Strategy Research Project

Is It Time for a United States Cyber Service?

by

Lieutenant Colonel Dexter C. Nunnally
United States Army

Under the Direction of:
Professor Howard C. Taylor, Jr.

United States Army War College
Class of 2018

The views expressed herein are those of the author(s) and do not necessarily reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

REPORT DOCUMENTATION PAGE

Form Approved--OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*
01-04-2018

2. REPORT TYPE
STRATEGY RESEARCH PROJECT

3. DATES COVERED *(From - To)*

4. TITLE AND SUBTITLE
Is It Time for a
United States Cyber Service?

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Lieutenant Colonel Dexter C. Nunnally
United States Army

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Professor Howard C. Taylor, Jr.

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U.S. Army War College, 122 Forbes Avenue, Carlisle, PA 17013

10. SPONSOR/MONITOR'S ACRONYM(S)

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

12. DISTRIBUTION / AVAILABILITY STATEMENT
Distribution A: Approved for Public Release. Distribution is Unlimited.
I understand this document will be included in a research database and available to the public. Author: ☒

13. SUPPLEMENTARY NOTES
Word Count: 7684

14. ABSTRACT

USCYBERCOM's elevation to a Functional Combatant Command (COCOM), pending nomination and confirmation of a Commanding General, places operational command of cyberspace operations under a COCOM with service component support. However, the nature of the threat and adversaries' advancing cyber capabilities may dictate a revolution in military affairs (RMA) for the DOD when it comes to cyberspace operations and the potential establishment of a cyber service. This monograph examines the efficacy of a separate cyber service using Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, Facilities, and Policy (DOTMLPF-P) spheres to assess the Department of Defense's current cyberspace efforts. Based on this analysis, the DOD's efforts to date appear sufficient to conduct cyberspace operations and a separate cyber service is not required.

15. SUBJECT TERMS
Cyberspace, USCYBERCOM, DOD, DOTMLPF

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT UU	**b. ABSTRACT** UU	**c. THIS PAGE** UU	UU	41	**19b. TELEPHONE NUMBER** *(w/ area code)*

Is It Time for a
United States Cyber Service?

(7684 words)

Abstract

USCYBERCOM's elevation to a Functional Combatant Command (COCOM), pending nomination and confirmation of a Commanding General, places operational command of cyberspace operations under a COCOM with service component support. However, the nature of the threat and adversaries' advancing cyber capabilities may dictate a revolution in military affairs (RMA) for the DOD when it comes to cyberspace operations and the potential establishment of a cyber service. This monograph examines the efficacy of a separate cyber service using Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, Facilities, and Policy (DOTMLPF-P) spheres to assess the Department of Defense's current cyberspace efforts. Based on this analysis, the DOD's efforts to date appear sufficient to conduct cyberspace operations and a separate cyber service is not required.

Is It Time for a United States Cyber Service?

> Cyberspace, like airspace, constitutes a vital operational venue for the U.S. military. Accordingly, it warrants what the sea, air, and land each have—an independent branch of the armed services.
>
> — Admiral James Stavridis, USN (Ret) and David Weinstein[1]

The 2017 National Defense Authorization Act (NDAA) elevated United States Cyberspace Command (USCYBERCOM) to a Functional Combatant Command (COCOM).[2] However, USCYBERCOM's elevation is pending two conditions: 1) The 3-star Army general's confirmation as the third USCYBERCOM Combatant Commander and 2) Publication of the 2018 Unified Command Plan (UCP)[3]. The NDAA's elevation language was a realization by the U.S. government that cyberspace and the threats to the United States (U.S.) were too numerous to relegate to a subunified command.[4] The elevation to unified command status assigns all active and reserve forces in the U.S. to USCYBERCOM to prepare cyber troops for assigned missions.[5] However, the NDAA's current actions may not be enough. Russia's alleged interference in the 2016 U.S. Presidential election, the 2014 Office of Personnel Management data breach by the Chinese, North Korea's 2014 Sony cyber attack (see endnote for the definition), and Iran's cyber-attacks targeting the U.S. banking system in 2012 are just a few of the significant cyber events to garner national attention.[6] Symantec's Internet Security Threat Report (ISTR) identified the U.S. as the top country affected by data breaches and identity theft in 2016. The FBI reports that the financial losses due to internet fraud exceeded $1.33 billion in 2016. Cyber incidents of this magnitude pose a national security threat to the U.S. by the potential loss of American lives, property destruction, policy objectives or economic interests affected.[7] These ongoing threats could be the impetus for Department of Defense (DOD) consideration of a cyber service.[8] However, there is currently no consensus among senior leaders or within the DOD on the need for a separate cyber service. For example, Admiral Stavridis, USN (ret) and Admiral Rogers, USN, USCYBERCOM Commander, both espouse different opinions on this issue.[9] The increasing cyber threat necessitates an analysis of the current DOD cyber effort to determine if a cyber service is warranted. This monograph examined existing Doctrine, Organization, Training, Materiel, Leadership, Personnel, and Facilities areas concerning cyberspace efforts (DOTMLPF). This paper did not analyze the policy arena (DOTMLPF-P) for this paper. Analysis indicates that the DOD's ongoing cyberspace efforts meet strategic and operational requirements, invalidating the need for a separate cyber service in the current operational and strategic environment.

Cyber Threats

The threats arrayed against the U.S. run the gamut of state and non-state actors all looking for ways to counter U.S. hegemony and harm the homeland. The capabilities coupled with the intentions of these actors exacerbate the cyber threat to U.S. critical infrastructure. In a 2016 hearing, the House Homeland Security Committee identified China, Russia, DPRK, and Iran as the premier nation-state cyber threats to the U.S. The committee also named criminal and terrorist organizations such as ISIS as non-state actors with expanding cyber capabilities.[10] The U.S. Intelligence Community's assessment of the cyber threat does not deviate from those identified in the House Homeland Security Committee testimony.[11]

China is one of the cyber threat actors identified in the 2017 National Security Strategy. As a near-peer competitor, China actively targets the U.S. with cyber-attacks.[12] Before 2015, the Chinese conducted cyber espionage against U.S.

companies and government agencies without impunity as part of its routine cyber-attacks. However, bilateral commitments agreed to by the U.S. and China led to a decrease in the volume of attacks, but not a cessation.[13] The U.S. intelligence community believes China will continue to conduct cyber espionage operations against U.S. government, U.S. companies, and U.S. allies.[14]

Russia is another nation-state that actively uses the cyber domain against the U.S.[15] As a near-peer cyberspace competitor, Russia's capabilities threaten all elements of U.S. national power: diplomatic, information, military, economic. Russian cyber actors also target federal and state governments and U.S. critical infrastructure. Moscow uses cyber-attacks to influence its adversaries and has taken a more aggressive approach since its 2008 Georgian invasion. Russia's most recent actions include efforts to affect the 2016 U.S. and 2017 French national elections.[16] The nature of the cyber-attacks and targets selected indicate authorization at the most senior levels of the Russian government.[17] The U.S. intelligence community assesses that Russia continues to conduct offensive cyber operations targeting the U.S. and its allies to support the Russian military and national objectives.[18]

Iran is the third state actor that uses cyber-attacks against the U.S. In 2012, the U.S. Department of Justice indicted seven Iranians (alleged members of the Iranian Revolutionary Guard Corps) for conducting cyber-attacks against the U.S. banking industry.[19] Tehran directly targeted the U.S. again in 2013, when an Iranian hacker infiltrated an industrial control system of a U.S. dam.[20]

North Korea is the final major state actor with cyber capabilities of immediate concern to the U.S.; Pyongyang's 6000-person strong cyber force is rapidly improving.

The 2014 Sony attack and data exfiltration of South Korean military plans from its military network are recent examples of the rogue regime's successful cyber-attacks.[21] North Korea's ability to conduct cyber-attacks against U.S. commercial entities and threaten U.S. allies, specifically in Southeast Asia, illuminate Pyongyang's emerging capacity, competence, and propensity for cyber warfare.[22]

Cyber as a weapon is quickly becoming an arrow in the quiver of terrorists as well. The primary use of cyberspace by terrorists like the Islamic State of Iraq and Ash-Sham (ISIS) is "to organize, recruit, spread propaganda, raise funds, collect intelligence, inspire action by followers, and coordinate operations. Other terrorist organizations such as Hezbollah and HAMAS focus their cyber efforts inside and outside the Middle East."[23]

The most effective non-state actor threatening the U.S. in the cyber domain originates in the criminal sector. Cyber-attacks by criminal organizations are the purview of other U.S. governmental agencies, such as the Federal Bureau of Investigation (FBI). Criminal organizations routinely use malware such as "ransomware" in their illicit money-making schemes. Criminals use these tools for theft, extortion, and other criminal activities.[24] These activities concern the DOD because these actors often use phishing emails to target their victims.[25] This activity is also a concern because there appears to be a nexus between nation-state actors and criminal organizations. For example, last year the US attributed the 'WannaCry' ransomware cyber-attack to North Korea.[26] The DOD's reliance on unclassified networks provides a gateway into the Department of Defense Information Network (DODIN). In many cases, criminal organizations now employ programmers to write malicious code, salespeople to sell their products (malware), and dedicated support personnel similar to legitimate information technology (IT) and cybersecurity firms.[27] A nation-state could utilize a criminal organization to steal sensitive data from the DOD – this tactic delays identification of the actor.

DOD Cyber Force Structure

DOD's cyber force structure began in 2009 with the creation of USCYBERCOM as a sub-unified command assigned to United States Strategic Command (USSTRATCOM).[28] USCYBERCOM achieved full operational capability (FOC) on 31 October 2010.[29] The establishment of USCYBERCOM aligned DOD cyber defense under a subunified command with global authorities and responsibilities to protect the Department of Defense Information Network (DODIN) and its data, support joint military commander objectives, and defend U.S. critical infrastructure.[30]

USCYBERCOM is responsible for U.S. cyberspace operations but does not train or equip the cyberspace mission forces (CMF). The 133 teams under USCYBERCOM's operational control achieved initial operational capability in 2016 (IOC) and must reach FOC in 2018.[31] However, the individual services (Army, Navy, Air Force, Marine, National Guard, and Coast Guard) provide these forces and manage their training, funding, doctrine, and assignments.

Four mission teams comprise USCYBERCOM's cyber mission force (133 total). The teams are Cyber National Mission Force, Cyber Combat Mission Force, Cyber Protection Force, and Cyber Support teams. Operational control of Cyber National Mission Force teams resides with USCYBERCOM. The personnel on these teams rotate through the Cyber National Mission Force, Cyber Combat Mission Force, and Cyber Support Force teams regardless of service. The Cyber Protection Force teams are service specific. Cyber Combat Mission Force teams operate at the operational level in support of COCOMs. Cyber Protection Force teams operate at the operational and tactical-levels in support of their respective Service component commands and services. Cyber Support teams assist the Cyber National and Combat Mission Force teams with analytic and planning support. The personnel on these teams rotate through the Cyber National Mission Force, Cyber Combat Mission Force, and Cyber Support Force teams regardless of their service. The Cyber Protection Force teams are service specific. Additionally, each military service established a Joint Force Headquarters-Cyber (JFHQ-C) component command to support USCYBERCOM and defend their respective portions of the DODIN. These JFHQs are Army Cyber (ARCYBER), Marine Forces Cyber (MARFORCYBER), Air Force Cyber (AFCYBER), U.S. Navy Fleet Cyber (FLTCYBER), and U.S. Coast Guard Cyber Command (CGCYBERCOM). Each JFHQ-C component command provides Cyber Combat Mission Force teams to their supported COCOMs for conducting cyber operations.[32] [33]

Doctrine

Joint and service-specific cyberspace operations doctrine appear nested to support cyber missions across the range of operations in all domains. The convergent thought and themes in all of the doctrine are that cyber is a domain that supports operations and is characterized by the interdependence of each, land, air, sea, space and cyber. Some of these documents are more detailed than others, yet, each services' doctrine or strategy uses joint language to describe the cyberspace operating environment and the forces required to conduct full-spectrum operations. There are also unique capabilities established within the services to support organic combat formations, but the CMF concepts are the same across each service. At this time, analysis of the DOD and service-specific doctrine appears sufficient to support current DOD cyberspace operations. Therefore, a separate cyber service is not currently needed.

Doctrine is the foundation for strategy, campaign plans, and operations in the DOD. These documents provide the baseline guidance for how the military conducts day-to-day operations and in crisis. Joint Publication 3-12-Redacted (JP 3-12(R)), *Cyberspace Operations*, provides the doctrinal template for cyberspace operations in a joint environment. In broad terms JP 3-12(R) “introduces cyberspace and its integration into joint operations, explains cyberspace operations and their relationship to joint functions, covers authorities, roles and responsibilities; and discusses planning and coordination of cyberspace operations.”[34] Subsequently, each service published doctrine that incorporates and expands on JP 3-12(R).

Army Doctrine (includes National Guard and Reserves). The Army published Field Manual 3-12 (FM 3-12), Cyberspace and Electronic Warfare Operations in April 2017. The field manual describes the tactics used to address future challenges through the planning, integration, and synchronization of cyberspace electronic warfare operations. “Due to the rapidly evolving cyberspace domain, the Cyber COE will review and update FM 3-12 and supportive publications on a frequent basis to keep pace with a continuously evolving cyberspace domain.”[35]

Marine Corps Interim Publication 3-32Ei (MCIP 3-32Ei), Marine Corps *Cyberspace Operations*, is the USMC’s doctrinal publication to the field. This document is an interim publication to indoctrinate Marine Corps forces on cyberspace operations, specifically Marine Air-Ground Task Force commanders (MAGTF) and elaborate on

“Marine Corps-specific information and procedures addressed in JP 3-12.”[36] The interim publication defines Marine cyber organization and roles and responsibilities in the cyberspace domain down to the MAGTF-level. The document also describes the DOD CMF construct and how it supports joint, combined, and Marine forces at each echelon.

The U.S. Air Force’s (USAF) complement to JP 3-12 is Annex 3-12 *Cyberspace Operations*. Similar to the Army’s FM 3-12, the USAF annex uses the same numbering convention as the joint doctrine making it easier for other services to identify. Annex 3-12 defines the operational environment, challenges, and threats to cyberspace operations. Other significant aspects of the document address the integration of cyberspace operations across domains; policy related to command and organization of cyberspace forces; the structure of cyberspace forces; command and control (C2) of cyberspace forces; and the design of cyberspace operations.[37]

The Air Force’s Annex 3-12 also provides a functional analysis of how Air Force cyberspace operations and doctrine nests with the DOD doctrine and national strategy. Appendix B of the annex affords an Airman overarching cyberspace doctrine from the national-level to service specific. This level of specificity allows Air Force cyber and operating forces to understand what documents inform cyberspace planning and operations planning in support of joint, combined and Air Force forces conducting full-spectrum operations.

The Navy codified its cyberspace operations in two documents: Naval Warfare Publication 3-13 (NWP), *Information Operations* and a strategic document titled *Navy Cyber Power 2020*. NWP 3-13 aligns with how the Navy has organized itself. The publication references information-related capabilities such as cyberspace, electronic warfare, military deception, and others.[38] This holistic approach to cyberspace operations is encapsulated in U.S. Fleet Cyber and U.S. Tenth Fleet (FCC-C10F) as the central operating authority responsible for many of these information-related capabilities.[39] In keeping with joint doctrine, this publication uses joint language to discuss cyberspace functional operations – offensive cyber operations, defensive cyber operations, and DOD information network operations.[40]

The *Navy Cyber Power 2020* provides the strategic vision and framework for naval cyberspace operations. The strategy identifies distinct qualities the Navy must possess to succeed and a way ahead to build a cyber force capable of conducting cyberspace operations in the future.[41] There are four key focus areas the Navy underpins their strategy on to achieve its vision for cyberspace operations:

- Integrated Operations
- Optimized Cyber Workforce
- Technology Innovation and Requirements
- PPBE and Acquisition Reform

Navy Cyber Power 2020 coupled with NWP 3-13 postures the Navy to conduct cyberspace operations in support of joint, combined, and naval forces.

The vision in the *USCG's Cyber Strategy* states "We will ensure the security of our cyberspace, maintain superiority over our adversaries, and safeguard our Nation's critical maritime infrastructure." This document serves as the official doctrine for USCG cyberspace operations. It is nested with both JP 3-12 and National Security Strategy as evidenced by its recognition that cyber is an existential economic and national security challenge to the nation. The USCG defines three strategic priorities in its strategy:

defending cyberspace, enabling operations, and protecting infrastructure. In addition to these strategic priorities, the USCG cyber framework articulates numerous supporting factors to ensure long-term success in meeting its strategic goals in the cyber domain. These supporting factors are[42]:

- Recognition of cyberspace as an operational domain
- Developing cyber guidance and defining mission space
- Leveraging partnerships to build knowledge, resource capacity, and an understanding of Marine Transportation System (MTS) vulnerabilities
- Sharing of real-time information
- Organizing for success
- Building a well-trained cyber workforce
- Making thoughtful future cyber investments

The cyber framework laid out in the USCG's Cyber Strategy document coupled with its unique ability to conduct cyberspace operations in the legal (Title 50) and defense (Title 10) arenas align the service with the DOD and other government agencies.

The services sufficiently aligned their respective doctrine with the DOD to mitigate cyber threats targeting the nation and the U.S. armed forces. The synchronization at echelon of cyberspace guidance reduces the need for a separate cyber service in today's cyber contested environment.

Organization

The current organizational structure across the DOD, United States Army Reserve (USAR), National Guard Bureau (NGB), and United States Coast Guard

(USCG) appear to attain unity of effort on a global scale to defend the DODIN. Each service created a service component headquarters in support of and responsive to USCYBERCOM. These headquarters also serve as the central authority responsible for their respective portions of the DOD and conducting operations in and through cyberspace. Some organizations further enhanced cross-domain synergy by combining space, information operations, and SIGINT into one headquarters to attain information dominance. The USCG CPT is interoperable with DOD CMFs. Based on an analysis of joint and service cyberspace organizational construct there is not a requirement for a cyber service within the DOD.

The USCYBERCOM Combatant Commander is dual-hatted as the National Security Agency Commanding General. This command structure allows USCYBERCOM to utilize NSA’s network infrastructure and intelligence apparatus to conduct global cyberspace operations. Additionally, each service established a service component headquarters to support USCYBERCOM’s mission and centralize cyberspace authorities and operations within their respective branches (Fig. 1). In 2015, USCYBERCOM and the Defense Information Systems Agency (DISA) established Joint Forces Headquarters-DODIN (JFHQ-DODIN) as the DOD-lead for DODIN and DCO-Internal Defense Measures (DCO-IDM) operations. As the global synchronizer for these operations, JFHQ-DODIN has tactical control (TACON) of JFHQ-the service cyberspace components and directive authority (DA) over supporting defense agencies and field activities.[43]

In its effort meet DOD cyber requirement(s) and support multi-domain battle Headquarters Department of the Army (HQDA) established ARCYBER in 2010.

ARCYBER's mission is to attain information domination and freedom of action in and through cyberspace in support of Army operations while denying the same to the enemy. It has three subordinate units that operate in various information and cyberspace mediums – Network Enterprise Technology Command (NETCOM), 1st Information Operations (IO) Command, Cyber Protection Brigade, and 780th Military Intelligence (MI) Brigade.[44]

Additionally, Headquarters Department of the Army (HQDA) created a cyberspace branch to manage electronic warfare (29-series) and cyberspace (17-series) professionals. This branch's focus is offensive and defensive cyberspace operations. The Signal Corps governs the Army's communications professionals and maintains its traditional emphasis on global management of the Army's portion of the DODIN – the third component of cyberspace operations. The Army National Guard (ARNG) and USAR are cyber mission force partners.

MARFORCYBER, established in 2009, is the Marine Corps' service component to USCYBERCOM and the central authority directing and coordinating Marine cyberspace operations to the Corps. MARFORCYBER's operational control spans two organizations, the Marine Corps Network Operations and Security Center (MCNOSC) and Company L, Marine Cryptologic Support Battalion. Through these two organizations, MARFORCYBER conducts full-spectrum cyberspace operations to maintain freedom of action in cyberspace for the MAGTF, joint, and combined forces across all domains while denying the same capability to the adversary.[45] On 01 March 2018, the USMC released Marine Admin Message 136/18 announcing the establishment of a new occupational field, cyberspace 1700.[46]

In 2005, the USAF added cyberspace operations to its mission statement. The first service to fully recognize cyberspace as a domain and its importance to Air Force operations. Four years later the USAF designated its 24th Air Force (24 AF), under Air Force Space Command (AFSPC) "as the operational level organization responsible for conducting the full range of cyber missions for the U.S. Air Force and for providing forces to combatant commanders in support of military operations."[47] In 2010, the USAF designated 24th AF as the Air Force service component to USCYBERCOM, Air Force Cyber Command (AFCYBER). AFCYBER achieves operational synergy in the air, space, and cyber domains with three subordinate units conducting operations in and through cyberspace in support of Air Force operations: the 688th Cyberspace Wing (IO), 67th Cyberspace Wing (Cyberspace Operations), and 5th Combat Communications Group (Expeditionary Communications and air traffic control).[48] The Air National Guard (ANG) is a cyber mission force partner.

The United States Navy established U.S. Fleet Cyber (USFLTCYBER) in 2010, and U.S. Tenth Fleet is the numbered service in support of the mission (FCC-C10F). The 3-star Admiral is dual-hatted as the commander for both organizations. USFLTCYBER is the Navy's service component to USCYBERCOM and provides centralized operational authority over Navy networks, cryptologic and signals intelligence, IO, cyber, EW, and space capabilities for naval forces. U.S. Tenth Fleet provides the operational command structure for the personnel assigned to USFLTCYBER and directs operations in and through cyberspace, space, and the electromagnetic spectrum for naval commanders worldwide.[49] FCC-C10F focuses on three mission areas to accomplish its mission:

- Operate the Network as a Warfighting platform
- Conduct Tailored Signals Intelligence
- Deliver warfighting effects through cyberspace

The United States Coast Guard (USCG) established Coast Guard Cyber Command (CGCYBERCOM) in 2011. The headquarters' vision is "to establish and maintain a secure and resilient cyber operating environment for Coast Guard and marine operations." As the service's cyber component, CGCYBERCOM provides cyberspace capabilities in support of DHS cyber missions and Coast Guard operations. It conducts cyberspace operations across a range of operations that include Title 10 (DOD), Title 50 (Intelligence Community) and Title 33/14 (Law Enforcement) authorities focused on protecting USCG networks and the nation's maritime transportation system (MTS).[50]

Additional components of the USCG's cyber platform are the Assistant Commandant for Command, Control, Communications, Computers, and Information Technology (C4IT/CG-6) and the Office of Cyberspace Forces (CG-791). As defined in its FY15-19 Strategic Plan the CG-6 identifies five goals; the first goal is cyberspace operations.[51] CG-6 "enhances mission effectiveness by preventing C4, Intelligence, Surveillance, Reconnaissance, and IT (C4ISR&IT) security incidents, such as cyber-attacks and intrusions and enhancing C4ISR&IT security mitigation and recovery."[52]

The CG-791 works to obtain cyberspace capabilities, competencies, and capacity to meet operational requirements. Three subordinate directorates that support CG-791 are Cyberspace Planning and Resources, Cyberspace Operations Policy, and Cyberspace Strategy.[53] Additionally, the USCG stood up a CPT in February 2017 with a planned FOC of 2019. The team is interoperable with both DOD CMFs and Department of Homeland Security (DHS) cybersecurity operation teams. The USCG CPT's primary roles are to protect US maritime critical infrastructure and support DHS incident response for .gov and .com (as requested by industry) incidents.[54]

Each service received the DOD's directive to create cyber mission forces and executed expeditiously. The services' adherence to the DOD strategic guidance and USCYBERCOM's role as the coordinating authority for global cyberspace operations establish unity of effort. The current organizational model for cyberspace operations adequately lessens the need for a cyber service based on the current threat environment.

Training

DOD's training plan and oversight of CMF team training ensure a baseline standard across the force. Additionally, DOD Information Assurance certification requirements, joint exercises, and service-specific training that increases training of CMF and other cyber workforce professionals increases overall readiness. DOD's standardization of total CMF training and the ability for cyber workforce personnel to attend other service schools promotes the unity of effort and collaboration among all CMF and cyber workforce personnel. A separate cyber service is not presently required to ensure coordinated and standardized cyberspace training.

Training focuses on how the DOD prepares to fight tactically – starting with basic training through joint and combined exercises. An analysis of the cyber workforce begins with advanced individual training for some services (USAF, USN, USA) and unit or joint training for others (USCG and USMC).

After standing up USCYBERCOM in 2010 and establishing the service requirements for CMF teams, DOD with USCYBERCOM developed the training plan for the force. Usually, organizing, training, educating and equipping troops is a Title 10 responsibility of the services.[55] However, cyberspace's dynamic operating environment and the myriad threats facing the nation and the DOD required a joint training plan to establish a baseline across the force effectively. One of the strategic goals in the 2015 DOD Cyber Defense Strategy is building and maintaining "ready forces and capabilities to conduct cyberspace operations." The three foundational principles required to accomplish this goal are enhanced training and stronger private sector support.[56] Some of the key critical enablers for the success of the strategy are[57]:

- A persistent training environment.
- Viable career paths for CMF team members.
- Develop and implement exchange programs with private industry.
- Establish an enterprise-wide cyber modeling and simulation capability.

The Cyber Forces Concept of Operations and Employment Training and Readiness manual identifies the training required for all CMF team personnel and positions (active component, reserve component, and civilian). This document enables DOD oversight of a robust sustainment program and ensures future proficiency and CMF capacity to allow continuous cyberspace operations.[58] Although DOD and USCYBERCOM provided a detailed plan in the Cyber Strategy, the services were expected to develop and implement long-term plans to train their respective CMF teams and cyber workforces.[59]

The Army's training begins with advanced individual training or the warrant and basic officer leadership course for EW, Cryptologic Warfare specialists, and Signal personnel (specifically 25Bs, 25Es, 25As, and 255-series)[60]. However, the Signal Corps' computer network defense operators (25D), information protection technicians (Warrant 255S), information systems engineer (26B) and Cyber's Career Management Field-17 (CMF-17) are assessed similarly to Special Forces recruitment. An experienced noncommissioned officer (NCO), officer, or warrant officer volunteers to transition into these career management fields. Upon successful completion of the required training, the individual is awarded the career management field.

The Army also established the Cyber Center of Excellence (CCoE) at Fort Gordon, Georgia. The CCoE houses the Signal and Cyber schools for the Army; the commandants of each school are "responsible for training execution, leader development, education, and personnel proponent responsibilities for each branch."[61] Two final initiatives are a modification of cyber and signal course requirements to meet USCYBERCOM standards and ARCYBER's decision to leverage COCOM and NETCOM exercises as training opportunities for its CMF teams and align collective training tasks with joint standards.[62]

Similar to the Army, the Marine Corps does not assess entry-level personnel into its CMF teams. The Marine Corps pulls personnel from other qualified feeder specialties to fill the ranks of its cyber forces. The Marine Corps uses joint, other DOD, Marine, and other service schools to train its cyberspace workforce. The Marine Corps developed two cyber programs for Marine cybersecurity personnel, the Information Assurance Scholarship Program (IASP) and Northern Virginia Community College Advanced

Standing Initiative (NVCC ASI). IASP is the primary program used to train the cybersecurity workforce with more than 600 graduates placed in cybersecurity and IA positions across the DOD. The NVCC ASI allows the Marine Corps to transfer 22 military education courses into college credits towards an Associate's degree in cybersecurity.[63]

Since 2009, the Air Force has developed comprehensive training, recruitment, retention, management, and training programs for its cyber workforce. The Air Force focuses on educating its workforce, as well as, assisting the other services.

Some of the programs developed and implemented by the Air Force to train its cyber workforce are: 1) An Advanced Cyber Education Program for ROTC cadets majoring in (computer science, computer engineering, or electrical engineering) from all services hosted by the Air Force Institute of Technology's Center for Cyberspace Research during the summer; 2) An intelligence cyber analyst course for digital network analysts and training programs to develop the cyber workforce professionals with an emphasis on undergraduate cyberspace training, DCO, and intermediate network warfare training; and 3) Allowing certain cyber workforce specialties to serve consecutive cyberspace tours at different locations to develop experience as part of their career progression.[64]

The Navy's progression towards full integration of its cyber workforce resulted in programs like the Cyber Warfare Engineer (CWE). The program's recruitment focus is enlisted and civilian personnel with cyber-related degrees for commissioning. The service requirement is five years at which time the CWE can transition into the Navy

Information Warfare or Information Professional communities or leave the Navy and enter the DOD civilian workforce.

The primary enlisted occupational specialties in the Navy's cyber workforce are Cryptologic Technician Networks (CTN) and Information Systems Technicians (IT). The primary feeder course for CTNs is the Joint Cyber Analysis Course (JCAC), and for ITs, it is the 19-week Network and Telecommunications Architecture and Information Assurance course. Additionally, all ITs are required to attain DOD Information Assurance certifications, and a subset must attend an 18-week System Administrator course. The Naval Postgraduate School's (NPS) Master of Science in Applied Cyber Operations is also available to CTNs, ITs, and other services' cyber personnel. Navy graduates of the course receive a specialty code and follow-on assignment to Navy CMF teams.

In 2017, the Coast Guard began developing a Cyberspace Workforce Human Capital plan to "prioritize and implement a cyberspace workforce transformation that aligns with DOD standards and the USCG Cyber and Human Capital strategies." The CG-791 office provides programmatic oversight, training, equipping, and operational policy for the cyberspace workforce.[65]

The Coast Guard's Cyber Strategy identifies requirements to ensure long-term success as it develops and trains its cyber workforce. The Coast Guard focuses on ensuring its entire force has cybersecurity training to operate in the cyberspace domain. Additionally, the strategy emphasizes recruitment, education, training, and retaining technically competent cyberspace professionals. The Coast Guard, just like the other services, looks to partner with DHS, DOD, and academia to ensure training and education that remains ahead of technological developments.[66]

USCYBERCOM promulgated the training standards for CMFs, and each service established training plans for their respective non-cyber workforces based on USCYBERCOM and DOD training plans. The current training model reduces the need for a cyber service today.

Materiel

An analysis of materiel at the DOD-level validates the current DOD cyberspace construct. The DOD's cyberspace strategy and CMF organization ensure oversight of cyberspace materiel development and procurement. In this case, the services primary requirement is to fund the acquisition of the required tools for their respective CMF teams and cyber workforces. The only points of contention lie with the USCG and the National Guard CMF elements. A separate cyber service could facilitate materiel resourcing across the DOD.

Materiel analysis of a cyber service requirement examines all of the resources needed to equip CMF teams and cyber workforce personnel absent a new development effort.[67] The tools used by the CMF to conduct cyberspace operations are a mixture of DOD-developed and commercial-off-the-shelf (COTS) equipment and technology. The research and development conducted by the military in coordination with the private sector significantly enhance DOD cyberspace capabilities. However, some of this technology exists in the commercial sphere and is available to anyone with a computer, financial resources, and the desire.[68]

As the global cyberspace proponent and authority, USCYBERCOM provides direction and oversight of hardware and software R&D and procurement. In testimony to the Senate Armed Services Committee, Admiral Rogers acknowledged the need to reassess authorities and delegations and if the CMF has the right mix of manpower and capabilities. Rogers also advocated for more structured coordination with private industry to protect U.S. critical infrastructure against attack.[69] USCYBERCOM's role as the global proponent and authority for cyberspace operations is similar to USSOCOM's role for special forces operations.[70]

The cyber domain, DOD's Cyber Strategy, and the CMF concept reduces the various requirements for the services to develop service-specific tools for cyberspace operations. Unlike the other physical domains, the services are not competing for resources to execute their respective mission sets. At the joint and service-level each organization has CMF teams that are responsible for executing DOD's cyber missions: "defend the DODIN and information; defend the homeland and national interests, and support operational and contingency operations."[71]

Two key objectives of the DOD strategy that enhance oversight of cyberspace materiel procurement for CMF teams and infrastructure are the development of the Unified Platform and acceleration of research and development at the DOD-level. The Unified Platform is an initiative to develop the detailed requirements to integrate disparate cyber platforms and build an interoperable and extendable network of cyber capabilities. This enables full-spectrum cyberspace operations in support of national requirements by the CMF. The second objective, accelerated R&D, seeks partnerships with the private sector to provide cutting-edge technologies to defend U.S. cyberspace interests and expand the capacity of CMF and the cyber workforce.[72]

Another critical aspect of ensuring cyberspace materiel procurement is coordinated and streamlined is DOD's move from the DODIN to the Joint Information Environment (JIE). JIE implementation ensures DOD asset owners and DIB partners meet the cybersecurity standards necessary to protect DOD networks.[73] JFHQ-DODIN's Joint Regional Security Stack (JRSS) initiative is part of the JIE implementation.

The main points of contention exist within the USCG and the National Guard CMF elements. These organizations must protect their portions of the DODIN, but they effectively belong to DHS (USCG) or the individual states (ARNG/ANG). DHS provides the USCG's budget, and the ARNG/ANG have three distinct funding streams; this could affect the ability of these organizations to procure cyberspace materiel validated, authorized, and required by USCYBERCOM.[74]

The materiel analysis of DOD and service-level cyberspace efforts identifies areas of risk especially with the NGB and USCG CMF forces. A separate cyber service responsible for all DOD CMFs could facilitate materiel resourcing and funding to maintain materiel alignment across all CMFs.

Leadership and Education

Leadership and education for cyberspace is a holistic approach that leverages DOD, USCYBERCOM, the services, other government agencies (OGAs), industry, and academia to prepare senior leaders, CMF teams, the cyber workforce, and the force at large for cyberspace operations. An education system that is 80% DOD/joint versus 20% service-specific ensures commonality across the force. The DOD and USCYBERCOM define the educational and certification standards for the CMF and cyber workforce. These programs influence PME and continuing education. The DOD's current organizational model appears to refute the need for a separate cyber service.

In cyberspace, the educational requirement is evolving with the domain. CMF, DOD cyber workforce personnel, and operational commanders require a mixture of formal military and civilian educational opportunities to remain relevant and knowledgeable. An education versed in the art and science of cyberspace operations is critical to defending national and DOD interests in cyberspace.

DOD and USCYBERCOM established the initial and ongoing educational requirements for the CMF and the DOD cyber workforce at large. DODD 8570 certifications and courses like Joint Advanced Cyber Warfare, Joint Cyber Analysis, Joint Network Attack, and Ethical Hacking are a few of the educational initiatives established by USCBYERCOM and the DOD. Additionally, Cyber Beacon, an annual conference hosted by NDU's College of Information and Cyberspace, brings together senior decision-makers from DOD, OGAs, the private sector, and academia to assess national security in cyberspace; a vital component of this assessment is the cyberspace education requirements. In 2014, attendees provided an estimate that 80% of DOD's cyber education and training is standard across the force and the remaining 20% is service-specific.[75] The DOD created the DOD Cyber Awareness Challenge computer-based course to educate non-cyber personnel. This is an annual requirement for all DOD personnel with network access to the DODIN.

DOD also established some cyber fellowships for Senior Service College selectees and mid-grade leaders as broadening opportunities. NDU and academic institutions, such as NDU and Carnegie Mellon, administers these fellowships for the DOD.

The Army's establishment of a Cyber Branch and cyber school created a formal professional military education (PME) pipeline for 17-series cyber professionals. A component of the CCoE, one of the Cyber school's vital missions is to provide cyber-related training and education for all Soldiers and civilians, not just cyber professionals.

The Marine Corps does not have a separate cyber branch for its cyber professionals or the cyber workforce. PME for Marine CMF personnel is the USCYBERCOM program and MOS-producing schools. Its cyber workforce education also occurs through the MOS-training for its communicators and SIGINT personnel.

The Navy introduced its CWE program as one way to educate its cyber workforce. After completing the CWE program, course graduates receive commissions as Navy officers with a 5-year commitment. The Navy is also developing plans to train its civilian cyber workforce and create positions to maintain longevity and continuity. The other PME programs for its cyber workforce are the CTN and IT specialties. There are also continuing education opportunities for CMF and cyber workforce Sailors and civilians at the Naval Postgraduate School.[76]

The Air Force was the first service to create a cyber specialty and develop PME for its cyber workforce. The 33-series cyber specialty combines the intelligence and communications communities. The Air Force also promotes cyberspace training and education for its JROTC and ROTC programs nationwide; the Advanced Cyber Education summer program for ROTC cadets from all the services is another educational opportunity aimed at future officers. PME and continuing education in cyberspace abound for uniformed and civilian cyber workforce professionals. Other examples are Undergraduate Cyberspace Training, Intermediate Network Warfare, and graduate-level courses offered at the Air Force Institute of Technology.[77]

Currently, the USCG leverages the DHS, the other services, and joint cyberspace education courses to educate its cyber workforce in conjunction with the PME for its feeder specialties. The Coast Guard's Cyber Strategy identifies cyberspace education and training as critical for its entire workforce, not just cyberspace operators. The strategy focuses on developing cyberspace awareness programs for all uniformed and civilian personnel in addition to a career path for cyberspace operators that emphasizes cybersecurity, cyber intelligence, cyber law enforcement missions, cyber support to critical infrastructure, and cyber effects operations. There are also plans to incorporate cybersecurity into the curricula at the USCG Academy, merchant marine academies, and other training programs.[78]

The decision to define the educational and certification standards for CMFs and cyber workforces at the DOD and USCYBERCOM-level created synergy for the services. The DOD's foresight in this area lessens the need for a separate cyber service at this time.

Personnel

The analysis of the personnel challenges faced at the joint and service-level suggests a separate cyber service is more beneficial to the DOD. While two services attained FOC ahead of schedule, the USAF and USMC are not there yet. Additionally, the USCG just established its one team in February 2017. The manning challenges faced by each service centers on how the uniformed CMF personnel are managed and assigned by their respective services. CMF personnel are required to perform non-cyber jobs for career progression, especially in the Army and Marine Corps. Based on these challenges, it is foreseeable in the future that the CMF teams are not as experienced and trained as their predecessors based on the transition in and out of cyber and non-cyber assignments. A separate cyber service provides the capability to manage the careers and assignments of CMF teams that are essential to national security.

The personnel analysis examined “the availability of qualified personnel during peacetime, wartime, and contingency operations.”[79] Personnel are an essential aspect of operations in any domain, but especially cyberspace. A man-made domain, cyberspace requires personnel to enable freedom of action through cyberspace and to deny the same to the adversary. USCYBERCOM and the services are working to achieve CMF FOC by FY2018.

USCYBERCOM’s mandate is 6200 personnel across 133 teams for CMF FOC NLT 30 September 2018. The command currently has 5000 personnel or 80% of its manning requirement for the teams. Minus its civilian manning, the military services provide USCYBERCOM headquarters and CMF military personnel for the command.[80] Due to emerging and increasing cyberspace threats to the DOD and the nation, stand up of some CMF teams resulted in the commitment of some squads to the fight before achieving full mission readiness.[81]

> The reality is, because of the dynamics of cyber, we have needed to apply capacity as soon as we’re generating it,” Rogers said. “And so we find ourselves in a situation – a little unusual in the military arena – wherein as soon as we get a basic framework, we have been deploying the teams and putting them against challenges.[82]

A CMF team must complete USCYBERCOM validation to attain its FOC determination.[83]

The Chief of Staff of the Army (CSA) directed the force to achieve 100% manning of its mandated 41 CMF teams (1519 personnel) as required by DOD. Army active-CMF teams achieved FOC at the end of September 2017.[84] The USAR and ARNG are establishing an additional 21 CPTs.[85]

The DOD tasked the USMC to establish 13 CMF teams with a directed FOC of 2018. MARFORCYBER currently has 1000 Marine and civilian personnel assigned from occupational specialties in SIGINT, data, networks, or cyber protection. The USMC does not now have a separate cyber MOS. The uniformed personnel on these teams rotate between MARFORCYBER and other USMC assignments in their respective specialties.[86]

The U.S. Navy's CMF requirement is 40 teams, and on 03 November 2017 USCYBERCOM assessed those teams as FOC.[87] FCC/C10F is the central authority responsible for CMF teams, and the other functions critical to Navy Information Operations facilitates management and assignment of cyberspace workforce personnel and CMF teams.

The USAF's obligation to the DOD CMF effort is 39 teams – this includes the ANG and Reserve teams.[88] These teams consist of personnel drawn from the 24th and 25th Air Force. "The AF is leveraging personnel within its force to fill out CMF teams, which will continue to grow over the next 12-14 months. There are programs in place to cross-flow Airmen into the Cyber Operator career field."[89] USAFCYBER commanding general, Major General Christopher Weggeman anticipates FOC of USAF CMF teams by 30 June 2018.[90]

The DOD did not task the USCG to establish CMF teams, but the USCG created a team to support DHS and defend its portion of the DODIN. In addition to this CPT, the Coast Guard's communications and intelligence personnel are involved in operating, protecting, and defending Coast Guard networks. Together, civilian and uniformed personnel in the USCG's CPT, communications, and intelligence communities ensure freedom of action through cyberspace for the USCG, provide cyber support to DHS, and protect critical maritime infrastructure for the U.S. Developing the cyber workforce is an objective in the USCG's cyber strategy.[91]

Personnel challenges present the principal justification for the nation to establish a separate cyber service with the DOD. Each service has potential issues manning their respective cyber mission forces. A separate cyber service could provide better talent management of personnel critical to DOD cyberspace operations.

Facilities

Facilities analysis identifies potential seams as it pertains to the DODIN. The Coast Guard, Navy, and Marine Corps are not participating in the JRSS construct at this time. This bifurcation results in a portion of the network that is protected by a single entity (JFHQ-DODIN) and a part that is protected by three separate services. An adversary can take advantage of this seam in the DODIN to access or deny the DOD freedom of action in cyberspace. The current network organization does not impede a separate cyber service responsible for the DODIN. Additionally, a cyber service does not require extensive coordination of security protocols across the DODIN to conduct cyberspace operations.

A facilities consideration of DOD cyberspace operations focuses on real property, facilities, and networks (DODIN). Networks are not physical locations like buildings, but in the cyber domain, one must consider network infrastructure. Probably more so than the actual physical locations.[92]

Cyberspace operations lend themselves to remote procedures. All a cyber operator typically requires to access or deny entry to the cyber domain is a computer and a network. Hardstand facilities are not a prerequisite to enable freedom of action through cyberspace. Cyber operators can access the cyber domain from strategic, tactical, or mobile networks. The ability to conduct cyberspace operations from remote locations to enable freedom of action through cyberspace makes this a truly global domain with persistent accessibility. Thus, the separate physical headquarters maintained by USCYBERCOM (collocated with NSA), JFHQ-DODIN, the service component headquarters, service Network Operations and Security Centers, and service Regional Cyber Centers are not impediments to collaborative cyberspace operations. However, the distinct networks operated and maintained at the joint and service level requires close coordination to ensure security protocols are in place to allow seamless cyberspace operations across the DODIN. Additionally, the multiple network entry points into the DODIN (joint and service) require persistent surveillance to detect, mitigate, and defend against cyber intrusions and cyber-attacks. USCYBERCOM is addressing this issue through flattening of the DODIN with the implementation of JRSS's that are maintained and operated by JFHQ-DODIN. Deployment of the JRSS centralizes security of the DODIN into regional architectures vice separate service data centers at individual service posts and bases. Currently, the only services participating in the JRSS construct are the Army and the Air Force.[93]

The DOD is working to reduce seams in the DODIN that abet threat access to the network. A separate cyber service with responsibility for the DODIN could reduce the need for extensive coordination across COCOMs and services and accelerate response time to a cyber-attack.

Conclusion

The cyberspace threat is an adversary with global reach and the ability to challenge U.S. national interests, threaten critical infrastructure, and contest the employment and deployment of DOD forces from home station to the area of operations. The interdependence between the physical domains of war and cyberspace demand that the DOD assess its progress and integration of cyberspace operations. There are advocates at the senior leader levels for creating a separate cyber service. One such advocate is ADM Stavridis, USN (Ret) – In his 2015 testimony before the Senate Armed Services Committee, ADM Stavridis told the committee it was time to consider a separate service for the cyber domain based on the nature of the threat.[94] Another advocate for a separate cyber service is Congressman Royce (R-CA), House Foreign Affairs Committee Chairman. In a September 2015 hearing, Congressman Royce suggested the creation of the Air Force post-WWII is the raison d'etre for a separate cyber service. However, a DOTMLPF analysis does not support a cyber service at this time. This review does not mean that the current model is without challenges.[95]

For example, career management of CMF personnel (Personnel) may eventually result in sustainment problems from an educational and training standpoint. The current service model focuses on leadership and technical competence, especially at the senior leader levels. As cyber troops get promoted, they become less an operator and more a supervisor. Cyberspace training is costly, and an operator must do the job to remain proficient. The services must figure out how to manage the careers of this emerging force to ensure readiness.

Another challenge exists in the facilities arena (Facilities) as it pertains to providing a persistent network for live environment cyber training. The DODIN is an operational network and is not conducive to cyberspace operations training. There are considerable risks to conducting operations, particularly offensive cyber operations and defensive cyber operations-response actions on this strategic and operational network.

A final challenge is the inclusion of the NGB and USCG (Materiel) into the overall DOD Cyber Strategy. DOD must ensure the funding is available to support materiel resourcing for these organizations. Cyberspace operations cannot be an afterthought if the NGB and USCG are to be capable partners in the cyberspace fight.

However, these are not insurmountable challenges for the DOD. As with any strategy, plan, or operation, the DOD must periodically reassess its approach to determine what is working and what must be fixed or discarded. As long as the DOD, USCYBERCOM, and the services continue to assess and adapt the cyber strategy, a separate cyber service does not serve the nation's security interests or provide added-value to DOD cyberspace operations.

Endnotes

[1] James Stavridis and David Weinstein, "Time for a U.S. Cyber Force," *Proceedings Magazine*, January 2014, https://www.usni.org/magazines/proceedings/2014-01/time-us-cyber-force (accessed November 21, 2017).

[2] U.S. Congress, *National Defense Authorization Act for Fiscal Year 2017*, 114th Cong., 2nd sess. (January 04, 2016), 358, https://www.gpo.gov/fdsys/pkg/BILLS-114s2943enr/pdf/BILLS-114s2943enr.pdf (accessed January 24, 2018).

[3] The UCP, signed by the President of the United States, establishes missions and areas of responsibility for all COCOMs. The existing UCP (2011) does not list USCYBERCOM as a functional combatant command. See U.S. Department of Defense, "Unified Command Plan," map depicting the current geographic and functional Combatant Commands' areas of responsibility, http://archive.defense.gov/ucc/ (accessed January 24, 2018).

[4] Donald Trump, "Statement by President Donald J. Trump on the Elevation of Cyber Command," August 18, 2017, https://www.whitehouse.gov/briefings-statements/statement-president-donald-j-trump-elevation-cyber-command/ (accessed January 24, 2018).

[5] U.S. Congress, *National Defense Authorization Act for Fiscal Year 2017*, 358.

[6] Daniella Diaz, "CIA Director Stands By Intel Community Assessment Russia Meddled In Election," *CNN: Politics*, November 11, 2017, http://www.cnn.com/2017/11/11/politics/mike-pompeo-cia-donald-trump-white-house-russia-meddling/index.html, (accessed November 22, 2017); Dominic Rushe and agencies, "OPM hack: China blamed for massive breach of US government data," *The Guardian*: US ed., June 05, 2015, https://www.theguardian.com/technology/2015/jun/04/us-government-massive-data-breach-employee-records-security-clearances, (accessed November 22, 2017); "Sony cyber-attack: North Korea faces new US sanctions," *BBC*, January 03, 2015, http://www.bbc.com/news/world-us-canada-30661973, (accessed November 22, 2017); Eric Chabrow, "7 Iranians Indicted for DDoS Attacks Against U.S. Banks," *BankInfo Security*, May 24, 2016, https://www.bankinfosecurity.com/7-iranians-indicted-for-ddos-attacks-against-us-banks-a-8989 (accessed November 22, 2017); JP 3-12 (II-5) defines a cyberspace attack as: "Cyberspace actions that create various direct denial effects in cyberspace (i.e., degradation, disruption, or destruction) and manipulation that leads to denial that is hidden or that manifests in the physical domains." The actions include deny, degrade, disrupt, destroy, and manipulate. However, for this monograph, cyber attack includes data exfiltration and cyber espionage activities as well.

[7] U.S. Department of Defense, *2015 DOD Cyber Strategy* (Washington, D.C: U.S. Department of Defense, April 2015), 2, https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf (accessed March 03, 2018).

[8] Symantec, *Internet Security Threat Report,* April 2017, 50, https://digitalhubshare.symantec.com/content/dam/ent/collat/reports/RPT_ISTR-Main-Report_EN.pdf?aid=elq_&elqTrackId=a4536141fdba4e639c7e80d98f3e522f&elqaid=3783&elqat=2 (accessed January 24, 2018); U.S. Federal Bureau of Investigation, *2016 Internet Crime Report*, https://www.fbi.gov/news/stories/ic3-releases-2016-internet-crime-report (accessed January 24, 2018).

[9] ADM Stavridis believes DOD needs a cyber service for the cyber domain, see James Stavridis and David Weinstein, "Time for a U.S. Cyber Force;" ADM Rogers stated DOD does not need a cyber service for cyberspace operations. See Mark Pomerleau, "Rogers: Cyber Doesn't Need Its Own Military Branch," *Cyber Defense*, January 21, 2016, https://defensesystems.com/articles/2016/01/21/rogers-cyber-doesnt-need-to-be-separate-branch.aspx (accessed January 24, 2018).

[10] U.S. Congress, House, Homeland Security Committee, Subcommittee on Cybersecurity and Infrastructure Subcommittee, *Emerging Cyber Threats to the United States,* 114th Cong., 2nd sess., February 25, 2016, https://homeland.house.gov/hearing/emerging-cyber-threats-to-the-united-states/ (accessed November 23, 2017).

[11] Daniel R. Coats, Director of National Intelligence, *Statement for the Record: Worldwide Threat Assessment of the U.S. Intelligence Community*, Senate Select Committee on Intelligence, 115th Cong., 1st sess., May 11, 2017, 1, https://www.dni.gov/index.php/newsroom/congressional-testimonies/item/1757-statement-for-

the-record-worldwide-threat-assessment-of-the-u-s-intelligence-community-before-the-ssci (accessed February 11, 2018).

[12] Donald Trump, *National Security Strategy of the United States of America* (Washington, DC: The White House, December 18, 2017), 21, https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf (accessed February 10, 2018).

[13] Coats, *Statement for the Record: Worldwide Threat Assessment,* 1.

[14] Ibid.

[15] Trump, *National Security Strategy of the United States of America*, 26.

[16] Eleanor Beardsley, "France Warns Russia To Stay Out Of Its Presidential Election," *NPR*, February 21, 2017, https://www.npr.org/2017/02/21/516375420/france-warns-russia-to-stay-out-of-its-presidential-election (accessed February 10, 2018).

[17] Coats, *Statement for the Record: Worldwide Threat Assessment,* 1.

[18] Ibid.

[19] Eric Chabrow, "7 Iranians Indicted for DDoS Attacks Against U.S. Banks,' March 24, 2016, *ISMG Network*, BankInfoSecurity, https://www.bankinfosecurity.com/7-iranians-indicted-for-ddos-attacks-against-us-banks-a-8989 (accessed November 22, 2017).

[20] Coats, *Statement for the Record: Worldwide Threat Assessment,* 1-2.

[21] David E. Sanger, David D. Kirkpatrick, and Nicole Perlroth, "The World Once Laughed at North Korean Cyber Power. No More," October 15, 2017, *The New York Times*, https://www.nytimes.com/2017/10/15/world/asia/north-korea-hacking-cyber-sony.html?emc=edit_ta_20171015&nl=top-stories&nlid=55770758&ref=headline&_r=1 (accessed November 26, 2017).

[22] Coats, *Statement for the Record: Worldwide Threat Assessment,* 2.

[23] Ibid.

[24] Ibid.

[25] Conner Forrest, "Phishing is the easiest way to steal sensitive data, hackers say," *TechRepublic.com*, September 19, 2017, https://www.techrepublic.com/article/phishing-is-the-easiest-way-to-steal-sensitive-data-hackers-say/ (accessed February 10, 2018).

[26] Elise Hu, "North Korea Responsible For 'WannaCry' Ransomware Attack, U.S. Says," *NPR*, December 19, 2017, https://www.npr.org/2017/12/19/571868305/north-korea-responsible-for-wannacry-ransomware-attack-u-s-says (accessed March 03, 2018).

[27] Gordon M. Snow, Assistant Director, Cyber Division, FBI, *Statement Before the Senate Judiciary Committee, Subcommittee on Crime and Terrorism,* April 12, 2011, https://archives.fbi.gov/archives/news/testimony/cybersecurity-responding-to-the-threat-of-cyber-crime-and-terrorism (accessed November 26, 2017).

[28] U.S. Strategic Command, “U.S. Cyber Command (USCYBERCOM),” http://www.stratcom.mil/Media/Factsheets/Factsheet-View/Article/960492/us-cyber-command-uscybercom/ (accessed November 26, 2017).

[29] Ibid.

[30] U.S. Department of Defense, “All Cyber Mission Force Teams Achieve Initial Operating Capability,” October 24, 2016, https://www.defense.gov/News/Article/Article/984663/all-cyber-mission-force-teams-achieve-initial-operating-capability/ (accessed November 26, 2017).

[31] Ibid.

[32] Ibid.

[33] “Cyber Mission Teams are also assigned to both the Cyber National Mission Force and Joint Force Headquarters DoD Information Networks, CYBERCOM component headquarters.

The Cyber National Mission Force plans, directs, and synchronizes full-spectrum cyberspace operations to deter, disrupt, and if necessary, defeat adversary cyber actors to defend the nation. Its “defend the nation” missions include:

-- When directed by the president or secretary of defense, defending the U.S. and its interests against cyberattacks of significant consequence and defense of the nation’s critical infrastructure when significant consequences may include loss of life, significant damage to property, serious adverse U.S. foreign policy consequences or serious economic impact on the United States.

-- Alignment to the most sophisticated cyber adversaries: nation-state cyber adversaries and non-nation-state or emerging threats.

Joint Force Headquarters DoD Information Networks provides command and control of DoD Information Network operations and defensive cyber operations internal defensive measures globally to coordinate the protection of DoD component capabilities enabling power projection and freedom of action across all warfighting domains. Its cyber protection teams actively work to harden DoD network boundary defenses.”

[34] U.S. Joint Chiefs of Staff, *Cyberspace Operations*, Joint Publication 3-12 (Washington, DC: U.S. Joint Chiefs of Staff, February 05, 2013), v, https://fas.org/irp/doddir/dod/jp3_12r.pdf (accessed February 11, 2018).

[35] U.S. Department of the Army, *Army Cyberspace and Electronic Warfare Operations*, Field Manual 3-12 (Washington, D.C: U.S. Department of the Army, April 11, 2017), Foreword, https://armypubs.army.mil/ProductMaps/PubForm/FM.aspx (accessed February 11, 2018).

[36] U.S. Marine Corps, *Marine Corps Cyberspace Operations,* Marine Corps Interim Publication 3-32Ei (Quantico, VA: U.S. Marine Corps, May 02, 2016), Foreword, https://www.doctrine.usmc.mil/.

[37] U.S. Air Force, *Cyberspace Operations*, Annex 3-12, (Washington, DC: U.S. Air Force, November 30, 2011), 1, http://www.doctrine.af.mil/Doctrine-Annexes/Annex-3-12-Cyberspace-Ops/ (accessed February 11, 2018).

[38] U.S. Department of the Navy, *Navy Information Operations*, Navy Warfare Publication 3-13 (Norfolk, VA: Navy Warfare Development Command, February 2014), 3-1, https://ndls.nwdc.navy.mil/.

[39] Ibid, 4-3.

[40] Ibid, 3-4.

[41] Kendall L. Card and Michael S. Rogers, *Navy Cyber Power 2020,* November 2012, i, http://www.public.navy.mil/fcc-c10f/Strategies/Navy_Cyber_Power_2020.pdf (accessed February 11, 2018).

[42] U.S. Coast Guard, *United States Coast Guard Cyber Strategy* (Washington, DC: U.S. Coast Guard, June 2015), 12, http://www.overview.uscg.mil/Portals/6/Documents/PDF/CG_Cyber_Strategy.pdf (accessed February 11, 2018).

[43] Patrick Daniel, *JFHQ-DODIN Update,* AFCEA Symposium, April 21, 2016, 4-6, https://disa.mil/~/media/Files/DISA/News/Conference/2016/AFCEA-Symposium/1-LtColDaniel_JFHQ-DODIN.pdf (accessed February 11, 2018).

[44] U.S. Army Cyber Command, "About Army Cyber," http://www.arcyber.army.mil/Organization/About-Army-Cyber (accessed March 03, 2018).

[45] U.S. Marine Corps, *Marine Corps Cyberspace Operations,* 2-1-2-2.

[46] U.S. Marine Corps, *Establishment Of The Cyberspace 1700 Occupational Field (OCCFLD)*, MARADMINS Number 136/18, March 01, 2018, http://www.marines.mil/News/Messages/Messages-Display/Article/1454562/establishment-of-the-cyberspace-1700-occupational-field-occfld/ (accessed March 02, 2018).

[47] Air Forces Cyber, "24th Air Force – AFCYBER," http://www.afcyber.af.mil/About-Us/Fact-Sheets/Display/Article/458567/24th-air-force-afcyber/ (accessed March 03, 2018).

[48] Ibid.

[49] U.S. Fleet Cyber Command, "U.S. Tenth Fleet," http://www.public.navy.mil/fcc-c10f/Pages/usfleetcybermission.aspx (accessed December 22, 2017).

[50] U.S. Coast Guard Cyber Command, "Driving Mission Execution, August 2011, 2-3," http://aapa.files.cms-plus.com/SeminarPresentations/2011Seminars/11OpsSafetyIT/Felker_John.pdf (accessed February 11, 2018).

[51] U.S. Coast Guard, *FY15-19 Command, Control, Communications, Computers, Intelligence, Surveillance, Reconnaissance and Information Technology (C4ISR&IT) Strategic Plan Fiscal Years 2015-2019,* 7, http://www.dcms.uscg.mil/Portals/10/CG-6/FY15-19_C4ISRandIT_Strategic_Plan.pdf?ver=2016-12-05-161842-567 (accessed March 03, 2018).

[52] U.S. Coast Guard, "Assistant Commandant for C4&IT," http://www.dcms.uscg.mil/Our-Organization/Assistant-Commandant-for-C4IT-CG-6/ (accessed December 22, 2017);

http://www.dco.uscg.mil/Our-Organization/Assistant-Commandant-for-Capability-CG-7/CG-791/ (accessed December 22, 2017).

[53] Ibid.

[54] “Telfair Brown, “The Coast Guard’s Cyber Operating Forces,” August 23, 2017, *DVIDS*, video file, https://www.dvidshub.net/video/545307/coast-guards-cyber-operating-forces (accessed December 22, 2017).

[55] Title 10, United States Code, Armed Forces, Vol. III, 112th Cong., 1st sess. (January 07, 2011), iii, https://www.gpo.gov/fdsys/pkg/CPRT-112HPRT67344/pdf/CPRT-112HPRT67344.pdf (accessed January 24, 2018).

[56] U.S. Department of Defense, *2015 DOD Cyber Strategy* (Washington, DC: U.S. Department of Defense, April 2015), 17, https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf (accessed February 11, 2018).

[57] Ibid, 17-19.

[58] U.S. Department of Defense, *Unclassified//For Official Use Only: Cyber Mission Analysis*, (Washington, DC: U.S. Department of Defense, August 21, 2014), 23, https://publicintelligence.net/dod-cyber-mission-analysis/ (accessed February 11, 2018).

[59] Ibid, 22.

[60] The 25B Information Technology Specialist; 25E Electromagnetic Spectrum Manager; 25A Signal Officer; 255A Information Systems Technician and 255N Network Management Technician in addition to the 25D and 255S comprise the operational and tactical computer network defense team managed by the Division or Brigade-level Signal officer.

[61] Jennifer Buckner, “Unclassified//For Official Use Only: Federated Cyber Training: Leveraging Cyberspace,” 3, briefing slides, Fort Gordon, GA: U.S. Army Cyber School, 2014, https://www.afcea.org/events/augusta/14/documents/BucknerMedicalTechNet2014.pdf (accessed February 11, 2018).

[62] Ibid.,” 13.

[63] Ibid., 17.

[64] Ibid., 14-15.

[65] Chad Saylor, “Toward a Coast Guard Cyberspace Workforce,” *Coast Guard All Hands*, March 09, 2017, http://allhands.coastguard.dodlive.mil/2017/03/09/it-takes-a-cyber-village/ (accessed December 26, 2017).

[66] U.S. Coast Guard, *United States Coast Guard Cyber Strategy*, 24, 36,

[67] Defense Acquisition Univerisity, “DOTmLPF-P Analysis,” *Acquisition Encyclopedia*, https://www.dau.mil/acquipedia/Pages/ArticleDetails.aspx?aid=d11b6afa-a16e-43cc-b3bb-ff8c9eb3e6f2 (accessed December 15, 2017).

[68] "Top 15 Security Utilities and Download Hacking Tools," *Darknet.org.uk*, September 11, 2017, https://www.darknet.org.uk/2006/04/top-15-securityhacking-tools-utilities/ (accessed February 10, 2018).

[69] Sean D. Carberry, "Rogers: 'cyber war' is here to stay," *FCW*, March 9, 2017, https://fcw.com/articles/2017/05/09/cyber-war-is-here-to-stay.aspx (accessed December 27, 2017).

[70] United States Special Operations Command, "Title 10 Authorities," http://www.socom.mil/about/title-10-authorities (accessed December 27, 2017).

[71] U.S. Department of Defense, *2015 DOD Cyber Strategy,* Introduction.

[72] U.S. Department of Defense, *2015 DOD Cyber Strategy*, 18-19.

[73] Buckner, "Unclassified//For Official Use Only: Federated Cyber Training," 10.

[74] Funding Streams for the Army and Air National Guard: 1) USA or USAF 2) Congressional additions provided by Congress for specific projects, programs or grants and 3) National Guard and Reserve Equipment Account (NGREA), which provides Congressionally-added funding for the National Guard and other reserve components to acquire new equipment and rebuild, refurbish and modernize existing systems. See National Guard Association of the United States, "Issue: Funding for Equipment and Modernization," https://www.ngaus.org/issues-advocacy/priorities-issues/funding-equipment-and-modernization (accessed December 27, 2017).

[75] Jon Brickey and David Di Tallo, *Cyber Beacon 2014 Workshop Repor*t, 6, https://www.afcea.org/events/augusta/14/documents/BucknerMedicalTechNet2014.pdf (accessed February 11, 2018).

[76] Buckner, "Unclassified//For Official Use Only: Federated Cyber Training," 15-16.

[77] Buckner, "Unclassified//For Official Use Only: Federated Cyber Training," 14-15; Jon Brickey and David Di Tallo, Cyber Beacon 2014 Workshop.pdf, 9.

[78] U.S. Coast Guard, *United States Coast Guard Cyber Strategy*, 28, 33.

[79] Defense Acquisition Univerisity, "DOTmLPF-P Analysis," *Acquisition Encyclopedia*, https://www.dau.mil/acquipedia/Pages/ArticleDetails.aspx?aid=d11b6afa-a16e-43cc-b3bb-ff8c9eb3e6f2 (accessed December 15, 2017).

[80] U.S. Department of Defense, "All Cyber Mission Force Teams Achieve Initial Operational Capability," *U.S. Cyber Command News Release*, October 24, 2016, https://www.defense.gov/News/Article/Article/984663/all-cyber-mission-force-teams-achieve-initial-operating-capability (accessed December 26, 2017).

[81] Ibid.

[82] Ibid.

[83] Ibid.

[84] U.S. Army Cyber Command, "Active Army cyber teams fully operational a year-plus ahead of schedule," *Army.mil,* November 02, 2017, https://www.army.mil/article/196311/active_army_cyber_teams_fully_operational_a_year_plus_ahead_of_schedule (accessed December 26, 2017).

[85] Ibid.

[86] Hope Hodge Seck, "Marine Corps May Get a Cyber-Only MOS," *Military.com,* January 12, 2017, https://www.military.com/daily-news/2017/01/12/marine-corps-get-cyber-only-mos.html (accessed December 26, 2017.

[87] Jared Serbu, "DoD declares Army, Navy cyber teams fully capable," *Federal News Radio*, November 03, 2017, https://federalnewsradio.com/defense/2017/11/dod-declares-army-navy-cyber-teams-fully-capable/ (accessed December 26, 2017).

[88] Mark Pomerleau, "Air Force Cyber Boss Sets Early Deadline For Full Operational Capability," *Fifth Domain*, September 01, 2017, https://www.fifthdomain.com/dod/air-force/2017/09/01/air-force-cyber-boss-sets-early-deadline-for-full-operational-capability/ (accessed February 10, 2018).

[89] Mark Pomerleau, "Air Force Bolsters Its Cyber Ranks by 40%," *Defense Systems*, January 04, 2016, https://defensesystems.com/articles/2016/01/04/air-force-boosts-cyber-ranks.aspx (accessed February 10, 2018).

[90] Mark Pomerleau, "Air Force Cyber Boss Sets Early Deadline."

[91] U.S. Coast Guard, *United States Coast Guard Cyber Strategy*, 28.

[92] Defense Acquisition University, "DOTmLPF-P Analysis."

[93] Defense Information Systems Agency, "Joint Regional Security Stacks," http://disa.mil/initiatives/jrss (accessed December 24, 2017).

[94] U.S. Congress, Senate, Committee on Armed Services, *Hearing to Receive Testimony on Increasing the Effectiveness of Military Operations*, 114th Cong., 1st sess., December 10, 2015, 18, https://www.armed-services.senate.gov/imo/media/doc/15-95%20-%2012-10-15.pdf (accessed February 11, 2018).

[95] Mark Pomerleau, "Rogers: Cyber Doesn't Need Its Own Military Branch."