to a catastrophic national or economic security event (Cybersecurity 2017). Furthermore, the Title 6 statute charges the Secretary of Homeland Security and Secretary of Commerce in coordination with relevant stakeholders such as critical infrastructure owners to improve "the resilience of the internet communications and ecosystem" by decreasing the threat of automated and distributed cyberspace attacks (Cybersecurity 2017).

The Title 6 statute, *Domestic Security,* also orders the Director of National Intelligence, the Secretary of Homeland Security, the SecDef, and the Attorney General to facilitate information sharing of cyber threat indicators and defensive measures with USG and non-USG organizations including the private sector (Cybersecurity 2017). In addition, Title 6 grants private sector companies the ability to monitor and conduct defensive measures of their private networks and other non-USG organizations' networks upon consent. Similarly, Title 6 requires USG organizations to exercise and implement cybersecurity practices on federal networks (Cybersecurity 2017).

Title 10, Armed Forces

The USCYBERCOM operates under Title 10*, Armed Forces,* authority to organize, train and equip the cyber mission forces from the service components to defend and preserve U.S. national interests (Theohary and Harrington 2015, 13). Title 10, *Armed Forces*, grants USCYBERCOM the authority to conduct "offensive operations in cyberspace" (Theohary and Harrington 2015, 16). In the 2019 National Defense Authorization Act, the Title 10 statutes specifically state that the SecDef maintains the authority to "develop, prepare, coordinate, and, when appropriately authorized to do so, to conduct military cyber operations in response to cyber attacks and cyber activities" against U.S. national interests (Chesney 2018b).

Additionally, the Title 10 authority grants the SecDef authority to execute "clandestine military activities or operations in cyberspace, to defend the United States and interests of the United States" (Chesney 2018b). Chesney assesses that the Title 10 authority for cyberspace operations expands the scope to areas below the level of armed conflicts such as influence, force protection, and deterrence to address the gray zone conflict in the cyberspace domain (Chesney 2018b). Moreover, the policy also highlights that the "United States should employ all instruments of national power, including the use of offensive cyber capabilities, to deter if possible, and respond to when necessary, all cyber attacks or other malicious cyber activities" against U.S. national interests (Cyber Matters 2018).

Title 18, Crimes and Criminal Procedures

The Department of Justice, primarily through the FBI, is the principal organization for crime prevention and prosecution of criminals operating in the cyberspace domain under Title 18, *Crimes and Criminal Procedure,* authority (JCS 2018a, III-3). Under Title 18, the Computer Fraud and Abuse Act (CFAA) enforces criminal and civil liabilities against cyberspace actors who intentionally access networks or computers without permission resulting in damages to computers and theft of data (McGhee 2014, 27). Also, under Title 18 authority, the U.S. federal law enforcement agencies, such as the FBI, can prosecute against persons committing cyber espionage. In this statute, cyber espionage encompasses criminal acts including but not limited to identify theft, the disclosure of classified information, and intellectual property theft (e.g., trade secrets) (McGhee 2014, 32).

In October 2017, U.S. Congress introduced a bipartisan bill named "Active Cyber Defense Certainty Act" to amend the CFAA to authorize individuals and private sector companies the legal authority to take active cyber defense measures. Active cyber defense authorizes private sector companies to conduct activities outside their networks to monitor and attribute malicious cyberspace actors, disrupt cyberspace attacks, and retrieve and destroy stolen data (Grave 2017). As of April 2019, the "Active Cyber Defense Certainty Act" remains as a draft document in the U.S. House of Representatives (U.S. Congress 2017).

Title 32, National Guard

The National Guard maintains the fiscal and mission authorities and is responsible for conducting cyberspace actions under Title 32 status (NGB 2019, 218). The President and the SecDef also have authority to execute operational missions in cyberspace under Title 32 in Defense Support to Civil Authorities' role. Under the Title 32 authority, the National Guard is not able to conduct DCO-RA and offensive cyberspace operations; however, the National Guard has the authorization to conduct DCO to identify malicious cyberspace activities on DODIN (NGB 2019, 218-219).

Title 50, War and National Defense

The national level intelligence community operates under Title 50, *War and National Defense*, authority to conduct military and foreign intelligence operations in the cyberspace domain (JCS 2018a, III-3). Under Title 50 authority, The National Security Agency (NSA) is responsible for conducting signal intelligence which encompasses activities such as computer network exploitation to collect foreign intelligence and data from adversary information systems or networks (Schoka 2019). Within this legal constraint, the NSA does not possess the authority to conduct offensive cyberspace operations against adversary networks (Sulmeyer 2017b). The former commander of

United States Cyber Command (USCYBERCOM), General Keith Alexander, noted that the NSA and USCYBERCOM maintain a collaborative relationship by design; however, each organization has a separate and distinct mission with different authorities (Wall 2011, 117).

U.S. Cyberspace Organizations

United States Cyber Command Vision

To support the *2018 National Defense Strategy,* USCYBERCOM establishes a command vision to achieve and maintain superiority in cyberspace to defend and protect U.S. interests (USCYBERCOM 2018, 2). The command vision also promulgates guidance for defending and advancing U.S. interests in collaboration with domestic and foreign partners such as the FBI and DHS (USCYBERCOM 2018, 2). In addition, the command vision describes the operational environment stating that adversarial malicious cyberspace actors conduct operations against the U.S. interests below the threshold of armed conflict (USCYBERCOM 2018, 3). These state-sponsored malicious cyberspace actors understand United States policy constraints, specifically "high threshold for response to adversary activity," which enables freedom of action against the United States without reprisal (USCYBERCOM 2018, 3).

Similar to the *DOD Cyber Strategy,* the USCYBERCOM's command vision puts forth a concept to "defend forward as close as possible to the origin of adversary activity" to disrupt adversaries' operations against the United States at a threshold below the level of armed conflict (USCYBERCOM 2018, 4). Consequently, the USCYBERCOM's command vision seeks a policy framework to shorten the approval process for enabling U.S. response action against malicious cyberspace activities (USCYBERCOM 2018, 5).

The command vision also emphasizes a whole-of-government approach capable of adapting and operating in an everchanging cyberspace domain to continuously shape the environment (USCYBERCOM 2018, 4). Specifically, USCYBERCOM will strengthen partnership with the "Defense Information Systems Agency, the National Security Agency (NSA), and the rest of the Intelligence Community" to coordinate and share information on malicious cyberspace activities against U.S. national interests (USCYBERCOM 2018, 7). Moreover, the command vision calls for USCYBERCOM to collaborate with and leverage the capabilities of private sectors, military service components, allied partners, and academia (USCYBERCOM 2018, 9). The collaboration with various cybersecurity partners will enable information sharing and operational planning to counter malicious cyberspace activities against the United States and allied interests (USCYBERCOM 2018, 9).

Department of Homeland Security Cybersecurity Strategy

Much like the DOD, the DHS established the *DHS Cybersecurity Strategy* to support the strategic objectives in the *National Security Strategy* in May 2018. Through the strategy, DHS aims to secure cyberspace, enabling essential services such as electricity and health care as well as reducing vulnerabilities in networks supporting U.S. critical infrastructure (DHS 2018, 1). Additionally, the *DHS Cybersecurity Strategy* highlights that growing interconnected systems and low cost of cyber capabilities increase potential threats to U.S. critical infrastructure from state and nonstate actors (DHS 2018, 2).

In support of the *National Security Strategy,* the *DHS Cybersecurity Strategy* outlines five pillars for managing and mitigating cybersecurity risks (DHS 2018, 3). The first pillar, risk identification, aims to understand and assess growing cybersecurity risks to U.S. interests (DHS 2018, 3). The second pillar, vulnerability reduction, directs DHS to protect federal government information systems and networks from malicious cyberspace activities. In the third pillar, threat reduction, DHS' goal is to prevent and disrupt nonstate actors and criminal use of cyberspace to harm U.S. interests (DHS 2018, 3).

In the *DHS Cybersecurity Strategy*, the fourth pillar, consequence mitigation, charges DHS to coordinate and collaborate with the community and interagency partners to respond to cyber incidents (DHS 2018, 3). Finally, the fifth pillar, enable cybersecurity outcomes, seeks to strengthen the security and reliability of the global cyberspace domain supporting U.S. CIKR (DHS 2018, 3). Moreover, the fifth pillar aims to improve and prioritize DHS cybersecurity activities to actualize the goals in all the pillars (DHS 2018, 3). Within the strategy, DHS will work with private sectors, federal, and nonfederal partners to accomplish the cybersecurity goals outlined in the five pillars.

More specifically, the *DHS Cybersecurity Strategy*'s third pillar focuses on disrupting criminal use of cyberspace. The strategy establishes objectives to counter illicit cyber-criminal activities and cyberspace threats to U.S. personal data and critical infrastructure (DHS 2018, 16). The third pillar also calls for DHS to develop relationships with law enforcement organizations to counter malicious cyberspace activities (DHS 2018, 17). Also, in the fourth pillar, consequence mitigation, one of the objectives aims to increase DHS cooperation with law enforcement agencies, the intelligence community, and other entities to respond to the cyberspace threats (DHS 2018, 21).

Department of State Cybersecurity Policy

The White House issued a *Presidential Executive Order (EO) on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* to direct executive departments and agencies to manage cybersecurity risks to their respective networks and infrastructure in May 2017 (Trump 2017b). Additionally, the Presidential EO called on the executive branch to provide cybersecurity support to the owners of U.S. CIKR (Trump 2017b). In response to the Presidential EO, the Department of State (DOS) issued two recommendations to the President for cybersecurity-related matters.

In May 2018, the DOS published a recommendation for “Protecting American Cyber Interests through International Engagement” in response to the May 2017 Presidential EO. The recommendation addresses challenges in the cyberspace environment such as increasing vulnerabilities of interconnected information communication technologies (ICT), state and non-state cyberspace threats to U.S. interests and critical infrastructure, and preservation of free and open Internet (Office of the Coordinator for Cyber Issues 2018b). In this recommendation and strategy, the DOS’ goal is to strengthen USG’s ties and cooperation with foreign partners and allies to combat cyberspace threats and improve cybersecurity (Office of the Coordinator for Cyber Issues 2018b). Through this strategy, the DOS seeks to ensure that the Internet remains a global common as “valuable and viable tools for future generations” (Office of the Coordinator for Cyber Issues 2018b). Furthermore, this strategy calls for DOS to support existing U.S. interagency efforts regarding international engagement for cyberspace related matters (Office of the Coordinator for Cyber Issues 2018b).

Within the DOS International Engagement strategy, the document outlines five objectives to further U.S. interests with foreign partners in cyberspace. The first objective of the strategy is to “increase international stability and reduce the risk of conflict” due to cyberspace threats and malign activities (Office of the Coordinator for Cyber Issues 2018b). Second, the strategy identifies an objective for identifying and taking actions against malicious cyberspace actors and activities (Office of the Coordinator for Cyber Issues 2018b). Also, the strategy promotes a free and open Internet to uphold human rights as the third objective. The strategy’s fourth objective aims to maintain the “essential role of non-governmental stakeholders” within the Internet and cyberspace governance area (Office of the Coordinator for Cyber Issues 2018b). Finally, the International Engagement strategy will advance and preserve international norms of the global cyberspace (Office of the Coordinator for Cyber Issues 2018b).

Congruently, in May 2018, the DOS published a recommendation for “Deterring Adversaries and Better Protecting the American People from Cyber Threats” (Office of the Coordinator for Cyber Issues 2018a). In recommendation and strategy, the document highlights the malicious cyberspace actors’ threat to the United States' economy and democracy by “steal[ing] from Americans [and] creat[ing] insecurity domestically” (Office of the Coordinator for Cyber Issues 2018a). To deter the threats, the strategy’s end states are to free the United States from cyberspace attacks that constitute a use of force (below the level of armed conflict) and reduce destabilizing malicious cyberspace activities against U.S. interests falls the threshold of armed conflict (Office of the Coordinator for Cyber Issues 2018a). The DOS strategy promulgates the USG to deter malicious cyber actors through the denial of benefits and cost imposition (Office of the Coordinator for Cyber Issues 2018a).

In support of the end states, the DOS strategy identifies four key elements for deterring malicious cyberspace actors and activities. The first element is to develop a policy for establishing criteria for malign activities and behaviors in cyberspace to apply appropriate cost imposition methods (Office of the Coordinator for Cyber Issues 2018a). The second element calls for the USG to develop a range of consequences and options to take against malicious cyberspace activities below the threshold of the use of force (level of armed conflict) (Office of the Coordinator for Cyber Issues 2018a). Additionally, the third element recommends the USG to "conduct interagency policy planning for the . . . imposition of consequences" against malicious cyberspace activities below the level of armed conflict (Office of the Coordinator for Cyber Issues 2018a). Furthermore, the strategy emphasizes building a partnership with foreign partners and allies to bolster the effects of deterrence and cost imposition as the fourth and final element (Office of the Coordinator for Cyber Issues 2018a).

Department of Justice's Cyber Digital Task Force

The Department of Justice (DOJ) established a Cyber-Digital Task Force to determine how the department can effectively respond to cyberspace threats to the United States in February 2018 (Office of the Deputy Attorney General 2018, xi). In the opening remarks, DOJ Deputy Attorney General, Rod Rosenstein, highlighted the recent trends of malicious cyberspace actors targeting U.S. citizens, businesses, military, and government as well as the undermining of U.S. democratic systems and values. Regarding this trend, Rosenstein emphasized that countering cybercrime and malicious cyberspace activities is the DOJ's highest priorities (Office of the Deputy Attorney General 2018).

The DOJ is an integral member of the USG in protecting and defending U.S. democratic processes against malign foreign influence operations (Office of the Deputy Attorney General 2018, 1). The DOJ employs the FBI as the primary investigative agency to work with intelligence community partners to identify and disrupt foreign influence operations including malicious cyberspace activity (Office of the Deputy Attorney General 2018, 6-7). To combat foreign influence operations, the DOJ publicly reveals and investigates the malign activity and cyberspace threats to U.S. democratic institutions (Office of the Deputy Attorney General 2018, 1). Moreover, the DOJ, in concert with interagency partners, supports financial sanctions, diplomatic efforts, and intelligence sharing to counter foreign influence and cyberspace threats against the United States (Office of the Deputy Attorney General 2018, 7-8).

Also, the DOJ is responsible for "detecting, deterring, and disrupting cyber threats" to the United States (Office of the Deputy Attorney General 2018, 48). The DOJ counters malicious cyberspace actors through evidence collection during incident response, online reconnaissance, undercover investigations, and analysis of financial transactions to disrupt the cyberspace threats (Office of the Deputy Attorney General 2018, 48). As cyberspace threat is global, the DOJ will cooperate with foreign governments to share information to mitigate incident and malicious activities outside of the United States (Office of the Deputy Attorney General 2018, 56).

The DOJ also partners with foreign governments to "extradite persons charged with or convicted of certain crimes" including cybercriminals (Office of the Deputy

Attorney General 2018, 58-9). In conjunction, the DOJ, through FBI and in partnership with the private sector, seeks to interdict malicious cyberspace activities by denying actors access to infrastructure and capabilities for cyberspace operations (Office of the Deputy Attorney General 2018, 69). The DOJ assists and provides legal and policy support to interagency partners executing cyberspace operations against malicious cyberspace actors to ensure actions are in accordance with the U.S. Constitution (Office of the Deputy Attorney General 2018, 75).

In addition to the foreign and interagency partnerships, the FBI established several programs to collaborate and share information with private sectors on cybersecurity matters. Some of the DOJ-FBI and private partnership programs are Domestic Security Alliance Council, InfraGard, National Cyber-Forensic and Training Alliance (NCFTA), National Domestic Communications Assistance Center, and Internet Crime Complaint Center (IC3) (Office of the Deputy Attorney General 2018, 87). Through these programs, the FBI issues warning and notifications of compromise and cyber intrusion to private sectors as well as receive information on malicious cyberspace activity from victims (Office of the Deputy Attorney General 2018, 88).

Federal Bureau of Investigation

The Federal Bureau of Investigation (FBI) has the responsibility to lead the United States' efforts to investigate and prosecute crime per the 2003 *President's National Strategy to Secure Cyberspace* (FBI 2019a). To accomplish the mission, the FBI leads the National Cyber Investigative Joint Task Force (NCIJTF) to coordinate with intelligence communities and law enforcement agencies to investigate, mitigate, and disrupt malicious cyberspace activity (FBI 2019a). Furthermore, the FBI will continue collaboration with industry partners, cybersecurity researchers, and academia to respond and counter cyberspace threats against U.S. interests through programs such as NCFTA and IC3 (FBI 2019a).

The 2008 Comprehensive National Cybersecurity Initiative (CNCI) created the FBI-led NCIJTF to establish a whole-of-government approach to address and defend against cyberspace threats to U.S. interests (FBI 2019b). At the national level, the FBI-led NCIJTF's aim is to collaborate and integrate with interagency and law enforcement operations against cyber terrorists, state-sponsored intellectual property theft, and cybercriminals (FBI 2019b). On the local level, the FBI maintains Cyber Task Forces (CTF) in all fifty-six field offices to counter malicious cyberspace activities with state and local law enforcement entities. The CTF "synchronizes domestic cyber threat investigations in the local community through information sharing, incident response, and joint enforcement and intelligence actions" (FBI 2019b). As an example, the CTFs collaborate and coordinate with private companies and institutions to share information regarding the cyberspace threats (FBI 2019b).

Public-Private Partnership in Cyberspace

The cyberspace domain is mostly dominated by the private sector. General Nakasone, CDRUSCYBERCOM, emphasizes that building a robust public-private partnership in cyberspace is a top priority, citing that ninety percent of networks supporting critical infrastructure belong to the private sector (JFQ 2019, 5). Adam Segal, the Director of the Digital and Cyberspace Policy Program at the Council on Foreign Relations, estimates more than ninety percent of U.S. military and intelligence communications transmit through privately owned backbone telecommunication networks (Segal 2017, 67). Additionally, Segal infers that the “most talented hackers are in the private sector and private security firms such as CrowdStrike, FireEye, and Cylance” (Segal 2017, 67).

Despite USG’s reliance on the private sector, the relationship between the USG and private sectors began to fall apart following Edward Snowden’s disclosure of U.S. intelligence community targeting U.S. internet systems and platforms for collection information (Segal 2017, 67-68). In 2017, federal agencies, including the FBI, sought U.S. information technology (IT) companies to “provide the technological means to bypass encryption, known as exceptional access or creating backdoors” for intelligence and national security purposes. However, technology companies rejected USG requests for a backdoor to their respective online platforms, arguing that backdoors pose a security threat and compromise for all users on the platforms (Segal 2017, 69).

To bridge the gap between the USG and the private sector, White House and DOD officials began outreach to technology companies in Silicon Valley during the Obama Administration (Segal 2017, 72). To strengthen the relationship, Secretary of Defense Ashton Carter created the Defense Innovation Unit Experimental (DIUx) to facilitate collaboration between DOD and private sector to harness technology companies’ innovation through an agile procurement process in support of the U.S. military. Additionally, in March 2016, Secretary Carter established the Defense Innovation Advisory Board to solicit advice from technology companies’ experts and leaders, including Apple’s CEO, in addressing national security issues (Segal 2017, 72).

The malicious cyberspace activities from state and nonstate actors pose a significant national security challenge for the United States. Megan Brown, a senior fellow at National Security Initiative, highlights that the malicious cyberspace activities and threats require collaboration between cybersecurity companies, suppliers, academia, and the USG (Brown 2018, 2). There are existing USG policies for cybersecurity public-private partnership (PPP). In 2015, the White House issued EO 13691, “Promoting Private Sector Cybersecurity Information Sharing,” that enforces DHS to develop and establish Information Sharing and Analysis Organizations (ISAOs) consisting of public and private sector entities (Obama 2015). The purpose of the ISAOs is to “create information sharing related to cybersecurity risk and incidents” between USG and the private sector (Obama 2015).

In July 2018, the Secretary of DHS also noted that the private sector owned the majority of critical infrastructure networks and emphasized the importance of PPP in defending the said networks at the National Security Summit (Brown 2018, 2). Brown connotes that the National Institute of Standards and Technology (NIST) provides a framework for cybersecurity PPP by facilitating an open and transparent forum for private industry and academic expertise to share best practices and standards for mitigating cyberspace threats to CIKR (Brown 2018, 6). Brown further argues that private industries can assess the malicious cyberspace threats to their respective networks as well as apply mitigation techniques, which can inform and increase the PPP’s shared understanding of the cyberspace threats to U.S. national interests (Brown 2018, 11). Moreover, Brown recommends that U.S. policymakers create “safer ways for companies to manage and discuss vulnerabilities” in software and hardware with USG organizations (Brown 2018, 17).

Theories on Cyberspace

Global Commons in Cyberspace

The cyberspace domain is part of the global commons. In the 2010 Quadrennial Defense Review (QDR), the DOD identified "cyberspace as a global commons or domain, along with air, sea and space" (Theohary and Harrington 2015, 2). As defined in chapter one, global commons are areas outside the jurisdiction of sovereign states and where every state has access to said areas. Roger Hurwitz, a research scientist at the Massachusetts Institute of Technology, determined that states, organizations, and individuals' actions and behaviors in the cyberspace domain are "not subject to a central authority" similar to the global commons (Hurwitz 2012, 21).

In October 2016, the Joint Chiefs of Staff developed and approved the Joint Concept for Access and Maneuver in the Global Commons (JAM-GC). The JAM-GC enables the U.S. joint forces to "maintain access to and maneuver through the global commons, project power, and defeat an adversary attempting to deny freedom of action to the [United States] and allied forces" (Hutchens, Dries, Perdew, Bryant, and Moores 2017, 135). Although global commons are international areas of sea, air, space, and cyberspace, the JAM-GC concept highlights that the global commons' importance to U.S. national interests and security (Hutchens et al. 2017, 136-137). The concept aims to compete and contest against peer and near-peer adversaries from threatening and countering the United States' ability to project power and defend access to the global commons, including the cyberspace domain.

In contrast, Sam Tangredi, the Director of the Institute for Future Warfare Studies at the Naval War College, argues that cyberspace as a global common is a misleading and false analogy (Tangredi 2018, 1). Tangredi cites authoritarian governments, such as the Chinese Communist Party (CCP), that are denying access to their sovereign cyberspace (e.g., the Great Firewall of China) and changing the domain from global commons to cyber "territorial seas" (Tangredi 2018, 1). He illustrates that territorial seas are ocean waters within twelve miles of a coastline where states can exercise sovereign rights (Tangredi 2018, 5). Moreover, Tangredi highlights that the coastal state can block access against illicit activities (e.g., illegal fishing, drugs) to their respective territorial seas (Tangredi 2018, 5). Therefore, Tangredi recommends replacing the analogy of cyberspace as a global common to cyber "territorial seas" (Tangredi 2018, 10). Similarly, Andrew Liaropoulos of the University of Piraeus in Greece states that cyberspace does not meet the legal criteria of a global commons given that the physical infrastructures that store and transfer data and make up the Internet are in sovereign territories (Liaropoulos 2016, 15).

Deterrence in Cyberspace

For the past decade, state and nonstate actors, such as Russia and China, executed cyberspace attacks and exploitation against the United States, most notably the Russian hacking operations during the 2016 U.S. presidential campaign. In these instances, the United States' response to cyberspace incidents failed to deter malicious cyberspace actors' operations against U.S. interests. Michael Sulmeyer, the director at Cyber Security Project, cites three main problems with cyberspace deterrence. First, Sulmeyer asserts that the "United States has more to lose than its adversaries" because the United States has advanced technological innovation and intellectual properties without safeguarding them in the cyberspace domain (Sulmeyer 2018). Sulmeyer further notes that the Cold War deterrence does not work in cyberspace given that the United States and the Soviet Union were both equally vulnerable to the opposing parties' nuclear weapons (Sulmeyer 2018).

Additionally, Sulmeyer emphasizes the difficulty in convincing state and nonstate cyberspace actors that the repercussions and costs of malign behavior in cyberspace outweigh the benefits (Sulmeyer 2018). Sulmeyer notes that presenting a credible threat to change an adversary's decision-making calculus is difficult as it relates to understanding perceptions. Furthermore, Sulmeyer believes that measuring the effectiveness and monitoring the progress for deterrence in cyberspace domain is "virtually impossible" (Sulmeyer 2018). Based on this assessment, Sulmeyer concludes that the United States is unable to determine whether malicious cyberspace activities cease due to a U.S. response action or to an unknown failure within cyberspace operation (Sulmeyer 2018).

Rather than pursuing deterrence in cyberspace, Sulmeyer assesses that the United States should conduct a cyberspace operations campaign against malicious cyberspace actors' infrastructure and online accounts to sabotage their capabilities against U.S. interests (Sulmeyer 2018). Also, Sulmeyer expresses that the United States should continue to take indirect measures, such as sanctions, to impose cost and limit access to resources for malicious cyberspace actors (Sulmeyer 2018). Moreover, Sulmeyer believes that the current cyberspace operations occur below the level of armed conflict, which he labeled as the "gray zone" (Sulmeyer 2018).

Similarly, James Andrew Lewis, the Director of Technology Policy Program at Center for Strategic and International Studies (CSIS), assesses that U.S.' adversaries develop cyberspace strategy to avoid retaliation by conducting operations at a threshold below the level of armed conflict (Lewis 2018b, 9). Like Sulmeyer, Lewis also explains that a Cold War-style deterrence in cyberspace is not achievable due to the low threshold of malicious cyberspace activities (Lewis 2018b, 9). Lewis further highlights that the United States and its allies are unable to respond through military deterrent force against malicious cyberspace activities that fall in the "gray zone" (or area) (Lewis 2018b, 16). Additionally, Lewis surmised that indictment and sanctions are effective measures to counter malicious cyberspace activities. However, Lewis believes that the most effective response is a U.S. proportional counter cyberspace operation to control escalation in the cyberspace domain (Lewis 2018b, 38).

The former U.S. cyberspace strategy based on deterrence theory is difficult to enforce due to the clandestine nature of the cyberspace domain. Michael Fischerkeller, a researcher at the Institute of Defense Analyses, explains that deterrence strategy requires the knowledge of the source of perceived cyberspace threat to proportionally deter malign behaviors. However, Fischerkeller notes that malicious cyberspace actors use cyberspace to conceal their operations and attribution, making it difficult for the United States to deter the culprits in this domain (Fischerkeller 2017). Also, Fischerkeller infers that the United States should adopt a strategy of "active and persistent engagement in cyber operations" to ensure a strategic advantage over adversarial nation-state actors (Fischerkeller 2017).

The purpose of deterrence is to intimidate and threaten opponents through coercion to prevent the escalation of hostilities. Jim Chen, a professor of Cybersecurity Studies at National Defense University, explains that the current deterrence strategies employ denial and punishment methods based on conventional deterrence models (Chen 2017, 101). However, Chen assesses that the effectiveness of deterrence by punishment in cyberspace has a minimal impact due to the clandestine nature of cyberspace operations (Chen 2017, 102). Chen further expounds that deterrence by denial can pressure and deter adversaries from multiple domains (e.g., law enforcement action and sanctions), but the approach requires a "near-perfect collaboration from all relevant domains . . . [which] is difficult to achieve" (Chen 2017, 102).

Chen believes that cyberspace capabilities weapons are not as catastrophic as nuclear weapons; therefore, the scope of U.S. retaliatory responses in cyberspace are limited (Chen 2017, 103). Moreover, Chen argues that deterrence by engagement and surprise is a viable method for pressuring and dissuading adversaries from conducting malicious cyberspace activities (Chen 2017, 104-105). An example of deterrence by surprise is generating responses, such as surprise warning message or video clips, to scare and coerce malicious cyberspace actors (Chen 2017, 105).

Akin to the issues stated above, Dorothy Denning, a professor at Naval Postgraduate School, identified several challenges to deterrence in cyberspace such as attribution of the perpetrator, low barrier to entry in acquiring cyber weapons, and difficulties in enforcing international norms in the cyberspace domain (Denning 2015, 11). Denning believes that the deterrence by denial model is a viable option for deterring malicious cyberspace activities using existing cybersecurity programs and practices (Denning 2015, 12). Cybersecurity programs and practices such as anti-spoofing technologies and vulnerability patching can stop malign actors from executing a successful denial of service or phishing attacks (Denning 2015, 12). As a result of this study, Denning advocates for more effective cybersecurity practices by integrating cybersecurity "during the design, development, installation, and operation of new cyber technologies" (Denning 2015, 14).

Similar to the Joint DOD definition, Joseph Nye Jr., professor and former Dean of the John F. Kennedy School of Government at Harvard University, defines deterrence as dissuading an actor from a certain action by making the said actor believe the cost exceeds the expected benefit (Nye 2017, 45). Echoing earlier remarks on deterrence in cyberspace, Nye assesses that nuclear deterrence is not transferrable to the cyberspace domain because the United States' aim for nuclear deterrence is "total prevention" (Nye 2017, 45).

Highlighting the difference between nuclear and cyber deterrence, Nye articulates the difficulties of deterring malign behavior in cyberspace similar to preventing crime (Nye 2017, 45). As such, Nye cites the 2014 North Korean-sponsored cyberspace attack against SPE and 2016 Russian influence campaign against U.S. democratic systems as failures of deterrence but classifies the events as "relatively low-threshold attacks" (Nye 2017, 48). Similar to James Lewis' analysis above, Nye observes that past state-sponsored and nonstate cyberspace attacks and events fell into the "gray zone" between war and peace (Nye 2017, 48). Like many experts on cyberspace deterrence, Nye also argues that the problem of attribution increases the difficulty in deterring malign behavior in the cyberspace domain (Nye 2017, 49).

In World War II, deterrence against bombing major cities failed. However, the impacts and severe consequences of chemical and biological weapon attacks against Chinese soldiers and Japanese civilians deterred Adolf Hitler from using the capability against Allied forces in fear of retaliation (Nye 2017, 53). Likewise, Nye assesses that transparency of offensive cyberspace capabilities may deter malicious cyberspace activities as it highlights the severity and threat of retaliation (Nye 2017, 54).

According to Nye, the four means of deterrence and dissuasion in cyberspace are the "threat of punishment, denial by defense, entanglement, and normative taboos" (Nye 2017, 54). Of note, many earlier scholars emphasize deterrence of denial as defensive cybersecurity, but Nye highlights that expending a malicious actor's time and resource, through offensive means, can increase cost over expected benefits (Nye 2017, 54). Also, Nye believes that security cooperation and assistance with allies and coalition partners can bolster deterrence in cyberspace (Nye 2017, 57).

Regarding cyberspace deterrence, Colonel Timothy McKenzie, a fellow at the Air Force Research Institute, assesses that the current U.S. strategy does not possess the key elements for an effective deterrence against malicious cyberspace activities. As such, McKenzie identifies four key elements for an effective deterrence as "deterrent declaration, penalty measures, credibility, and fear" (McKenzie 2017, 11). Like other experts, McKenzie believes that defending and securing U.S. networks and systems are critical; however, he deems that deterrence by denial, through cyber defenses alone, is a passive strategy and will likely be unsuccessful at deterring malign behavior in cyberspace (McKenzie 2017, 11). McKenzie further observes that some states, such as North Korea and Iran, are resilient against soft power pressure, such as economic sanctions. In these cases, McKenzie emphasizes that the United States may require a "credible threat of military actions" to deter malicious cyberspace activities against U.S. interests (McKenzie 2017, 13).

The transmission of information in and through cyberspace globally enables global economic systems, nation-states' governance capabilities, militaries, and social organizations (Lawlor-Russell 2015, 153). Alison Lawlor Russell, a professor at Merrimack College, investigates the strategic implications of Anti-Access and Area Denial in the cyberspace domain. In the traditional domain, Anti-Access and Area Denial is to deny the adversary freedom of action and entry into a contested area through the control of the battlespace (Lawlor-Russell 2015, 155).

Russell states that strategic cyber Anti-Access and Area Denial is the "ability to gain control of the network or infrastructure of cyberspace and manipulate it in such a way as to deny a state the ability to use cyberspace in any capacity" (Lawlor-Russell 2015, 156). Similar to the concept of deterrence by denial, states can deny an adversary access to critical infrastructure by actively "driv[ing] the enemy out of cyberspace" (Lawlor-Russell 2015, 156). From a vulnerability standpoint, Russell notes that malicious cyberspace actors could cut off countries from cyberspace through cyberspace operations against physical infrastructures, such as Internet exchange points, that connect the countries to the Internet (Lawlor-Russell 2015, 156).

Persistent Engagement in Cyberspace

In an interview, General Paul Nakasone, CDRUSCYBERCOM, infers that the threat of cyberspace capability or weapon system is not as effective as using capabilities to change adversaries' decision calculus for conducting malicious cyberspace activities against U.S. interests (JFQ 2019, 3). Nakasone defines persistent engagement as "the concept that states we [USCYBERCOM] are in constant contact with our adversaries in cyberspace, and success is determined by how we 'enable' and 'act'" (JFQ 2019, 6). He further expounds that the “enable” component of the persistent engagement concept is to enable interagency partners and private sectors. The “act” component of the persistent engagement concept is conducting cyberspace operations outside of U.S. borders to understand adversaries’ capabilities and intent (JFQ 2019, 6-7).

The USCYBERCOM is shifting its strategic concept from a “response force” through DCO-RA to a “persistent force” to contest adversaries’ malicious cyberspace activities and efforts in cyberspace against U.S. national interests. Nakasone assesses that a persistent force, in concert with interagency, private sector, and foreign partners, will impose and increase costs to adversaries’ malicious cyberspace activities against the United States (Nakasone 2019b, 11). The persistent engagement concept empowers USCYBERCOM to contest adversaries’ malicious cyberspace activities and execute decisive action in periods below the level of armed conflict in support of the *DOD Cyber Strategy*’s objective of defending forward (Nakasone 2019b, 12). Furthermore, Nakasone draws a parallel from the physical to the cyberspace domain in that the “U.S. naval forces do not defend by staying in port, and our airpower does not remain at airfields. They patrol the seas and skies to ensure they are positioned to defend [the homeland]” (Nakasone 2019b, 12).

CHAPTER 3

RESEARCH METHODOLOGY

Introduction

This qualitative research begins with assumptions that the USG lacks a comprehensive whole of society approach for countering malicious cyberspace activities and that deterrence of "gray zone" cyberspace attacks against U.S. interests is unattainable (Creswell 2007, 37). This study uses the qualitative constructivist-interpretivist format to conduct a literature review and collect multiple sources of data and evidence to support the analysis in Chapter 4 (Creswell 2007, 43, 47).

The author establishes qualitative primary and subordinate research questions to guide and scope the research and analysis of this study (CGSC 2018, 27). The primary research question of this study is as follows "as deterrence in cyberspace fails, how can the United States develop a whole of society approach in the informational domain to proactively compete and contest state-sponsored malicious cyberspace actors and activities against U.S. national interests in a state below the level of armed conflict?" The subordinate questions address the aspects of policy considerations, capability requirements, and organizational structure and responsibilities imperative for answering the primary question.

Data Collection

The previous literature review on the comprehensive theoretical and strategic framework on cyberspace as a global common, a capability, and a domain is the basis for the data collection that informs the analysis in a subsequent chapter (CGSC 2018, 30).

Also, the literature review provides a broad spectrum of viewpoints and opinions on cyberspace deterrence, defending forward concept (e.g., active cyberspace defense), and cyberspace policies. Through the literature review, the collection of data for this research study primarily consists of national strategic documents, USG organizations' official websites and documents, subject matter expert opinion articles, scholarly journals, and open source news articles. The criteria for assessing credibility and trustworthiness of the collected data are (1) origin of information (e.g., reputable digital libraries such as JSTOR and Ebscohost), (2) authority (e.g., subject matter expert's accounts), and (3) relevance (e.g., connection between collected data and thesis) (BYU 2019).

The organization of the literature review uses the categories of national-level strategies on cyberspace, USG cyberspace organizations, and theories on cyberspace (e.g., deterrence and global commons). The first category of national-level strategies on cyberspace provides the purpose and the requirement for a U.S. whole of society approach for competing in cyberspace as well as understanding policy implications. Additionally, the national-level strategies inform the significant impacts of the cyberspace domain to the instrument of national powers—diplomatic, information, military, and economics. An observation of the national-level strategies also highlights gaps in cyberspace capabilities and policies.

The second category of USG cyberspace organizations identifies respective interagency missions (ends), operational approaches (ways), and capabilities (means) to achieve the goals of national-level strategies. The second category also depicts the overlap as well as diverse mission sets within the USG for cybersecurity and cyberspace operations. An analysis of the various USG cyberspace organizations, including the private sector, assists in identifying ways to integrate capabilities in support of a whole of society approach.

Finally, the third category of the literature review, theories on cyberspace, provides subject matter experts' opinion and analysis of the application of deterrence theory in cyberspace and sovereignty and global commons in the cyberspace domain. Subject matter experts' assessment of cyberspace deterrence and global commons informs USG policies and options for proactively competing and contesting malicious cyberspace activities. Furthermore, subject matter experts' analysis can assist in the determination of what constitutes appropriate use of cyberspace force.

In addition to the literature review, this research study will collect qualitative data on USSOUTHCOM's Joint Interagency Task Force – South (JIATF-South) using scholarly journals, periodicals, USG official websites, public statements, and open source material to form a case study. The collection of data will focus on doctrine, organizational structure, leadership, and policies for JIATF-South to form a solution for a whole of society approach in the cyberspace domain.

Data Analysis and Synthesis

This research study will analyze and examine the case study of USSOUTHCOM's JIATF-South. A case study involves "the study of an issue explored through one or more cases within a bounded system . . . through detailed, in-depth data collection involving multiple sources of information" (Creswell 2007, 73). This study will explore the issue of establishing a USG whole of society approach to counter malicious cyberspace activities below the level of armed conflict. The author of this study will conduct a direct interpretation of the case studies by looking at a “single instance and draw meaning from it without looking for multiple instances” (Creswell 2007, 163)

The research study will conduct an in-depth inquiry of the bounded case on JIATF-South. This paper focuses on JIATF-South as their mission focusing on transnational issues similar to the malicious cyberspace threats to U.S. national interests. JIATF-South’s mission is to “detect and monitor illicit trafficking across all domains and facilitate international and interagency interdiction to enable the disruption and dismantlement of illicit and converging threat networks in support of national and hemispheric security” (JIATF-South 2019b). This organization integrates federal, state, and local agencies, interagency, U.S. military, the intelligence community, and foreign partners to solve a transnational problem critical to U.S. national security.

This research study will analyze JIATF-South through the lens and criteria of doctrine, organization, leadership, and policy. The Joint Capabilities Integration Development System (JCIDS), a DOD capability gap and solution analysis, forms the basis for the case study’s research criteria (JCS 2018b). The author will systematically identify and weigh strength, weaknesses, opportunities, and threats (SWOT) of the proposed JCIDS criteria. The SWOT analysis assists research analysis in exploring “possibilities for new efforts or solutions to problems” as well as determine changes to current efforts (KU 2018). The goal of SWOT analysis is to identify and recognize the weaknesses and threats to the current approach to competing and contesting malicious cyberspace activities against the United States by “countering them with a robust set of strategies that build upon strength and opportunities” (KU 2018). In addition to the JCIDS criteria, this analysis will explore this task force’s impacts and implications for integrating the instruments of national power (diplomatic, information, military, and economic).

Table 1. SWOT Analysis for Case Study

		DOTMLFP-P FRAMEWORK			
		DOCTRINE	ORGANIZATION	LEADERSHIP	POLICY
JIATF-SOUTH	STRENGTH				
	WEAKNESS				
	OPPORTUNITIES				
	THREATS				

Source: Created by author.

Summary

The primary purpose of this study is to advocate for changes in current policies and methods for a whole of society approach to proactively compete and contest adversarial malicious cyberspace activities against the United States. This qualitative research methodology—using case study analysis of JIATF-South—will inform the findings and recommendation for identifying the whole of society solution in the cyberspace domain. An in-depth SWOT analysis will help mitigate the author’s bias by identifying both strength and weaknesses as well as threats for this case study. Furthermore, a thorough analysis of JIATF-S will provide a framework for solving complex transnational issues such as cyberspace threats against U.S. national interests.

CHAPTER 4

ANALYSIS

Introduction

This chapter will form the analysis using SWOT framework to answer the primary research question on establishing a whole of society approach to effectively compete and contest adversary cyberspace actors' malign activities against the homeland during steady-state operations or in a period below the level of armed conflict (USAF 2015). The root causes of the problem for the lack of comprehensive U.S. cyberspace actions against malicious cyberspace activity are slow USG bureaucratic process, information stovepipes, and the ineffective integration of interagency operational capabilities (Abercrombie-Winstanley 2018). This chapter will address the secondary research questions by examining the case study of JIATF-South's doctrine, organization, leadership, and policies as well as its application for solving the transnational issue of countering malicious cyberspace activity.

The United States understands the importance of the cyberspace domain. In the fiscal year 2019, the President's Budget contained a $15 billion budget authority for cybersecurity-related activities which is about $580 million increase from the previous year (Trump 2019, 273). However, for the past decade, there was a lack of common understanding or concept for what constitutes an appropriate shaping activity in the cyberspace domain to proactively seize the initiative against adversary cyberspace actors during a time of relative peace (USAF 2015). Therefore, in February 2019, General Paul Nakasone, CDRUSCYBERCOM, outlined a strategic approach for persistent engagement to partner, defend, compete, and contest against adversaries' actions against U.S.

government and military functions to the Senate Committee on Armed Services (Nakasone 2019a, 5).

General Nakasone defined persistent engagement as the "concept that states [USCYBERCOM is] in constant contact with adversaries in cyberspace, and success is determined by how [USCYBERCOM] enable[s] and act[s]" (JFQ 2019, 6). Within the persistent engagement approach, USCYBERCOM enables governmental and nongovernmental partners, such as FBI, DHS, or private sectors, through information sharing to counter malicious cyberspace activities against U.S. national interests. The persistent engagement approach also calls USCYBERCOM and interagency partners to proactively "defend forward" against adversaries in areas outside of U.S. borders in a period below the level of armed conflict (or gray zone) (JFQ 2019, 6-7).

Under persistent engagement, USCYBERCOM developed a concept of persistent presence to monitor an adversary's malign behaviors and actions in the cyberspace domain and to develop capabilities to disrupt malicious cyberspace activities. The concept of persistent presence allows USCYBERCOM and interagency partners to publicly release information on malicious software (malware) and vulnerabilities to private cybersecurity firms, such as antivirus vendors, to strengthen defenses of both private and public networks (Nakasone 2019a, 4). In addition, USCYBERCOM instituted a concept for persistent innovation to adapt and build cyber capabilities and develop tradecraft at a rapid pace in response to a dynamic operational environment (JFQ 2019, 7). The whole of society approach requires the integration of persistent engagement, persistent presence, and persistent innovation concepts to effectively address the root causes and the primary research question.

In 2008, the FBI established the NCIJTF to serve as the primary hub for coordinating and sharing information across the USG to support cyber threat investigations. The FBI-led NCIJTF is comprised of representatives from the U.S. intelligence community and federal law enforcement agencies to counter malicious cyberspace activities, such as intellectual property theft and cyber extortion (Hathaway, Demchak, Kerben, McArdle, and Spidalieri 2016, 11). The NCIJTF currently co-locates members from nineteen USG organizations in the intelligence, law enforcement and military fields to collaborate and share intelligence concerning strategic level cybersecurity threats and cyber actors. Moreover, the NCIJTF integrates coalition partners from the governments of Australia, Canada, and the United Kingdom to formalize international participation in cybersecurity (IG 2015, 5).

The NCIJTF is an exemplary model for information sharing concerning cyberspace threats to the United States. NCIJTF integrated non-FBI representatives in key leadership positions to ensure unity of effort. In March 2014, the NCIJTF designated a high-ranking NSA official as the Principal Deputy Director of the task force to strengthen interagency coordination beyond the FBI (IG 2015, 6). Despite the improvement in coordination, NCIJTF faces some challenges in sharing information on malicious cyberspace activity to their interagency partners in a timely manner due to a lack of process, according to a 2015 DOJ inspector general audit report (IG 2015, 7).

While effective at information sharing, NCIJTF does not have authorities to execute cyberspace operations, control operational assets, and direct subordinate interagency units’ actions to counter malicious cyberspace activities against U.S. interests. Therefore, the USG needs to explore a national level JIATF to tackle the national security threats in the cyberspace domain effectively. In the following section, this research study will examine the strengths, weaknesses, opportunities, and threats of JIATF-South and the application of such an organizational model for solving cybersecurity problems.

Joint Interagency Task Force South

Background

In the 1980s, the Reagan administration established The Joint Interagency Task Force South (JIATF-South), formerly known as Joint Task Force 4 (JTF-4) and JIATF-East, to combat narcotrafficking in the United States through National Security Decision Directive 221 (Reagan 1986, 3). The *National Defense Authorization Act for Fiscal Year (FY) 1989* provided authority to designate a DOD-led organization, along with civilian law enforcement agencies and interagency partners, to monitor, counter, and interdict narcotrafficking thus creating JTF-4 under U.S. Southern Command (USSOUTHCOM) as a national task force (Munsing and Lamb 2011, 9-11). The JTF-4's (JIATF-South's predecessor) mission was "to create an intelligence fusion center with a communications network that would allow it to collect and disseminate information; to conduct detection and monitoring missions with DOD assets; to coordinate interagency detection and monitoring missions" (Munsing and Lamb 2011, 12).

In 1994, the Office of National Drug Control Policy's National Interdiction Command and Control Plan replaced DOD's JTF-4 with JIATF-East and designated the organization as a national task force (Bozin 1996). The designation as a national task force enabled JIATF to remain inside the military chain of command while exercising control of capabilities and assets from civilian law enforcement and interagency partners

(Office of National Drug Control Policy 1999). In addition to law enforcement capabilities, national intelligence agencies, such as the National Security Agency's (NSA) Cryptologic Service Group, provided intelligence support to JIATF-East (Munsing and Lamb 2011, 24).

In April 2003, USSOUTHCOM changed the name of JIATF-East to JIATF-South to align closely with USSOUTHCOM's area of responsibility (Munsing and Lamb 2011, 31). As of March 2019, JIATF-South's mission is to "conduct detection and monitoring (D&M) operations throughout their Joint Operating Area to facilitate the interdiction of illicit trafficking in support of national and partner nation security" (JIATF-South 2019a). The JIATF focuses on both air and maritime illicit trafficking through a six million square mile area called the transit zone (Stavridis 2008, 111). In February 2018, Admiral Kurt Tidd, the former commander of USSOUTHCOM, highlighted in his Command Posture Statement that JIATF-South set a record number of narcotrafficking interdictions in 2017 with the "disruption of 283 metric tons of cocaine and the detention of nearly 900 suspected members [of] drug trafficking organizations" (Tidd 2018, 14).

Over the past ten years, JIATF-South's successes encompass imposing costs to narcotrafficking activities, increasing the risk of prosecution for drug traffickers, and interdicting approximately 50 percent for cocaine shipment globally (Carter 2015, 21). Given its successes, JIATF-South is a model for interagency operations and cross-functional teams to solve a complex transnational problem such as countering narcotrafficking. In the following sections, this study will analyze the strength, weakness, opportunities, and threats of JIATF-South's doctrine, organization, leadership, and policies.

Doctrine

Strength

The existing joint DOD doctrine on *Interorganizational Cooperation* is the foundation for the creation and structure of JIATF-South. As JIATF-South is an enduring national level task force, the *Interorganizational Cooperation* doctrine dictates an EO from the U.S. President—who leads the National Security Council and Homeland Security Council—and directs all charter members to allocate and provide resources and materiel to the JIATF (JCS 2017a, E-1). The National Interdiction Command and Control Plan (NICCP) requires U.S. interagency organizations to provide forces to coordinate with JIATF (Munsing and Lamb 2011, 37). The strength of establishing JIATF-South as a national level JIATF in accordance with joint doctrine allows the organization to possess capabilities to conduct operational activities. In addition, a national level JIATF model provides a basis of common doctrine, joint military services' interoperability, and common terminology such as D&M.

The charter members—including interagency organizations and foreign partners—operate in JIATF-South voluntarily as part of a "coalition of the willing" under the NICCP (Pope 2014, 31). Dr. Christopher Lamb, a research fellow at the National Defense University, observed that civilian interagency organizations often meet their commitment and provide more contribution and support than required to achieve unity of effort towards a common goal (Munsing and Lamb 2011, 37). Moreover, a primary reason for the success of JIATF-South's voluntary system and interagency cooperation is the "strong sense of unified purpose" in the charter members (Flavin 2018, 43).

The NICCP grants the director of JIATF-South authorities to task subordinate interagency members and units to the task force to meet the mission requirements (Flavin 2018, 44). As such, the JIATF-South director maintains tactical control over the subordinate interagency units to direct actions and operations. In this model, the parent interagency organizations maintain operational control over their respective assets (Munsing and Lamb 2011, 37). The strength of JIATF-South's command and control relationship is that the director possesses the flexibility to adjust the task force to adapt and accomplish the complex mission of countering narcotrafficking in a fluid environment without requiring administrative restructuring.

Weakness

The "coalition of the willing" approach of a national level JIATF is highly effective in achieving unity of effort within a multi-stakeholder organization. However, charter members maintain the rights to reallocate their resources and manpower to their respective mission requirements. In crises, DOD, Coast Guard, and other federal agencies may need to dedicate manpower to respond to emergencies such as natural disasters (e.g., Katrina Hurricane), pulling away resources from JIATF-South. Given this voluntary system, the JIATF model creates significant challenges in planning for long-term operations due to potential shortfalls in resources and capabilities (Munsing and Lamb 2011, 37).

The disadvantage of the JIATF-South voluntary model is that the task force is unable to select preferred personnel from the interagency partners. The interagency partners volunteer and assign personnel to JIATF-South their respective mission requirements and priorities (Munsing and Lamb 2011, 61). In the 1990s, the interagency and intelligence community initially viewed JIATF-South's predecessor as an ineffective organization; therefore, interagency partners sent personnel that were unqualified and unfit for the task force (Munsing and Lamb 2011, 61).

Opportunities

The "coalition of the willing" approach is an exemplary model for gaining interagency organizations' and coalition partners' buy-in to a common mission of countering illicit trafficking. JIATF-South will maintain a voluntary force to attract a workforce across the USG who are passionate about the unified purpose thus achieving unity of effort. While maintaining a voluntary force, the National Security Council can amend the NICCP to account for a memorandum of understanding (MOU) to require charter members and stakeholders to provide minimum resources to enable JIATF-South's flexible deterrent options (FDO). FDOs are pre-planned and deterrence-oriented actions to resolve problems without armed conflict (JCS 2017a, II-5). This MOU presents an opportunity to safeguard the enduring successes of the JIATF-South. Furthermore, resources for the FDO—codified in Annex V (Interagency Coordination)—will enable JIATF-South J5 to conduct long-term operational planning (JCS 2017a, II-8).

Threats

The voluntary nature of the task force presents a limited threat to JIATF-South's manpower and resources. As stated above, JIATF-South is known as a successful model for interagency coordination; however, JIATF-South must maintain its success and effectiveness to attract highly motivated and qualified personnel to work in the staff. Additionally, JIATF-South needs to consider and account for the equities, goals, and incentives of their interagency partners to draw them to provide personnel and capabilities to the organization (Munsing and Lamb 2011, 57). The lack of consideration for charter members' interests will likely result in the loss of mutual trust which diminishes the overall effectiveness of interagency coordination. In the event JIATF-South becomes ineffectual, the task force risks becoming a "dumping ground for undesirable" personnel like its predecessor was (Munsing and Lamb 2011, 61).

Organization

Strength

The Government Accountability Office (GAO) credited and acknowledged USSOUTHCOM's success in its interagency collaboration more than other joint military organizations because of JIATF-South's organizational model (GAO 2009, 26). Many experts on interagency coordination regarded JIATF-South as the "gold standard" for joint, interagency, intergovernmental, and multinational (JIIM) integration and collaboration (Munsing and Lamb 2011, 1). The JIATF-South organization is headed by a U.S. Coast Guard (USCG) rear admiral as the Director and a senior executive from U.S. Customs and Border Protection (CBP) as the Vice Director with a senior foreign service officer serving as the Director's Foreign Policy Advisor (JCS 2017a, E-1; Pope 2011, 119). Within the organizational leadership, the Directors of Intelligence and Operations are from U.S. military services, the Deputy Director of Intelligence is from Drug Enforcement Administration (DEA), and the Deputy Director of Operations is from CBP or DHS (JCS 2017a, E-3).

The JIATF-South organization integrates a wide range of USG interagency partners and national intelligence organizations. The national level intelligence agencies represented in the task force are Central Intelligence Agency (CIA), Defense Intelligence Agency (DIA), National Reconnaissance Office (NRO), National Geospatial-Intelligence Agency (NGA), National Security Agency (NSA), and Office of Naval Intelligence (ONI). Additionally, the Department of State (DOS), the Department of Justice, and the Department of Transportation provide support and contribute to JIATF-South's mission. (Porche III, Paul, Serena, Clarke, Johnson, and Herrick 2017, 10).

The integration of various law enforcement, diplomatic, and intelligence agencies enables JIATF-South to seamlessly develop intelligence sources that can help cue D&M of illicit trafficking globally. Also, JIATF-South's partnership with law enforcement and CBP allows the organization to effectively seize drugs through appropriate tools and authorities, resulting in successful prosecution and informants for follow-on operations (Munsing and Lamb 2011, 34). The integration of interagency, law enforcement, and intelligence capabilities become a force multiplier for JIATF-South.

The JIATF-South's Joint Interagency Intelligence Operations Center (JIIOC) incorporates and collocates intelligence analysts from CBP, DEA, FBI, and Homeland Security Investigations (HSI) to maintain shared understanding, support current operations, and eliminate stovepiping of information and actionable intelligence (JCS 2017a, E-3). Analysts from participating organizations provide to "tear line" versions of their intelligence reports thereby protecting their equities while maximizing information sharing (Porche III et al. 2017, 13). The JIIOC integration of analysts from various USG agencies increases mutual trust and encourages cross-pollination of ideas, perspectives, and solutions. Similarly, the Joint Operations Command Center empowers the Director of

JIATF-South to command, control, and coordinate the employment of JIIM assets and capabilities to support its mission (JCS 2017a, E-3).

In addition to interagency collaboration, JIATF-South is a multinational task force with representatives from Latin American countries as well as coalition partners from the U.S. European Command area of responsibility (Pope 2011, 119). Canada, France, the Netherlands, and the United Kingdom provide materiel support, such as ships and aircraft, to enable JIATF-South operations against illicit trafficking (JCS 2017a, E-3). In the task force, there are liaison officers (LNO) and representatives from countries including but not limited to Argentina, Brazil, Chile, Colombia, Dominican Republic, Ecuador, El Salvador, Mexico, and Peru (Porche III et al. 2017). Central American partners account for nearly 50 percent of JIATF-South's maritime interdiction operations of illicit trafficking (Tidd and Morton 2017, 14). Like the JIIOC, the robust representation of coalition partners in JIATF-South build trust and unity of effort as well as legitimacy towards a common goal. Furthermore, the multinational LNO program bolsters JIATF-South's intelligence collection capabilities and extends its operational reach (Pope 2011, 119).

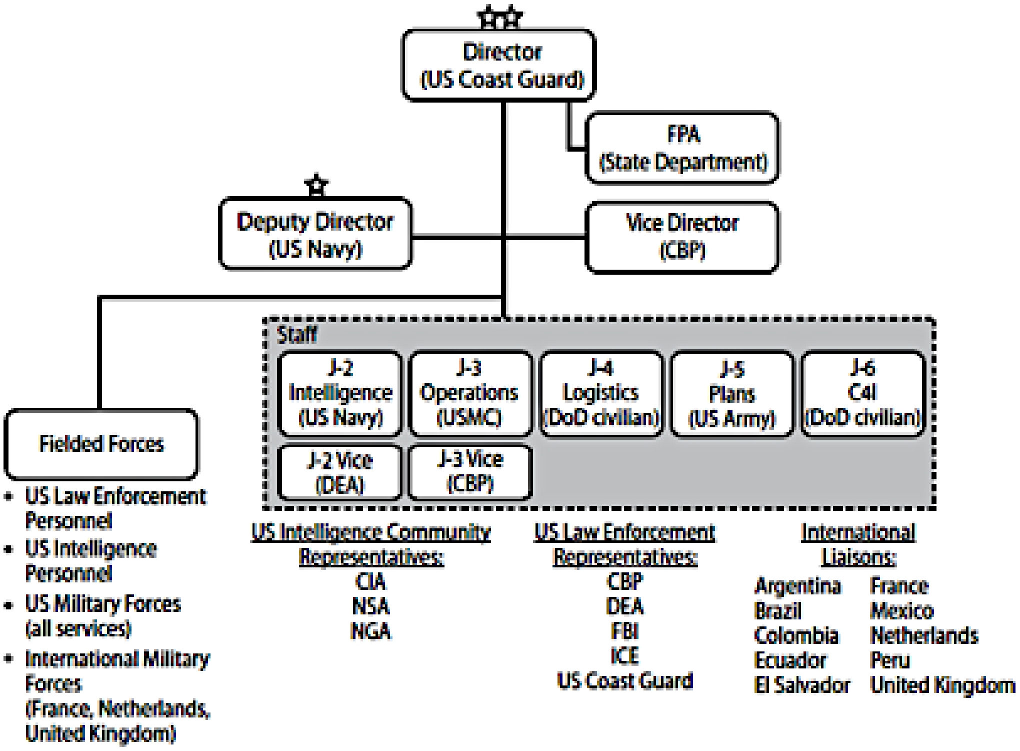

Figure 1. JIATF-South Organizational Structure

Source: Robert S. Pope, *Interagency Task Forces: The Right Tools for the Job* (Maxwell AFB, AL: Air University Press, 2011), 120.

Weakness

The JIATF-South's integration of JIIM workforce and capabilities are integral to the successes of the task force. In a JIIM environment, participating organizations and stakeholders will prioritize their own respective goals and parent agencies' missions. Therefore, there will be some instances where interagency and coalition partners will withhold sensitive intelligence or information to protect their equities (Porche III et al. 2017, 15). This perception of unwillingness to share information may cause tension and fracture trust. To avoid this tension, JIATF-South must institute an organizational culture of mutual respect and patience for one another as a basic tenet of *Multinational Operation* (JCS 2013, I-3).

JIATF-South is a military organization with service members in key leadership positions. As a military command, the majority of JIATF-South personnel, specifically military service members, work for the organization on a rotational basis. Therefore, personnel turnover rate remains high at the task force – approximately half of the JIATF-South personnel turn over every two to three years (Munsing and Lamb 2011, 48). Although JIATF-South has established permanent civilian positions within the task force, the high turnover rate may significantly impact the transfer and the management of institutional knowledge.

Opportunities

Although the task forces integrate USG and international partners, JIATF-South lacks the inclusion of nongovernmental organization (NGO) and private sector entities to address the root cause of people turning to illicit activities and transnational criminal organizations (TCO). NGOs and private sectors focused on capacity building and foreign direct investments may amplify JIATF-South's capabilities by assisting local populace away from joint illicit trafficking and TCOs. The integration of NGOs and private sector entities' efforts for empowering the local populace ultimately supports JIATF-South's goal for reducing the overall amount of illicit trafficking.

Anecdotal data suggests that residents in Mexico believe drug traffickers create jobs and benefit the people because the Mexican government failed to aid the local populations (Carpenter 2013, 149). To address this problem, JIATF-South can enlist the help of Geneva Call (or a similar organization), a Swiss NGO, which works with armed nonstate actors, including TCOs, to comply with humanitarian norms and human rights laws to protect civilians in armed conflicts (Geneva Call 2019). Additionally, JIATF-South can partner with United Nations Office on Drugs and Crime (UNODC) to address the livelihood of people affected by poverty, food insecurity, and instability who are susceptible to engaging in illicit trafficking (UNODC 2019).

Threats

In a 2018 Senate Armed Services Committee hearing, Admiral Tidd highlighted the successes of JIATF-South interdiction efforts primarily due to coalition partners' contributions and assets in the fiscal year 2017. During the same hearing, Admiral Tidd asserted that JIATF-South was unable to target and interdict approximately eight hundred metric tons of cocaine due to the limited number of USG assets. Tidd expounded that the exponential volume of illicit trafficking activities far exceeds JIATF-South's capacity to respond to the events (Tidd 2018, 14-15). As such, budgetary constraints on the organization will have a significant impact on JIATF-South's activities and may lead to overburdening coalition partners' assets in future operations.

Leadership

Strength

The Director of JIATF-South maintains the authority to task and direct actions of subordinate military and interagency units, thus enabling unity of command (Pope 2011, 119). In addition, the JIATF-South leadership team is comprised of both senior military and civilian personnel, including coalition partners, with delegated decision-making authorities independent of their parent governmental agencies. One JIATF-South leader highlighted that most interagency civilian leaders at JIATF-South possess a rank of GS-15 and can represent their respective organizations which bolsters the autonomy of the task force (Munsing and Lamb 2011, 40). JIATF-South's integration of high-ranking interagency officials increases the speed for timely actions as well as streamlines bureaucratic processes and deconfliction.

Given the authorities and autonomy of the task force, JIATF-South leadership also empowers subordinates to begin initiatives, make decisions, and take actions to support the counter illicit trafficking mission. The members of JIATF-South indicated that there was a mutual trust between the leaders and subordinates resulting in "bottom-up empowerment" (Munsing and Lamb 2011, 65). The leadership style of JIATF-South resembles the U.S. Army's mission command philosophy of commanders exercising authority and direction to enable disciplined initiative and empower agile and adaptive leaders and subordinates (HQDA 2012, 1-1).

Weakness

Illicit drug trafficking is historically a transnational crime and often considered a law enforcement matter (Kuhns and Phillips, 3). However, key JIATF-South leadership positions, such as the Director and the Directors for Intelligence and Operations, are assumed by military service officers while the Deputy Director positions are law enforcement and border patrol officials (Pope 2011, 119). Although not guaranteed, a military leadership assuming the lead role for a criminal issue may create tensions and disrupt cohesion with the law enforcement community. Furthermore, under USCG leadership, JIATF-South often focuses narrowly on interdicting illicit trafficking and drug shipments in the seas (Munsing and Lamb 2011, 34). The JIATF-South leadership must continue to encompass the goals and incentives of their interagency and coalition partners to build a cohesive team towards a common purpose.

Opportunities

Although JIATF-South is a military-led organization, the task force can explore interagency officials serving in director roles and key leadership positions. A 2011 Joint Advanced Warfighting School thesis recommended that JIATF leadership organization should institute and provide a "cyclic leadership opportunity for the senior personnel from all agencies [including] non-military personnel [to] serve in positions of authority and decision-making" (Webber 2011, 59). The inclusion of civilian members in key leadership positions on a rotational basis will generate new ideas and courses of action and also cross train personnel for continuity purposes.

In a JIIM environment, JIATF-South's integration of military, law enforcement, intelligence, diplomatic, and coalition partners provides a unique opportunity to strengthen U.S. national security as a whole. Each charter member of JIATF-South brings differing cultures, capabilities, ideas, and situational awareness. It is up to the JIATF-South leadership to create a culture and climate of tolerance and appreciation of the myriad organizations that contribute to the success of the task force (Davis 2017, 51). Moreover, JIATF-South leadership must not attempt to change interagency or coalition partners but instead look to find overlapping interests ("coupler") to empower subordinates to pursue a common mission (Davis 2017, 56).

Threats

The threat of toxic leadership exists in organizational level entities including JIATF-South. A toxic leader in a position of authority within JIATF-South will undermine the unity of effort across military, interagency, and coalition partner to counter illicit trafficking. Dr. George Reed, the dean of the School of Public Affairs at the University of Colorado, defines a toxic leader as those who "engage in numerous destructive behaviors and who exhibit certain dysfunctional personal characteristics" (Reed 2015, 11). Additionally, Reed further defines destructive leadership behavior as:

> the systematic and repeated behaviour by a leader, supervisor or manager that violates the legitimate interest of the organisation by undermining and/or sabotaging the organisation's goals, tasks, resources, and effectiveness and/or the motivation, well- being or job satisfaction of his [or] her subordinates. (Reed 2015, 12).

A JIATF-South leader highlighted that individuals with "hard-charging big ego" who are focused more on "polishing their careers" often were not successful in the task force given the collaborative nature of the organization (Munsing and Lamb 2011, 61). To mitigate the threat of toxic leadership, JIATF-South maintains the authority to remove or fire personnel, including interagency civilians, to ensure unity of effort and command (Munsing and Lamb 2011, 62). The JIATF-South leadership must be cognizant and vigilant in preventing toxic and destructive leadership in the organization. Additionally, the JIATF-South leadership's actions must remain transparent and accountable to USSOUTHCOM.

Policy (Authorities)

Strength

Under the auspices of NICCP, the JIATF-South can leverage multiple authorities and capabilities of the military, law enforcement, interagency, and coalition partners in achieving its mission of counter illicit trafficking. The former Director of JIATF-South, Rear Admiral (RADM) Joseph Nimmich, noted that the strength of the task force is the "ability to mix and match capabilities and authorities to optimize the operational effectiveness of assets" (Porche III et al. 2017, 13). As an example, a law enforcement detachment on a U.S. Navy ship can extend the operational reach of its prosecution and investigative authorities (Porche III et al. 2017, 13). In this case, JIATF-South does not have to request authorities or obtain approval for law enforcement authorities during an operation against drug smugglers, thus increasing tempo and responsiveness (Munsing and Lamb 2011, 39).

Table 2. Authorities of JIATF-South's Participating Organizations

PARTICIPATING ORGANIZATIONS	AUTHORITIES
Central Intelligence Agency Defense Intelligence Agency National Security Agency National Reconnaissance Organization National Geospatial-Intelligence Agency	Title 50: War and National Defense (Foreign Intelligence)
Drug Enforcement Administration	Title 3: The President Title 21: Food and Drug (Controlled Substances Act)
Federal Bureau of Investigation	Title 18: Crimes and Criminal Procedure
U.S. Immigration and Customs Enforcement	Title 8: Aliens and Nationalities Title 18: Crimes and Criminal Procedure Title 19: Customs Duties
U.S. Customs and Border Protection	Title 8: Aliens and Nationalities Title 18: Crimes and Criminal Procedure Title 19: Customs Duties
U.S. Coast Guard	Title 14: Coast Guard Title 18: Crimes and Criminal Procedure Title 19: Customs Duties
U.S. Army National Guard U.S. Air National Guard	Title 10: Armed Forces Title 32: National Guard
U.S. Army U.S. Air Force U.S. Marines U.S. Navy	Title 10: Armed Forces

Source: Created by author.

Weakness

The JIATF-South can integrate or "mix and match" authorities and capabilities of the charter members, including foreign partners, to achieve unity of effort against illicit trafficking as stated above. However, as a military organization, JIATF-South is unable to conduct law enforcement operations including search and seizures independently. This stipulation requires JIATF-South to transition targets for interdiction to coalition partners or law enforcement agencies (e.g., USCG) to execute the operation (Yeatman 2006, 27). Under JIATF-South, each military service, interagency entity, intelligence agency, and law enforcement organizations must only execute operations within the legal limits of their respective authorities. While this may cause some disruption, the collocation of JIATF-South's participants mitigates the potential loss of continuity in operations against narcotraffickers.

Opportunities

The JIATF-South's joint operating area (JOA) is a forty-two million-square-mile area that encompasses Central America, South America, the Caribbean, Pacific Ocean, and South Atlantic Ocean; however, the JOA does not include the Continental United States (Munsing and Lamb 2011, 23). JIATF-South is a military organization and is, therefore, precluded from employing military assets for domestic purposes including illicit trafficking (Yeatman 2006, 27). There is an opportunity to enhance unity of efforts for domestic operations by removing barriers to employ military capabilities to interdict illicit trafficking in the United States as a defense support to civil authority (DSCA) activity through modifications in policies or legal restrictions (Blum and McIntyre, 27).

In addition to interdiction operations, JIATF-South can incorporate the Department of Treasury's (DOT) Office of Foreign Asset Control (OFAC) as a permanent member to leverage their authority to sanction TCOs, international narcotics traffickers, and other entities supporting illicit trafficking (DOT 2019b). Potential JIATF-South's operations against threat finance supporting TCOs will significantly impact the end-to-end illicit drug supply chain globally. If DOT's OFAC becomes a charter member of JIATF-South, the task force will be able to leverage their Title 31 authority (Money and Finance) to disrupt adversaries' revenue generated from illicit trafficking (DOT 2019a).

Threats

JIATF-South enjoys little oversight given the successes and trust in the organizations (Munsing and Lamb 2011, 56). The minimal oversight increases the efficiency of the task force to execute operations against narcotraffickers in a timely and expedient manner. However, the lack of oversight may present a danger of JIATF-South abusing the use of broad interagency authorities outside the scope of their mission. While the possibility of abuse is unlikely, the JIATF-South leadership must be cognizant of the legal limitations of their day-to-day activities and operations. The JIATF-South leadership must take into account the staff judge advocates' legal services and advice prior to conducting interdiction operations (JCS 2017a, II-28).

Application of JIATF Model for Cyberspace Operations

A Case for Joint Interagency Task Force -Cyberspace Operations

The USG needs a whole of society approach for engaging adversary cyberspace actors and activities akin to freedom of navigation program or operation in a JIIM environment. General Nakasone, CDRUSCYBERCOM, highlighted that "[U.S.] naval forces do not defend by staying in port, and [U.S.] airpower does not remain at airfields," but they regularly patrol the multi-domains of sea and air to deter malign activities and defend the United States (Nakasone 2019b, 11). The freedom of navigation program is a joint DOD and DOS effort to ensure states respect the sovereignty of other nations within the maritime domain and maintain international laws and norms. The U.S. Navy conducts freedom of navigation operations to secure sea lines of communication for economic (e.g., international trade) and national security (e.g., disaster relief) purposes (Mandsager 1997, 117). Furthermore, the U.S. Navy executes freedom of navigation operations during peacetime and at levels below armed conflicts.

Similarly, the U.S. national security leadership and the DOD can take lessons from JIATF-South to establish an organization that leverages diplomatic, information, military, and economic (DIME) tools to protect cyberspace lines of communication against actors waging "campaigns against American political, economic, and security interests without ever physically crossing our border" (Trump 2017a, 12). The daunting task of countering malicious cyberspace activities is not a solely military or a USCYBERCOM problem, but a whole of society issue. As cyberspace attacks affect all aspects and ways of American life, this will require close integration of multiple governmental agencies (e.g., FBI and DHS), private sectors, the industrial base, and coalition partners to mitigate and solve the problem through the lens of JIIM. In the sections below, this paper will walk-through how the United States can create a national-level cyberspace task force as a potential desired state by applying the SWOT analysis of the JIATF-South case study.

Doctrine

The Executive Office of the President holds power to develop and issue a national level directive to formulate a national level JIATF for cyberspace operations (JIATF-CO) (JCS 2017a, E-1). This national level directive can model the Executive Office of the

President's Office of National Drug Control Policy's NICCP which created JIATF-South as a national level JIATF in 1994 (Flavin 2018, 41). The National Security Council and Homeland Security Council can issue a supplemental mandate to direct all agencies supporting JIATF-CO to provide actual resources and manpower to the organization (JCS 2017a, E-1). Moreover, the mandate will require all JIATF-CO personnel, including private sector companies, to maintain the necessary security clearance to maximize the capabilities of JIIM organizations.

The national level directive for establishing JIATF-South will detail key charter members, roles, responsibilities, functional protocols, terms of reference, and command and control (C2) relationships (JCS 2017a, E-1). Additionally, the cyberspace operations directive should describe the strategic objectives and interests of U.S. national security documents including the *National Security Strategy*, *National Cyber Strategy*, and *DOD Cyber Strategy*. The directive should also outline the strategic concept of General Nakasone's persistent engagement to proactively compete and contest against U.S. strategic competitors, such as China and Russia, in cyberspace (DOD 2018b, 1).

This approach for the national level directive is similar to how the NICCP outlined strategic goals of drug interdiction in accordance with relevant national drug control programs for JIATF-South (Webber 2011, 5). As an example, the national level directive for cyberspace operations can direct JIATF-CO to pursue the *National Cyber Strategy*'s objectives of securing government and private sector; countering malicious cyberspace activities against U.S. interests; and ensuring open and secure Internet for economic security and prosperity (Trump 2018a, 2-3).

The directive will make a strategic shift away from deterrence in cyberspace and codify the "defend forward" concept in the *DOD Cyber Strategy* for JIATF-CO (DOD 2018b, 2). Additionally, the directive should establish LOEs for persistent engagement, persistent presence, and persistent innovation to focus on operations against malicious cyberspace activities below the level of armed conflict (Nakasone 2019a, 4-7). The common goals and strategic LOEs for JIATF-CO will achieve unity of effort and bring all instruments of national power against malicious cyberspace actors and activities.

Organization

Doctrinally, JIATFs are formal organizations led by DOD and U.S. civilian agencies with representatives from various interagency partners in pursuit of a common mission (JCS 2017a, E-1-E-2). The JIATF-CO may integrate a wide range of USG interagency partners, national intelligence organizations, federal law enforcement agencies, and coalitions partners to emulate the JIATF-South organizational model. Like JIATF-South, a military service officer will serve as the JIATF-CO Director while representatives from interagency partners will assume the roles of Vice Directors (Pope 2011, 119). As a hypothetical model, JIATF-CO could be led by a two-star US general or flag officer as the Director with a one-star US military officer as the Deputy Director. On the JIATF-CO leadership team, an NSA senior executive may serve as the Vice Director for Persistent Presence and an FBI senior special agent as the Vice Director for Persistent Engagement. Also, a senior DOS foreign service officer will serve as the Policy Advisor to the Director of JIATF-CO.

The USCYBERCOM, a unified combatant command, will maintain operational control and provide oversight for JIATF-CO. This command relationship models

USSOUTHCOM’s operational control over JIATF-South. As a military organization, the JIATF-CO’s organizational structure may be comprised of Directorate for Intelligence (J2); the Directorate for Operations (J3); the Directorate for Logistics (J4); the Directorate for Plans (J5); the Directorate for Command, Control, Communications, and Computers (C4) (J6); and the Directorate for Persistent Innovation (J8) (Pope 2011, 119).

Within the JIATF-CO staff, U.S. military officers will serve as the Directors of Intelligence and Operations, the Deputy Director of Intelligence may potentially be from DIA, and the Deputy Director of Operations may be from the FBI or DHS. A senior DOD civilian will assume the role as the Director of Logistics, and a private cybersecurity expert will serve as the Director of Persistent Innovation. Moreover, a senior civilian from the Defense Information Systems Agency may serve as the Director of C4 with an executive from a U.S. Internet Service Provider as the Vice Director of C4.

Collocation of the JIIM enterprise is the key to achieving unity of effort. Similar to JIATF-South, the JIATF-CO will maintain tactical control of the collocated subordinate military and civilian interagency units as well as coalition partners and private cybersecurity teams (Porche III et al. 2017, 13). The JIATF-CO should establish a Joint Interagency Intelligence Operations Center, or JIIOC, with intelligence analysts and cyber-forensic analysts from CIA, DIA, NGA, NSA, DOS, DOT, FBI, DHS, private cybersecurity firms, academia, as well as coalition partners to increase shared understanding and provide a common operating picture (Porche III et al. 2017, 13). The collocation of personnel and face-to-face interactions build mutual trust and eliminate stovepiping of information, enabling JIATF-CO to make a timely decision against malicious cyberspace activities. Furthermore, the collocation of key partners and relevant stakeholders allow for better management of participating organizations' equities and enable rapid interagency deconfliction process prior to execution of operations (Porche III et al. 2017, 15).

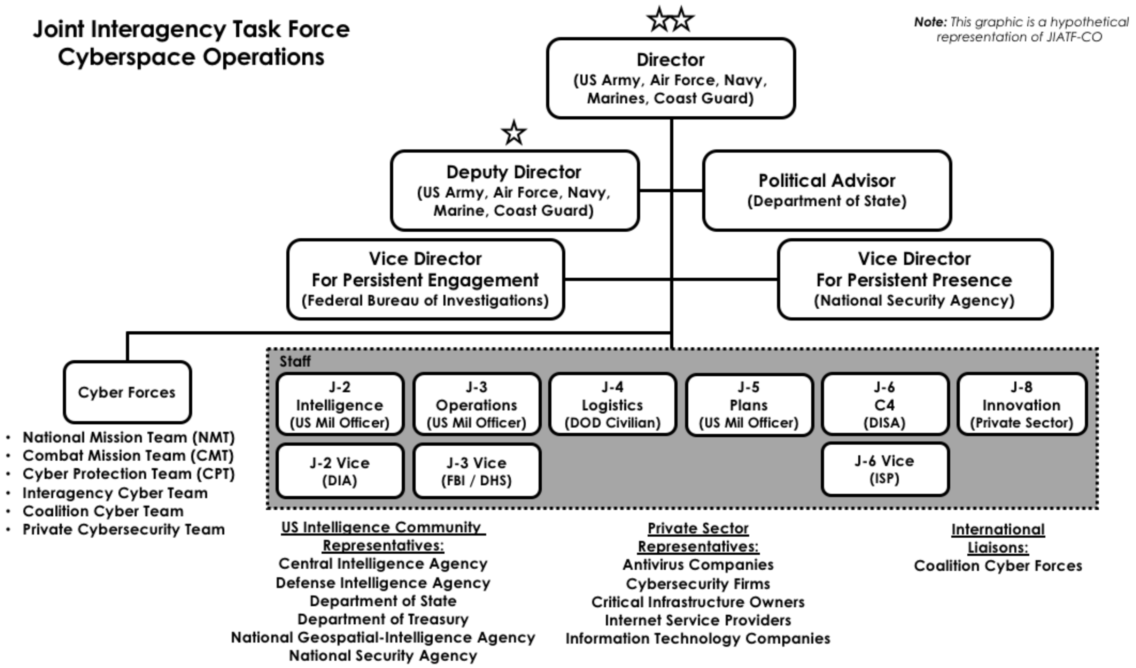
Joint Interagency Task Force Cyberspace Operations
Note: This graphic is a hypothetical representation of JIATF-CO
Director (US Army, Air Force, Navy, Marines, Coast Guard)
Deputy Director (US Army, Air Force, Navy, Marine, Coast Guard)
Political Advisor (Department of State)
Vice Director For Persistent Engagement (Federal Bureau of Investigations)
Vice Director For Persistent Presence (National Security Agency)
Cyber Forces
• National Mission Team (NMT)
• Combat Mission Team (CMT)
• Cyber Protection Team (CPT)
• Interagency Cyber Team
• Coalition Cyber Team
• Private Cybersecurity Team
Staff
J-2 Intelligence (US Mil Officer)
J-3 Operations (US Mil Officer)
J-4 Logistics (DOD Civilian)
J-5 Plans (US Mil Officer)
J-6 C4 (DISA)
J-8 Innovation (Private Sector)
J-2 Vice (DIA)
J-3 Vice (FBI / DHS)
J-6 Vice (ISP)
US Intelligence Community Representatives:
Central Intelligence Agency
Defense Intelligence Agency
Department of State
Department of Treasury
National Geospatial-Intelligence Agency
National Security Agency
Private Sector Representatives:
Antivirus Companies
Cybersecurity Firms
Critical Infrastructure Owners
Internet Service Providers
Information Technology Companies
International Liaisons:
Coalition Cyber Forces

Figure 2. JIATF-CO Organizational Structure

Source: Created by author.

Leadership

As a national level JIATF, the Director of JIATF-CO will gain the authority to task and direct actions of the subordinate military, interagency, and coalition partners within the task force in support of the counter-malicious cyberspace activities mission (Pope 2011, 119). Like JIATF-South, the JIATF-CO leadership team will be comprised of both senior military and civilian personnel as well as private sector executives in an advisory role. These senior personnel must have decision-making authorities from their respective organizations to enable timely execution of cyberspace operations and other instruments of national powers against malicious cyberspace actors and activities (Munsing and Lamb 2011, 40). Also, it will be incumbent of the JIATF-CO leadership to instill a culture of mutual trust and respect to ensure unity of effort. In building trust, the JIATF-CO leadership team will account for and protect the equities (e.g., proprietary information) of interagency organizations, private cybersecurity firms, and coalition partners.

In *One Mission,* empowered execution is the decentralization and delegation of decision-authorities to "those actors closest to the issues" (Fussell and Goodyear 2017, 2). As such, JIATF-CO should adopt the concept of empowered execution to enable its JIIM teams, including the cyber forces, to act with autonomy to support the counter malicious cyberspace activities mission. As exemplified in JIATF-South, the JIATF-CO leadership must build mutual trust and exercise "bottom-up empowerment" between the leaders and subordinates to increase team cohesion, operational creativity, and unity of effort while accepting prudent risks (Munsing and Lamb 2011, 65).

Policy (Authorities)

The current authorities and policies, such as the Presidential Policy Directive 20, do not enable timely integration of JIIM authorities, including military cyberspace operations, to proactively compete and contest adversaries in cyberspace below the level of armed conflict (McGhee 2016, 52). In the current operating environment, the authorities for executing military cyberspace operations are mainly for responding to malicious cyberspace attacks in defense of the homeland. The Joint Publication 3-12, Cyberspace Operations, outlines that “under the authorities of the SecDef, DOD uses cyberspace capabilities to shape cyberspace and provide integrated offensive and defensive options for the defense of the nation” (JCS 2018a, xii-xiii). In defense of the nation, cyber forces focused on DCO-RA in response to adversary cyberspace actors’ actions against U.S. interests since the creation of USCYBERCOM. The purpose of JIATF-CO is to leverage various USG authorities to shift from a “cyber response” concept to a “cyber persistence” to empower whole of society actions during periods of relative peace (Nakasone 2019b, 12).

The National Defense Authorization Act for Fiscal Year 2019 (NDAA FY19) further reinforces and affirms SecDef’s authorities to conduct military cyberspace operations including clandestine operations in the cyberspace domain (U.S. Congress 2018). The law grants authority to SecDef to execute military cyberspace operations. However, the SecDef should further delegate this authority to the Director of JIATF-CO to effectively improve the agility and speed of planning and executing cyberspace operations below the level of armed conflict. Many joint force commanders (JFC) assess that cyber authorities are “too restrictive” suggesting that further delegation of authorities will enable agility and flexibility in support of the JFC’s objectives (Pomerleau 2017b). Regarding cyberspace operations’ authorities and approval, General Raymond Thomas, commander of Special Operations Command, highlights that “the limiting factor for cyber effectiveness continues to evolve around policy and process” (Pomerleau 2017b).

USCYBERCOM and the NSA enabled the FBI and DHS to disrupt Russian cyberspace actors’ attempts to interfere with U.S. political processes in 2018 (JFQ 2019, 6-7). To expand this interagency collaboration, the JIATF-CO will emulate JIATF-

South's ability to integrate authorities and capabilities seamlessly. Similar to the NICCP, the Executive Office of the President's national level directive for cyberspace should stipulate that the Director of JIATF-CO can "mix and match" authorities of the military, intelligence, diplomatic, law enforcement, economic, and private cybersecurity sectors (Porche III et al. 2017, 13).

In addition, the national level directive will grant authority to the Director of JIATF-CO to assume tactical control of the subordinate military, interagency, coalition, and private sector partners' personnel and assets to accomplish the mission. Tactical control is "an authority over assigned or attached forces or commands, or military capability or forces, made available for tasking" (JCS 2017b, III-4). JIATF-CO's ability to leverage both domestic security and military (armed forces) authorities may increase flexibility in combating malicious cyberspace activities in the United States and abroad. Moreover, the integration of JIIM capabilities will enable JIATF-CO to effectively employ the instruments of national power—including sanctions, indictments, and diplomatic efforts—against malicious cyberspace actors. Examples of potential JIATF-CO member organizations' authorities are in the table below.

Table 3. Authorities of Potential JIATF-CO’s Participating Organizations

PARTICIPATING ORGANIZATIONS	**AUTHORITIES**
Central Intelligence Agency Defense Intelligence Agency National Security Agency National Geospatial-Intelligence Agency	Title 50: War and National Defense (Foreign Intelligence [FI])
Department of Homeland Security	Title 6: Domestic Security Title 50: War and National Defense (FI)
Department of State	Title 22: Foreign Relations Title 50: War and National Defense (FI)
Department of Treasury	Title 31: Money and Finance Title 50: War and National Defense (FI)
Federal Bureau of Investigation	Title 18: Crimes and Criminal Procedure Title 50: War and National Defense
U.S. Army National Guard U.S. Air National Guard	Title 10: Armed Forces Title 32: National Guard
U.S. Army U.S. Air Force U.S. Marines U.S. Navy	Title 10: Armed Forces

Source: Created by author.

Summary

This chapter finds the JIATF-South organizational structure and standard operating procedures provide a blueprint for a whole of society approach to proactively compete and contest state-sponsored malicious cyberspace actors and activities against U.S. national interests in a state below the level of armed conflict. A qualitative SWOT analysis of JIATF-South’s doctrine, organization, leadership, and policy areas found the net strength greatly outweighs the weaknesses and threats (see table 4). Furthermore, this study observed that the JIATF-South model provides tailorable and applicable opportunities to tackle the growing cybersecurity problem set.

The DOD and national security leaders can use lessons learned from the presidentially-approved NICCP to develop policies and modify doctrine to increase adaptability and flexibility for cyberspace operations against malicious cyberspace activities below the level of armed conflict (Flavin 2018, 41). Additionally, JIATF-South's command structure provides insight into how the DOD can formulate JIATF-CO as a national level JIATF (JCS 2017a, E-1). Finally, the JIIM nature of JIATF-CO will serve as a model for strengthening the public-private relationship to secure and protect the critical infrastructure supporting global commons lines of communications in cyberspace (JFQ 2019, 5).

President Abraham Lincoln once said, "a house divided against itself cannot stand" (Neely 1982). A significant challenge in establishing JIATF-CO as a whole of society approach is the integration of private cybersecurity firms into the task force. The public-private relationship in the cybersecurity arena remains weak following Snowden's disclosure of intelligence community practices (Segal 2017, 67-68). To restore trust, the USG must account for private cybersecurity sector interests in the national level directive including but not limited to mutual goals and clearly articulated rules of engagement. Given the scope of this case study, this analysis did not explore how the USG can strengthen partnership with private cybersecurity firms in support of its national interests. In addition to public-private partnership issues, the USG needs to consider the challenges of recruitment, turnovers, and retention of talented cyber operations officers and soldiers to create a robust and capable JIATF-CO (Dill 2018, 57).

Table 4. Summary of SWOT Analysis for JIATF-South

		DOTMLFP-P FRAMEWORK			
		DOCTRINE	ORGANIZATION	LEADERSHIP	POLICY
JIATF-SOUTH	STRENGTH	- Establishes enduring task force (TF) - Allocates resources to TF - Voluntary IA cooperation - Authorizes the TF to assume TACON over JIIM teams	- Effective integration of JIIM capabilities - Collocation of JIIM partners - Information sharing across the organization	- Civil and military representation - “Bottom-up Empowerment” - Delegation of decision-making power enables autonomy	- “Mix and Match” authorities - Enables unity of command and effort
	WEAKNESS	- Inability to conduct long-term planning	- IA protection of their equities may project the perception of stovepipe - High turnover rate	- Directorates led by military officers with IA deputies may cause tension	- Legal restriction in transferring authorities within JIIM partners
	OPPORT-UNITIES	- Establish MOU for resources for long-term plans	- Integration of NGOs and private sector	- Cyclical JIIM leaders for positions of authority	- Expand authorities for domestic interdiction operations
	THREATS	- Not accounting the consideration of IA equities and interest	- Budgetary constraints	- Toxic leaders	- Potential abuse of power due to minimal oversight

Source: Created by author.

Conclusion

This chapter concludes that the JIATF-South is the “gold standard” and an exemplary model for JIIM integration and collaboration to solve complex transnational problems. Several attributes of JIATF-South are applicable for addressing the current challenges against malicious cyberspace activities as well as for meeting the national security objectives in the cyberspace domain. Furthermore, the JIATF-South model provides a framework for operationalizing USCYBERCOM’s persistent engagement concept. The following chapter will capture recommendations and implications of establishing a JIATF-CO based on the findings of SWOT analysis of the JIATF-South case study.

CHAPTER 5

CONCLUSIONS AND RECOMMENDATIONS

Introduction

In March 2019, the U.S. Attorney General irrefutably reported—in a summary of the Special Council's report—that there were two main Russian efforts to influence the 2016 U.S. Presidential election. The first effort involved Russian Internet Research Agency's operations to propagate misinformation on online and social media platforms to sow social discord with the intent of interfering with the elections. Concurrently, in their second effort, the Russian government executed cyberspace operations to exploit, collect, and disseminate damaging information on the U.S. Democratic Party organizations to influence the elections (Barr 2019, 2). These coordinated Russian efforts did not exceed the threshold of the level of armed conflict; therefore, the USG initially failed to act and respond in the cyberspace domain.

In response to the Russian efforts against the U.S. national interests, General Nakasone, CDRUSCYBERCOM, formed a Russia Small Group to prevent interference and influence operations in cyberspace against the U.S. political processes and systems. The USCYBERCOM-led Russia Small Group was an interagency partnership between USCYBERCOM and NSA with assistance from FBI and DHS personnel. This small group successfully secured and defended political systems supporting the 2018 U.S. mid-term elections (JFQ 2019, 6-7). The successes of the Russian Small Group depicted a glimpse of JIIM integration and collaboration in the cyberspace domain at a relatively small scope and scale. Based on this anecdotal observation, how does the United States replicate and expand this success to include the whole of society to address the concerns and interests of the national security strategies on cyberspace?

Research Questions

The primary research question is "as deterrence in cyberspace fails, how can the United States develop a whole of society approach in the cyberspace domain to proactively compete and contest state-sponsored malicious cyberspace actors and activities against U.S. national interests in a state below the level of armed conflict?"

The secondary research questions are what changes in policy or doctrine is necessary for enabling the United States to proactively compete and contest state-sponsored malicious cyberspace actors in a state below the level of armed conflict? What are the methods and means (e.g., the range of military operations) for the United States to compete and contest state-supported malicious cyberspace actors and activities against U.S. national interests other than deterrence? In support of U.S. national interests, how does the United States secure and defend the global commons and lines of communication in the cyberspace domain? What U.S. organization is responsible for integrating and executing the instruments of national power against state-sponsored malicious cyberspace actors and activities?

The primary purpose of this research was to determine how the USG can develop a whole of society approach in the cyberspace domain to proactively compete and contest malicious cyberspace actors and activities in a state below the level of armed conflict or in the "gray zone." Also, this paper addressed subordinate research questions concerning policies, methods, and an organizational model for framing a whole of society approach to support national-level objectives in cyberspace. The analysis on the feasibility of such a whole of society approach drew from an extensive literature review in Chapter 2. The literary review contained the categories of national-level cyber strategies, USG cyberspace organizations, and concepts on cyberspace (e.g., deterrence and persistent engagement).

The study bounded the scope of the analysis using a qualitative research approach to examine a case study on JIATF-South to answer the primary research question. In addition, this research study conducted an in-depth SWOT analysis on some elements of DOTMLPF-P for JIATF-South—specifically doctrine, organization, leadership, and policy—to formulate the answers to the subordinate research questions regarding policies, methods, and an organizational model. Based on the SWOT analysis, a hypothetical JIIM organization informs an opportunity for the whole of society approach in the cyberspace domain to counter malicious cyberspace actors and activities in a state below the level of armed conflict.

Conclusions

What can be learned from the JIATF-South case study that can help inform the development of a whole of society approach for cyberspace operations today? The interpretation of the research evidence finds that JIATF-South is a feasible model for how the United States established a unity of effort across the USG to solve transnational problems such as malicious cyberspace activities against U.S. interests. The Presidentially-approved executive order, the NICCP, grants the JIATF-South interagency resources and capabilities; authorities to task and direct interagency teams; and permanent status as a standing national task force (Munsing and Lamb 2011, 37). Additionally, the JIATF-South conducts operations against illicit trafficking below the level of armed conflict and in a time of relative peace. Also, JIATF-South attained unity of effort by accounting for volunteer interagency and coalition partners' interests and establishing a unifying vision and mission (Flavin 2018, 43).

The JIATF-South's organizational model is comprised of various military services, interagency organizations, law enforcement, and coalition forces at every echelon of the task force (Pope 2011, 119). Thus, JIATF-South can integrate and take full advantage of the military, law enforcement, diplomatic, and intelligence capabilities at its disposal. JIATF-South is also an agile and creative organization as their leadership embraces the philosophy of "bottom-up empowerment" (Munsing and Lamb 2011, 41). The "bottom-up empowerment" philosophy delegates decision-making authorities to subordinates which allows the task force to become more adaptive and imaginative in countering global illicit trafficking. Additionally, the ability to leverage multiple USG authorities and capabilities emboldens the task force to act autonomously and effectively to interdict illicit trafficking in support of national security goals.

Based on the SWOT analysis of JIATF-South, the United States can develop a whole of society approach through the establishment of a national level JIATF-CO to fulfill the common cybersecurity goals of the JIIM enterprise. There are several strengths in JIATF-South's doctrine, organization, leadership, and policy that are applicable for addressing the current challenges against malicious cyberspace activities. However, the USG should recognize the weaknesses and deficient areas in JIATF-South to avoid potential pitfalls and shortcomings for JIATF-CO.

U.S. policymakers and military planners must consider and address the implications of the current USG relationship with the private cybersecurity sector when creating an organization such as JIATF-CO (Segal 2017, 67-68). The current legal authorities and public-private cybersecurity partnership restrict U.S. governmental organizations, including a hypothetical JIATF-CO, from organizing and directing private cybersecurity companies' personnel and operations. Moreover, similar to JIATF-South's personnel turnover problem, the U.S. military faces a significant challenge in talent management for cyber operations officers and soldiers, specifically in the areas of recruitment and retention (Dill 2018, 57).

The recommendations below will address how the United States can develop and operationalize a whole of society approach to proactively compete and contest state-sponsored malicious cyberspace actors and activities against U.S. national interests in a state below the level of armed conflict. This research study's analysis and application of JIATF-South components to a hypothetical national level JIATF for cyberspace operations form the basis for the recommendations. The recommendations will focus on the areas of national level directive and authorization; integrated JIIM and private sector command structure; and bottom-up empowerment leadership style.

Recommendations

Cyber National Level Directive and Authorization

First, the United States should formulate and implement a national level directive, such as a National Security Policy Directive, to establish a standing JIATF responsible for planning, coordinating, and executing a whole of society campaign to counter malicious cyberspace activities against U.S. interests (JCS 2017a, E-1). A National Security Policy Directive codifies specific joint services, interagency, coalition partners, and the private sector as permanent charter members to form and operationalize a national level JIATF-CO. Additionally, the National Security Policy Directive should legally permit the Director of JIATF-CO to task and direct subordinate units' authorities and capabilities, including interagency and coalition partners, to conduct operations in support of national goals in cyberspace (Porche III et al. 2017, 13).

Integrated JIIM Plus Private Sector (JIIM+P) Command Structure

Second, the USG could create a JIATF-CO military command structure that integrates JIIM personnel in both staff and leadership positions (Pope 2011, 119). Within the JIATF-CO, the USG should establish a JIIOC with collocated intelligence analysts and cybersecurity specialists from various joint service, interagency, and coalition partner organizations—including private cybersecurity firms and academia—to maintain shared understanding and enable timely cyberspace operations against adversaries in cyberspace (Porche III et al. 2017, 13). Furthermore, the JIATF-CO can adopt a cyclical leadership system to allow personnel from interagency and coalition partners to serve in positions of authority and decision-making (Webber 2011, 59).

The DOD and the U.S. national security leadership can establish and assign JIATF-CO under USCYBERCOM. Moreover, the DOD and the U.S. national security leadership can expand the existing Cyber National Mission Force to model JIATF-South's command structure to fulfill this proposal. The Cyber National Mission Force is USCYBERCOM's joint subordinate organization responsible for planning, directing, and synchronizing full-spectrum cyberspace operations to deter, disrupt, and defeat adversary cyberspace actors to defend U.S. national interests (USCYBERCOM 2019). Also, the Cyber National Mission Force recently implemented a system to provide intelligence on malicious cyberspace activities to the private sector and federal agencies (Pomerleau

2018). By modifying an existing organization, the USG can expedite the process and reduce the cost for building a national level JIATF for cyberspace operations.

Bottom-Up Empowerment Leadership Style

Finally, the JIATF-CO leadership should institute a leadership philosophy and style of "bottom-up empowerment" within the organization (Munsing and Lamb 2011, 65). This "bottom-up empowerment" leadership style will require JIATF-CO to delegate decision-making power to subordinate personnel from joint services, interagency, and coalition partners. As JIATF-CO leadership instills trust in their subordinates, the cyber operators, analysts, and subject matter experts will feel empowered to contribute and take initiative in support of the organizational goals. Therefore, the "bottom-up empowerment" leadership style will ultimately increase the autonomy and overall effectiveness of the task force.

Suggestions for Further Research

This research study narrowly focused on examining a JIATF model—specifically in the areas of doctrine, organization, leadership, and policy—and its applicability as a whole of society approach for countering malicious cyberspace activities against U.S. national interests. The JIATF organizational model only represents one type of format for integrating JIIM personnel and capabilities. A future research study could focus on comparing and contrasting other existing interagency organizational frameworks with the JIATF organizational model to explore other options for a whole of society approach within the cyberspace domain.

The private sector owns approximately ninety percent of the cyberspace domain and networks supporting CIKR (JFQ 2019, 5). As such, the analysis and findings of this research study conclude that the integration of private cybersecurity firms within a JIATF command structure is critical for creating a unity of effort against malicious cyberspace actors and activities. However, the research study does not examine how a national level JIATF can organize, direct, guide, or advise private sector organizations' operations from a legal and policy perspective. A future study could include an in-depth analysis of overcoming current policy and legal constraints on PPP in the areas of cybersecurity and cyberspace operations.

In addition, this research study identified that the current public-private relationship in the cybersecurity arena remains weak following Snowden's disclosure of intelligence community practices (Segal 2017, 67-68). Given the scope of this research study, the analysis did not investigate how the USG can develop and maintain mutual trust between the JIATF-CO and private cybersecurity firms. A follow-on research study can encompass how the USG can conduct confidence-building measures with the private cybersecurity sector from a social science and leadership perspective.

Final Conclusion

The ancient Greek philosopher, Aristotle, famously said, "the whole is greater than the sum of its parts." Fast-forward over two millennia later. This phrase remains true regarding interagency coordination and collaboration to counter adversary actions against U.S. national interests in the cyberspace domain. The former Commander of USCYBERCOM Admiral Mike Rogers emphasized that "no single entity has all the necessary insight, authorities, capabilities, or resources to protect and defend the [United

States] and allied interests in cyberspace," highlighting the need for a whole of society approach (Rogers 2015, 1).

A qualitative analysis found that JIATF-South provides a framework for how the USG can integrate and coordinate joint services, interagency, coalition partners, and private sector capabilities to achieve the strategic objectives outlined in the *National Security Strategy*. As such, US policymakers and military planners can use the lessons from JIATF-South in conjunction with its key ingredient of doctrine, organizational structure, leadership philosophy, and policies to formulate a national level JIATF for the cyberspace domain.

REFERENCE LIST

Abercrombie-Winstanley, Gina. 2018. "A Diplomat in a Cyber World: Working with CYBERCOM." American Foreign Service Association, 4 May. Accessed 4 February 2019. http://www.afsa.org/diplomat-cyber-world-working-cybercom.

Barlyn, Suzanne. 2017. "Global Cyber Attack Could Spur $53 Billion In Losses: Lloyd's of London." *Reuters*, July 16. Accessed 4 February 2019. https://www.reuters.com/article/us-cyber-lloyds-report/global-cyber-attack-could-spur-53-billion-in-losses-lloyds-of-london-idUSKBN1A20AB.

Barr, William. 2019. *The Special Counsel's Report*. Washington, DC: U.S. Department of Justice, 24 March. Accessed 4 April 2019. https://www.politico.com/f/?id=00000169-b13e-dce8-a5e9-b1be04990000.

Bayuk, Jennifer, Jason Healy, Paul Rohmeyer, Marcus Sachs, Jeffrey Schmidt, and Joseph Weiss. 2012. *Cyber Security Policy Guidebook*. Hoboken, NJ: John Wiley and Sons, Inc. Accessed 4 February 2019. https://onlinelibrary.wiley.com/doi/book/10.1002/9781118241530.

Belk, Robert, and Matthew Noyes. 2012. *On the Use of Offensive Cyber Capabilities: A Policy Analysis on Offensive U.S. Cyber Policy*. Cambridge, MA: Harvard Kennedy School, 20 March. Accessed 4 February 2019. https://www.belfercenter.org/sites/default/files/files/publication/cybersecurity-pae-belk-noyes.pdf.

Blum, H. Steven, and Kerry McIntyre. 2012. "Enabling Unity of Effort in Homeland Response Operations." Strategic Studies Institute, U.S. Army War College, Carlisle, PA, April. Accessed 30 March 2019. https://www.jstor.org/stable/resrep11373

Bossert, Thomas. 2017. "Press Briefing on the Attribution of the WannaCry Malware Attack to North Korea." The White House. 19 December. Accessed 9 February 2019. https://www.whitehouse.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacry-malware-attack-to-north-korea-121917/.

Bozin, William. 1996. *William G. Bozin, Office of National Drug Control Policy, Executive Office of the President, Senate Caucus on International Narcotics Control and the House Committee on Transportation Subcommittee on Coast Guard and Maritime Transportation*. Washington, DC: Government Publishing Directorate, 12 September. Accessed 4 February 2019. https://fas.org/irp/congress/1996_hr/j960912b.htm.

Breland, Ali. 2017. "Thousands attended protest organized by Russians on Facebook." *The Hill*, 31 October. Accessed 4 February 2019. https://thehill.com/policy/technology/358025-thousands-attended-protest-organized-by-russians-on-facebook.

Brigham Young University (BYU). 2019. “Step-by-Step Guide & Research Rescue: Evaluating Credibility.” BYU Library, 23 January. Accessed 14 February 2019. http://guides.lib.byu.edu/c.php?g=216340&p=1428399.

Brown, Megan. 2018. *Cyber Imperative: Preserve and Strengthen Public-Private Partnership*. Fairfax, VA: The National Security Institute at George Mason University’s Antonin Scalia Law School, 11 October. Accessed 4 February 2019. http://nationalsecurity.gmu.edu/wp-content/uploads/2018/10/Cyber-Imperative-Final-Web.pdf.

Buchanan, Ben. 2018. “The Implications of Defending Forward in the New Pentagon Cyber Strategy.” *Council on Foreign Relations Blog*, 25 September. Accessed 9 January 2019. https://www.cfr.org/blog/implications-defending-forward-new-pentagon-cyber-strategy.

Bureau of Public Affairs. 2018. “Sanctions Announcement on Russia.” U.S. Department of State, 19 December. Accessed 4 February 2019. https://www.state.gov/r/pa/prs/ps/2018/12/288213.htm.

Cable News Network (CNN). 2018. “2016 Presidential Campaign Hacking Fast Facts.” 24 November. Accessed 4 February 2019. https://www.cnn.com/2016/12/26/us/2016-presidential-campaign-hacking-fast-facts/index.html.

Carpenter, Ami. 2013. “Changing Lenses: Conflict Analysis and Mexico’s ‘Drug War’.” *Latin American Politics and Society55*9, no. 3 (Fall): 139-160. Accessed 22 March 2019. https://www-jstor-org.lumen.cgsccarl.com/stable/pdf/43284851.pdf.

Carter, Alexander. 2015. “Improving Joint Interagency Coordination: Changing Mindsets.” *Joint Forces Quarterly* 79, no. 4 (October): 19-26. Accessed 22 March 2019. https://ndupress.ndu.edu/JFQ/Joint-Force-Quarterly-79/.

Center for Strategic and International Studies (CSIS). 2018. “Significant Cyber Incidents.” 30 August. Accessed 30 August 2018. https://www.csis.org/programs/cybersecurity-and-governance/technology-policy-program/other-projects-cybersecurity.

Chang, Amy. 2014. *Warring State: China’s Cybersecurity Strategy.* Washington, DC: Center for a New American Security, 3 December. Accessed 14 February 2019. https://www.cnas.org/publications/reports/warring-state-chinas-cybersecurity-strategy.

Chen, Jim. 2017. “Cyber Deterrence by Engagement and Surprise.” *PRISM* 7, no. 2, (December): 100-107. Accessed 17 February 2019. https://apps.dtic.mil/dtic/tr/fulltext/u2/1044758.pdf.

Chesney, Robert. 2018a. “The 2018 DOD Cyber Strategy: Understanding ‘Defense Forward’ in Light of the NDAA and PPD-20 Changes Lawfare.” *Lawfare Blog,* 25 September. Accessed 3 January 2019. https://www.lawfareblog.com/ 2018-DOD-cyber-strategy-understanding-defense-forward-light-ndaa-and-ppd-20-changes.

———. 2018b. “New Authorities for Military Cyber Operations and Surveillance, Including TMA?” *Lawfare Blog,* 27 June. Accessed 17 February 2019. https://www.lawfareblog.com/new-authorities-military-cyber-operations-and-surveillance-including-tma.

Cieply, Michael, and Barnes Brooks. 2014. “Sony Cyberattack, First a Nuisance, Swiftly Grew into a Firestorm.” *The New York Times*, 30 December. Accessed 31 January 2019. https://www.nytimes.com/2014/12/31/business/media/sony-attack-first-a-nuisance-swiftly-grew-into-a-firestorm-.html.

Command and General Staff College (CGSC). 2018. Student Text 20-10, *Master of Military Art and Science (MMAS) Research and Thesis.* Fort Leavenworth, KS: CGSC, 16 August.

Creswell, John. 2007. *Qualitative Inquiry and Research Design*. Thousand Oaks, CA: Sage Publications Inc.

Cyber Matters. Public Law 115–232. *U.S. Code 10* (2018), § 394. Accessed 17 February 2019. http://uscode.house.gov/view.xhtml?path=/prelim@title10/subtitleA/part1/ chapter19&edition=prelim.

Cybersecurity. Executive Order no. 13800. *U.S. Code 6* (2017), § 2. Accessed 17 February 2019. http://uscode.house.gov/view.xhtml?path=/prelim@title6/chapter6 &edition=prelim.

Davis, John, Benjamin Boudreaux, Jonathan William Welburn, Jair Aguirre, Cordaye Ogletree, Geoffrey McGovern, and Michael Chase. 2017. *Stateless Attribution: Toward International Accountability in Cyberspace*. Santa Monica, CA: RAND Corporation, 2017. Accessed 5 February 2019. https://www.rand.org/content/ dam/rand/pubs/research_reports/RR2000/RR2081/RAND_RR2081.pdf.

Davis Jr., William. 2017. “Why We Keep Getting It Wrong: What Makes the JIIM so Different?” *InterAgency Journal* 8 no. 4 (August): 48-56. Accessed 27 March 2019. http://thesimonscenter.org/wp-content/uploads/2017/11/IAJ-8-4-2017-pg48-56.pdf.

Denning, Dorothy. 2015. “Rethinking the Cyber Domain and Deterrence.” *Joint Forces Quarterly* 77, no. 2 (April): 8-15. Accessed 5 February 2019. https://ndupress. ndu.edu/JFQ/Joint-Force-Quarterly-77/Article/581864/rethinking-the-cyber-domain-and-deterrence/.

DeSimone, Antonio, and Nicholas Horton. 2017. *Sony's Nightmare before Christmas: The 2014 North Korean Cyber Attack on Sony and Lessons for U.S. Government Actions in Cyberspace*. Laurel, MD: Johns Hopkins Applied Physics Laboratory, 20 November. Accessed 5 February 2019. https://www.jhuapl.edu/Content/documents/SonyNightmareBeforeChristmas.pdf.

Dill, Karen. 2018. "Cybersecurity for the Nation: Workforce Development" *The Cyber Defense Review* 3 no. 2 (Summer): 55-64. Accessed 6 April 2019. https://www.jstor.org/stable/10.2307/26491223.

Echevarria, Antulio. 2016. "Operating in the Gray Zone: An Alternative Paradigm for U.S. Military Strategy." Monograph, Strategic Studies Institute, U.S. Army War College, Carlisle, PA, 4 April. Accessed 5 February 2019. https://ssi.armywar college.edu/pubs/display.cfm?pubID=1318.

Federal Bureau of Investigation (FBI). 2019a. "Addressing Threats to the Nation's Cybersecurity." 26 January. Accessed 26 January 2019. https://www.fbi.gov/file-repository/addressing-threats-to-the-nations-cybersecurity-1.pdf/view.

———. 2019b. "Cyber Task Forces: Building Alliances to Improve the Nation's Cybersecurity." 26 January 2019. Accessed 26 January 2019. https://www.fbi.gov/file-repository/cyber-task-forces-fact-sheet.pdf/view.

———. 2019c. "National Cyber Investigative Joint Task Force." 17 January. Accessed 17 January 2019. https://www.fbi.gov/investigate/cyber/national-cyber-investigative-joint-task-force.

Federal Emergency Management Agency (FEMA). 2008. *Critical Infrastructure and Key Resources Support Annex*. Washington, DC: Department of Homeland Security, January. Accessed 15 October 2018. https://www.fema.gov/pdf/emergency/nrf/nrf-support-cikr.pdf.

Finkle, Jim, and Christopher Bing. 2018. "China's hacking against U.S. on the Rise: U.S. intelligence official." *Reuters*. 11 December. Accessed 4 February 2019. https://www.reuters.com/article/us-usa-cyber-china/chinas-hacking-against-u-s-on-the-rise-u-s-intelligence-official-idUSKBN1OA1TB.

Fischerkeller, Michael. 2017. *Toward a Credible Strategy for Cyberspace*. Alexandria, VA: Institute for Defense Analyses, December. Accessed 17 January 2019. https://www.ida.org/idamedia/Corporate/Files/Publications/Insights/D-8859-fischerkeller.pdf.

Flavin, Bill. 2018. *Stabilization: A New Approach to Whole of Government Operational Planning and Execution*. Carlisle, PA: Army War College, June. U.S. Army Peacekeeping and Stability Operations Institute. Accessed 18 March 2019. https://publications.armywarcollege.edu/pubs/3540.pdf.

Freund, Eleanor. 2017. *Freedom of Navigation in the South China Sea: A Practical Guide*. Cambridge, MA: Harvard Kennedy School's Belfer Center for Science and International Affairs, June. Accessed October 15, 2018. https://www.belfercenter.org/publication/freedom-navigation-south-china-sea-practical-guide.

Fussell, Chris and Charles Goodyear. 2017. *One Mission: How Leaders Build a Team of Teams*. New York: Portfolio / Penguin.

Geneva Call. 2019. "Mission." 22 March. Accessed 22 March 2019. https://genevacall.org/who-we-are/.

Grave, Thomas. 2017. *Active Cyber Defense Certainty Act: Bipartisan Bill Empowers Americans to Develop New Defenses against Cyber Attack*. Washington, DC: U.S. Congress, October. Accessed 8 April 2019. https://tomgraves.house.gov/uploadedfiles/acdc_expaliner.pdf.

Hathaway, Melissa, Chris Demchak, Jason Kerben, Jennifer McArdle, and Francesca Spidalieri. 2016. *United States of America Cyber Readiness at a Glance*. Arlington, VA: Potomac Institute for Policy Studies, September. Accessed 26 March 2019. http://www.potomacinstitute.org/images/CRI/CRI_US_Profile_Web.pdf.

Headquarters, Department of the Army (HQDA). 2012. Army Doctrine Reference Publication 6-0, *Mission Command*. Washington, DC: Government Publishing Directorate, September.

Hurwitz, Roger. 2012. "Depleted Trust in the Cyber Commons." *Strategic Studies Quarterly*, Fall 2012 (January): 20-44. Accessed 4 February 2019. https://apps.dtic.mil/dtic/tr/fulltext/u2/a619087.pdf.

Hutchens, Michael, William Dries, Jason Perdew, Vincent Bryant, and Kerry Moores. 2017. "Joint Concept for Access and Maneuver in the Global Commons." *Joint Forces Quarterly* 84 (January): 134-139. Accessed 17 January 2019. https://ndupress.ndu.edu/Media/News/Article/1038867/joint-concept-for-access-and-maneuver-in-the-global-commons-a-new-joint-operati/.

Jensen, Eric. 2017. "Risk Informed, but Not Risk Averse: The National Security Strategy Approach to Cyber Ops." *Just Security Blog*, 22 December. Accessed 11 October 2018. https://www.justsecurity.org/50066/risk-informed-risk-averse-national-security-strategy-approach-cyber-ops/.

Joint Chiefs of Staff. (JCS) 2013. Joint Publication 3-16, *Multinational Operations*. Washington, DC: Department of Defense, July. Accessed 26 March 2019. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_16.pdf.

———. 2014. Joint Publication 3-13, *Information Operations*. Washington, DC: Department of Defense, November. Accessed 15 October 2018. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13.pdf.

———. 2017a. Joint Publication 3-08, *Interorganizatonal Cooperation*. Washington, DC: Department of Defense, October. Accessed 15 October 2018. http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_08pa.pdf.

———. 2017b. Joint Publication 3-0, *Joint Operations*. Washington, DC: Department of Defense, January. Accessed October 15, 2018. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_0ch1.pdf?ver=2018-11-27-160457-910.

———. 2018a. Joint Publication 3-12, *Cyberspace Operations*. Washington, DC: Department of Defense, June. Accessed 15 October 2018. http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf?ver=2018-07-16-134954-150.

———. 2018b. *Manual for the Operation of the Joint Capabilities Integration and Development System*. Washington, DC: Defense Acquisition University, August. Accessed 28 January 2019. https://www.dau.mil/cop/rqmt/DAU%20 Sponsored%20Documents/Manual%20-%20JCIDS,%2031%20Aug%202018.pdf.

Joint Force Quarterly (JFQ). 2019. "An Interview with Paul M. Nakasone." *Joint Forces Quarterly* 92 no. 1 (January): 4-9. Accessed 2 March 2019. https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-92/jfq-92_4-9_Nakasone-Interview.pdf.

Joint Interagency Task Force South (JIATF-South). 2019a. "Joint Interagency Task Force South." March. Accessed 2 March 2 2019. https://www.jiatfs.southcom.mil/.

———. 2019b. "About Us." February. Accessed 12 February 2019. https://www.jiatfs.southcom.mil/About-Us/.

Kollars, Nina, and Jacquelyn Schneider. 2018. "Defending Forward: The 2018 Cyber Strategy is Here." *War on the Rocks Blog*, 20 September. Accessed 9 January 2019. https://warontherocks.com/2018/09/defending-forward-the-2018-cyber-strategy-is-here/.

Kramer, Franklin, Robert Butler, and Catherine Lotrionte. 2017. *Cyber and Deterrence: The Military-Civil Nexus in High-End Conflict*. Brent Scowcroft Center on International Studies. Washington, DC: Atlantic Council, January. Accessed 9 January 2019. https://www.atlanticcouncil.org/images/publications/Cyber_and_Deterrence_web_0103.pdf.

Kuhns, Joseph, and Matthew Phillips. 2018. "Illicit Drug Trafficking," in *Transnational Crime and Global Security*. Santa Barbara, CA: ABC-CLIO.

Lawlor-Russell, Allision. 2017. *Strategic Anti-Access/Area Denial in Cyberspace*. Cambridge, MA: Cambridge University Press.

Lewis, James. 2018a. *Economic Impact of Cybercrime - No Slowing Down*. Santa Clara, CA: McAfee, February. Center for Strategic and International Studies. Accessed 2 March 2019. https://www.csis.org/analysis/economic-impact-cybercrime.

———. 2018b. *Rethinking Cybersecurity: Strategy, Mass Effect, and States*. Washington, DC: Center for Strategic and International Studies, January. Center for Strategic and International Studies. Accessed 2 March 2019. https://www.csis.org/analysis/rethinking-cybersecurity.

Liaropoulos, Andrew. 2016. "Exploring the Complexity of Cyberspace Governance: State Sovereignty, Multistakeholderism, and Power Politics." *Journal of Information Warfare* 15, no. 4 (December): 14-26.

Mandsager, Dennis. 1997. "The U.S. Freedom Navigation Program: Policy, Procedures, and Future." *International Law Studies* 72 (November): 113-127. Accessed 28 February 2019. https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1465&context=ils.

Marist Poll. 2018. *NPR/Marist Poll Results September 2018: Election Security*. Poughkeepsie, NY: Marist College, September. Accessed 5 February 2019. http://maristpoll.marist.edu/wp-content/uploads/2018/09/NPR_Marist-Poll_National-Nature-of-the-Sample-and-Tables_September-2018_1809111654.pdf#page=3.

Marks, Joseph. 2018. "The Annual Cost of U.S. Cybercrime Could Top $100 Billion." *Nextgov,* 16 February. Accessed 9 August 2018. https://www.nextgov.com/cybersecurity/2018/02/annual-cost-us-cybercrime-could-top-100-billion/146068/.

Marwan, Samar. 2017. "CrowdStrike Helped Trace the DNC Hack to Russia -- Now Business Is Booming." *Forbes*, 27 July. Accessed 5 February 2019. https://www.forbes.com/sites/samarmarwan/2017/07/11/crowdstrike-helped-trace-the-dnc-hack-to-russia-now-business-is-booming/#377d26e74434.

Matishak, Martin. 2018. "What we know about Russia's election hacking." *Politico*, 18 July. Accessed January 17, 2019. https://www.politico.com/story/2018/07/18/russia-election-hacking-trump-putin-698087.

Mazanec, Brian. 2015. *The Evolution of Cyber War: International Norms for Emerging-Technology Weapons*. Lincoln: University of Nebraska Press.

Mazarr, Michael. 2015. "Mastering the Gray Zone, Understanding a Changing Era of Conflict." Monograph, Strategic Studies Institute, U.S. Army War College, Carlisle, PA, 2 December. Accessed 5 February 2019. https://ssi.armywarcollege.edu/pubs/display.cfm?pubID=1303

McGhee, James. 2016. “Liberating Cyber Offense.” *Strategic Studies Quarterly* 10 no. 4 (Winter): 46-63. Accessed 16 April 2019. https://www.jstor.org/stable/ 10.2307/2627.

———. 2014. “Hack, Attack or Whack; The Politics of Imprecision in Cyber Law.” *Journal of Law and Cyber Warfare* 4 no. 1 (Winter): 13-41. Accessed 8 April 2019. https://www.jstor.org/stable/10.2307/26441247.

McKenzie, Timothy. 2017. *Is Cyber Deterrence Possible?* Air Force Research Institute Papers. Maxwell AFB, AL: Air University, 1 January. Accessed 5 February 2019. https://www-jstor-org.lumen.cgsccarl.com/stable/resrep13817

Meer, Sico Van Der. 2015. *Signalling as a Foreign Policy Instrument to Deter Cyber Aggression by State Actors.* Clingendael, Netherland: Netherlands Institute of International Relations, December. Accessed 5 February 2019. https://www. clingendael.org/sites/default/files/pdfs/PB_Signalling_as_a_foreign_policy_instrument_SvdM.pdf.

Munsing, Evan, and Christopher Lamb. 2011. *Joint Interagency Task Force-South: The Best Known, Least Understood Interagency Success*. Washington, DC: National Defense University Press, June. Institute for National Strategic Studies Strategic Perspective. Accessed 13 February 2019. https://ndupress.ndu.edu/ portals/68/documents/stratperspective/inss/strategic-perspectives-5.pdf.

Nakashima, Ellen. 2015. “Hacks of OPM databases compromised 22.1 million people, federal authorities say.” *The Washington Post*, 9 July. Accessed 9 August 2018. https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/?utm_term=.5f0a1d9cd5e3.

Nakasone, Paul. 2019a. *Statement of General Paul M. Nakasone, Commander, United States Cyber Command before the Senate Committee on Armed Services*. Senate Committee on Armed Services. Washington, DC: U.S. Government Publishing Directorate, 14 February. Accessed 2 March 2019. https://www.armedservices. senate.gov/download/nakasone_02-14-19.

———. 2019b. “A Cyber Force for Persistent Operations.” *Joint Forces Quarterly* 92 no. 1 (January): 10-14. Accessed 2 March 2019. https://ndupress.ndu.edu/Portals/ 68/Documents/jfq/jfq-92/jfq-92.pdf.

National Cybersecurity and Communications Integration Center. 2018b. “National Cybersecurity and Communications Integration Center.” Accessed 17 December 2018. https://www.dhs.gov/national-cybersecurity-and-communications-integration-center.

National Guard Bureau (NGB). 2019. *2019 Domestic Operations Law and Policy*. Washington, DC: National Guard Bureau, 28 November. Accessed 8 April 2019. https://www.ngbpdc.ngb.army.mil/Portals/27/Publications/special%20documents/2019%20Domestic%20Operations.pdf?ver=2018-12-17-145332-387

Neely, Mark E. Jr. 1982. *The Abraham Lincoln Encyclopedia*. New York: Da Capo Press, Inc.

Nye, Joseph. 2017. "Deterrence and Dissuasion in Cyberspace." *International Security* 41, no. 3 (Winter 2016/17): 44-71. Accessed 31 January 2019. https://www.belfercenter.org/publication/deterrence-and-dissuasion-cyberspace.

Obama, Barack H. 2015. "Executive Order -- Promoting Private Sector Cybersecurity Information Sharing." 13 February. Accessed 16 February 2018. https://obamawhitehouse.archives.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari.

Office of National Drug Control Policy. 1999. *National Interdiction Command and Control Plan.* Washington, DC: The Executive Office of the President, 1 May.

Office of the Coordinator for Cyber Issues. 2018a. *Recommendations to the President on Deterring Adversaries and Better Protecting the American People from Cyber Threats*. Washington, DC: U.S. Department of State, 31 May. Accessed 24 January 2019. https://www.state.gov/s/cyberissues/eo13800/282011.htm.

———. 2018b. *Recommendations to the President on Protecting American Cyber Interests through International Engagement*. Washington, DC: U.S. Department of State, 31 May. Accessed 24 January 2019. https://www.state.gov/s/cyberissues/eo13800/281980.htm.

Office of the Deputy Attorney General. 2018. *Report of the Attorney General's Cyber Digital Task Force*. Washington, DC: U.S. Department of Justice, 2 July. Accessed 26 January 2019. https://www.justice.gov/ag/page/file/1076696/download.

Office of the Director for National Intelligence (DNI). 2017. *Assessing Russian Activities and Intentions in Recent U.S. Elections.* Washington, DC: Office of the Director of National Intelligence, 6 January. Accessed 31 January 2019. https://www.dni.gov/files/documents/ICA_2017_01.pdf.

Office of the Inspector General (IG). 2015. *Audit of the Federal Bureau of Investigation's Implementation of Its Next Generation Cyber Initiative*. Washington, DC: U.S. Department of Justice, July. Accessed 26 March 2019. https://oig.justice.gov/reports/2015/a1529.pdf.

Pomerleau, Mark. 2017a. "Cyber is being normalized with traditional military operations." Fifth Domain, 14 September. Accessed 17 January 2019. https://www.fifthdomain.com/DOD/2017/09/14/cyber-is-being-normalized-with-traditional-operations/.

———. 2017b. "What Trump's National Security Strategy says on Cyber." Fifth Domain, 18 December. Accessed 11 October 2018. https://www.fifthdomain.com/civilian/2017/12/18/what-trumps-national-security-strategy-says-on-cyber/.

———. 2018. "Here's how Cyber Command's 'defend forward' strategy protects the nation in cyberspace." Fifth Domain, 19 November. Accessed 6 April 2019. https://www.fifthdomain.com/DOD/2018/11/19/heres-how-cyber-commands-defend-forward-strategy-protects-the-nation-in-cyberspace/.

Pope, Robert. 2011. "Interagency Task Forces: The Right Tools for the Job." *Strategic Studies Quarterly* 5, no. 2 (Summer): 113-152. Accessed 2 March 2019. https://www-jstor-org.lumen.cgsccarl.com/stable/e26270552.

———. 2014. *U.S. Interagency Regional Foreign Policy Implementation: A Survey of Current Practice and an Analysis of Options for Improvement*. Maxwell AFB, AL: Air University Press, June. Air Force Research Institute. Accessed 18 March 2019. https://media.defense.gov/2017/Apr/07/2001728530/-1/-1/0/B_0134_POPE_INTERAGENCY_FOREIGN_POLICY.PDF.

Porche III, Isaac, Christopher Paul, Chad Serena, Colin Clarke, Erin-Elizabeth Johnson, and Drew Herrick. 2017. *Tactical Cyber: Building a Strategy for Cyber Support to Corps and Below*. Santa Monica, CA: RAND Corporation, 26 April. Accessed 2 March 2019. https://www.rand.org/content/dam/rand/pubs/research_reports/RR1600/RR1600/RAND_RR1600.pdf.

Reagan, Ronald W. 1986. *National Security Decision Directive 221, Narcotics and National Security*. Washington, DC: White House, 8 April. Accessed 28 February 2019. https://catalog.archives.gov/id/6879807.

Reed, George. 2015. *Tarnished: Toxic Leadership in the U.S. Military*. Lincoln, NE: Potomac Books.

Richwine, Lisa. 2014. "Cyber attack could cost Sony studio as much as $100 million." *Reuters*. 9 December. Accessed 17 January 2019. https://www.reuters.com/article/us-sony-cybersecurity-costs/cyber-attack-could-cost-sony-studio-as-much-as-100-million-idUSKBN0JN2L020141209.

Rogers, Michael. 2015 "A Challenge for the Military Cyber Workforce." *Military Cyber Affairs* 1, no. 1. (December): 1. Accessed 4 April 2019. http://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1012&context=mca.

Schelling, Thomas. 1966. *Arms and Influence*. New Haven, CT: Yale University Press.

Schmitt, Gary. “A few Thoughts on the New Cyber Strategy.” *AEIdeas Blog*, 21 September. American Enterprise Institute. Accessed 9 January 2019. http://www.aei.org/publication/a-few-thoughts-on-the-new-cyber-strategy/.

Schoka, Andrew. 2019. “Cyber Command, the NSA, and Operating in Cyberspace: Time to End the Dual Hat.” *War on the Rocks Blog*, 3 April. Accessed 8 April 2019. https://warontherocks.com/2019/04/cyber-command-the-nsa-and-operating-in-cyberspace-time-to-end-the-dual-hat/.

Segal, Adam. 2017. “Bridging the Cyberspace Gap: Washington and Silicon Valley.” *PRISM* 7, no. 2 (December): 66-77. Accessed 28 February 2019. https://www.hsdl.org/?view&did=806910.

Stavridis, James. 2008. “Whatever Happened to the ‘War on Drugs’?” *Joint Forces Quarterly* 51, no. 4 (October): 109-113. Accessed 22 March 2019. https://apps.dtic.mil/dtic/tr/fulltext/u2/a496253.pdf.

Sulmeyer, Michael. 2017a. “Cybersecurity in the 2017 National Security Strategy.” *Lawfare Blog*, 19 December. Accessed 10 October 2018. https://www.lawfareblog.com/cybersecurity-2017-national-security-strategy.

———. 2017b. *Military Cyber Issues*. Cyber Policy Task Force. Washington, DC: Center for Strategic Studies and International Studies, 5 January. Accessed 8 April 2019. https://csis-prod.s3.amazonaws.com/s3fs-public/170110_CSIS_Cyber_Policy_Discussion_Papers.pdf.

———. 2018. “How the U.S. Can Play Cyber-Offense.” Belfer Center for Science and International Affairs, Harvard Kennedy School, 22 March. Accessed 10 January 2019. https://www.belfercenter.org/publication/how-us-can-play-cyber-offense-0.

Symantec. 2017. “What you need to know about the WannaCry Ransomware.” 23 October. Accessed 3 February 2019. https://www.symantec.com/blogs/threat-intelligence/wannacry-ransomware-attack.

Tangredi, Sam J. 2018. “From Global Commons to Territorial Sea: A Naval Analogy for the Nationalization of Cyberspace.” *Military Cyber Affairs* 3, no. 1 (July): 1-11. Accessed 4 February 2019. https://scholarcommons.usf.edu/mca/vol3/iss1/5/.

Terdiman, Daniel. 2018. “U.S. More Vulnerable to Weaponized Cyberattacks Than You Think.” *Fast Company*, 10 March. Accessed 28 February 2019. https://www.fastcompany.com/40542648/the-u-s-is-more-vulnerable-to-weaponized-cyberattacks-than-you-think.

Theohary, Catherine, and Anne Harrington. 2015. *Cyber Operations in DOD Policy and Plans: Issues for Congress*. Congressional Research Service Report for Congress. Washington, DC: Library of Congress, 5 January. Accessed 28 February 2019. https://fas.org/sgp/crs/natsec/R43848.pdf.

Tidd, Kurt. 2018. *Posture Statement of Admiral Kurt W. Tidd, Commander, United States Southern Command before the 115th Congress Senate Armed Services Committee*. Senate Armed Services Committee. Washington, DC: U.S. Government Publishing Directorate, 15 February. Accessed 2 March 2019. https://www.southcom.mil/Portals/7/Documents/Posture%20Statements/SOUTHCOM_2018_Posture_Statement_FINAL.PDF?ver=2018-02-15-090330-243.

Tidd, Kurt, and Tyler Morton. 2017. "U.S. Southern Command: Evolving to Meet 21st-Century Challenges." *Joint Forces Quarterly* 86 no. 3 (July): 11-19. Accessed 26 March 2019. https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-86/jfq-86.pdf.

Trump, Donald J. 2017a. *National Security Strategy of the United States of America*. Washington, DC: The White House, 18 December. Accessed 16 February 2019. https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

———. 2017b. "Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure." 11 May. Accessed 22 January 2019. https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/.

———. 2018a. *National Cyber Strategy of the United States of America*. Washington, DC: The White House, 20 September. Accessed 16 February 2019. https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

———. 2018b. *The Cost of Malicious Cyber Activity to the U.S. Economy*. Washington, DC: The Council of Economic Advisers, Executive Office of the President, February. Accessed 9 August 2018. https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf.

———. 2019. *Cybersecurity Funding*. Washington, DC: The White House, February. Accessed 9 April 2019. https://www.whitehouse.gov/wp-content/uploads/2018/02/ap_21_cyber_security-fy2019.pdf.

United Nations (UN). 2013. *Global Governance and Governance of the Global Commons in the Global Partnership for Development beyond 2015*. New York: United Nations, January. Accessed 15 October 2018. http://www.un.org/en/development/desa/policy/untaskteam_undf/thinkpieces/24_thinkpiece_global_governance.pdf.

United Nations General Assembly. 2012. *Political Declaration of the High-level Meeting of the General Assembly on the Prevention and Control of Non-communicable Diseases*, 66th Sess. Agenda item 117. New York: United Nations, 24 January. Accessed 15 October 2018. http://www.who.int/nmh/events/un_ncd_summit 2011/political_declaration_en.pdf.

United Nations Office on Drugs and Crime (UNODC). 2019. “Alternative Development.” 23 March. Accessed 23 March 2019. https://www.unodc.org/unodc/en/alternative-development/index.html.

University of Kansas (KU). 2018. “Section 14. SWOT Analysis: Strengths, Weaknesses, Opportunities, and Threats.” University of Kansas Community Tool Box, 2018. Accessed 17 February 2019. https://ctb.ku.edu/en/table-of-contents/assessment/assessing-community-needs-and-resources/swot-analysis/main.

U.S. Air Force (USAF). 2015. *Volume 1 Basic Doctrine: Steady-State Operations*. Maxwell AFB, Montgomery AL: Curtis E. LeMay Center for Doctrine Development and Education, February. Accessed 9 January 2019. https://www.doctrine.af.mil/Portals/61/documents/Volume_1/V1-D35-Steady-State-Ops.pdf.

U.S. Congress. 2017. House. Active Cyber Defense Certainty Act. HR 4036. 115th Cong., 1st sess. (1 November). Accessed 8 April 2019. https://www.congress.gov/bill/115th-congress/house-bill/4036/all-actions-without-amendments.

———. 2018. House. John S. McCain National Defense Authorization Act for Fiscal Year 2019. HR 115-232. 115th Cong., 2d sess. (13 August). Accessed 17 February 2019. https://www.congress.gov/bill/115th-congress/house-bill/5515/text.

U.S. Cyber Command (USCYBERCOM). 2018. *Command Vision for U.S. Cyber Command: Achieve and Maintain Cyberspace Superiority.* Ft. Meade, MD: U.S. Cyber Command, April. Accessed 15 October 2018. https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010.

———. 2019. “Cyber Mission Force Achieves Full Operational Capability.” 17 May. Accessed 6 April 2019. https://DOD.defense.gov/News/Article/Article/1524747/cyber-mission-force-achieves-full-operational-capability/.

U.S. Department of Defense (DOD). 2018a. *Summary of the 2018 National Defense Strategy of the United States of America*. Washington, DC: U.S. Department of Defense, January. Accessed 9 January 2019. https://DOD.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

———. 2018b. *Summary: Department of Defense Cyber Strategy 2018*. Washington, DC: U.S. Department of Defense, September. Accessed 9 January 2019. https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

U.S. Department of Homeland Security (DHS). 2018. *U.S. Department of Homeland Security: Cybersecurity Strategy*. Washington, DC: U.S. Department of Homeland Security, 15 May. Accessed 17 January 2019. https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf.

U.S. Department of the Treasury (DOT). 2019a. "Code of Federal Regulations (CFR)." 7 March. Accessed 26 March 2019. https://www.treasury.gov/resource-center/sanctions/
pages/cfr-links.aspx.

———. 2019b. "Office of Foreign Assets Control - Sanctions Programs and Information." 26 February. Accessed 26 March 2019. https://www.treasury.gov/ resource-center/sanctions/Pages/default.aspx.

U.S. Government Accountability Office (GAO). 2009. *Interagency Collaboration: Key Issues for Congressional Oversight of National Security Strategies, Organizations, Workforce, and Information Sharing, GAO-09-904SP*. Washington, DC: Government Accountability Office, September.

U.S. Northern Command. 2019. "About USNORTHCOM." March. Accessed 26 March 2019. https://www.northcom.mil/About-USNORTHCOM/.

Votel, Joseph, David Julazadeh, and Weilun Lin. 2018. "Operationalizing the Information Environment: Lessons Learned from Cyber Integration in the USCENTCOM AOR." *Cyber Defense Review* 3, no. 3 (December): 1-5. Accessed 17 February 2019. https://cyberdefensereview.army.mil/Portals/6/ CDR_V3N3_VOTEL_JULAZADEH_LIN_OperationalizingInfoEnvironment_ARTICLE_E2.pdf?ver=2018-12-21-222351-220.

Wall, Andru. 2011. *Demystifying the Title 10-Title 50 Debate: Distinguishing Military Operations, Intelligence Activities & Covert Action*. Cambridge MA: Presidents and Fellows of Harvard College, December. Accessed 6 April 2019. https://harvardnsj.org/2011/12/demystifying-the-title-10-title-50-debate-distinguishing-military-operations-intelligence-activities-covert-action/.

Webber, Anthony. 2011. "Interagency Coordination and Effectiveness: Employing the JIATF Model." Master's Thesis, Joint Forces Staff College, Joint Advanced Warfighting School, Norfolk, VA, 16 June. Accessed 26 March 2019. https://apps.dtic.mil/dtic/tr/fulltext/u2/a548085.pdf.

Wheeler, Tarah. 2018. "In Cyberwar, There are No Rules: Why the World Desperately Needs Digital Geneva Conventions." *Foreign Policy*, 12 September. Accessed 11 October 2018. https://foreignpolicy.com/2018/09/12/in-cyberwar-there-are-no-rules-cybersecurity-war-defense/.

Wolff, Josephine. 2018. “Trump’s Reckless Cybersecurity Strategy.” *The New York Times*, 2 October. Accessed 9 January 2019. https://www.nytimes.com/2018/10/02/opinion/trumps-reckless-cybersecurity-strategy.html.

Yeatman, Richard. 2006. “JIATF-South: Blueprint for Success.” *Joint Forces Quarterly* 42, (Fall): 26-27. Accessed 17 February 2019. https://apps.dtic.mil/dtic/tr/fulltext/u2/a520650.pdf.

Yourish, Karen. 2018. “How Russia Hacked the Democrats in 2016.” *The New York Times*, 13 July. Accessed 9 January 2019. https://www.nytimes.com/interactive/2018/07/13/us/politics/how-russia-hacked-the-2016-presidential-election.html.