UNITED STATES ARMY WAR COLLEGE PRESS
Carlisle Barracks, PA
STRENGTH ~ WISDOM

IMPLICATIONS OF SERVICE CYBERSPACE COMPONENT COMMANDS FOR ARMY CYBERSPACE OPERATIONS

Jeffrey L. Caton

U.S. ARMY WAR COLLEGE
SSI
STRATEGIC STUDIES INSTITUTE

The United States Army War College

The United States Army War College educates and develops leaders for service at the strategic level while advancing knowledge in the global application of Landpower.

The purpose of the United States Army War College is to produce graduates who are skilled critical thinkers and complex problem solvers. Concurrently, it is our duty to the U.S. Army to also act as a "think factory" for commanders and civilian leaders at the strategic level worldwide and routinely engage in discourse and debate concerning the role of ground forces in achieving national security objectives.

The Strategic Studies Institute publishes national security and strategic research and analysis to influence policy debate and bridge the gap between military and academia.

The Center for Strategic Leadership contributes to the education of world class senior leaders, develops expert knowledge, and provides solutions to strategic Army issues affecting the national security community.

The Peacekeeping and Stability Operations Institute provides subject matter expertise, technical review, and writing expertise to agencies that develop stability operations concepts and doctrines.

The School of Strategic Landpower develops strategic leaders by providing a strong foundation of wisdom grounded in mastery of the profession of arms, and by serving as a crucible for educating future leaders in the analysis, evaluation, and refinement of professional expertise in war, strategy, operations, national security, resource management, and responsible command.

The U.S. Army Heritage and Education Center acquires, conserves, and exhibits historical materials for use to support the U.S. Army, educate an international audience, and honor Soldiers—past and present.

STRATEGIC STUDIES INSTITUTE

The Strategic Studies Institute (SSI) is part of the U.S. Army War College and is the strategic-level study agent for issues related to national security and military strategy with emphasis on geostrategic analysis.

The mission of SSI is to use independent analysis to conduct strategic studies that develop policy recommendations on:

- Strategy, planning, and policy for joint and combined employment of military forces;
- Regional strategic appraisals;
- The nature of land warfare;
- Matters affecting the Army's future;
- The concepts, philosophy, and theory of strategy; and,
- Other issues of importance to the leadership of the Army.

Studies produced by civilian and military analysts concern topics having strategic implications for the Army, the Department of Defense, and the larger national security community.

In addition to its studies, SSI publishes special reports on topics of special or immediate interest. These include edited proceedings of conferences and topically oriented roundtables, expanded trip reports, and quick-reaction responses to senior Army leaders.

The Institute provides a valuable analytical capability within the Army to address strategic and other issues in support of Army participation in national security policy formulation.

Strategic Studies Institute
and
U.S. Army War College Press

IMPLICATIONS OF SERVICE CYBERSPACE COMPONENT COMMANDS FOR ARMY CYBERSPACE OPERATIONS

Jeffrey L. Caton

February 2019

The views expressed in this report are those of the author and do not necessarily reflect the official policy or position of the Department of the Army, the Department of Defense, or the U.S. Government. Authors of Strategic Studies Institute (SSI) and U.S. Army War College (USAWC) Press publications enjoy full academic freedom, provided they do not disclose classified information, jeopardize operations security, or misrepresent official U.S. policy. Such academic freedom empowers them to offer new and sometimes controversial perspectives in the interest of furthering debate on key issues. This report is cleared for public release; distribution is unlimited.

*****

This publication is subject to Title 17, United States Code, Sections 101 and 105. It is in the public domain and may not be copyrighted.

*****

Comments pertaining to this report are invited and should be forwarded to: Director, Strategic Studies Institute and U.S. Army War College Press, U.S. Army War College, 47 Ashburn Drive, Carlisle, PA 17013-5238.

*****

This manuscript was funded by the U.S. Army War College External Research Associates Program. Information on this program is available on our website, *http://ssi.armywarcollege.edu/*, at the Opportunities tab.

*****

All Strategic Studies Institute (SSI) and U.S. Army War College (USAWC) Press publications may be downloaded free of charge from the SSI website. Hard copies of certain reports may also be obtained free of charge while supplies last by placing an order on the SSI website. Check the website for availability. SSI publications may be quoted or reprinted in part or in full with permission and appropriate credit given to the U.S. Army Strategic Studies Institute and U.S. Army War College Press, U.S. Army War College, Carlisle, PA. Contact SSI by visiting our website at the following address: *http://ssi.armywarcollege.edu/*.

*****

The Strategic Studies Institute and U.S. Army War College Press publishes a quarterly email newsletter to update the national security community on the research of our analysts, recent and forthcoming publications, and upcoming conferences sponsored by the Institute. Each newsletter also provides a strategic commentary by one of our research analysts. If you are interested in receiving this newsletter, please subscribe on the SSI website at the following address: *http://ssi.armywarcollege.edu/newsletter/*.

ISBN 1-58487-797-9

FOREWORD

The *2018 National Defense Strategy* admonishes the Department of Defense (DoD) to invest in the continued development and integration of cyber capabilities into joint military operations. In this monograph, Mr. Jeffrey Caton examines the current paradigm of how the service cyberspace component commands operate as a mixture of common joint practices and service-unique means and methods. His research was completed in September 2017; thus, it does not address the May 2018 elevation of U.S. Cyber Command (USCYBERCOM) to a unified command, or that all Air Force Cyber Command's (AFCYBER's) Cyber Mission Force (CMF) teams achieved full operational capability in 2018.

Mr. Caton argues that the properly balanced fusion of this somewhat dissimilar force may yield a synergy that enhances unity of effort through standardization as well as exploits the distinct strengths of each service. He notes that the Army has made great strides through efforts such as the establishment of the Cyber branch and Cyber Center of Excellence (CCoE), and he provides recommendations to build on these successes in the areas of training, doctrine, and professional development. Further, Mr. Caton asserts that great opportunities await sage leaders who embrace the enduring traditions of Landpower with a vision for how they can be improved by operations in the rapidly evolving domain of cyberspace. His work herein should inform

the ongoing activities of USCYBERCOM as well as individual service cyberspace organizations.

DOUGLAS C. LOVELACE, JR.
Director
Strategic Studies Institute and
U.S. Army War College Press

ABOUT THE AUTHOR

JEFFREY L. CATON is president of Kepler Strategies LLC, Carlisle, Pennsylvania, a veteran-owned small business specializing in national security, cyberspace theory, and aerospace technology. He is also an intermittent professor of program management with Defense Acquisition University. From 2007 to 2012, Mr. Caton served on the U.S. Army War College (USAWC) faculty; this included serving as an associate professor of cyberspace operations and defense transformation chair. Over the past 9 years, he has presented lectures on cyberspace and space issues related to international security in the United States, Sweden, the United Kingdom, Estonia, Kazakhstan, and the Czech Republic, supporting programs such as the Partnership for Peace Consortium and the North Atlantic Treaty Organization Cooperative Cyber Defence Center of Excellence. His current work includes research examining the recent elevation of U.S. Cyber Command (USCYBERCOM) to be a unified command as well as the evolving role of the U.S. Army with nuclear operations as part of the External Research Associates Program of the Strategic Studies Institute (SSI). Mr. Caton is also a member of the Editorial Board for *Parameters* magazine. He served 28 years in the U.S. Air Force working in engineering, space operations, joint operations, and foreign military sales including command at the squadron and group levels. Mr. Caton holds a bachelor's degree in chemical engineering from the University of Virginia, a master's degree in aeronautical engineering from the Air Force Institute of Technology, and a master's degree in strategic studies from the Air War College.

SUMMARY

A fundamental tenet of the 2015 *DoD Cyber Strategy* is to achieve and maintain cybersecurity by a joint team effort across the whole-of-government. Some of the key Department of Defense (DoD) members of this cyberspace team are the service component cyber commands that report to U.S. Cyber Command (USCYBERCOM). U.S. Army Cyber Command (ARCYBER) conducts cyberspace-related missions of which some are common to the other service component and others are unique. To perform efficiently and effectively as part of the joint Cyber Mission Force (CMF), it is important for Army leaders and policymakers to understand the interfaces and boundaries among the service cyberspace components. Such knowledge can help to avoid unnecessary duplication as well as provide venues for sharing lessons learned and best practices.

The emerging DoD CMF includes forces from all military services that may reflect artifacts in their organization, training, and operation that are influenced by service cultures. Such diversity offers challenges and opportunities for senior leaders and policymakers entrusted with creating a joint force that can operate professionally in and through cyberspace.

This monograph examines how the Army may benefit by adopting processes and practices from other service cyberspace forces to the operations of ARCYBER. It focuses on the central question: "What is the context in which different military services approach cyberspace component operations internally as well as with the DoD?" To address this question, the study is divided into four major sections. The first section provides a background of the mission and structure of USCYBERCOM and the tenets of current joint cyberspace

operations doctrine. Next, the monograph explores the mission, organization, training, and equipping of each of the four service cyberspace components as well as the Coast Guard contributions. The third section analyzes how the service components support the USCYBERCOM mission as well as common trends and service culture influences among their operations. Finally, the author provides recommendations for DoD and Army leaders to consider for the enhancement of joint and service cyberspace operations.

The material presented herein is limited to unclassified and open source information available before September 2017, thus any classified discussion must occur within other venues. Also, the discussion regarding service cyberspace components will not be comprehensive due to classification and space requirements; instead, the monograph uses representative examples or illustrative vignettes to guide the discourse. The monograph includes recommendations related to cyber training ranges, cyber professional development, doctrine, and integration with operations in traditional domains.

IMPLICATIONS OF SERVICE CYBERSPACE COMPONENT COMMANDS FOR ARMY CYBERSPACE OPERATIONS

INTRODUCTION

The 2015 *DoD Cyber Strategy* states, "As a matter of first principle, cybersecurity is a team effort within the U.S. Federal government."[1] Some of the key Department of Defense (DoD) members of this cyberspace team are the service component cyber commands that report to U.S. Cyber Command (USCYBERCOM). Army Cyber Command (ARCYBER) conducts cyberspace-related missions of which some are common to the other service component and others are unique. To perform efficiently and effectively as part of the joint Cyber Mission Force (CMF), it is important for Army leaders and policymakers to understand the interfaces and boundaries among the service cyberspace components. Such knowledge can help to avoid unnecessary duplication as well as provide venues for sharing lessons learned and best practices.

The emerging DoD CMF includes forces from all military services that may reflect artifacts in their organization, training, and operation that are influenced by service cultures. Such diversity offers challenges and opportunities for senior leaders and policymakers entrusted with creating a joint force that can operate professionally in and through cyberspace.

This monograph examines how the Army may benefit by adopting processes and practices from other service cyberspace forces to the operations of ARCYBER. It is divided into four major sections. The first section provides a background of the mission and structure of USCYBERCOM and the tenets of current joint

cyberspace operations (CO) doctrine. Next, the monograph explores the mission, organization, training, and equipping of each of the four service cyberspace components as well as the Coast Guard contributions. The third section analyzes how the service components support the USCYBERCOM mission as well as common trends and service culture influences among their operations. Finally, the author provides recommendations for DoD and Army leaders to consider for the enhancement of joint and service CO.

The material presented herein is limited to unclassified and open source information, thus any classified discussion must occur within other venues. Also, the discussion regarding service cyberspace components will not be comprehensive due to classification and space requirements; instead, the monograph uses representative examples or illustrative vignettes to guide the discourse.

The acronyms used within this monograph are many and refer to complex military terms. Therefore, appendix I of this volume has been included to assist the reader in understanding and remembering which acronym pertains to which term.

DOD CYBERSPACE OPERATIONS

What is the context in which different military services approach cyberspace components internally as well as with DoD? This section explores this question in three ways. First, it presents a brief historical background of the formation and operation of USCYBERCOM. Next, it describes the doctrinal foundations of joint CO. Finally, it defines the common roles and responsibilities of a service cyberspace component command.

United States Cyber Command

> USCYBERCOM plans, coordinates, integrates, synchronizes and conducts activities to: direct the operations and defense of specified Department of Defense information networks and; prepare to, and when directed, conduct full spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries.[2]

USCYBERCOM was initially established in June 2009 and reached full operational capability in October 2010 as a sub-unified command reporting to United States Strategic Command (USSTRATCOM). The Commander, USCYBERCOM, is also dual-hatted as the Director of the National Security Agency and Chief, Central Security Service.[3] In accordance with the National Defense Authorization Act for Fiscal Year (FY) 2017, on August 18, 2017, President Donald Trump directed DoD to initiate the processes necessary to elevate USCYBERCOM to become a unified combatant command.[4] Details regarding the implementation of this reorganization are still being developed. Thus, this monograph will limit discussion to USCYBERCOM in its roles and responsibilities prior to this change.

In his May 2017 Senate testimony, Admiral Michael Rogers, Commander, USCYBERCOM, identified his top mission priority as the defense of the DoD information network (DODIN), with the main threats being those posed by state-based cyber actors. The key elements of this defense are Cyber Protection Teams (CPTs) and the Defense Information Systems Agency as well as "the Services, NSA [National Security Agency], and the Defense Cyber Crime Center."[5] Also, the Joint Staff Directorate for Command, Communications, and

Computer/Cyber (JS J6) is coordinating efforts with all combatant commanders to identify "Mission Relevant Cyberspace Terrain."[6]

The CPTs working DODIN protection are but one part of the larger CMF, which is the main operating force for USCYBERCOM. Admiral Rogers summarizes the focus of this capability as follows:

> We [USCYBERCOM] will posture the CMF to deliver effects across all phases of operations; to improve operational outcomes by increasing resilience, speed, agility, and precision; to generate operational outcomes that support DoD strategy and priorities; to create a model for successful Reserve and National Guard integration in cyberspace operations; and finally to strengthen partnerships across the government, with our allies, and with the private sector.[7]

In addition to the CPTs, the CMF has mission forces to support and protect the nation and combatant commands in cyberspace. Cyber CMFs are comprised of Combat Mission Teams (CMTs), Combat Support Teams (CSTs), and CPTs, and they operate through Joint Force Headquarters (JFHQs). Cyber National Mission Forces are comprised of National Mission Teams (NMTs), National Support Teams (NSTs), and CPTs, and they operate as directed by the President to defend against threats to the homeland.[8] Collectively, the MCF reached its initial operating capability on October 21, 2016, with 133 teams totaling about 5,000 individuals. Officials expect to achieve full operational capability with over 6,200 individuals by September 30, 2018.[9]

USCYBERCOM staff and JS J6 set the pipeline training course standards for the CMF. In January 2017, the JS J6 completed the CMF Training Transition Plan

that introduces "a joint training model and addresses the Cyber Mission Force Reserve Component training demand."[10] As with other joint forces, training standards and readiness reporting for the CMF have been integrated into the Defense Readiness Reporting System.[11]

Joint Cyberspace Operations

Joint Publication (JP) 3-12 (R), *Cyberspace Operations*, provides the overarching doctrine that describes joint cyberspace organizations and missions as well as provides guidance on the planning and execution of CO. JP 3-12 divides these operations into three broad categories: DODIN operations, offensive cyberspace operations (OCO), and defensive cyberspace operations (DCO) that is further broken into DCO-Internal Defensive Measures and DCO-Response Actions.[12] Table 1 provides the definitions for these terms.

Cyberspace Operation Type	Definition*
DoD Information Network (DODIN) operations	DODIN operations are actions taken to design, build, configure, secure, operate, maintain, and sustain DOD communications systems and networks in a way that creates and preserves data availability, integrity, confidentiality, as well as user/entity authentication and non-repudiation. These include proactive actions which address the entire DODIN, including configuration control and patching, IA measures and user training, physical security and secure architecture design, operation of host-based security systems and firewalls, and encryption of data. (p. II-3)
Offensive Cyberspace Operations (OCO)	Cyberspace operations intended to project power by the application of force in or through cyberspace. (p. GL-4)

Table 1. Joint Cyberspace Operations Doctrinal Definitions[13]

Cyberspace Operation Type	Definition*
Defensive Cyberspace Operations (DCO)	Passive and active cyberspace operations intended to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities, and other designated systems. (p. II-2)
• DCO-Internal Defensive Measures (IDM)	• Internal defensive measures are those DCO that are conducted within the DODIN. They include actively hunting for advanced internal threats as well as the internal responses to these threats. (p. II-3)
• DCO-Response Actions (RA)	• Deliberate, authorized defensive measures or activities taken outside of the defended network to protect and defend Department of Defense cyberspace capabilities or other designated systems. (p. GL-4)
*Definitions are excerpted from Joint Publication 3-12 (R).	

Table 1. Joint Cyberspace Operations Doctrinal Definitions (cont.)

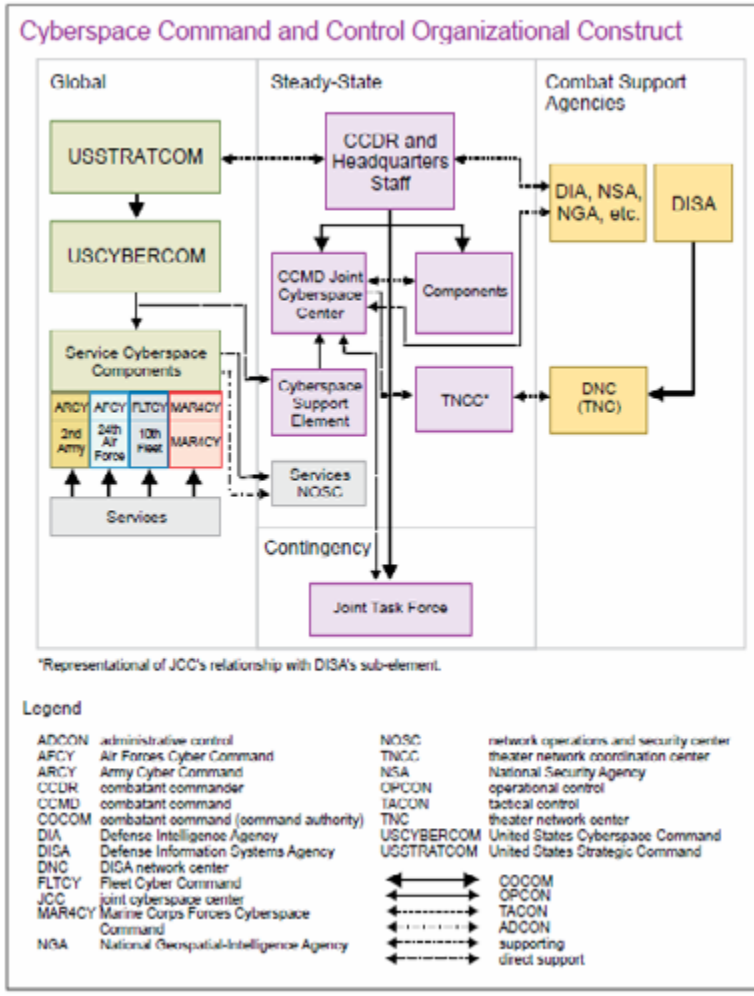
Since joint CO are categorized by intent, JP 3-12 also describes four types of cyberspace actions that are common to missions that require specific effects in cyberspace: cyberspace defense; cyberspace intelligence, surveillance, and reconnaissance; cyberspace operational preparation of the environment; and cyberspace attack. The publication also discusses how CO support the joint warfighting functions of command and control, intelligence, fires, movement and maneuver, sustainment, and protection.[14] JP 3-12 also offers guidance on expanding CO to interorganizational and multinational venues.[15]

To provide training, enhance proficiency, and evolve CMF and related cyber forces, USCYBERCOM conducts many different events including the annual Cyber Flag and Cyber Guard exercises. Cyber Flag is "a joint and combined military exercise focused on training and validating the CMF's capabilities and readiness to execute all phases of conflict across defensive

and offensive capabilities."[16] The exercise allows CPTs to apply their skills against cyber opposing forces as well as provides opportunities for NMTs and CMTs to practice OCO. Cyber Guard focuses on DODIN operations and protection of critical infrastructure in a compromised cyberspace environment. Its scope has expanded over five iterations to involve state and federal government as well as allied participation.[17] The sixth annual Cyber Guard conducted in June 2017 was co-led by USCYBERCOM, the Department of Homeland Security (DHS), and the Federal Bureau of Investigation (FBI). The exercise scenario "was developed based on [a] whole-of-nation event" and included participants from 22 countries.[18]

Service Cyberspace Components

From its inception, USCYBERCOM was organized to leverage cyberspace components provided by the Army, Marine Corps, Navy, and Air Force. Figure 1 depicts the original concept of cyberspace command and control among USSTRATCOM, USCYBERCOM, services, combat support agencies, and combatant command joint forces. The January 2017 Memorandum of Agreement between DoD and DHS clarified the Coast Guard role for cyber operations: "For purposes of securing, operating, and defending the [DODIN], Coast Guard Cyber Command will be responsible to the direction of, and report to, the Commander, U.S. Cyber Command."[19] While the current version (2013) of JP 3-12 provides overarching roles and responsibilities for service chiefs, it does not provide guidance on the formation and management of their cyberspace components, nor does it provide any mention of the CMF.[20]



Source: U.S. Department of Defense.

Figure 1. Cyberspace Command and Control Organizational Construct[21]

Service components perform several common functions; each is responsible for operating a Joint Forces Headquarters-Cyber (JFHQ-C) as well as staffing, training, and equipping various teams of the CMF.[22]

They also have responsibilities as a cybersecurity service provider (CSSP) that relate directly to the USCYBERCOM top priority to protect DODIN:

> Cybersecurity services include capabilities to implement DoD Component activities addressing vulnerability assessment and analysis; vulnerability management; malware protection; continuous monitoring; incident handling; insider threat [processes] to identify and evaluate anomalous user activity; and warning intelligence and AS&W [attack sensing and warning] to protect the DODIN.[23]

To improve DODIN protection, Defense Information Systems Agency is partnering with the Army and Air Force to consolidate and standardize the equipment and software necessary for network security. The approach involves the deployment of joint regional security stacks (JRSS) to increase visibility, efficiency, and effectiveness of DODIN operations.[24] Figure 2 provides details on how JFHG-DODIN, CMF teams, CSSPs, and other cybersecurity organizations interface to achieve shared situational awareness that enables cybersecurity and DCO actions. To improve the cybersecurity of materiel solutions using the defense acquisition system, the Under Secretary of Defense for Acquisition, Technology, and Logistics added Enclosure 14, "Cybersecurity in the Defense Acquisition System" to its capstone guidance document for DoD acquisition (DODI 5000.02) in February 2017.[25]

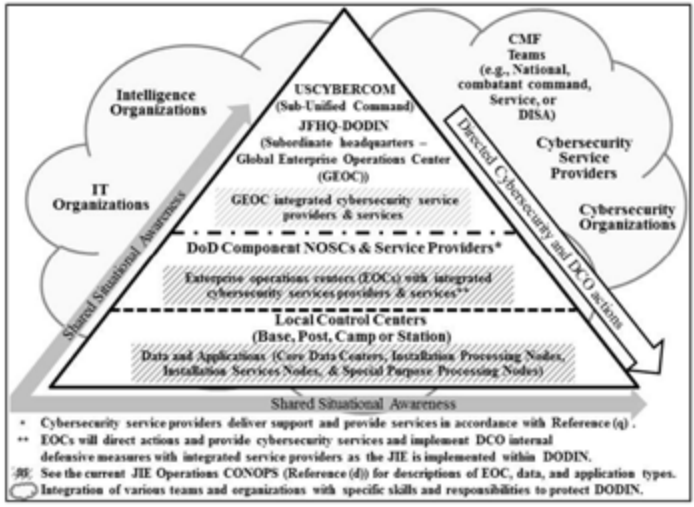
1. CYBERSECURITY ACTIVITIES INTEGRATION

a. DoD Components will organize and integrate cybersecurity activities to support DODIN operations and DCO internal defensive measures consistent with published orders and directives.

b. DoD Component subordinate organizations and authorizing officials responsible for systems will comply with orders or directives from CDRUSSTRATCOM and their DoD Component authority designated to direct the security, operations, and defense of the DoD Component's portion of the DODIN.

c. Figure 1 represents the flow of information between organizations to implement directed DODIN operations and DCO internal defensive measures. DoD requires horizontal and vertical DODIN situational awareness across DoD organizations. The figure shows the transition to JIE with the placement of enterprise operations centers (EOCs), core data centers, installation processing nodes, installation services nodes, and special purpose processing nodes.

Figure 1. DODIN Operations, DCO Internal Defensive Measures, and Situational Awareness



Source: U.S. Department of Defense.

Figure 2. Cybersecurity Integration into DODIN Operations[26]

Having established an understanding of the context in which the four military service cyberspace components operate, let us now explore each of them in their protocol order: Army, Marine Corps, Navy, and

Air Force. This will also include a brief summary of the Coast Guard cyberspace command.

ARMY SERVICE CYBERSPACE COMPONENT

ARCYBER was established in October 2009 and reached full operational capability in October 2010 as the lead Army organization for CO. In 2014, ARCYBER was designated as the Army Force Component Headquarters to USSTRATCOM, and its commander was dual-hatted as Commander, 2d Army that was reactivated as the single point of contact for Army network operations.[27] In January 2017, ARCYBER's role as an operational-level Army force was elevated to the status of Army service component command to USSTRATCOM, with the provision that it would become the ASCC to USCYBERCOM when it becomes a unified command. At that time, the 2d Army was disestablished and its Network Enterprise Technology Command reassigned to ARCYBER. The Headquarters, Department of the Army (HQDA) General Order directing these changes also noted that:

> to ensure unity of effort, the HQDA Chief Information Officer/G-6, the HQDA Deputy Chief of Staff G-3/5/7, and the Commander, ARCYBER will maximize communications and information in the execution of their missions and functions.[28]

To aid in this process, ARCYBER had previously established (in July 2016) a Cyber Directorate in the HQDA G-3/5/7 office to coordinate cyberspace doctrine, policy, organization, and resourcing.[29]

Headquarters ARCYBER is currently split, based with elements at Fort Belvoir, VA, Fort Meade, MD, and Fort Gordon, GA. Groundbreaking occurred in

November 2016 for a new consolidated headquarters facility at Fort Gordon—with its first phase to be completed by 2018, the second phase to support CPT operations by 2019, and its full capability for over 2,000 personnel by 2020.[30] Four Army lieutenant generals have served as the commander of ARCYBER thus far: Rhett A. Hernandez (October 2010 to September 2013), Edward C. Cardon (September 2013 to October 2016), Paul M. Nakasone (October 2016), and Stephen G. Fogarty (May 2018 to present).

Mission

> United States Army Cyber Command directs and conducts integrated electronic warfare, information and cyberspace operations as authorized, or directed, to ensure freedom of action in and through cyberspace and the information environment, and to deny the same to our adversaries.[31]

In his May 2017 Senate testimony, Nakasone stated three priorities for ARCYBER:

> Aggressively Operating and Defending Our Networks, Data, and Weapons Systems; Delivering Effects against Our Adversaries; and Designing, Building and Delivering Integrated Capabilities for the Future Fight.[32]

Currently the Army assesses its network compliance and readiness to pursue these priorities using processes that measure conformity with policy, regulation, and law through various scorecards and inspections. ARCYBER worked with JFHQ-DODIN to evolve its compliance-based readiness inspections to a risk-based operational inspection that provides risk assessments for specific mission critical tasks, thus assisting commanders in resource prioritization. ARCYBER

also prioritizes its basic cybersecurity hygiene requirements based in part on the visibility achieved through the DoD Cybersecurity Scorecard process.[33]

One of the key concepts for the ARCYBER mission is the Cyber Electromagnetic Activities (CEMA) Support to Corps and Below (CSCB) program initiated in 2015 with four primary purposes:

> Define what offensive and defensive cyber effects to integrate at the echelon Corps and below; Determine expeditionary Defensive Cyberspace Operations, Offensive Cyberspace Operations, Electronic Warfare, and Information Operations capability for deployed tactical forces; Leverage Combat Training Centers (CTCs) and operational deployments to inform CEMA Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, and Facilities development (DOTMLPF); and Determine the enduring CEMA environment at CTCs.[34]

CSCB has supported six rotations at Army Combat Training Centers (CTCs) since its inception, with the most recent involving the 2d Armored Brigade Combat Team, 1st Infantry Division, at the National Training Center in Fort Irwin, CA. CSCB has also supported operations at the Joint Readiness Training Center in Fort Polk, LA, as well as exercises like Operation DANGER FOCUS, a combined-arms, live-fire exercise at Fort Riley, KS. At such events, ARCYBER support may include an adversary cyber opposing force element from the 1st Information Operations Command.[35] CSCB is designed to build upon the lessons learned of these activities to refine their support methods and processes.[36]

In addition to recurring DODIN and DCO tasks, ARCYBER may also be called upon to provide specific support, which may include OCO, to combatant

commanders. ARCYBER is the designated JFHQ-C to support U.S. Central Command, U.S. Africa Command, and U.S. Northern Command. Since June 2016, the ARCYBER commander has also served as the commander of Joint Task Force (JTF) ARES, which is "a Joint cyber operational headquarters providing cyber capabilities in support of US Central Command's counter-ISIS [Islamic State in Iraq and Syria] operations."[37] USCYBERCOM directed ARCYBER in the lead role in JTF-ARES with the following goal:

> Through the establishment of a JTF focused on countering ISIL [Islamic State in Iraq and the Levant] in cyberspace, USCYBERCOM will continue to create cyberspace conditions to support the dismantling of ISIL [redacted passage] in support of (ISO) United States Central Command (USCENTCOM) and to disrupt ISIL's ability to plan and execute attacks against the United States (US) and coalition partners while posturing for follow-on global CO.[38]

Other service components as well as the Cyber National Mission Forces also received tasks, but ARCYBER's unique duties as JTF commander included not only the establishment, planning, and operation of the JTF, but also the following tasks:

> Provide [redacted passage] C-ISR [intelligence, surveillance, and reconnaissance], and C-OPE [operational preparation of the environment] tactics and capability development tailored to deliver desired cyberspace effects as developed by JTF-ARES. . . . Provide technical development and assurance for future capabilities. . . . Develop estimate of funding required to establish and maintain JTF-ARES. . . . Provide risk assessment to existing ARCYBER/JFHQ-C (Army) missions based upon force reallocation to JTF-ARES.[39]

Organization

In his October 2016 article in *Army* magazine, then ARCYBER commander Lieutenant General Edward Cardon described how units with different mission focuses are necessary to conduct cyber operations properly. He summarized by stating:

> Unifying operational control of all Army cyberspace forces to include appropriate signal, military intelligence and cyberspace units is critical to operating, maintaining, securing and defending the Army's portions of the combined DoD Information Network [DODIN].[40]

Thus, the major ARCYBER units shown in figure 3 and described in table 2 have different focuses such as network operations, information operations, and intelligence. For the CMF, ARCYBER must provide 41 total teams: 4 NMTs, 3 NSTs, 8 CMTs, 6 CSTs, and 20 CPTs. As of May 2017, 33 of the Army teams were fully capable, with the remaining 8 teams projected to reach full operational capability by the end of September 2017. Current plans also call for an additional 21 total force CPTs, 10 from the Army National Guard, and 10 from the Army Reserve by 2021.[41]

Source: U.S. Army Cyber Command.

Figure 3. Major ARCYBER Unit Locations[42]

Unit	Mission	Joint Cyberspace Mission Areas
Network Enterprise Technology Command (NETCOM) (Fort Huachuca, AZ)	NETCOM leads global operations for the Army's portion of the DODIN, ensuring freedom of action in cyberspace while denying the same to our adversaries (p. 120).[43]	DODIN
1st Information Operations (IO) Command (Fort Belvoir, VA)	1st Information Operations Command (Land) provides IO and Cyberspace Operations support to Army and other Military Forces through: • Deployable Support Teams • Opposing forces support • Reachback planning and analysis • Specialized training In order to support freedom of action in the information environment and to deny the same to our adversaries.[44]	OCO
Cyber Protection Brigade (CPB) (Fort Gordon, GA)	To rapidly evaluate and act in response to unexpected and dynamic cyber situations; defend the nation in response to hostile action and imminent cyber threats; conduct global cyberspace operations to deter, disrupt, and defeat our adversary's cyberspace operations; and defend the United States through specialized cyber support missions.[45]	DCO
780th Military Intelligence (MI) Brigade (Fort Meade, MD)	The 780th Military Intelligence Brigade conducts signals intelligence and cyberspace operations to create operational effects in and through the cyberspace domain to gain and maintain freedom of action required to support the Army and Joint requirements while denying the same to our adversaries.[46]	

Table 2. Major ARCYBER Units

All ARCYBER activities are monitored and controlled by the Army Cyber Operations and Integration Center (ACOIC), an operational element of ARCYBER headquarters. It provides cyberspace situational awareness in part through the coordination of five regional cyber centers assigned to Europe, Southwest Asia, Pacific, Korea, and the continental United

States.[47] These regional cyber centers also serve as the Army CSSPs, which concentrate protection against known network threats. The Cyber Protection Brigade (CPB) uses its cyberspace maneuver force of 20 CPTs to conduct active reconnaissance and response actions for more sophisticated threats. The CPB also supports the protection of critical infrastructure of the Army as well as infrastructure administered by the Army Corps of Engineers, such as dams and hydroelectric plants.[48]

In 2014, the Army established the Cyber branch as "a maneuver branch with the mission to conduct defensive and offensive cyberspace operations . . . the only branch designed to directly engage threats within the cyberspace domain."[49] In addition, to support the integration of electromagnetic spectrum (EMS) operations with cyber operations, the Army approved a phased approach to convert the Electronic Warfare (EW) occupational specialty (Functional Area [FA] 29) to the Cyber branch (FA 17), to begin in 2018. As of May 2017, the Army Cyber force (FA 17 and FA 29) stands at 2,331 Soldiers: 557 officers, 305 warrant officers, and 1,469 enlisted.[50] However, the estimated need for a fully operational ARCYBER is over 3,800 military and civilians with core cyber skills.[51]

There are explicit cyber career fields for officers, warrant officers, and enlisted personnel within the Cyber branch; together these comprise the core of the Army cyber force. The Cyber Operations Officer's (17A) primary purpose is to "lead, plan, and direct both defensive and offensive cyberspace maneuvers and effects operations in and through the cyberspace domain."[52] The warrant officer position of Cyber Operations Technician (170A) performs as an advisor to command staffs regarding the use of CO assets and personnel and "integrates cyberspace effects into warfighting functions in

an effort to optimize combat effectiveness."[53] Enlisted members can perform as a Cyber Operations Specialist (17C) with duties that cover the range of CO, as well as a Cyber Network Defender (25D) with duties focused on DCO.[54] CO may also involve several other related career fields in the areas of network operations, cryptology, signals, and intelligence. Appendix II describes position descriptions and duties.

In January 2017, the Army initiated a cyberspace-effects career program for civilians as well to add expertise to the cyber force that is not found in existing military training courses.[55] The new career field "will unify all Cyberspace Effects civilian employees into a single cross-disciplinary model for training and management of multiple Occupational Specialties."[56] The program will also align Cyberspace Effects civilians with FA17 officer counterparts, thus they will be subject to the same USCYBERCOM joint training requirements.

To address the challenge of recruiting cyberspace-related personnel in a highly competitive job market, the Army is implementing direct commissioning (lateral entrance into force) aimed at skill sets such as "computer programming, mathematics, network operations, cryptology, data science, or nanotechnology."[57] Also, the Army will continue to leverage expertise from industry and other sectors via the total force concept. To support such efforts, the reorganization of Army Reserve Information Operations Command to Army Reserve Cyberspace Operations Group was implemented in October 2016.[58] Army Reserve Cyberspace Operations Group current plans are to have 10 Reserve CPTs by 2021.[59]

Training

ARCYBER conducts its CMF training in individual, collective, and mission rehearsal courses and events.[60] In 2015, the Army proponent of CO shifted from ARCYBER to the U.S. Army Training and Doctrine Command with its establishment of the U.S. Army Cyber Center of Excellence (CCoE) at Fort Gordon, GA. Thus, the CCoE became "the Army's center of gravity for institutionalizing cyberspace, to include developing the necessary doctrinal, organizational, training, and materiel activities and policies."[61] Moreover, the CCoE will help to evolve and integrate Army cyberspace, EW, and signal operations into joint force requirements.[62]

For individual training focused on building core CO knowledge and competencies, the CCoE's Army Cyber School executes programs that meet ARCYBER requirements, which include joint standards of USCYBERCOM J7.[63] Introductory Army Cyber School courses include the Basic Officers Leader Course, the warrant officer training program with basic and advanced courses, and the enlisted Advanced Individual Training, which has its first phase as the Navy Joint Cyber Analysis Course (JCAC) at Pensacola, FL.[64] The first CCoE classes for Cyber branch lieutenants were completed in May 2016, and in March 2017 for warrant officers and enlisted personnel. A total of 583 Cyber branch members were trained in FY 2016 and 1,200 additional students are scheduled for FY 2017.[65]

Collective CO training utilizes ARCYBER and CCoE capabilities that provide "simulated, virtual, and real-world operational events on ranges and networks that stress individual and team capabilities."[66] During FY 2017, Army CMF teams were scheduled for

about 80 collective training events, including Cyber Guard and Cyber Flag as well as plans for 48 internal mission rehearsal events. These activities may involve joint, interagency, and partner nation participation, thus making such training a crucial means for building team proficiencies and preparing for actual CO missions.[67]

After several years of development, Field Manual (FM) 3-12, *Cyberspace and Electronic Warfare Operations*, was released in April 2017 as an expansion of, and replacement for, FM 3-38, *Cyber Electromagnetic Activities* (February 2014). FM 3-12 strives to consolidate CO, EW, and CEMA fundamentals and guidance into one document as well as to provide a coherent paradigm of how these capabilities enable Army operations. Its definitions and discussion of CO missions are consistent with JP 3-12 and mark the starting point of broader treatise not only of EW but also on EMS operations and spectrum management. FM 3-12 also addresses the relationships CO and EW have with information operations, intelligence, space operations, and targeting. Figure 4 depicts how CO and EW missions and actions interface internal to and external to the DODIN.[68] FM 3-12 does a good job of explaining the basics of CO and EW, including how these operations are integrated into military planning processes. However, it does a very poor job of articulating the Army's role in joint CO; it is devoid of any explicit reference to the CMF or any of its teams or the myriad responsibilities of ARCYBER as an ASCC.

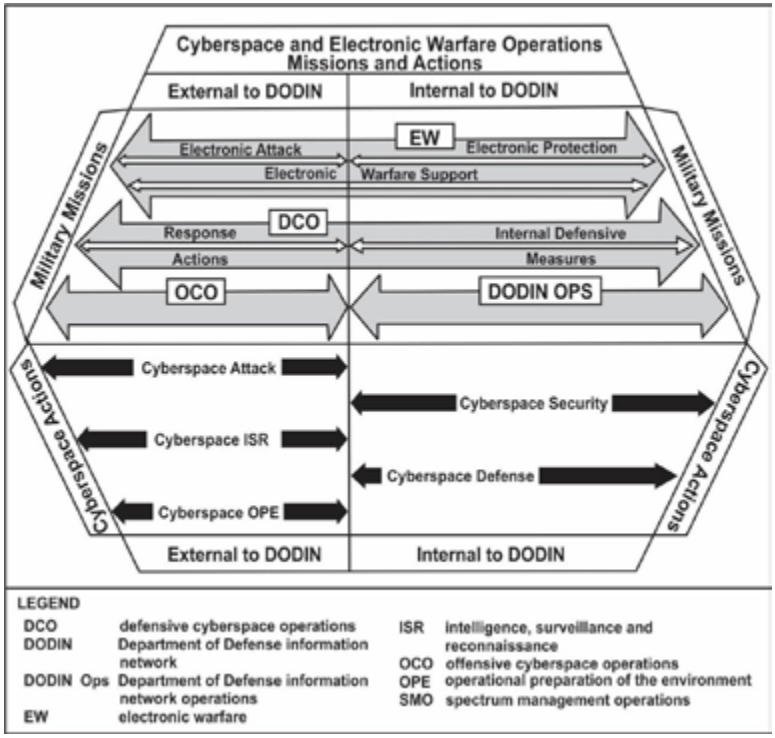


Figure 4. Army Cyberspace and Electronic Warfare Operations—Missions and Actions[69]

Equipping

ARCYBER is supporting several efforts toward the Army Network Modernization to include such efforts as JRSS migration and other upgrades, some in partnership with the Defense Information Systems Agency and the Air Force.[70] The envisioned end state is to achieve improved "cybersecurity by collapsing networks, reducing their attack surface area, improving bandwidth and reliability, and upgrading defense capabilities."[71] The Army is also leveraging less conventional

expertise and resources from organizations like the U.S. Digital Service and Defense Digital Service, which facilitated the "Hack the Army" initiative in late 2016. In only 22 days, 371 registered researchers targeted Army recruiting websites and reported 118 previously unknown vulnerabilities that could result in network or data breaches.[72]

A key enabler of CMF development and refinement is the acquisition of the Persistent Cyberspace Training Environment (PCTE). DoD designated the Army as the acquisition lead for PCTE as well as the Executive Agent for Cyber Training Ranges.[73] PCTE will provide individual and collective training as well as mission rehearsal for joint and service applications at three levels of virtual fidelity.[74] The Army Program Executive Office for Simulation, Training and Instrumentation held an Industry Day for potential PCTE vendors in November 2016, as well as one for the National Cyber Range Complex acquisition in June 2017.[75]

The Army Rapid Capabilities Office is helping to equip Army CMF teams with accelerated delivery of capabilities for high-priority mission needs using prototyping of deployable hardware and software. Prototype DCO kits were used to support a May 2017 training rotation for the 2d Armored Brigade, 1st Infantry Division at the National Training Center.[76] Since CMF materiel needs will continue to evolve, the CCoE is working with U.S. Army Training and Doctrine Command's Army Capabilities Integration Center to identify science and technology needs for future Army CO capabilities that touch on several areas of the CEMA concept.[77] The Army may pursue some of these capabilities through the Cyber Innovation Challenge, a collaborative effort amongst ARCYBER, the CCoE, and the Assistant Secretary of the Army for

Acquisition, Logistics, and Technology. The program forms a diverse consortium of industry, academia, and government members and uses flexible acquisition methods to produce prototype equipment, often from nontraditional sources. A goal of the Cyber Innovation Challenge is to award vendor contracts only 90 days after a requirement is announced.[78]

MARINE CORPS SERVICE CYBERSPACE COMPONENT

U.S. Marine Corps Forces Cyberspace (MARFORCYBER) was initially established in October 2009, and reached full operational capability in 2013 with the first commander, Lieutenant General George J. Flynn, dual-hatted as Commander, Marine Corps Combat Development Command. The original plans for the new command called for approximately 800 personnel dedicated to explicit cyberspace work.[79] Subsequent commanders of MARFORCYBER served as Marine major generals: Vincent Stewart (June 2013 to January 2015); Daniel O'Donohue (January 2015 to September 2015); and Loretta E. Reynolds (September 2015 to present). It is of interest to note that Stewart was selected to lead the Defense Intelligence Agency as a Lieutenant General and was nominated to become deputy commander of USCYBERCOM in June 2017.[80]

Headquarters MARFORCYBER is located at Fort Meade, MD, with a current authorized staff of 189 Marines and 32 civilians. Groundbreaking for a new headquarters building occurred in October 2015, with occupancy projected by December 2017. It will remain at Fort Meade and be located in the National Security Agency-East Cyber Campus complex.[81]

Mission

> COMMARFORCYBERCOM enables full spectrum cyberspace operations, to include the planning and direction of Marine Corps Enterprise Network Operations (MCEN Ops), defensive cyberspace operations (DCO) in support of Marine Corps, Joint and Coalition Forces, and the planning and, when authorized, direction of offensive cyberspace operations (OCO) in support of Joint and Coalition Forces, in order to enable freedom of action across all warfighting domains and deny the same to adversarial forces.[82]

In her May 2013 Senate testimony, Reynolds discussed her top three priorities for MARFORCYBER. The top priority is "to secure, operate, and defend the Marine Corps' portion of the [DODIN], the MCEN [Marine Corps Enterprise Network]."[83] The MCEN is part of the larger Marine Corps Cyberspace Environment, which also includes tactical networks and weapons systems information elements.[84] In 2015, MCEN transitioned from being contractor managed to being MARFORCYBER controlled, and efforts to improve performance and reduce vulnerability continue.[85] The second priority is "to provide ready, capable cyber forces to USCYBERCOM" primarily through various CMF teams that will be discussed in the next section of this monograph. The third priority of Reynolds is "to add cyberspace warfighting expertise to the Marine Air Ground Task Force (MAGTF)," which is the core warfighting structure of the Marine Corps.[86]

The Marine Corps Operating Concept: How an Expeditionary Force Operates in the 21st Century was released in September 2016 to describe how the Marine Corps will operate in 2025 and beyond, as well as the capabilities required for future activities. Among the critical tasks identified for future forces is a "Broader Concept of

Combined/Information Warfare" which includes the following cyberspace-related goals:

- Keep pace with ever-changing technologies to succeed on a battlefield where the ability to conduct cyberspace operations is as important as the ability to perform command and control, maneuver, or fires.
- Continue to mature our global cyberspace operations capabilities to include employment of Cyberspace Protection Teams as maneuver elements.
- Deliver cyberspace and electronic warfare fires via a wide variety of MAGTF ground and air platforms.
- Maintain access and control of cyberspace, the electromagnetic spectrum, and space at decisive times and places to achieve MAGTF objectives.[87]

This operating concept emphasizes the roles and actions of information operations in the space and cyberspace domains, but does not discuss any roles of cyberspace forces as the supported effort. Further, Marine Corps Warfighting Publication 3-40.4, *Marine Air-Ground Task Force Information Operations*, states:

> there will be operations and capabilities that blur the line between cyberspace operations and EW and may require case-by-case determination when electronic warfare and cyberspace operations are assigned separate release authorities.[88]

To help address such operational seams, the Marine Corps is developing the Cyberspace and Electronic Warfare Coordination Cell (CEWCC) concept "to operationalize the cyberspace domain and the electromagnetic spectrum (EMS) as interrelated maneuver spaces through which military advantage can be gained or lost."[89] Two military EW officers summed up the concept in more operational terms in a 2015 *Marine Corps Gazette* article: "CEWCC exists to simplify the complex

problem of maneuver in the EMS and/or cyberspace for the MAGTF commander . . . analogous to a fire support coordination center (FSCC)."[90]

The July 2017 MAGTF Information Environment Operations Concept of Employment presents Information Environment (IE) Operations as a combination of six operational capabilities: cyberspace, EMS, space, influences, deception, and inform. The concept leans forward to consider a future when DCO and OCO authorities may extend down to the MAGTF commander and advises:

> as this occurs, there must be a command and control mechanism in place for the MIG [Marine Expeditionary Force Information Group] and MIG COC [Combat Operations Center] to plan and execute OCO as a type of MAGTF fires.[91]

Organization

MARFORCYBER has two major subordinate commands: Marine Corps Cyberspace Operations Group (MCCOG) and the Marine Corps Cyberspace Warfare Group (MCCYWG). Table 3 describes their missions. The MCCOG performs global network operations and MCEN defense as an operational force command apportioned to USSTRATCOM. It was established in December 2016 when it assumed the tasks of the former Marine Corps Network and Operations Security Center. To support its continuity of operations as required by the DoD, MARFORCYBER developed a plan to provide a MCCOG alternate site at the Marine Corps Information Technology Center in Kansas City, MO; the plan will be implemented as funding is made available.[92] The MCCYWG, often referred to as the

Cyber Warfare Group, was activated in March 2016 with responsibilities to identify capability requirements as well as provide training, certifying, and sustaining readiness for CMF teams.[93] Also, if tasked and authorized, the Cyber Warfare Group can conduct OCO that may include computer network exploitation as well as cyberspace intelligence, surveillance, and reconnaissance, and operational preparation of the environment.[94]

Unit	Mission*	Joint Cyberspace Mission Focus
Marine Corps Cyberspace Operations Group (MCCOG) (Marine Corps Base Quantico, VA)	Executes Marine Corps Department of Defense Information Network (DODIN) Operations and Marine Corps Defensive Cyberspace Operations (DCO) in order to enhance freedom of action across warfighting domains, while denying the efforts of adversaries to degrade or disrupt this advantage through cyberspace.	DODIN DCO
Marine Corps Cyberspace Warfare Group (MCCYWG) (Fort Meade, MD)	Organizes, trains, equips, provides administrative support, manages readiness of assigned forces, and recommends certification and presentation of Cyber Mission Force (CMF) Teams to U.S. Cyber Command. The MCCYWG plans and conducts full spectrum cyberspace operations as directed by COMMARFORCYBER in support of service, combatant command, joint, and coalition requirements.	DCO-RA OCO
*Descriptions excerpted from the official website of U.S. Marine Corps Forces, Cyberspace Command.		

Table 3. Major MARFORCYBER Units[95]

MARFORCYBER contributes 13 teams to the CMF: 1 cyber NMT, 3 CMTs, 1 CST, and 8 CPTs, with 3 of the CPTs retained and oriented toward MARFORCYBER missions. As of May 2017, 9 of the 13 tests have reached full operational capability, with the remaining 4 teams expected to reach full operational capability during FY 2018.[96] In 2015, the JFHQ-C MARFORCYBER reached its full operational capability assigned to support U.S. Special Operations Command planning and operation.[97] Key Marine military occupational

specialties directly related to CO include the Cyber Network Operations Officer (0605), warrant officer position military occupational specialties of Cyber Network Operations Engineer (0650), and the enlisted military occupational specialties of Cyber Network Operator (0651), Cyber Network Systems Chief (0651), and Cyber Security Chief (0689). Appendix III provides duty descriptions of these positions.

Training

During his 2010 congressional testimony, Lieutenant General Flynn noted, "a typical Cyber Marine will require 2 years of classroom and on-the-job training to be proficient in cyberspace operations."[98] Such training would include the the JCAC, the Joint Network Attack Course, and other DCO specialty courses, all followed by on-the-job training. To enhance CO proficiency and teamwork, MARFORCYBER utilizes persistent training environments that may include web-based training like that developed with the Carnegie Mellon University Software Engineering Institute.[99] The Marine Corps also developed a cyber range in 2015 not only to train Marine cyberspace operators, but also some of those Marines who work with communications, intelligence, and operational planning.[100] Going beyond the virtual training environment, MARFORCYBER teams also participate in training activities such as the I MEF Large Scale Exercise 2016 held at Marine Corps Air Station Miramar, CA. The exercise included DCO support and advice from a U.S. Navy captain.[101]

In October 2014, the Marine Corps released its first cyberspace doctrine, Marine Corps Interim Publication 3-401.02, *Marine Corps Cyberspace Operations*. The

document has restricted access, but the public description states that the CO doctrine addresses "how the Marine Corps is currently organized to conduct cyberspace operations, planning considerations, and emerging changes that will affect our cyberspace operations capability and capacity."[102] The target audience for Marine Corps Interim Publication 3-401.02 is MAGTF commanders and their staff. Their growing experience with CO will feed into a refined and enduring doctrine document in the near future. Defense industry analyst Jared Serbu noted that this initial CO doctrine reflects the current Marine view "that cyber capabilities are not treated as a specialized field, but instead are tightly integrated into Marine air-ground task forces and managed by commanders just like any other warfighting tool."[103] Indeed, the Marine Corps vision for its future force, *Expeditionary Force 21*, indicates that the CEWCC concept geared toward MAGTF support is an integral part of current Marine doctrine for CO and EMS operations.[104]

Equipping

MCEN modernization continues with efforts to improve its security and defense by reducing the number of potential attack nodes and hardening those that remain.[105] Staying true to its expeditionary mission heritage, MARFORCYBER may equip its CPTs with the Deployable Mission Support System hardware and software for DCO. This allows for a smaller CPT element to operate from a forward-deployed location with reach-back technical support from its home station. The Marine's Force Design 2025 effort includes the addition of DCO-Internal Defensive Measures companies and EW companies as elements of each MEF.[106]

In 2015, Marine Commandant General Joseph Dunford established a cyber force whose assignment included the improvement of cyberspace capability acquisition. The result was the development of a Cyber Advisory Team under Marine Corps Systems Command that operates in two process time frames: emergency acquisitions for fielding capabilities in less than 30 days, and urgent acquisition for fielding capabilities between 30 and 180 days.[107] In the summer of 2016, the Cyber Advisory Team accomplished its first emergency acquisition that leveraged off-the-shelf equipment to provide Marine CPTs with cybersecurity capabilities.[108] The Marine Corps also leverages industry to provide flexible and adaptive support of its cyberspace training programs using the indefinite delivery, indefinite quantity contracting process; three such contracts worth almost $48 million were awarded in December 2016.[109]

NAVY SERVICE CYBERSPACE COMPONENT

U.S. Fleet Cyber Command (FCC or FLTCYBERCOM) was established, and U.S. 10th Fleet was recommissioned in January 2010, with Vice Admiral Bernard J. McCullough III as commander of both units, sometimes identified as FCC/C10F. Headquarters for both commands were created at Fort Meade, MD, in part to utilize the infrastructure of the Naval Network Warfare Command located there. Tenth Fleet previously operated from 1941 to 1945 as the Navy lead for anti-submarine warfare; the command deactivated with the end of World War II.[110] In his September 2010 congressional testimony, McCullough noted that the responsibilities of FLTCYBERCOM went beyond those of other service cyberspace components, acting as the

Navy's "central authority for networks, cryptology, signals intelligence, information operations, cyber, electronic warfare and space in support of forces afloat and ashore."[111] As such, the commander, FLTCYBERCOM reports directly to the Chief of Naval Operations (CNO). Subsequent FCC/C10F commanders (all Vice Admiral) were: Michael S. Rogers (September 2011-April 2014); Jan E. Tighe (April 2014-July 2016); and Michael M. Gilday (July 2016-present). Rogers went directly from this command to become commander of USCYBERCOM.

With FLTCYBERCOM entrusted to maintain, defend, and operate the Navy's networks, the Naval Information Forces Command (NAVIFOR) accomplishes the tasks of organizing, training, and equipping cyberspace forces. Until 2016, NAVIFOR was known as the Naval Information Dominance Force, which was established in 2014 with a mission that included "providing combat-ready information warfare forces, which are forward deployable, fully trained, properly manned, capably equipped, always ready, well maintained and combat sustainable."[112] To provide cyberspace expertise to the headquarters staff, in 2015 the CNO established the Navy Cybersecurity Division within the Navy N2/N6 and tasked it to oversee cybersecurity strategy and policy compliance as well as advocate for related requirements.[113]

Mission

The mission statement of FLTCYBERCOM is:

> The mission of Fleet Cyber Command is to serve as central operational authority for networks, cryptologic/signals intelligence, information operations, cyber, electronic warfare, and space capabilities in support of forces afloat and ashore; to direct Navy cyberspace operations globally to deter and defeat aggression and to ensure freedom of action to achieve military objectives in and through cyberspace; to organize and direct Navy cryptologic operations worldwide and support information operations and space planning and operations, as directed; to execute cyber missions as directed; to direct, operate, maintain, secure, and defend the Navy's portion of the Department of Defense Information Networks [DODIN]; to deliver integrated cyber, information operations, cryptologic, and space capabilities; to deliver a global Navy cyber common operational picture; to develop, coordinate, assess, and prioritize Navy cyber, cryptologic/signals intelligence, space, information operations, and electronic warfare requirements; to assess Navy cyber readiness; and to exercise administrative and operational control of assigned forces.[114]

Whereas, the mission statement of U.S. Tenth Fleet is:

> The mission of Tenth fleet is to serve as the Numbered Fleet for Fleet Cyber Command and exercise operational control of assigned Naval forces; to coordinate with other naval, coalition and Joint Task Forces to execute the full spectrum of cyber, electronic warfare, information operations and signal intelligence capabilities and missions across the cyber, electromagnetic and space domains.[115]

In his May 2015 Senate testimony, Gilday identified five strategic goals for FLTCYBERCOM:

1. Operate the Networks as a Warfighting Platform.

2. Conduct Tailored Signals Intelligence.

3. Deliver Warfighting Effects Through Cyberspace.

4. Create Shared Cyber Situational Awareness.

5. Establish and mature [the] Navy's Cyber Mission Forces.[116]

These goals apply to a daunting Navy network that includes "more than 500,000 end user devices; an estimated 75,000 network devices (e.g., servers, domain controllers); and approximately 45,000 applications and systems across three security enclaves," all within the cyberspace domain.[117]

One of the most formative events for FLTCYBERCOM was Operation ROLLING TIDE, which was the response to an adversary intrusion into the Navy's unclassified networks and command and control capabilities. Conducted from August 2013 to February 2014, Operation ROLLING TIDE was the Navy's "first named operation launched specifically to counter cyber activity," and it redefined how the Navy approached network defense and cyber threat response.[118] This "shot-across-the-bow" in cyberspace led Navy leadership to form the aptly named Task Force Cyber Awakening (TFCA), a year-long effort to baseline Navy cybersecurity and the organizational structures that develop and support it. Organized into four task groups that examined capabilities, hardening, cybersecurity, and technical standards, the results of TFCA informed the current structure and operation of FLTCYBERCOM.[119]

Organization

The scope of FLTCYBERCOM is impressive, with an operational force of 16,500 active duty, reserve component, and civilians across 24 active commands and 32 reserve commands. Table 4 lists the 18 units that reported directly to FLTCYBERCOM as of August 2017. Because of its diverse responsibilities, only about 35 percent of FLTCYBERCOM operational forces directly conduct CO missions.[120] Operations under 10th Fleet are structured as a typical Navy Task Force that are task organized into several mission areas: network operations, network defense, information operations, fleet and theater operations, research and development, and cryptologic support.[121]

	Unit	Mission
Network Operations	Naval Network Warfare Command (NETWARCOM) (Suffolk, VA)	Execute tactical-level command and control to direct, operate, maintain, and secure Navy communications and network systems for Department of Defense Information Networks; leverage Joint Space capabilities for Navy and Joint Operations.[122]
	Naval Communications and Telecommunications Area Master Station (NCTAMS) PAC NCTAMS LANT	Delivers and defends responsive, resilient, and secure computer and telecommunications systems, providing information superiority for global maritime and joint forces.[123]
	Naval Satellite Operations Center (NAVSOC) (Point Magu, CA)	. . . responsible for managing, operating and maintaining assigned satellite systems to provide reliable satellite services to the joint warfighter in support of naval and national requirements.[124]
Network Defense	Navy Cyber Defense Operations Command (NCDOC) (Suffolk, VA)	Execute Defensive Cyberspace Operations. Enable global power projection through proactive network defense [serves as the Navy's CSSP].[125]
	Navy Information Operations Command (NIOC) (Pensacola, FL)	. . . execute cyberspace operations and SIGINT tasks in support of naval and joint forces and national tasking authorities.[126]

Table 4. Major FLTCYBERCOM Cyberspace-Related Units [127]

	Unit	Mission
Information Operations	NIOC Norfolk	. . . advances Information Operations war fighting capabilities for Naval and Joint Forces by providing operationally focused training and planning support; developing doctrine, tactics, techniques, and procedures; advocating requirements in support of future effects-based warfare; and managing functional data for Information Operations.[128]
Fleet and Theater Operations	NIOC Texas NIOC Georgia NIOC Hawaii NIOC Colorado NIOC Bahrain NIOC Yokosuka	Conduct SIGINT, cyber and information operations for Fleet, Joint and National Commanders, which enhance the war fighting effectiveness of our Navy and the Nation.[129]
	Cryptologic Warfare Group 6 (CWG-6) (Fort Meade, MD)	Deliver Information Warfare capabilities to the Fleet. Provide and deploy trained Sailors, expertise, and equipment to support Signals Intelligence and Cyberspace operations for Naval and Joint Forces.[130]
Research and Development	Navy Cyber Warfare Development Group (NCWDG) (Washington, DC)	. . . serves as the Navy's Center for Cyber Warfare innovation. As directed by U.S. Fleet Cyber Command, NCWDG civilian and military personnel discover and exploit adversary vulnerabilities, delivering Cyber tactics and capabilities to the U.S. Navy using rapid prototyping and acquisition authority.[131]
Global Command and Control Support	Naval Computer and Telecommunications Station (NAVCOMTELSTA) Bahrain NAVCOMTELSTA Naples, Italy NAVCOMTELSTA Yokosuka, Japan	. . . provide reliable, available and secure communications and information technology services critical to naval success in the . . . [supported] region.[132]
	CTF 1000	Provide cryptologic services. (Full mission statement of this unit is not released to the general public.)

Table 4. Major FLTCYBERCOM Cyberspace-Related Units (cont.)

FLTCYBERCOM contributes 40 teams to the CMF: 4 NMTs, 3 NSTs, 8 CMTs, 5 CSTs, and 20 CPTs. As of April 2017, 26 of the teams were at full operational capability, with the remaining 14 projected to reach full operational capability ahead of the October 2018 target. Plans are also in place to add 298 cyber reserve

billets by October 2017 that are individually aligned to augment DCO capabilities for CPTs and JFHQ-C, as well as to support possible surge efforts. In February 2017, FLTCYBERCOM formed an interim Cyber Forward Element in Hawaii to support the maturing capabilities and capacity of its JFHQ-C that supports U.S. Pacific Command (USPACOM). This will enable command and control of not only the Navy CMF teams of the JFHQ-C, but also the three Air Force and two Army CMF teams assigned to it.[133]

The skill specialty areas of FLTCYBERCOM personnel match the diversity of its operational organizations. The Navy established the Information Dominance Corps in 2009 as their vehicle "to dominate the modern information-related disciplines of intelligence, cyber, networks, space, oceanography, meteorology, and electronic warfare."[134] Enlisted ratings within this corps that are related to CO include several in the Cryptologic Technician series: Interpretive, Maintenance, Networks, Collection, and Technical. Also included in the enlisted positions are Intelligence Specialist and Information Systems Technician.

Potential CMF members also include Navy chief warrant officers in several specialty series: 781X Information Warfare Technician, 782X Information Systems Technician, 783X Intelligence Technician, and 784X Cyber. Naval officers who may lead various cyberspace activities are the 1810 Cryptologic Warfare Officer and 1840 Cyber Warfare Engineer as well as 1820 Information Professional and 1830 Intelligence Officer. Appendix IV provides job descriptions for the key Navy cyber-related personnel within the Information Dominance Corps. Despite fierce competition for cyberspace expertise and leadership among government and industry, Gilday reported in May 2017 that current reenlistment bonuses and supplemental pay

measures were effective in achieving retention goals for enlisted members and that cyberspace-related officer retention was at 93 percent.[135]

Training

Mandatory joint certification standards inform current CMF training which is currently provided by USCYBERCOM and the National Security Agency. The Navy is working with the other services to build joint cyber training capabilities that could serve individual and team needs.[136] One of the greatest Navy contributions to joint cyberspace training is its administration of the Joint Cyber Analysis Course (JCAC), which is the initial training for many joint cyberspace operators. Comprised of 10 modules that cover 25 cyber topics, JCAC "is designed to take individuals who have minimal computer experience and make them proficient in cyber-analysis within 6 months."[137] For team proficiency training and certification, FLTCYBERCOM leverages opportunities such as Cyber Flag; for example, three of its CMF teams participated in the recent Cyber Flag 17.[138]

To foster continuous improvement in its information dominance forces, to include cyberspace operators, NAVIFOR established the Naval Information Warfare Development Command in 2017 "to advance the maturing of Information Warfare, including cyberspace operations, doctrine, training, Tactics, Techniques and Procedures."[139] The Naval Information Warfare Development Command and its focus on warfighting innovation have led some to liken it to be the "Top Gun" for information warfare. It uses high-intensity activities like its Composite Training Unit Exercises to certify that units are ready to operate in contested cyber environments.[140] The Naval Information Warfare

Development Command reached initial operating capability in March 2017, and is projected to reach full operational capability by April 2019.[141]

Equipping

FLTCYBERCOM looks to the Space and Naval Warfare Systems Command to acquire and sustain cyberspace-related capabilities and systems. Space and Naval Warfare Systems Command actively supports Cybersecurity Safety (CYBERSAFE), a program that emerged from TFCA efforts that concentrate on developing strict cybersecurity standards across Navy networks and platforms. In 2016, Space and Naval Warfare Systems Command finalized the first eight of these standards that build upon those of the National Institute of Standards and Technology.[142]

To adapt to the dynamic cyberspace environment, the Navy's Program Manager, Warfare 130, Information Assurance and Cyber Security Program Office was established in July 2010 with a goal "to rapidly and proactively field innovative capabilities that will keep the Navy ahead of the cyber threat."[143] The top programs of Program Manager, Warfare 130 include cryptography and key management, network security, and cyber analytics.[144] Looking toward the future, the Navy is looking to leverage automation in the form of artificial intelligence and cognitive computing to better understand activities inside warfighting networks.[145]

AIR FORCE SERVICE CYBERSPACE COMPONENT

The U.S. Air Force was the first military service to fully embrace CO, forming the Air Force Cyber Command (Provisional) in September 2007.[146] In 2008, Air Force Space Command was designated as the service

lead to organize, train, and equip cyberspace forces. Air Force Cyberspace Command (AFCYBER) and 24th Air Force were established in August 2009, reached initial operating capability in January 2010, and was declared fully operational in September 2010. AFCYBER is headquartered at Joint Base San Antonio-Lackland and reports to Air Force Space Command, Peterson Air Force Base, CO.[147] Like other service cyberspace components, AFCYBER is the service CSSP and operates a JFHQ-C. Unique responsibilities of the Air Force include serving as Executive Agent for the DoD Cyber Crime Center which includes responsibility for the Defense Industrial Base (DIB) Cyber Security Activities.[148] There have been five AFCYBER commanders, all major generals: Richard E. Webber (August 2009-April 2011); Suzanne M. Vautrinot (April 2011-June 2013); James Kevin McLaughlin (June 2013-July 2014); Burke Wilson (July 2014-July 2016); and Chris P. Weggeman (July 2016-present). It is of interest to note that McLaughlin was selected to become deputy commander of USCYBERCOM in August 2014.

Mission

> The 24th Air Force Commander also serves as the Service Cyber Component Provider to United States Cyber Command. As Air Forces Cyber (AFCYBER), its' [sic] mission is 'American Airmen delivering full-spectrum, global cyberspace capabilities and effects for our Service, the Joint Force, and our Nation.' Through daily cyber tasking orders, AFCYBER directs units around the world to conduct cyberspace operations across six Lines of Effort; Build, Operate, Secure and Defend the Air Force Information Network (AFIN) and directed mission critical cyber terrain, Extend cyber capabilities to the tactical edge of the modern battlefield and Engage the adversary in support of combatant and air component commanders.[149]

Consistent with his fellow service cyberspace component commanders, Weggeman stated in his May 2017 Senate testimony that the defense of DoD and Air Force networks is the number one mission of AFCYBER. The implementation of this mission includes AFCYBER's role as the CSSP for the Air Force Network (AFNET) as well as for the Air Force Information Network (AFIN) portion of the DODIN. He also described three transformational initiatives that support this priority. The first is the Air Force Information Dominance Platform, which is a network architecture that improves performance and reliability as well as enhances system vulnerability management and incident response. Air Force Information Dominance Platform implementation will proceed in concert with the JRSS migration efforts led by the Defense Information Systems Agency. The second initiative is the Cyber Squadron Initiative to apply active cyber defense using Cyber Mission Defense Teams that help unit commanders mitigate risks to their critical missions. In 2014, the 50th Space Communications Squadron served as the successful vanguard of this program.[150] The third initiative is the Cyber Resiliency of Weapons Systems, which is a program to improve cyber resiliency to existing and new weapon system acquisition and sustainment.[151]

With regard to the support of warfighter CO, Weggeman's *Commander's Strategic Vision* stated his top strategic priorities for AFCYBER as: "Employ Multi-Domain and Integrated Cyberspace Capabilities in support of Combatant and Air Force Component Commanders."[152] AFCYBER operations follow a Cyber Tasking Cycle process similar to that used to generate Air Tasking Orders for air operations. The 624th Operations Center implements the process to develop Cyber Tasking Orders that task cyberspace forces.[153] To

conduct the required CO, the Air Force has seven standard cyberspace weapons systems available that are summarized in table 5. In July 2015, AFCYBER established the Cyberspace Multi-Domain Innovation Team in part to better address operations in anti-access/area denial (A2/AD) environments through the integration of CO; intelligence, surveillance, and reconnaissance; and EW capabilities to deliver multi-domain capabilities.[154]

Cyberspace Weapon System Name	Description*
Cyberspace Defense Analysis (CDA) (17XX suffix A)	Conducts Defensive Cyberspace Operations by monitoring, collecting, analyzing, and reporting on sensitive information released from friendly unclassified systems, such as computer networks, telephones, email, and USAF websites. (p. 8)
Cyber Security and Control System (CSCS) (17XX suffix B)	Provide 24/7 network operations and management functions and enable key enterprise services within Air Force unclassified and classified networks . . . [and support] defensive operations within those Air Force networks. (p. 8)
Air Force Intranet Control (AFINC) (17XX suffix C)	[Serves as] the top level boundary and entry point into the Air Force Information Network (AFIN), and controls the flow of all external and interbase traffic through standard, centrally managed gateways. The AFINC weapon system consists of 16 Gateway Suites and two Integrated Management Suites. (p. 8)
Cyberspace Vulnerability Assessment/ Hunter (CVA/Hunt) (17XX suffix D)	Executes vulnerability, compliance, defense and non-technical assessments, best practice reviews, penetration testing and Hunter missions on AF and DoD networks & systems. Hunter operations characterize and then eliminate threats for the purpose of mission assurance. The weapon system can perform defensive sorties world-wide via remote or on-site access. (pp. 8-9)
Cyber Command and Control Mission System (C3MS) (17XX suffix E)	[Synchronized] other AF cyber weapon systems to produce operational level effects in support of Combatant Commanders worldwide. C3MS provides operational level Command and Control (C2) and Situational Awareness (SA) of AF cyber forces, networks and mission systems. C3MS enables the 24th Air Force Commander (24 AF/CC) to develop and disseminate cyber strategies and plans, then execute and assess these plans in support of AF and Joint warfighters. (p. 9)
Air Force Cyberspace Defense (ACD) (17XX suffix F)	Prevent, detect, respond to, and provide forensics of intrusions into unclassified and classified networks. This weapon system supports the AF Computer Emergency Response Team in fulfilling their responsibilities. (p. 9)
Network Attack System (NAS) (17SX suffix G)	(Details of this system are not releasable to the general public)
*Descriptions are excerpted from U.S. Air Force, *AFSC 17X Cyberspace Operations Officer, Career Field Education and Training Plan*.	

Table 5. Air Force Cyberspace Weapon Systems[155]

Organization

The major units assigned to AFCYBER are two Cyberspace Wings and one Combat Communications Group. Each wing has three operations groups, which in turn have several numbered squadrons that focus on different aspects of the overall cyberspace mission. Table 6 lists these major units as well as their mission statements.

Unit	Mission	Joint Cyberspace Mission Focus
67th Cyberspace Wing (Joint Base San Antonio, TX)	. . . executes a full range of cyber operations including the integrated planning and employment of military capabilities to achieve desired combat effects across the interconnected analog and digital portion of the Battlespace-Air Force Network Ops. Comprised of over 2,500 Airmen, civilians, and contractors across three Operations Groups with 31 units at 17 worldwide locations, the 67th CW employs 5 cyberspace weapon systems conducting global network operations, defensive cyberspace operations, and offensive cyberspace operations in support of Air Force, Joint Force Commander, and Combatant Commander taskings.[155] Major subordinate units: 26th Cyberspace Operations Group 26th Cyberspace Operations Group 67th Cyberspace Operations Group (Kelly Field Annex, TX) 690th Cyberspace Operations Group (Joint Base San Antonio, TX)[156]	DODIN, DCO, OCO
688th Cyberspace Wing (Joint Base San Antonio, TX)	. . . executes a diverse mission set of cyberspace capability development, test, and assessment; develops and validates cyber tactics; integrates cyber into Air Force Warfare Center training events; employs cyber protection teams to defend priority Department of Defense networks and systems against priority threats; and operates the Air Force cyber and information operations formal training units.[156] Major subordinate units: 38th Cyberspace Engineering Installation Group (Tinker Air Force Base, OK) 318th Cyberspace Operations Group (Joint Base San Antonio, TX) 688th Cyberspace Operations Group (Scott Air Force Base, IL)[157]	DCO

Table 6. Major AFCYBER Units

Unit	Mission	Joint Cyberspace Mission Focus
5th Combat Communications Group (Joint Base San Antonio-Lackland, TX)	Extend tactical cyberspace capabilities at the speed of need for the Joint Force and the Nation. . . . The group's two combat communications mission squadrons and one support squadron deploy in support of joint task force, combatant command, and Air Force flying wing operations and exercises. The 5 CCG also serves in an advisory capacity for two Air National Guard combat communications groups and Air Force Reserve Combat Communications squadrons with more than 2,500 people in subordinate squadrons located throughout the United States. [158]	DCO
624th Operations Center (Joint Base San Antonio-Lackland, TX)	. . . serves as the command and control element of the 24th Air Force. Its mission is to 'Command and Control cyberspace forces: Operate, Defend, and Engage.' The 624 OC consists of four divisions: Intelligence, Surveillance, and Reconnaissance, Combat Plans, Combat Operations, and Strategy and reports directly to the 24th Air Force Commander. The 624 OC receives orders and tasks from United States Cyber Command and in turn tasks 24th Air Force subordinate units to perform a wide range of cyber missions in support of Air Force and joint force commanders.[159]	

Table 6. Major AFCYBER Units (cont.)

AFCYBER contributes 39 teams to the CMF: 4 NMTs, 2 NSTs, 8 CMTs, 5 CSTs, and 20 CPTs. As of May 2017, over 50 percent of AFCYBER teams were at full operational capability, and the remaining teams should be at the operational capability by the end of FY 2018. There are also five total force CMF teams: two Air National Guard CPTs and three Air Force Reserve CPTs.[160] AFCYBER uses a force employment methodology of cyber force packages that allow more flexibility in employment.[161] Thus, the 2 Air National Guard CPTs are manned by personnel from 12 Air National Guard squadrons.[162]

The Air Force has three military personnel classifications that explicitly involve CO and thus are authorized to wear the CO badge. For officers, the cyberspace specialties are Network Operations (17DX) and Cyber

Warfare Operations (17SX); the specialty codes include suffixes to indicate the specific cyber weapon systems they operate (see Appendix V for details). Of interest is the fact that only the 17SX suffixes include network attack systems and OCO platforms.[163] For enlisted members, the operational specialty is Cyberspace Warfare Operations (1B4X1). There are also several other enlisted specialties that are authorized to wear the cyberspace support badge; they include Cyber Systems Operations (3D0X2), Cyber Surety (3D0X3), Computer Systems Programming (3D0X4), and Cyber Transport Systems (3D1X2). Appendix V provides the job description for the Air Force cyberspace operational and support specialties.

Training

In his 2016 *Cyber Defense Review* article, then-AFCYBER commander Major General Ed Wilson provided a concise summary of his command's training process:

> Today, we operate a training pipeline with Undergraduate Cyberspace Training delivered by our Air Education and Training Command (AETC), and weapons system Initial Qualification Training, which is at our user command Field Training Unit (FTU). More specialized Mission Qualification Training is conducted either at the FTU or the gaining unit, which complements the training and mission certification of our intelligence specialists inbound to our cyber units.
>
> A critical step towards normalizing cyberspace operations is the continued incorporation of advanced concepts in technical training school, which better equips our Airmen for the challenges they face in an increasingly contested operating environment.[164]

AFCYBER crew training is a continuous and progressive process, hence the command established a Ready Cyber Crew program to ensure operators not only maintain their DoD certification requirements but also increase their proficiency and mission effectiveness.[165]

To support this process, the 328th Weapons School established the Cyber Weapons Instructor Course at Nellis Air Force Base, NV, and graduated its first class of eight cyber warfare officers in June 2012.[166] The implementation of the Cyber Weapons Instructor Course is a significant step in the full integration and normalization of CO with the more traditional Air Force weapons training related to fighter and bomber aircraft. Evidence of this progress can be found in the increasing role that CO plays in capstone Air Force combat exercises, such as the recent Red Flag 17-1 at Nellis Air Force Base during January and February 2017. Since the first incorporation of a distributed virtual simulation capability in Red Flag 15-2 (March 2015), "the multi-domain exercise is evolving to include more realistic scenarios by increasing the use of cyber capabilities and other non-kinetic effects in planning and warfighting."[167]

Equipping

To support the cybersecurity and resilience of new and existing weapons systems acquisition, the Air Force established the Weapons Systems Cyber Resiliency program. The program adopts a multipronged approach to achieve mission assurance, system assurance, and resilience of Air Force operations and sustainment. The Weapons Systems Cyber Resiliency program is part of the larger Air Force Cyber Campaign

Plan, a program with two major goals: "1) to 'bake in' cyber resiliency into new weapon systems and 2) mitigate critical vulnerabilities in fielded weapon systems."[168] The Cyber Campaign Plan is administered by the Cyber Resiliency Office for Weapon Systems organization across seven lines of actions, and it addresses cyber resiliency related to critical infrastructure.[169]

The AFCYBER *Commander's Strategic Vision* includes a strategic priority to "Equip the Force through Rapid, Innovative Fielding of Cyber Capabilities."[170] The Air Force Life Cycle Management Center is a partner toward this goal through the Rapid Cyber Acquisition and Real Time Operations and Innovation initiatives. These programs include streamlined contract and budgeting authorities that significantly reduce the time to procure cyberspace systems. The establishment of the Cyber Proving Ground in 2016 provided further resources for Air Force engineers and acquisition personnel to aid cyberspace operators in developing and testing new systems. During 2017, the Cyber Proving Ground helped to accelerate development and fielding of cyberspace capabilities to protect the Air Force Satellite Control Network as well as to provide "two unique capabilities" to support JTF-ARES.[171]

COAST GUARD SERVICE CYBERSPACE COMPONENT

> The mission of the United States Coast Guard Cyber Command (CGCYBERCOM) is to identify, protect against, and counter electromagnetic threats to the maritime interests of the United States, provide cyber capabilities that foster excellence in the execution of Coast Guard operations, support DHS Cyber missions, and serve as the Service Component Command to US Cyber Command.[172]

The U.S. Coast Guard's Vision for Operating in the Cyber Domain: *We will ensure the security of our cyberspace, maintain superiority over our adversaries,* and safeguard our Nation's critical maritime infrastructure* [emphasis and italics in original].[173]

Coast Guard Cyber Command (CGCYBERCOM) was established at full operational capability in 2013 with operational responsibilities to both the DoD and DHS. In 2015, CGCYBERCOM set three strategic priorities to guide its development until 2025: Defending Cyberspace, Enabling Operations, and Protecting Infrastructure. Its operational fortes include protection of the Maritime Transportation System and the U.S. maritime critical infrastructure, both of which are vital to the economic, political, and military elements of U.S. national power. CGCYBERCOM has unique law enforcement authorities that allow it to partner well with DHS, the FBI, and other federal government entities as well as with foreign governments.[174]

With regard to its Defending Cyberspace priority, the January 2017 Memorandum of Agreement between DoD and DHS directed that CGCYBERCOM "will adhere to DoD cybersecurity requirements, standards, and policies," and will be responsible for Coast Guard-operated [DODIN] systems.[175] CGCYBERCOM does not have JFHQ-C responsibilities, but it will make a contribution to the CMF. CGCYBERCOM formed an initial CPT in February 2017, which is planned to comprise 39 personnel when completed in 2019. The CPT conducted its first joint operation in May 2017 and a squad formed in August 2017 "to perform missions as part of DHS hunt and incident response teams for dotgov and dotcom incidents, including industrial control systems for national critical infrastructure."[176] To support the development of its cyberspace force, the Coast Guard formed the Office of Cyberspace Forces

(CG-791) in March 2017 to lead the effort to organize, train, equip, develop operational policy, and administer programmatics.[177] In May 2017, CGCYBERCOM stood up its Battle Bridge that serves as the operations center for Coast Guard CO. Located near Headquarters, Coast Guard in Washington, DC, the Battle Bridge is part of the larger and distributed Coast Guard Network Operations and Security Center (NOSC) that combines three previous network operations and defense functions into a unified force.[178]

JOINT CYBERSPACE MISSION SUPPORT COMPARISON AND FINDINGS

Having reviewed each service cyberspace component separately, let us now examine how they collectively support common missions as well as contrast how this support may differ in certain ways. This section does not present a comprehensive analysis of all capabilities that may support CO. Rather, it provides a qualitative survey of several issues of interest to joint CO. Although CGCYBERCOM provides valuable support to warfighters, we will not address their contributions in this section, since they provide less than 1 percent of the CMF and do not operate a JFHQ-C.

With the addition of the Coast Guard's CPT, the total active CMF stands at 134 teams. Table 7 lists the CMF contributions of each service cyberspace component broken out by team type. The mission workload is distributed equally among Army, Navy, and Air Force with each having about 30 percent of the CMF and the Marine Corps providing the other 10 percent. The number of specific teams in each service follows the same pattern of distribution. Collectively, CPTs comprise just over half of the teams in the CMF.

Active Service Component	Total CMF Teams	Cyber National Mission Force		Cyber Combat Mission Force		Cyber Defense
		NMT	NST	CMT	CST	CPT
Army	41	4	3	8	6	20
Marine Corps	13	1	0	3	1	8
Navy	40	4	3	8	5	20
Air Force	39	4	2	8	5	20
Coast Guard	1	0	0	0	0	1
Total	134	13	8	27	17	69
Total Force: National Guard (NG) and Reserve Contributions						
Army NG	0	0	0	0	0	11
Army Reserve	0	0	0	0	0	10
Air NG	1	0	0	0	0	2
Air Force Reserve	0	0	0	0	0	3

Table 7. Service Contributions to Cyber Mission Force[179]

All of the services are incorporating total force elements into their CO organizations. Table 7 also lists the National Guard and Reserve teams identified by the Army and Air Force as augmentation to the CMF. Thus far, the Army's teams are operated as separate units in one state. In contrast, some Air Force teams are built from elements of several squadrons that may be located in different states.[180] The current Navy plan is to have 298 Reserve billets that are aligned with specific active CPTs vice being organized as separate teams. Assuming an average CPT size of 39 personnel, the Navy billets are equivalent to over 7 CTPs.

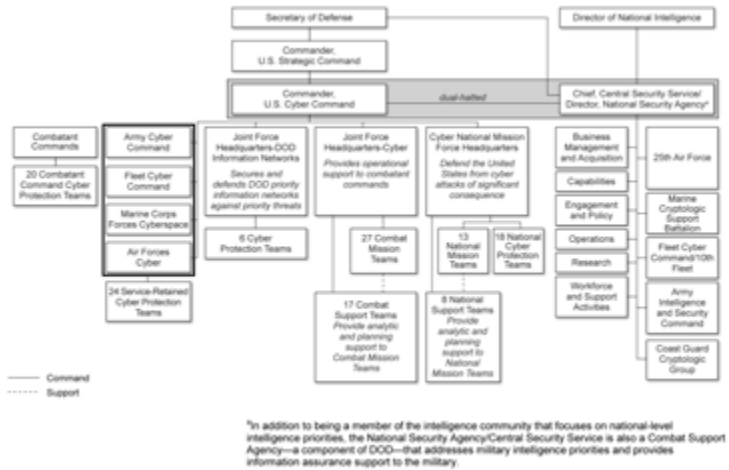
CMF teams are assigned to five types of command elements within USCYBERCOM: Headquarters Cyber National Mission Force (HQ CNMF), JFHQ-C, JFHQ-DODIN, combatant commands, and services. Table 8 presents the distribution of CMF teams to each of these areas, and figure 5 portrays these elements in a

traditional organizational hierarchy chart. Almost one-fourth of the total CMF is dedicated to protect military networks, with services retaining 24 CPTs (18 percent of the CMF) under their command for this mission and another 6 CPTs (5 percent of the CMF) commanded by JFHQ-DODIN. Headquarters CNMF located at Fort Meade, MD, controls a composite of 39 teams (29 percent of the CMF) from all services assigned to CO related to defense of the U.S. homeland. The CNMF also partners extensively with the National Security Agency, DHS, the FBI, and the intelligence community.[181] Collectively, combatant commands have almost half of the CMF assigned to support them—20 CPTs (15 percent of the CMF) under their direct command as well as another 44 teams (33 percent of the CMF) commanded by the 4 service JFHQ-Cs. Since these forces are joint by design, they may each contain CMF teams from more than one service component. The assignment of combatant commands to JFHQ-C is as follows:

- JFHQ-C MARFORCYBER: U.S. Special Operations Command;
- JFHQ-C ARCYBER: U.S. Northern Command, U.S. Central Command, and U.S. Africa Command;
- JFHQ-C FLTCYBER: U.S. Pacific Command and U.S. Southern Command; and,
- JFHQ-C AFCYBER: U.S. European Command, U.S. Strategic Command, and U.S. Transportation Command.[182]

Organization	CMF Teams Commanded	Percent of Total CMF
JFHQ-C	27 CMTs + 17 CSTs	33%
HQ CNMF	13 NMTs + 8 NSTs + 18 CPTs	29%
Services	24 CPTs	18%
Combatant Commands	20 CPTs	15%
JFHQ-DODIN	6 CPTs	5%

Table 8. Command of CMF Teams in USCYBERCOM[183]



Source: U.S. Government Accountability Office.

Figure 5. Organizational Chart of the Leadership Arrangement for the National Security Agency, Central Security Service, and U.S. Cyber Command[184]

The unique lexicons and operational structures that help to define different service cultures are apparent in several forms within the service cyberspace component commands. Table 9 summarizes some examples of how service-unique influences manifest in their

cyberspace components. While each service's cyberspace doctrine is consistent with JP 3-12 tenets, different service paradigms are developed to integrate cyberspace with other activities, such as EMS operations, space operations, EW, and IO. These paradigms are usually designed to best support the service's typical combat unit—for example, the Brigade Combat Team (BCT) for the Army or MAGTF for the Marines.

Service	Service DODIN Segment	Core Service Combat Structures	Cyber-related Doctrinal Paradigms
Army	LandWar Net	Brigade Combat Team (BCT), Corps	CEMA, CSCB
Marine Corps	MCEN	MAGTF	CEWCC
Navy	Navy Marine Corps Internet	Task Force, Carrier Strike Group	Information Dominance
Air Force	AFNET, AFIN	Fighter or Bomber Wing	CMIT

Table 9. Service-Unique Influences on Cyberspace Components

All services are facing challenges in recruiting and retaining qualified cyberspace troops, such as those listed in table 10. Retention tools currently in use for officers and enlisted personnel include Selective Reenlistment Bonus, Special Duty Assignment Pay, and Assignment Incentive Pay. The DoD caps Selective Reenlistment Bonus payments at $25,000, and Special Duty Assignment Pay and Assignment Incentive Pay ranged between $350 and $800 per month in FY 2015. Although these incentives may seem expensive, they can offset the costs of training new personnel. A 2017 Government Accountability Office report cited a service estimate of these costs to range from $23,000 to over $500,000 depending on how much specialized training is required.[185] Another potential mitigation effort for

the CMF staffing challenge is to incorporate more civilian positions on CMF teams. A 2016 study from the Institute for Defense Analyses concluded that such a change has the potential to save as much as $130 million annually without compromising DoD standards. The study accounted for the requirement to maintain military personnel in positions that may involve direct participation in cyber hostilities. The Navy and Army would have the most to gain from this change since the Air Force and Marine Corps CMF teams already include a significant amount of civilians.[186]

Officer	Warrant Officer	Enlisted
ARMY		
17A Cyber Operations Officer (29 Electronic Warfare)	170A Cyber Operations Technician	17C Cyber Operations Specialist 25D Cyber Network Defender 25U Signal Support Sys Specialist 35T Military Intel Sys Maintainer 35Q Cryptologic Network Warfare Spec
MARINE CORPS		
0605 Cyber Network Operator Officer	0650 Cyber Network Operations Engineer	0651 Cyber Network Operator 0659 Cyber Network Systems Chief 0681 Information Security Technician 0689 Cyber Security Chief
NAVY		
1810 Cryptologic Warfare 1820 Information Professional 1830 Intelligence 1840 Cyber Warfare Engineer	781X Information Warfare Technician 782X Information Sys Technician 783X Intelligence Technician 784X Cyber	27XX Information Systems Technician Cryptologic Technicians (various types) Intelligence Specialist
AIR FORCE		
17C0 Cyberspace Ops Commander 17DX Network Operations 17SX Cyber Warfare Operations	Not Applicable	1B4X1 Cyberspace Warfare Operator

Table 10. Key Service Cyberspace Personnel Designations[187]

The CMF should achieve full operational capability in FY 2018 and be ready to meet today's needs, but what challenges might the future CMF face? The Army and Marine Corps are working together to develop the concept of Multi-Domain Battle (MDB) as "an approach for ground combat operations against a sophisticated peer enemy threat in the 2025-2040 timeframe."[188] MDB anticipates that future adversaries will likely "degrade key capabilities by limiting access to space, cyberspace, and the electromagnetic spectrum" as part of A2/AD operations.[189] Thus, MDB places greater emphasis on CO, IO, and EMS operations to help ensure synchronization capabilities that enable effective combined arms activities.[190] In their 2017 article in *Cyber Defense Review*, Lieutenant General Nakasone and Major Charlie Lewis argue that the defense of joint networks is a foundation of MDB, noting, "fortifying the network affords commanders opportunities in other domains by enabling mission command."[191] They also explain how CO can contribute to the MDB tenet of using operations in one domain to open temporary windows of advantage in other domains. Indeed, the 2012 *Joint Operational Access Concept*, which provides a vision for the joint force to counter adversary A2/AD capabilities, states that because of this critical enabling role, "cyberspace operations likely will commence well in advance of other operations."[192]

What cyberspace-related capabilities may be required to help make concepts like MDB a reality? One of the greatest limitations of using cyberspace weapons against a sophisticated adversary is that they may be effective only once before the foe corrects the vulnerability exploited by the tool.[193] Consequently, it would be advantageous to have an agile acquisition process to replace the cyber "rounds" as they are expended. The existing rapid acquisition of cyberspace

capabilities of each service could be enabled by the DoD test community to help ensure the effectiveness of the weapon in a controlled cyber range. The DoD cybersecurity test community includes facilities and units from all services that could support such rapid development and testing.[194]

RECOMMENDATIONS

The four service cyberspace component commands that report to USCYBERCOM have less than a decade of development and operational experience. Considering this, their collective capabilities are impressive, and their value to joint and coalition warfighters continues to grow as the domain of cyberspace becomes more contested. To help guide the further progress of these forces, please consider the following recommendations.

Recommendation 1

The Army G-3/5/7 should fully embrace the responsibilities and opportunities related to its designation as DoD Executive Agent for Cyber Training Ranges.

In March 2016, Deputy Secretary of Defense Robert Work designated the Secretary of the Army as the DoD Executive Agent for Cyber Training Ranges, who in turn delegated the task to the Army Deputy Chief of Staff G-3/5/7.[195] The implementation of this activity will require close coordination with DoD components and the services to properly balance range requirements, usage, and cost efficiency. Further, this position will require cooperation and collaboration with the DoD Director, Test Resources Management Center, who was designated as the Executive Agent

for DoD Cyber Test Ranges. The interaction between the roles of these two executive agents is significant enough that the Director, Operational Test and Evaluation (DOT&E) has strongly recommended for years that there be a single Executive Agent for both sets of ranges.[196]

Recommendation 2

The Army should continue to develop and implement professional development courses focused on building leaders and elite forces in the Cyber branch. The ongoing challenges to fill critical Army cyber billets may cause a reasonable myopia toward the mere recruitment, training, and retention of qualified candidates. However, as the fledgling Cyber branch continues to mature, it should do so with a holistic vision for the branch that strives to keep cyber officers and noncommissioned officers on a path that not only builds their technical prowess, but also instills the aptitudes and values common to all Army leaders. The 2013 Army Cyber Institute publication, *Professionalizing the Army's Cyber Officer Force*,[197] provides such a roadmap, albeit one developed before the Cyber branch was established. With regard to the cyber abilities, it may be valuable to build a course designed to create an elite set of operators through enhanced and concentrated training. This may take the form of a Cyber Leader course similar to Ranger school (tab and all) as proposed in detail in the 2014 Army Cyber Institute report, *Toward a Cyber Leader Course: Not for the Weak or Faint Hearted*.[198]

Recommendation 3

The DoD and the Army should implement DOT&E recommendations to pursue a more holistic approach to cybersecurity and network operations.

Based on 7 years of conducting operational cybersecurity assessments on DoD networks and weapons systems, DOT&E recommended in its *FY 2016 Annual Report* that "the focus of cyber defense needs to expand beyond the traditional approaches of system protection and intrusion detection to encompass a broader view of system resilience."[199] DCO improvements could include less emphasis on perimeter defense and more emphasis on detecting and mitigating anomalous activity within the network, especially those indicative of advanced persistent threats. One means to enable this evolution in network defense is the use of Persistent Cyber Opposing Forces (PCO), a capability that USPACOM used during FY 2015 to identify and address mission critical vulnerabilities.[200] The efforts of PCO teams could be further enhanced if they were part of an overarching and ongoing assessment plan, such as the Cyber Assessment Master Plan method facilitated by DOT&E. A combatant commander can use a Cyber Assessment Master Plan to identify and implement a 3-year plan to systematically identify and assess their priority missions in a contested cyberspace environment.[201]

Recommendation 4

The DoD and the Army should continue to leverage appropriate expertise outside the military to augment their cyberspace planning, operation, and capability development.

DoD and Army leaders should recognize and accept the pragmatic reality that keeping organic cyberspace forces for the long term will remain very difficult in the competitive cyberspace market. They should continue to leverage external experience through National Guard and Reserve components as well as develop and maintain partnerships with federal and state agencies and departments to best utilize the resources available. Such collaborations may extend to allies and other international entities as appropriate. To better meet the unique cyberspace capability materiel requirements, cyberspace forces should take advantage of opportunities afforded by the Defense Innovation Initiative.[202]

Recommendation 5

Future updates of joint and Army cyberspace doctrine should explicitly address the missions and structures of CMF teams and JFHQ-C.

JP 3-12 was released in February 2013 when the details of CMF composition were still being worked, so the absence of any CMF references is understandable. However, FM 3-12 was released in April 2017 at which time over 80 percent of the Army's CMF teams had reached full operational capability, yet it did not provide any details on the their structure or use for service or joint missions. Considering the stated purposes of FM 3-12 to include joint operations, the CCoE lost a great opportunity to educate Army personnel writ large on how Army CMF teams operate and how the Army JFHQ-C supports combatant command operations; these significant oversights should be made a priority to correct.

Recommendation 6

ARCYBER and the Cyber CoE should work with the other service cyberspace components and the Joint Staff to explicitly communicate and clarify how each service is integrating CO with related activities.

It is unlikely that the services will reach consensus regarding how the roles and responsibilities of cyberspace forces interface and interact with forces that perform information operations, EW, EMS management, space operations, and other similar activities. Since many CO are expected to be joint operations, it may enhance the unity of effort for organizations such as the various JFHQ-Cs if its members all understood the commonalities and differences between service-unique constructs, such as the Army CEMA and Marine Corps CEWCC. One way to enable a better understanding of the different paradigms that describe how these capabilities overlap is to develop a living document that reports and compares how each service structures this synthesis.

Recommendation 7

The Army should work deliberately to have its leaders and Soldiers understand and regard cyberspace activities as an integral part of combat operations.

The *FY 2016 Annual Report* of the DoD DOT&E summarizes observations from 7 years of observing the evolution of service and joint cyberspace testing and exercises. In this summary, they noted, "DOD personnel too often treat network defense as an administrative function, not a warfighting capability."[203] A key symptom of this problem is the incongruity with how

cyberspace activities are often waved off in DoD exercises, especially the "reluctance to permit debilitating cyber attacks." Although the situation has improved as cyberspace forces mature in their capabilities and proficiency, willingly allowing an exercise environment that does not model the effects expected in the real world serves no one well. The DOT&E report admonished that "training in a benign environment is not acceptable in any other warfighting domain, nor should it be for cyber."[204] Former ARCYBER commander Lieutenant General Edward Cardon reflected in a 2016 *Cyber Defense Review* article on the ongoing progress the Army is making with fully embracing the concept of cyberspace maneuver as an integral part of combined arms maneuver, perhaps even as the supported element in the future. Looking toward future Army operations, he notes:

> ultimately, before the synergy of maneuver across cyber and land domains can be achieved, cyberspace operations will need to be normalized as a regular warfighting capability, and within a commander's vision of the battlefield.[205]

Recommendation 8

The DoD and the Army should promulgate the exploration and characterization of cyberspace as well as the development of theories of CO at the tactical, operational, and strategic levels.

While the operational structure and resources dedicated to military CO have progressed at a steady pace since the establishment of USCYBERCOM, this progress has proceeded largely along existing doctrinal lines. That is to say, the analysis and characterization

of cyberspace are often forced to fit within the relatively narrow confines of paradigms based on the physical limitations of land, sea, air, space, EMS, and human cognition. One can argue that cyberspace is the only domain that is ever expanding in its virtual size and complexity and is doing so at a rate that may defy human comprehension. Given this, the DoD and the Army should implement the systematic and continuous mapping and analysis of the realm of cyberspace to provide a more realistic model of its environment and the activities that are possible within it.

This enduring exploration of cyberspace should be guided by sound theory of the human exploitation of the domain as well as the tactical, operational, and strategic implications.[206] In turn, the results of the exploration should inform and refine these theories. Certainly, the process of such cyberspace investigation and theory development may be left to the random fortune of uncoordinated workshops, conferences, and articles (or even monographs such as this).[207] However, given the inherent opportunities and risks that wait to be discovered, a path of purposeful ignorance does not serve the nation well.[208]

Recommendation 9

The DoD and the Army should encourage open dialogue regarding the future evolution of military cyberspace missions, authorities, and organizational structures.

Even as USCYBERCOM begins its new journey as a unified combatant command—an elevation from sub-unified status that is not without controversy—some well-informed military experts assert that this may not provide sufficient authorities for future cyberspace

forces. In a 2014 *Proceedings* article, Admiral (retired) James Stavridis and Davis Weinstein examine the merits of creating a U.S. Cyber Force as "a stand-alone force [that] would eliminate both the unity-of-command problem and the interservice rivalries."[209] Further, they envision this new Cyber Force to "be smaller in size than the Marine Corps with comparatively low physical-fitness standards and noticeably relaxed grooming standards."[210] Since the current military establishment may not be ready for this rather radical proposal, a more reasonable step toward improved unity of effort in cyberspace is to establish a Joint Force Cyberspace Component commander akin to similar joint force component commanders for the land, maritime, and air domains.[211]

CONCLUDING REMARKS

The first 7 years of U.S. Cyber Command operations are paved with milestones that mark the steady operationalization of modern cyberspace as the newest domain of military conflict as well as a realm of international power. The creation of the CMF and JFHQ-C are significant steps toward improving the timeliness and effectiveness of CO that directly support combatant commands and the whole-of-government responses to cyberspace threats.

This monograph shows that the current paradigm of how the service cyberspace component commands operate is a mixture of common joint practices and service-unique means and methods. If properly balanced, the operational fusion of this somewhat dissimilar force may yield a synergy that enhances unity of effort through standardization as well as exploits the distinct strengths of each service. The Army has made great

strides through efforts such as the establishment of the Cyber branch and CCoE. Yet, greater opportunities await sage leaders who can embrace the worthy traditions of Landpower while having the courage to recognize and promulgate the inevitable—and perhaps fantastic—implications for these traditions emerging from the rapidly evolving domain of cyberspace.

ENDNOTES

1. Department of Defense (DoD), *The DoD Cyber Strategy,* Washington, DC: The Government Printing Office, April 2015, p. 3.

2. "U.S. Cyber Command (USCYBERCOM)," factsheet from U.S. Strategic Command website, available from *http://www.stratcom.mil/Portals/8/Documents/CYBERCOM_Fact_Sheet.pdf*, accessed December 7, 2018.

3. Statement of Admiral Michael S. Rogers, Commander, United States Cyber Command, before the Senate Committee on Armed Services, U.S. Senate, First Session, 115th Congress, May 9, 2017, available from *http://www.armed-services.senate.gov/imo/media/doc/Rogers_05-09-17.pdf*, accessed August 30, 2017.

4. "DoD Initiates Elevation Process for U.S. Cyber Command to a Unified Combatant Command," Release No. NR-297-17, Washington, DC: Department of Defense Press Operations, August 18, 2017, available from *https://dod.defense.gov/News/News-Releases/News-Release-View/Article/1282920/dod-initiates-elevation-process-for-us-cyber-command-to-a-unified-combatant-com/*, accessed August 24, 2017. The research for this monograph was completed in September 2017. On May 4, 2018, USCYBERCOM was formally established as the nation's 10th unified combatant command. See Jim Garamone, "Cybercom Now a Combatant Command, Nakasone Replaces Rogers," DoD News, Defense Media Activity, May 4, 2018, available from *https://www.defense.gov/News/Article/Article/1512994/cybercom-now-a-combatant-command-nakasone-replaces-rogers/*, accessed August 6, 2018.

5. Rogers testimony to Congress, pp. 2, 4-5.

6. Statement of Vice Admiral Marshall Lytle, Director Command, Control, Communications and Computers/Cyber, Joint Staff, before the Senate Armed Services Subcommittee on Cybersecurity, U.S. Senate, First Session, 115th Congress, May 23, 2017, p. 5, available from *http://www.armed-services.senate.gov/imo/media/doc/Lytle_05-23-17.pdf*, accessed August 15, 2017. Lytle stated, "cyber forces, cyber defenses and cyber terrain are the three main elements that determine the Joint Force's our (sic) ability to achieve the primary cyber missions [p. 4]." He described efforts to identify critical cyberspace terrain as:

> Further improving the defensibility of cyber terrain involves systematically identifying 'Mission Relevant Cyberspace Terrain' and obtaining situational awareness of that terrain in support of critical missions. Executing the DoD Cyber Strategy line of effort on mission assurance, the Joint Staff led a Department-wide initiative to bring together expert planners from the cyber defense and mission assurance communities to forge and codify a new approach to identifying the key cyber terrain that underpins the Joint Force's critical missions. This approach was vetted and refined during exercises. A formal Planning Order was sent out to all Combatant Commands last month toward that end, the culmination of 18 months of effort. (p. 5)

7. Rogers testimony to Congress, p. 1.

8. Ibid., pp. 5-7.

9. "All Cyber Mission Force Teams Achieve Initial Operating Capability," DoD News, Fort Meade, MD: U.S. Cyber Command, October 24, 2016, available from *https://dod.defense.gov/News/Article/Article/984663/all-cyber-mission-force-teams-achieve-initial-operating-capability/*, accessed October 31, 2018.

10. Lytle testimony to Congress, p. 6.

11. Ibid., p. 7.

12. Joint Chiefs of Staff, Joint Publication 3-12 (R), *Cyberspace Operations,* Washington, DC: Joint Chiefs of Staff, original release February 5, 2013, updated as unclassified public document on October 21, 2014, p. II-2, hereafter JP 3-12, *Cyberspace Operations*.

13. Ibid., pp. II-2–II-3, GL-4.

14. Ibid., pp. II-4–II-12. The cyberspace action of cyberspace attack consists of actions to manipulate or deny, with deny further broken into the actions of degrade, disrupt, or destroy.

15. Ibid., pp. IV-12–IV-15.

16. Mark Pomerleau, "An Exclusive Peek Inside Cyber Command's Premiere Annual Exercise," C4ISRNet website, June 30, 2017, available from *http://www.c4isrnet.com/2017/06/30/an-exclusive-peek-inside-cyber-commands-premiere-annual-exercise/*, accessed September 8, 2017. The primary training objectives for Cyber Flag 2017 were:

- Identify how the military can include cyber effects in an operation.
- Determine if teams can identify characteristics of the terrain—either in an offensive or defensive environment, depending on the team's mission set.
- Find out how teams react when critical infrastructure is compromised.
- Identify how the military can share information with partners and allies.

17. "Cyber Guard 16 Fact Sheet," Fort Meade, MD: U.S. Cyber Command Public Affairs, available from *https://dod.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Cyber-Guard-16-Fact-Sheet-FINAL.pdf,* accessed December 7, 2018.

18. "Allies, Partners Observe Cyber Guard Exercise," U.S. Cyber Command News Release, July 5, 2017, available from *https://dod.defense.gov/News/Article/Article/1238082/allies-partners-observe-cyber-guard-exercise/igphoto/2001773969/,* accessed October 31, 2018.

19. Memorandum of Agreement Between the Department of Defense and the Department of Homeland Security Regarding Department of Defense and U.S. Coast Guard Cooperation on Cybersecurity and Cyberspace Operations, Washington, DC: Department of Defense and Department of Homeland Security, January 19, 2017, p. 2, available from *https://media.defense.gov/2017/Jul/19/2001780017/-1/-1/0/DHS-DOD%20USCG%20*

CYBER%20MOA.PDF, accessed October 31, 2018, hereafter MOA Regarding DoD and USCG Cyberspace Operations.

20. JP 3-12, *Cyberspace Operations*, p. III-4. The roles and responsibilities of the service chiefs are:

> (1) Provide appropriate administration of and support to cyberspace forces assigned or attached to combatant commanders.
> (2) Train and equip forces for cyberspace operations for deployment/support to combatant commanders as directed by the Secretary of Defense. Services will provide cyberspace operations capabilities for deployment/support to combatant commanders as directed by the Secretary of Defense.
> (3) Remain responsible for compliance with USSTRATCOM's direction for operation and defense of the DODIN.
> (4) Coordinate with Commander U.S. Strategic Command to prioritize cyberspace mission requirements and force capabilities.
> (5) Provide users of the EMS regulatory and operational guidance in the use of radio frequencies through the authority of Army (Army Spectrum Management Office), Navy (Navy and Marine Corps Spectrum Center), and Air Force (Air Force Spectrum Management Office).

21. Image modified from "Figure IV-1. Cyberspace Command and Control Organization Construct," in JP 3-12, *Cyberspace Operations*, p. IV-8.

22. U.S. Cyber Command Combined Action Group, "Beyond the Build: How the Component Commands Support the U.S. Cyber Command Vision," *Joint Force Quarterly*, No. 80, 1st Quarter, 2016, pp. 86-93.

23. Department of Defense Instruction (DODI) 8530.01, *Cybersecurity Activities Support to DoD Information Network Operations*, Washington, DC: DoD Chief Information Officer, July 25, 2017 (change 1), p. 43, available from *http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/853001p.pdf*, accessed August 28, 2017, hereafter DODI 8530.01, change 1. CSSPs were previously called computer network defense service providers.

24. "Joint Regional Security Stacks: Increased Network Visibility, Shared Data, Stronger Defense," Defense Information

Systems Agency website page, available from *https://www.disa.mil/newsandevents/2018/joint-regional-security-stacks*, accessed October 31, 2018.

25. Under Secretary of Defense for Acquisition, Technology, and Logistics, DODI 5000.02, *Operation of the Defense Acquisition System*, Washington, DC: Department of Defense, January 7, 2015, incorporating change 3, August 10, 2017, pp. 155-168. Enclosure 14, "Cybersecurity in the Defense Acquisition System, " includes four activities to mitigate cybersecurity risks:

> a. Safeguard Program Information Against Cyber-Attack. . . . b. Design for Cyber Threat Environments. . . . c. Manage Cybersecurity Impacts to Information Types and System Interfaces to the [DODIN]. . . . d. Protect the System Against Cyber Attacks From Enabling and Supporting Systems. (pp. 157-162)

26. Excerpt and image modified from DODI 8530.01, change 1, pp. 33-34.

27. "History," U.S. Army Cyber Command website, available from *http://www.arcyber.army.mil/Organization/History/*, accessed September 2, 2017.

28. Headquarters, Department of the Army, *Designation of the United States Army Cyber Command as an Army Service Component Command, Alignment of the Army's Portion of the Department of Defense Information Network Roles and Responsibilities, Reassignment of the United States Army Network Enterprise Technology Command to Army Cyber Command, and Discontinuation of Second Army*, General Order No. 2017-07, Washington, DC: Headquarters, Department of the Army, January 18, 2017, p. 1. In this general order, the roles and responsibilities of USARCYBER are summarized as:

> USARCYBER is the primary Army headquarters responsible for conducting cyberspace operations (offensive cyberspace operations, defensive cyberspace operations, and Department of Defense Information Network operations), as directed and authorized on behalf of the Commander, USSTRATCOM or the Commander, USCYBERCOM. USARCYBER organizes, trains, educates, mans, equips funds, administers, deploys, and sustains Army cyber forces to conduct cyberspace operations.

Note that even though this order uses the acronym "USAR-CYBER" for the command, the most commonly used acronym remains "ARCYBER" which is used throughout this monograph.

29. Sean Lyngaas, "Army Readies New Cyber Directorate," FCW, The Business of Federal Government website, May 27, 2016, available from *http://www.fcw.com/articles/2016/05/27/frost-cyber-directorate.aspx*, accessed September 2, 2017.

29. "Groundbreaking Marks 'Leap Forward' for Army Cyberspace Operations," Fort Gordon, GA: U.S. Army Cyber Command, available from *http://www.army.mil/article/178917/groundbreaking_marks_leap_forward_for_army_cyberspace_operations*, accessed August 30, 2017.

31. "Our Mission," U.S. Army Cyber Command website, archived page available from *https://web.archive.org/web/20170831151120/http://www.arcyber.army.mil/Pages/ArcyberHome.aspx*, accessed September 2, 2017.

32. Statement by Paul M. Nakasone, Commanding General, U.S. Army Cyber Command, before the Subcommittee on Cybersecurity Committee on Armed Services, U.S. Senate, First Session, 115th Congress, May 23, 2017, available from *http://www.armed-services.senate.gov/imo/media/doc/Nakasone_05-23-17.pdf*, accessed August 15, 2017.

33. Ibid., p. 8. ARCYBER measures readiness in part through the CCORI which is describes as follows:

> Army Cyber Command partnered with JFHQ-[DODIN] to execute the next evolution of Cybersecurity inspections under the Command Cybersecurity Operational Readiness Inspection (CCORI), to replace the Command Cyber Readiness Inspection. The CCORI moves cybersecurity inspections from a compliance-based systems inspection to a risk-based Operational Commander's Mission focused inspection. The CCORI highlights the risks to operational missions within a Command by employing active external and internal threat actors against a Commander's mission critical systems. The CCORI outcome provides an operational risk measurement to mission by mission critical task and a system to assist Commanders in prioritizing cybersecurity resources.

34. Ibid., p. 10.

34. "Combat Training Center rotations continue to drive evolution of Army Cyber-Electromagnetic Activitie[s]," U.S. Army website article, June 29, 2017, available from *http://www.army.mil/article/190201/combat_training_center_rotations_continue_to_drive_evolution_of_army_cyber_electromagnetic_activitie*, accessed August 30, 2017. The article notes how CSCB activities have helped refine how cyber forces support battlefield operations:

> But perhaps the most visible product of the evolution of the CSCB program has been the formation of Expeditionary Cyber Teams (ECTs), tactical force augmentation packages that bring together offensive and defensive cyber operations Soldiers, information operations planners, electronic warfare technicians and intelligence analysts. ECTs are tailorable and scalable to mission needs, to provide maneuver commanders with increased capabilities that enable dominance of the cyber, electromagnetic, and information environments on the battlefield.

36. Sandra Jontz, "Taking Cyber War to The Front Lines," *Signal* online article, October 1, 2016, available from *http://www.afcea.org/content/Article-taking-cyber-war-front-lines*, accessed August 30, 2017. Specific focus areas for CSCB support include:

> The program [CSCB] is designed to explore new approaches to integrating cyber, with each training rotation building on the successes of the last. Some key topics covered in training include:
> - May 2015, 3rd BCT, 25th ID: Defending the Department of Defense Information Network (DODIN) and building offensive cyber operations capability.
> - June 2015, 75th Ranger Regiment: Employing commercial off-the-shelf technology to enhance network maneuvers.
> - November 2015, 1st BCT, 82nd Airborne Division: Defending against aggressive cyber attacks and strengthening cyber staffing procedures.
> - January, 2nd BCT, 2nd ID: Building an enduring cyber environment at the National Training Center and advancing defensive and offensive cyber operations at a brigade level, with targeting, fires and support to

intelligence gathering, as well as disruption of adversary command and control networks.
- August, 1st ABCT, 1st ID: Adding a modular expeditionary cyber team and integrating information operations and EW alongside defensive and offensive cyber capabilities.

37. Nakasone testimony to Congress, p. 7.

38. "USCYBERCOM TASKORD 16-003 To Establish Joint Task Force (JTF)-ARES To Counter the Islamic State of Iraq and the Levant (ISIL) In Cyberspace," May 4, 2016, U.S. Strategic Command Reading Room, Freedom of Information Request Library, posted April 19, 2017, p. 25, available from *http://www.stratcom.mil/Portals/8/Documents/FOIA/FOIA%2017-023,%2017-033,%2017-064%20-%20USCYBERCOM%20Joint%20Task%20Force%20Areas.pdf?ver=2017-04-19-111941-797*, accessed August 25, 2017. The FOIA document is a redacted copy of the Tasking Order and two related Fragmentary Orders, 01 (May 5, 2017) and 02 (June 13, 2016). The order describes the situation as:

> ISIL continues to leverage cyberspace to conduct command and control (C2), facilitate logistics and finance, produce, disseminate and distribute media, attract recruits, and plan and conduct external attacks. In turn, USCYBERCOM continues to plan and conduct cyberspace operations (CO) to counter ISIL in accordance with (IAW) Ref D based on Secretary of Defense (SecDef)-directed guidance and in coordination with (ICW) appropriate CCMDs. Through the establishment of a JTF focused on countering ISIL in cyberspace, USCYBERCOM will continue to create cyberspace conditions to support the dismantling of ISIL [redacted] in support of (ISO) United States Central Command (USCENTCOM) and to disrupt ISIL's ability to plan and execute attacks against the United States (US) and coalition partners while posturing for follow-on global CO.

39. Ibid., pp. 32-33.

40. Edward C. Cardon, "Maturing Cybercapabilities Critical to Army Future," *Army*, Vol. 66, No. 10, October 2016, p. 168.

41. Nakasone testimony to Congress, pp. 2, 7.

42. Graphic from "Army Cyber," U.S. Army Cyber Command, updated December 27, 2017, available from *https://www.goarmy.com/army-cyber/about-army-cyber-command.html*, accessed September 10, 2018.

43. "About," Network Enterprise Technology Command website, n.d., available from *http://www.army.mil/info/organization/unitsandcommands/commandstructure/netcom/#org-about*, accessed August 22, 2017. See also Benjamin Leitzel and Anthony Allard, eds., *Strategic Cyberspace Operations Guide,* Carlisle, PA: Center for Strategic Leadership, U.S. Army War College, June 1, 2016, p. 120, available from *https://csl.armywarcollege.edu/usacsl/Publications/StrategicCyberspaceOperationsGuide2016.pdf*, accessed September 14, 2018. Subordinate units of Network Enterprise Technology Command and their operational focus are:

- 5th Signal Command (Theater), Wiesbaden, Germany: USEUCOM and USAFRICOM;
- 7th Signal Command (Theater), Fort Gordon, GA: joint forces;
- 311th Signal Command (Theater), Fort Shafter, HI: USPACOM; and,
- 335th Signal Command (Theater), East Point, GA: USCENTCOM and USNORTHCOM.

Note that the 5th Signal Command (Theater) was inactivated in November 2016, and its mission restructured to the 2d Strategic Signal Brigade at Clay Kaserne, Germany. See "5th Signal Command Inactivates, 2nd Strategic Signal Brigade Restructures," U.S. Army website article, Wiesbaden, Germany: U.S. Army Europe, November 4, 2016, available from *http://www.army.mil/article/177825*, accessed September 11, 2017.

44. "Our Mission," 1st Information Operations Command website, available from *http://www.1stiocmd.army.mil/Home/Mission*, accessed September 4, 2017. Subordinate units of the 1st Information Operation Command and their operational focus are: 1st Battalion, Information Operation Planning and Operations Security Training; 2d Battalion, cyberspace opposing force operations and maintaining the Army's Computer Defense Assistance Program.

45. *Strategic Cyberspace Operations Guide*, p. 120.

46. "Welcome: Mission," 780th Military Intelligence Brigade website, available from *http://www.inscom.army.mil/msc/780mib/index.html*, accessed September 4, 2017. Subordinate units of the 780th MI Brigade are: 781st Military Intelligence Battalion (Vanguard), Fort Meade, MD; and 782d Military Intelligence Battalion (Cyber Legion), Fort Gordon, GA.

47. FM 3-12, *Cyberspace and Electronic Warfare Operations*, Washington, DC: Headquarters, Department of the Army, April 11, 2017, p. 3-3, available from *https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/ARN3089_FM%203-12%20FINAL%20WEB%201.pdf*, accessed August 8, 2017. ARCYBER regional cyber centers are described as follows:

> The regional cyber center is the single point of contact for operational status, service provisioning, incident response, and all Army network services in its assigned theater. It coordinates directly with tactical units to provide DODIN-A services, support to DODIN operations, and when required DCO to enable mission command and the warfighting functions.

48. Nakasone testimony to Congress, pp. 4-6.

49. "Cyber Operations Officer (17A)," Army recruiting website, available from *http://www.goarmy.com/careers-and-jobs/browse-career-and-job-categories/computers-and-technology/cyber-operations-officer.html*, accessed August 26, 2017.

50. Nakasone testimony to Congress, pp. 2, 12.

51. Statement by Lieutenant General Edward C. Cardon, Commanding General, U.S. Army Cyber Command and Second Army before the House Armed Services Committee, Subcommittee on Emerging Threats and Capabilities, Operationalizing Cyberspace for the Services, 1st Session, 114th Congress, March 4, 2015, p. 4, available from *https://docs.house.gov/meetings/AS/AS26/20150304/103093/HHRG-114-AS26-Wstate-CardonE-20150304.pdf,* accessed October 31, 2018.

52. Cyber Operations Officer (17A) website.

53. "170A—Cyber Operations Technician," Army recruiting website, available from *http://www.usarec.army.mil/hq/warrant/prerequ/WO170A.shtml*, accessed September 4, 2017.

54. See "Cyber Operations Specialist (17C)," Army recruiting website, available from *http://www.goarmy.com/careers-and-jobs/browse-career-and-job-categories/computers-and-technology/cyber-operations-specialist.html*, accessed August 26, 2017. See also "Cyber Network Defender (25D)," Army recruiting website, available from *http://www.goarmy.com/careers-and-jobs/browse-career-and-job-categories/computers-and-technology/cyber-network-defender.html*, accessed August 26, 2017. The career field is open to Staff Sergeants and above.

55. Sean Kimmons, "Cyber stands up civilian career field, mulls direct commissioning," Washington, DC: Army News Service, February 10, 2017, available from *http://www.army.mil/article/182153/cyber_stands_up_civilian_career_field_mulls_direct_commissioning*, accessed August 30, 2017.

56. Nakasone testimony to Congress, p. 12.

57. Ibid.

58. Erick Yates, "Reserve cyber unit talks readiness during Army House Liaison visit," East Point, GA: 335th Signal Command (Theater), March 9, 2017, available from *https://www.usar.army.mil/News/News-Display/Article/1108573/reserve-cyber-unit-talks-readiness-during-army-house-liaison-visit/*, accessed September 13, 2017.

59. Cardon, "Maturing Cybercapabilities Critical to Army Future," p. 169.

60. Nakasone testimony to Congress, pp. 8-9.

61. Cardon testimony to Congress, p. 2.

62. "The Facts: Training for Cyber Soldiers," fact sheet, U.S. Army Cyber Command and Second Army, p. 1, March 15, 2016. Key roles of the Army CCoE are:

> As the Army's force modernization proponent for cyberspace operations, signal/communications networks

and information services, and electronic warfare, the CCoE integrates and develops doctrine, organization, training, materiel, leadership, personnel and facilities, and coordinates with the Army Intelligence Center of Excellence for institutional intelligence support to cyberspace operations. The CCoE ensures Army cyberspace, electronic warfare and signal operations capabilities evolve with joint force requirements and capabilities. The Cyber School lays the foundation for development of skilled cyber forces that are trained to joint standards to meet combatant commanders' current and future force requirements.

63. Nakasone testimony to Congress, p. 9. Regarding the incorporation of joint training standards:

> The CCoE focuses on individual training and has begun training key USCYBERCOM J7 pipeline courses including Cyber Common Technical Core (equivalent to Intermediate Cyber Core, CPT Core Methodologies, Cyber Operations Planner Course, and the Joint Advanced Cyber Warfare Course.

64. "Training for Cyber Soldiers" fact sheet, p. 2. The initial cyberspace training courses offered by the Army Cyber School are described as:

> Newcomers to the Cyber branch will also complete resident training at the Cyber School. The first training offered was the Basic Officers Leader Course, started in August 2015. The school's catalog is expected to expand in phases through 2017. A two-tiered, 14-week warrant officer training program is planned for May 2016, with an advanced course for those who already have significant experience in cyber fields and a basic course for those newer to the work. The first new enlisted cyber Soldiers entered the Army in October 2015 and began Advanced Individual Training in February 2016. Because cyber operates as a part of a joint force, the first 22-week phase of Advanced Individual Training will be the Navy Joint Cyber Analysis Course at Pensacola, FL. The second 22-week phase will be at Fort Gordon.

65. Nakasone testimony to Congress, p. 2.

66. Cardon testimony to Congress, p. 6. With regard to Army cyberspace training, Cardon noted:

> Both ARCYBER and the Cyber CoE are developing robust collective training methods that include both simulated, virtual, and real-world operational events on ranges and networks that stress individual and team capabilities. We now require dedicated training facilities, support infrastructure and cyberspace live fire facilities consistent with joint range requirements at the Service and joint levels. Permanent training environments with dedicated facilities and resources will enable training innovations and further growth in capability and capacity available to combatant and Army commanders.

67. Nakasone testimony to Congress, p. 9.

68. FM 3-12, *Cyberspace and Electronic Warfare Operations*.

69. Graphic from Ibid., p. 1-6.

70. Nakasone testimony to Congress, pp. 4-5.

71. Edward C. Cardon, "Maturing Cyber Capabilities Critical to Army Future," U.S. Army News, September 21, 2016, available from *http://www.army.mil/article/175465*, accessed September 13, 2017.

72. *The U.S. Digital Service Report to Congress*, Washington, DC: U.S. Digital Service, July 2017, p. 12, available from *http://www.usds.gov/resources/USDS-July-2017-Report-to-Congress.pdf*, accessed August 30, 2017.

73. Office of the Under Secretary of Defense (Comptroller) Chief Financial Officer, *Defense Budget Overview: United States Department of Defense, Fiscal Year 2018 Budget Request*, Washington, DC: Department of Defense, May 2017, p. 3-9, available from *https://comptroller.defense.gov/Portals/45/Documents/defbudget/fy2018/fy2018_Budget_Request_Overview_Book.pdf*, accessed September 11, 2017.

74. Mark Pomerleau, "Army Spearheading Cyber Persistent Training Environment," *Defense News*, August 11, 2016, available from *http://www.defensenews.com/training-sim/2016/08/11/army-spearheading-cyber-persistent-training-environment/*, accessed September 1, 2017.

75. Claire Heininger, "Army taps innovation for cyber training," U.S. Army website article, Orlando, FL: U.S. Army News, November 7, 2016, available from *https://www.army.mil/article/178005/army_taps_innovation_for_cyber_training*, accessed September 1, 2017. See also Loren Blinde, "Army to Hold National Cyber Range Complex Industry Day," *Intelligence Community News*, May 17, 2017, available from *http://www.intelligencecommunitynews.com/army-to-hold-national-cyber-range-complex-industry-day/*, accessed September 11, 2017.

76. Nancy Jones-Bonbrest, "Prototypes rapidly deliver cyber capabilities," *U.S. Army News*, Washington, DC, June 20, 2017, available from *https://www.army.mil/article/189601/prototypes_rapidly_deliver_cyber_capabilities*, accessed September 1, 2017.

77. Army Capabilities Integrations Center, *Warfighters' Science and Technology Needs*, Fort Eustis, VA: U.S. Army Training and Doctrine Command, September 22, 2017, pp. 17-18, available from *http://www.arcic.army.mil/App_Documents/Army-Warfighters-ST-Needs-Bulletin.pdf*, accessed September 22, 2017. The prioritized cyberspace operations (CO) capability needs for the mid-term future (up to 2025) are: (1) Integrated Electronic Warfare; (2) Enhanced Spectrum Management Operations; (3) Cyber Situational Understanding; (4) Future Waveforms; and (5) Hardware Software Convergence. Candidate CO capabilities for far-term (beyond 2025) are: (1) Autonomous Active Cyber Defense; (2) Defensive Cyber Operations-Tactical; (3) Autonomous Cognitive Radio Frequency; (4) Assured Position, Navigation, and Timing; and, (5) Communications under Extreme RF Conditions.

78. Larry Jennings, "Leveraging Industry Innovation: An Army Cyber Innovation Challenge," *Cyber: The Magazine of the MCPA*, Vol. 1, No. 2, Fall 2016, pp. 8-11.

79. Statement of Lieutenant General George J. Flynn, Deputy Commandant for Combat Development and Integration before the Subcommittee on Terrorism, Unconventional Threats and Capabilities of the House Armed Services Committee Concering [sic] Operating in the Digital Domain: Organizing The Military Departments for Cyber Operations, 2d Session, 111th Congress, September 23, 2010, H.A.S.C. No. 111-180, Washington, DC: Government Printing Office, Appendix, pp. 36-42, available from

https://www.gpo.gov/fdsys/pkg/CHRG-111hhrg62398/pdf/CHRG-111hhrg62398.pdf, accessed September 14, 2017.

80. "General Officer Announcements," Release No. NR-232-17, Washington, DC: Department of Defense Press Operations, June 19, 2017.

81. Statement by Major General Lori E. Reynolds, Commander, Marine Corps Forces Cyberspace Command, before the Senate Armed Services Committee Subcommittee on Cybersecurity, Cyber Posture, U.S. Senate, 1st Session, 115th Congress, May 23, 2017, p. 9, available from *https://www.armed-services.senate.gov/imo/media/doc/Reynolds_05-23-17.pdf*, accessed August 15, 2017.

81. "U.S. Marine Corps Forces Cyberspace Command (MARFORCYBER)," U.S. Marine Corps Concepts and Programs website, available from *http://www.candp.marines.mil/Organization/Operating-Forces/US-Marine-Corps-Forces-Cyberspace-Command/*, accessed September 14, 2018.

83. Reynolds testimony to Congress, p. 3.

84. Marine Corps Bulletin 3100, "Operations and Defense of the Marine Corps Enterprise Network (MCEN)," Washington, DC: Headquarters, United States Marine Corps, July 14, 2017, enclosure 1, p. 1-1, available from *http://www.marines.mil/Portals/59/Publications/MCBUL%203100.pdf?ver=2017-07-14-113616-603*, accessed September 12, 2017. This document defines MCCE and MCEN as follows:

> Marine Corps Cyberspace Environment (MCCE). The Marine Corps' portion of the DODIN and all Marine Corps acquired, procured, or provisioned information systems and the associated collecting, processing, storing, managing, and transmission of information on all classified and non-classified networks, and components of the MCISR-E, including cyber discipline.
>
> Marine Corps Enterprise Network (MCEN). The MCEN is a segment of the MCCE, defined as the physical and logical information systems, PORs, applications, and networks that connect from the USMC Tier 2 boundary to the DISA Tier 1 Internet Access Point. The MCEN also includes active Marine

Corps tactical networks and networks aboard amphibious shipping.

85. Statement by Major General Daniel J. O'Donohue, Commanding General, Marine Corps Forces Cyberspace Command, before the Senate Armed Services Committee Subcommittee on Emerging Threats and Capabilities, Operationalizing Cyberspace for the Services, U.S. Senate, 1st Session, 114th Congress, March 4, 2015, p. 6, available from *https://docs.house.gov/meetings/AS/AS26/20150304/103093/HHRG-114-AS26-Wstate-ODonohueD-20150304.pdf,* accessed October 31, 2018.

86. Reynolds testimony to Congress, pp. 5, 7.

87. Marine Corps Warfighting Laboratory, *Marine Corps Operating Concept: How an Expeditionary Force Operates in the 21st Century*, Washington, DC: U.S. Marine Corps, September 2016, pp. 20-21, available from *https://www.mcwl.marines.mil/Portals/34/Images/MarineCorpsOperatingConceptSept2016.pdf?ver=2016-12-02-073359-207*, accessed September 12, 2017.

88. Headquarters, U.S. Marine Corps, MCWP 3-40.4, *Marine Air-Ground Task Force Information Operations*, Washington, DC: Department of the Navy, July 1, 2013, p. 3-9.

89. "MAGTF Cyberspace and Electronic Warfare Coordination Cell (CEWCC) Concept," MARADMINS Active Number: 362/14, July 24, 2014, available from *https://www.marines.mil/News/Messages/Messages-Display/Article/896528/magtf-cyberspace-and-electronic-warfare-coordination-cellcewcc-concept/*, accessed September 12, 2017.

90. Matthew E. Poole and Jason C. Schuette, "Cyber Electronic Warfare," *Marine Corps Gazette*, Vol. 99, No. 8, August 2015, p. 61.

91. Deputy Commandant for Combat Development and Integration, *Marine Air Ground Task Force Information Environment Operations Concept of Employment*, Marine Corps Base Quantico, VA: Marine Corps Combat Development Command, July 6, 2017, p. 23, available from *https://www.trngcmd.marines.mil/Portals/207/Docs/wtbn/MCCMOS/FINAL%20MAGTF%20IE%20OPS%20CoE%202017-07-06.pdf?ver=2017-11-16-090225-057,* accessed October 31, 2018.

92. Reynolds testimony to Congress, pp. 3-5. The continuity of operations policy and planning for Marine Corps Cyberspace Operations Group (MCCOG) is required by DoD Directive 3020.26, *Department of Defense Continuity Programs*.

93. Eric Keenan, "Marine Corps enters realm of cyberspace through new unit," Fort Meade, MD: Defense Media Activity, March 25, 2016, available from *https://www.marines.mil/News/News-Display/Article/705570/marine-corps-enters-realm-of-cyberspace-through-new-unit/*, accessed September 12, 2017. See also Reynolds testimony to Congress, p. 6.

94. MARFORCYBER Concepts and Programs website, available from *http://www.candp.marines.mil/Organization/Operating-Forces/US-Marine-Corps-Forces-Cyberspace-Command/*, accessed September 14, 2018:

> Key MCCYWG tasks include:
> - Conduct personnel management to organize and assign individuals to work roles and place them in work centers to ensure operational readiness of CMF Teams
> - Ensure all personnel are trained in accordance with USCYBERCOM Joint Cyberspace Training and Certification Standards and equipped to perform all duties and tasks outlined in the MARFORCYBER Mission Essential Task List
> - Plan for and, when authorized, conduct OCO including computer network exploitation . . . , cyberspace intelligence, surveillance, and reconnaissance . . . and operational preparation of the environment
> - Plan and conduct designated DCO in response to threats against the MCEN, supported combatant command . . . designated networks, and the Department of Defense Information Network
> - Advise COMMARFORCYBER on force employment considerations
> - Provide subject matter expertise for operational planning requirements

95. Table data from Ibid.

96. Reynolds testimony to Congress, p. 5.

97. Mark Pomerleau, "Marines put new cyber unit into play," Defense Systems website, April 5, 2016, available from *http://www.defensesystems.com/articles/2016/04/05/marine-corps-cyberspace-warfare-group.aspx*, accessed September 12, 2017.

98. Flynn testimony to Congress, p. 3.

99. O'Donohue testimony to Congress, pp. 4-5.

100. Dan Lamothe, "Heartbleed and beyond: Marine Corps 'cyber range' trains to fight off hackers," *The Washington Post*, July 8, 2015, available from *https://www.washingtonpost.com/news/checkpoint/wp/2015/07/08/heartbleed-and-beyond-marine-corps-cyber-range-trains-to-fight-off-hackers/?utm_term=.fa0ecec8bc29*, accessed September 17, 2017.

101. Garrett White, "Marines with I MEF strengthen cyber defensive capabilities," Marine Corps Air Station Miramar, CA: I Marine Expeditionary Force, August 23, 2016, available from *https://www.marines.mil/News/News-Display/Article/922514/marines-with-i-mef-strengthen-cyber-defensive-capabilities/*, accessed September 12, 2017.

102. "Availability of Marine Corps Interim Publication 3-40.02 Marine Corps Cyberspace Operations," MARADMINS Active Number: 532/14, October 21, 2014, available from *https://www.marines.mil/News/Messages/Messages-Display/Article/896719/availability-of-marine-corps-interim-publication-3-40o2-marine-corps-cyberspace/*, accessed September 12, 2017.

103. Jared Serbu, "Marine Corps building its first-ever cyber doctrine," Federal News Radio, April 15, 2015, available from *https://www.federalnewsradio.com/defense/2015/04/marine-corps-building-its-first-ever-cyber-doctrine/*, accessed September 14, 2017.

104. Headquarters U.S. Marine Corps, *Expeditionary Force 21, Forward and Ready: Now and in the Future*, Washington, DC: Department of the Navy, March 4, 2014, p. 36, available from *https://www.mccdc.marines.mil/Portals/172/Docs/MCCDC/EF21/EF21_Capstone_Concept.pdf*, accessed October 31, 2018. The inclusion of CEWCC in current USMC doctrine is summarized as:

> Doctrine for Cyberspace Operations and EMS Operations has undergone initial development and the Marine Corps are implementing a key component with the

> development of the Cyber Electronic Warfare Coordination Cell (CEWCC). The CEWCC coordinates the integrated planning, execution, and assessment of cyberspace and EMS operations across the MAGTF's operational environment to increase operational tempo and achieve military advantage. The MAGTF commander uses the CEWCC to ensure all organic and non-organic cyberspace and EMS-dependent capabilities are planned, executed, and assessed during all phases of an operation; and are incorporated into the MAGTF's operational design, concept of operations (CONOPS), scheme of maneuver, concept of fires support, intelligence operations, as well as in appropriate detailed plans and annexes. Additionally, the CEWCC provides an enhanced MAGTF capability for planning, requesting, and coordinating non-organic 'reach-back' support from external agencies to include Special Technical Operations. Because this support often requires long lead times and extensive coordination with national-level agencies, MAGTFs will rely heavily upon the CEWCC during deliberate planning, inter-deployment periods, and during preparation for deployment.

105. Reynolds testimony to Congress, pp. 3-4. Reynolds summarized ongoing MCEN modernization efforts on p. 3 as:

> Our priorities for improving our defenses this year include actions to flatten the Marine Corps network and improve our ability to sense the environment, harden the network through increased endpoint security, and decrease incident response time. To do this, we are aggressively seeking to consolidate legacy domains, implement a comply to connect capability and the WIN 10-operating system, and collapse regional service desks to an enterprise service desk.

106. Ibid., pp. 6-7.

107. Mark Pomerleau, "Marines Applying Rapid Acquisition in Cyberspace," *Marine Corps Times*, August 2, 2017, available from *https://www.marinecorpstimes.com/dod/marine-corps/2017/08/02/marines-applying-rapid-acquisition-in-cyberspace/*, accessed September 14, 2017.

108. Emily Greene, "Marine Corps Cyber Acquisition Just Got Faster," Marine Corps Base Quantico, VA: Marine Corps

Systems Command, October 12, 2016, available from *https://www.marines.mil/News/News-Display/Article/970947/marine-corps-cyber-acquisition-just-got-faster/*, accessed September 12, 2017.

109. Michael Peck, "Marine Corps Awards Cyber, IT Contracts to Three Firms," C4ISRNet website, December 14, 2016, available from *https://www.c4isrnet.com/home/2016/12/14/marine-corps-awards-cyber-it-contracts-to-three-firms/*, accessed September 16, 2017.

110. "Navy Stands Up Fleet Cyber Command, Reestablishes U.S. 10th Fleet," *U.S. Navy News*, Story No. NNS100129-24, Fort Meade, MD: Fleet Cyber Command/10 Fleet Public Affairs, January 29, 2010, available from *http://www.navy.mil/submit/display.asp?story_id=50954*, accessed September 18, 2017.

111. Statement of Vice Admiral Bernard J. McCullough III, Commander, United States Fleet Cyber Command, before the Subcommittee on Terrorism, Unconventional Threats and Capabilities of the Committee on Armed Services, House of Representatives, Operating in the Digital Domain: Organizing The Military Departments for Cyber Operations, 2d Session, 111th Congress, September 23, 2010, H.A.S.C. No. 111-180, Washington, DC: Government Printing Office, Appendix, pp. 25-34, available from *https://www.gpo.gov/fdsys/pkg/CHRG-111hhrg62398/pdf/CHRG-111hhrg62398.pdf*, accessed September 14, 2017.

112. "NAVIDFOR Changes Name to Naval Information Forces," Story Number NNS160209-08, Suffolk, VA: NAVIFOR Public Affairs, February 9, 2016, available from *http://www.navy.mil/submit/display.asp?story_id=93027*, accessed September 11, 2017.

113. Nancy Norton, "The U.S. Navy's Evolving Cyber/Cybersecurity Story," *The Cyber Defense Review*, Vol. 1, No. 1, Spring 2016, pp. 21-26, available from *https://cyberdefensereview.army.mil/Portals/6/Documents/CDR-SPRING2016.pdf?ver=2016-09-14-122108-290*, accessed October 31, 2018..

114. "U.S. Fleet Cyber Command Mission," U.S. Fleet Cyber Command/U.S. Tenth Fleet website, last modified January 8, 2015, archived page available from *https://web.archive.org/*

web/20170915155558/http://www.public.navy.mil/fcc-c10f/Pages/usfleetcybermission.aspx, accessed September 14, 2018.

115. "U.S. Tenth Fleet: Mission," U.S. Fleet Cyber Command/U.S. Tenth Fleet website, last modified December 1, 2010, available from *http://www.public.navy.mil/fcc-c10f/Pages/ustenthfleetmission.aspx*, accessed September 14, 2018.

116. Statement by Vice Admiral Michael M. Gilday, Commander, U.S. Fleet Cyber Command, U.S. Tenth Fleet, before the Senate Armed Services Committee, Subcommittee on Cybersecurity, Cyber Posture, U.S. Senate, 1st Session, 115th Congress, May 23, 2017, pp. 2-3, available from *https://www.armed-services.senate.gov/imo/media/doc/Gilday_05-23-17.pdf*, accessed August 15, 2017. Details on the five priorities for Fleet Cyber Command are:

> 1. Operate the Network as a Warfighting Platform: Defend Navy networks, communications and space systems, ensure availability and, when necessary, fight through them to achieve operational objectives.
> 2. Conduct Tailored Signals Intelligence: Meet the evolving SIGINT needs of Navy commands, including intelligence support to cyber.
> 3. Deliver Warfighting Effects Through Cyberspace: Advance our effects delivery capabilities to support a full spectrum of operations, including cyber, electromagnetic maneuver, and information operations.
> 4. Create Shared Cyber Situational Awareness: Create a shareable cyber common operating picture that evolves to full, immediate awareness of our network and everything that happens on it.
> 5. Establish and mature Navy's Cyber Mission Forces: Stand up 40 highly expert Cyber Mission Teams and plan for the sustainability of these teams over time.

117. Ibid., p. 3.

118. Ray Mabus, Navy Unit Commendation to U.S. Fleet Cyber Command and U.S. Tenth Fleet Citation, Washington, DC: Secretary of the Navy, 2014, available from *https://www.public.navy.mil/fcc-c10f/Fact%20Sheets/Navy%20Unit%20Commendation.2014.pdf*, accessed August 25, 2017. Significant actions cited in the commendation include:

> The efforts of these commands in strengthening governance and enforcing Navy-wide standards left the Navy's unclassified network with a fundamentally hardened and more defendable architecture. Operation ROLLING TIDE revolutionized Navy network defense strategy, improved command and control, developed an expedited process for mitigating network risks, and laid the foundation for defending Navy networks against future cyber threats.

119. Norton, pp. 24-25. For further details on Task Force Cyber Awakening, see also Sharon Anderson, "Navy's Jump Start on Cybersecurity Readiness, Task Force Cyber Awakening Leads the Charge," *CHIPS, The Department of the Navy's Information Technology Magazine*, January-March 2015, available from *http://www.doncio.navy.mil/chips/ArticleDetails.aspx?ID=5787*, accessed August 23, 2018.

120. Gilday testimony to Congress, p. 2.

121. McCullough testimony to Congress, pp. 27-28.

122. "NETWARCOM: Naval Network Warfare Command," NETWARCOM website, n.d., available from *http://www.public.navy.mil/FLTFOR/nnwc/Pages/default.aspx*, accessed September 10, 2017.

123. Naval Computer and Telecommunications Area Master Station Atlantic Public Affairs, "NCTAMS LANT Holds Change of Command Ceremony," Official Website of the United States Navy, June 18, 2015, available from *https://www.navy.mil/submit/display.asp?story_id=87717*.

124. Joshua J. Wahl, "NAVSOC Holds Change of Command, Celebrates 50th Anniversary," Official Website of the United States Navy, April 26, 2012, available from *https://www.navy.mil/submit/display.asp?story_id=66505*.

125. "Welcome to Navy Cyber Defense Operations Command (NCDOC) Website!" NCDOC, n.d., available from *https://www.public.navy.mil/FLTFOR/ncdoc/Pages/default.aspx*.

126. Mario Vulcano, "The Evolution of Corry Station (1922 – 2016)," under "Tenant Commands onboard Corry Station NASP Base," Station HYPO, blog entry posted March

18, 2016, available from *https://stationhypo.com/2016/03/18/the-evolution-of-corry-station-1922-2016/.*

127. OPNAVINST 5400.45, "Standard Navy Distribution List Shore Chain Of Command," Washington, DC: Department of the Navy, August 1, 2017, available from *https://www.doni.documentservices.dla.mil/SECNAV%20Manuals/Shore%20Activities%20and%20Detachments%20Under%20the%20Command%20of%20Secretary%20of%20Navy%20and%20Chief%20of%20Naval%20Operations.pdf*, accessed September 10, 2017. For all of the units listed in table 4, the following statement in OPNAVINST 5400.45 applies: "COMUSFLTCYBERCOM is the operational commander, echelon 2, immediate superior in command, reporting senior, and first flag officer [p. 2]." See also the various units described and listed in the Field Sites tab of the U.S. Fleet Cyber Command website, available from *https://www.public.navy.mil/fcc-c10f/Pages/home.aspx*.

128. David R. Finley, Jr., "New Navy OPSEC App is Out," Official Website of the United States Navy, December 3, 2015, available from *https://www.navy.mil/submit/display.asp?story_id=92265*.

129. "NIOC Georgia Mission Statement," NIOC GA, n.d., available from *http://www.public.navy.mil/FLTFOR/niocga/Pages/home.aspx*.

130. "Mission Statement," Cryptologic Warfare Group Six, n.d., available from *http://www.public.navy.mil/FLTFOR/cwg6/Pages/default.aspx*.

131. "Navy Cyber Warfare Development Group," Department of Computer Science, University of Maryland, n.d., available from *http://www.cs.umd.edu/cscareerfair/company/navy-cyber-warfare-development-group*.

132. Calvin B. Gates, "U.S. Naval Computer and Telecommunications Station Far East Holds Change of Command," Official Website of the United States Navy, October 22, 2015, available from *https://www.navy.mil/submit/display.asp?story_id=91675*.

133. Gilday testimony to Congress, p. 7.

134. Department of the Navy, *Navy Information Dominance Corps Human Capital Strategy, 2012-2017*, Washington, DC: Deputy Chief of Naval Operations for Information Dominance, 2012, pp. ii-iii, available from *http://www.public.navy.mil/fcc-c10f/Strategies/Navy_Information_Dominance_Corps_Human_Capital_Strategy.pdf*, accessed September 24, 2017.

135. Gilday testimony to Congress, p. 8. Also, see appendix IV of this monograph for sources of Navy personnel information.

136. Ibid., p. 9.

137. Thom Seith, "Joint Cyber Analysis Course Challenges New and Veteran Sailors," Official Website of the United States Navy, January 22, 2015, available from *http://www.navy.mil/submit/display.asp?story_id=85292*, accessed September 24, 2017.

138. "NIOC Pensacola Cyber Teams Participate in Cyber Flag 17 Exercise," *CHIPS, The Department of the Navy's Information Technology Magazine*, U.S. Fleet Cyber Command/U.S. 10th Fleet Public Affairs, July-September 2017, available from *http://www.doncio.navy.mil/chips/ArticleDetails.aspx?ID=9438*, accessed September 24, 2017.

139. Gilday testimony to Congress, p. 9.

140. Sydney J. Freedberg, Jr., "Navy Starts Up Cyber 'Top Gun' School: Information Warfighting Development Center," BreakingDefense, March 3, 2017, available from *https://www.breakingdefense.com/2017/03/navy-starts-up-cyber-top-gun-school-information-warfare-development-center/*, accessed September 24, 2017.

141. Megan Shutka, "Naval Information Warfighting Development Center Enters Initial Operational Capability," Official Website of the United States Navy, March 29, 2017, available from *http://www.navy.mil/submit/display.asp?story_id=99564*, accessed September 24, 2017.

142. Steven A. Davis, "Navy Finalizes 8 Cybersecurity Standards, Now Available to Industry," Official Website of the United States Navy, February 17, 2016, available from *http://www.navy.mil/submit/display.asp?story_id=93151*, accessed August 21, 2017.

The eight standards are: (1) Host Level Protection; (2) Network Firewall; (3) Network Intrusion Detection Systems and Intrusion Protection Systems; (4) Defense in Depth Functional Implementation Architecture; (5) Security Information and Event Management Implementation; (6) Information Security Continuous Monitoring; (7) Boundary Protection; and, (8) Vulnerability Scanning.

143. Isaac R. Porche III, Shawn McKay, Megan McKernan, Robert W. Button, Bob Murphy, Katheryn Giglio, and Elliot Axelband, *Rapid Acquisition and Fielding for Information Assurance and Cyber Security in the Navy*, Santa Monica, CA: RAND Corporation, 2012, p. iii.

144. "PMW 130 Information Assurance and Cyber Security Program Office," U.S. Navy factsheet, January 23, 2018, available from *https://www.public.navy.mil/spawar/PEOC4I/Documents/TearSheets/PMW130_FactSheet_2017_DistoA.pdf*, accessed February 8, 2019.

145. Robert K. Ackerman, "Navy Seeks Technologies for Cyber Fight," *The Cyber Edge*, *Signal Magazine*, April 1, 2017, available from *https://www.afcea.org/content/navy-seeks-technologies-cyber-fight*, accessed September 24, 2017.

146. "Defense Department Cyber Efforts: More Detailed Guidance Needed to Ensure Military Services Develop Appropriate Cyberspace Capabilities," Report GAO-11-421, Washington, DC: U.S. Government Accountability Office, May 2011, p. 8, available from *https://www.gao.gov/assets/320/318604.pdf,* accessed September 14, 2017.

147. *History of HQ Twenty-Fourth Air Force and 624th Operations Center*, Joint Base San Antonio-Lackland, TX: 24AF Office of History, January 17, 2014. The research for this monograph was completed in September 2017. On July 17, 2018, 24th Air Force higher headquarters officially shifted from Air Force Space Command to Air Combat Command. See R. J. Biermann, "24th Air Force Joins Air Combat Command, Welcomes New Commander," Air Forces Cyber Public Affairs, July 18, 2018, available from *https://www.af.mil/News/Article-Display/Article/1577754/24th-air-force-joins-air-combat-command-welcomes-new-commander/,* accessed November 1, 2018.

148. See Department of Defense Directive 5505.13E, *DoD Executive Agent for the DoD Cyber Crime Center*, Washington, DC: Department of Defense Chief Information Officer, change 1, July 27, 2017. See also Department of Defense Instruction 5205.13, *Defense Industrial Base Cyber Security Activities*, Washington, DC: Department of Defense Chief Information Officer, change 1, July 27, 2017, pp. 8-9.

149. "24th Air Force (Air Forces Cyber)," USAF fact sheet, February 8, 2017, available from *https://www.afcyber.af.mil/About-Us/Fact-Sheets/Display/Article/458567/24th-air-force-air-forces-cyber/*, accessed August 20, 2017.

150. "Squadron to Provide Defensive Cyber Operations," *Colorado Springs Business Journal*, March 10, 2017, available from *https://www.csbj.com/2017/03/10/squadron-to-provide-defensive-cyber-operations/*, accessed August 29, 2017.

151. Statement of Major General Chris P. Weggeman, Commander, 24th Air Force and Commander, Air Forces Cyber, Presentation to the Senate Armed Services Committee, Subcommittee on Cybersecurity, U.S. Senate, Subject: Military Cyber Programs and Posture, 1st Session, 115th Congress, May 23, 2017, pp. 4-6, available from *https://www.armed-services.senate.gov/imo/media/doc/Weggeman_05-23-17.pdf*, accessed August 15, 2017.

152. Chris P. Weggeman, *Commander's Strategic Vision*, Joint Base San Antonio, TX: 24th Air Force, March 24, 2017, p. 3, available from *http://www.afcyber.af.mil/Portals/11/documents/24%20AF%20Strategic%20Vision.pdf?ver=2017-03-08-112453-760*, accessed August 31, 2017. The other four AFCYBER Strategic Priorities are:

> 2. Develop and Empower Our Airmen and Take Care of Their Families. . . . 3. Lead Through Teamwork and Partnerships. . . . 4. Inculcate a Strong Warfighting Culture into Cyberspace Operations. . . . 5. Equip the Force through Rapid, Innovative Fielding of Cyber Capabilities. (pp. 4-7)

153. Annex 3-12, *Cyberspace Operations*, Maxwell Air Force Base, AL: Curtis E. LeMay Center, November 30, 2011, pp. 32-33.

154. Weggeman testimony to Congress, p. 10.

155. Table data compiled from Headquarters, U.S. Air Force, *AFSC 17X Cyberspace Operations Officer, Career Field Education and Training Plan*, Washington, DC: Department of the Air Force, June 1, 2015, pp. 8-9, available from *http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/cfetp17x/cfetp17x.pdf*, accessed August 20, 2017.

156. "67th Cyberspace Wing," U.S. Air Force fact sheet, November 2016, archived page available from *https://web.archive.org/web/20180220132644/http://www.afcyber.af.mil:80/About-Us/Fact-Sheets/Display/Article/458563/67th-cyberspace-wing/*, accessed September 12, 2018. The three subordinate units of the 67th Cyberspace Wing are: the 26th Cyberspace Operations Group, the 67th Cyberspace Operations Group, and the 690th Network Support Group.

157. "688th Cyberspace Wing," 24th Air Force website, archived page available from *https://web.archive.org/web/20180426075919/http://www.afcyber.af.mil/About-Us/Units/688th-Cyberspace-Wing/*, accessed September 12, 2018. Also, see "688th Cyberspace Wing," U.S. Air Force fact sheet, January 3, 2013, archived page available from *https://web.archive.org/web/20180220135840/http://www.afcyber.af.mil:80/About-Us/Fact-Sheets/Display/Article/458566/688th-cyberspace-wing/*, accessed September 12, 2018. The three subordinate units of the 688th Cyberspace Wing are: the 38th Cyberspace Engineering and Installation Group, the 318th Cyberspace Operations Group, and the 688th Cyberspace Operations Group.

158. "5th Combat Communications Group," U.S. Air Force fact sheet, March 28, 2017, archived page available from *https://web.archive.org/web/20180220141700/http://www.afcyber.af.mil:80/About-Us/Fact-Sheets/Display/Article/458564/5th-combat-communications-group*, accessed September 12, 2018.

159. "624th Operations Center," U.S. Air Force fact sheet, August 26, 2016, archived page available from *https://web.archive.org/web/20161121032044/http://24af.af.mil/DesktopModules/ArticleCS/Print.aspx?PortalId=11&ModuleId=1307&Article=731721*, accessed September 12, 2018.

160. Weggeman testimony to Congress, pp. 7-8.

161. USCYBERCOM Combined Action Group, "Beyond the Build," p. 91.

162. Sherri Hanson, "24 AF/JFHQ-Cyber/AFCYBER Warfighter Perspective," luncheon presentation, San Antonio, TX: AFCEA Alamo Chapter, August 18, 2015, available from *http://www.alamoafcea.org/resource/resmgr/Files/24_AF_Briefing_-_150818.pdf*, accessed August 22, 2017. See also Brian Dutcher, "Iowa Air National Guard Cyber Protection Team," luncheon presentation, Omaha, NE: CERT Cyber Security Forum, August 2016, available from *https://www.nebraskacert.org/csf/CSF-Aug2016.pdf*, accessed August 24, 2017.

163. *Air Force Officer Classification Directory, The Official Guide to the Air Force Officer Classification Codes*, Joint Base San Antonio-Randolph, TX: Headquarters Air Force Personnel Center, October 31, 2016, pp. 78-79, available from *http://www.il.ngb.army.mil/PDFs/EmploymentForms/AFOCD%20Oct%2016.pdf*, accessed August 28, 2016. The suffix codes for Air Force Specialty Codes 17DX and 17SX are: A = Cyberspace Defense Analysis (CDA); B = Cyber Security and Control System (CSCS); C = Air Force Intranet Control (AFINC); D = Cyberspace Vulnerability Assessment/Hunter (CVA/Hunt); E = Cyber Command and Control Mission System (C3MS); F = Air Force Cyberspace Defense (ACD); Y = General; and Z = Other.

164. Burke "Ed" Wilson, lead auth., and Gregory Gagnon, Heather Blackwell, Michael Medgyessy, Andrew Miller, Brendan Criswell, Brandon Oxton, Tavis Ha, David Sorensen, Suzette Elliott, contrib., auths., " Embedding Airmenship in the Cyberspace Domain: The First Few Steps of a Long Walk," *Cyber Defense Review*, Vol. 1, No. 1, Spring 2016, pp. 30-31, available from *https://cyberdefensereview.army.mil/Portals/6/Documents/CDR-SPRING2016.pdf?ver=2016-09-14-122108-290*, accessed September 4, 2017.

165. USCYBERCOM Combined Action Group, "Beyond the Build," p. 92.

166. Ken Lustig, "Weapons school integrates cyber warfare," Nellis Air Force Base, NV: 99th Air Base Wing Public Affairs, May 30, 2012, available from *https://www.nellis.af.mil/DesktopModules/*

ArticleCS/Print.aspx?PortalId=104&ModuleId=14424&Article=284777, accessed September 25, 2017.

167. Lori A. Bultman, "Red Flag evolves as ISR, cyber presence increases," Joint Base San Antonio–Lackland, TX: 25th Air Force, January 26, 2017, available from *http://www.af.mil/DesktopModules/ArticleCS/Print.aspx?PortalId=1&ModuleId=850&Article=1060700*, accessed September 25, 2017.

168. *DoD Budget Request Overview FY 2018*, pp. 7-24.

169. Danny Holtzman, "Cyber Resiliency Office for Weapon Systems (CROWS)," Headquarters Air Force briefing, May 19, 2017, slide 10, available from *https://docplayer.net/63719451-Cyber-resiliency-office-for-weapon-systems-crows.html*, accessed September 14, 2018. The CCP seven lines of action (LOA) are: LOA 1: Perform Cyber Mission Thread Analysis; LOA 2: "Bake-In" Cyber Resiliency; LOA 3: Recruit, Hire & Train Cyber Workforce; LOA 4: Improve Weapon System Agility & Adaptability; LOA 5: Develop Common Security Environment; LOA 6: Assess & Protect Fielded Fleet; and, LOA 7: Provide Cyber Intel Support.

170. Weggeman, *Commander's Strategic Vision*, p. 7.

171. Weggeman testimony to Congress, p. 11. The mission and activities of the USAF Cyber Proving Ground (CPG) are described as:

> Its [CPG] mission is to identify, enable, and accelerate the fielding of innovative, operationally relevant concepts to improve Air Force, Joint, and Coalition cyberspace operations capabilities. The CPG leverages 24th Air Force's innovation and development capabilities and the existing cyber acquisition capabilities of Air Force Lifecycle Management Center's Crypto and Cyber Systems Division. The CPG is a foundry which brings together cyber operators, air force acquisition and engineering professionals, and private sector vendors with potential solutions to close capability gaps. While CPG projects are small in scope and timeframe, they comprise a broad spectrum of challenges, from complex development and testing efforts, to simple technical evaluations of existing technologies.

172. John Felker, "Coast Guard Cyber Command: Driving Mission Execution," National Defense Industrial Association presentation, August 2011, slide 2, available from *https://ndiastorage.blob.core.usgovcloudapi.net/ndia/2011/jointmissions/WednesdayFelker.pdf*, accessed November 1, 2018.

173. *United States Coast Guard Cyber Strategy,* Washington, DC: U.S. Coast Guard, June 2015, p. 10, available from *https://www.uscg.mil/Portals/0/Strategy/Cyber%20Strategy.pdf*, accessed August 28, 2017.

174. USCYBERCOM Combined Action Group, "Beyond the Build," pp. 87, 89.

175. MOA Regarding DoD and USCG Cyberspace Operations, p. 2. Per the MOA, the Coast Guard has specific responsibilities to DoD and DHS, which include:

> The Coast Guard will adhere to DoD cybersecurity requirements, standards, and policies, and will be responsive to the direction of Commander, U.S. Cyber Command, for Coast Guard-operated [DODIN] systems and networks and for Coast Guard information systems and networks that directly affect the [DODIN] and DoD mission assurance, while complying with DHS oversight and compliance requirements for acquisition, the Federal Information Security Management Act, and financial audit reporting.

176. Telfair Brown, "The Coast Guard's Cyber Operating Forces," U.S. Coast Guard video, available from *http://www.dvidshub.net/video/545307/coast-guards-cyber-operating-forces*, accessed August 28, 2017.

177. Chad Saylor, "Toward a Coast Guard Cyberspace Workforce," posted by Connie Terrell, Coast Guard All Hands, The Official Blog of the Coast Guard Workforce, March 9, 2017, available from *http://allhands.coastguard.dodlive.mil/2017/03/09/it-takes-a-cyber-village/,* accessed November 1, 2018.

178. Coast Guard Cyber Command, "Coast Guard Opens New Unit to Combat Cyberspace Threat," posted by Connie Terrell, Coast Guard All Hands, The Official Blog of the Coast Guard Workforce, June 19, 2017, available from *http://allhands.coastguard.dodlive.mil/2017/06/19/*

coast-guard-opens-new-unit-to-combat-cyberspace-threat/, accessed November 1, 2018. Details of the new Coast Guard Battle Bridge include:

> The Battle Bridge will be the center for exercising command and control of Coast Guard cyberspace operations, including coordination with Department of Defense (DoD), Department of Homeland Security (DHS) and allies to operate and defend our networks, enable Coast Guard operations and support other Coast Guard operational commanders to protect maritime critical infrastructure. From the Battle Bridge, CGCYBER will receive orders and direction from the Coast Guard commandant and U.S. Cyber Command commander, to defend Coast Guard networks and information systems as part of the .mil within DoD networks, and direct Coast Guard operations in and through cyberspace to achieve missions. This will include directing operations of the new Coast Guard Cyber Protection Team, a deployable specialized force that will maneuver inside cyberspace to defeat adversaries.
>
> In partnership with DHS, the new CGCYBER Battle Bridge is located on the watch floor with the DHS Enterprise Security Operations Center, responsible for defending DHS Headquarters networks. This location and CGCYBER's growing relationship with the DHS National Cybersecurity and Communications Integration Center positions CGCYBER as a unique bridge between DHS and DoD cyber operations.
>
> The Battle Bridge is one element of the geographically distributed Coast Guard Network Operations and Security Center (NOSC), which conducts the operation and defense of all Coast Guard cyberspace. The NOSC combines organizational elements that conduct network operations and defense functions, specifically the CGCYBER Cyber Security Operations Center, TISCOM Enterprise Services Operations Division, and C4IT Service Center Centralized Service Desk into a unified NOSC. Network operations, treated as mission support over the past 25 years, are now understood across the joint force as operational functions.

179. The number of CMF teams in table 7 of this monograph is based on the sources cited in earlier sections that described

service cyberspace components, along with the original breakout for the CMF established in the 2014 *Quadrennial Defense Review*. See Department of Defense, *Quadrennial Defense Review 2014*, Washington, DC: U.S. Government Printing Office, March 4, 2014, pp. 14-15. The 2014 *Quadrennial Defense Review* called for a total of 133 cyber teams to be available by fiscal year 2019: 13 National Mission Teams (NMTs) with 8 National Support Teams (NSTs); 27 Combat Mission Teams (CMTs) with 17 Combat Support Teams (CSTs); 18 National Cyber Protection Teams (CPTs); 24 service CPTs; and 26 combatant command and DoD information network (DODIN) CPTs.

180. Hanson, "24 AF/JFHQ-Cyber/AFCYBER Warfighter Perspective."

181. USCYBERCOM Combined Action Group, "Beyond the Build," pp. 88-89.

182. "All Cyber Mission Force Teams Achieve Initial Operating Capability."

183. "Defense Cybersecurity: DOD's Monitoring of Progress in Implementing Cyber Strategies Can Be Strengthened," Report GAO-17-512, Washington, DC: U.S. Government Accountability Office, August 2017, available from *https://www.gao.gov/assets/690/686347.pdf*, accessed August 22, 2017.

184. Image taken from Ibid., p. 8.

185. "Military Compensation: Additional Actions Are Needed to Better Manage Special and Incentive Pay Programs," Report GAO-17-39, Washington, DC: U.S. Government Accountability Office, February 2017, available from *https://www.gao.gov/assets/690/682508.pdf*, accessed August 22, 2017.

186. Thomas H. Barth, Jerome J. Burke, Stanley A. Horowitz, Mark F. Kaye, Drew Miller, and Linda Wu, *Staffing for Cyberspace Operations: Summary of Analysis*, IDA Document NS D-8089, Alexandria, VA: Institute for Defense Analyses, August 2016, p. 6, available from *https://www.ida.org/idamedia/Corporate/Files/Publications/IDA_Documents/CARD/2016/D-8089.ashx*, accessed August 29, 2017. The conclusion and methodology of the analysis are summarized as:

> The IDA CMF staffing analysis concluded that a more civilian-intensive force mix could save the DoD approximately $130 million dollars annually while maintaining compliance with DoDI 1100.22.
>
> A central element of IDA's methodology was determining what positions involve direct participation in cyber hostilities, which are deemed military essential. Criteria involving the intention to cause harm and the existence of a causal link between the actions of a billet holder and the infliction of damage were used. Upon this determination, the IDA research team developed an alternative force mix that satisfied the staffing criteria as economically as possible. The researchers calculated the full costs of military, government civilian, and contractor personnel for each Service's current force mix and the IDA alternative. (p. 2)

187. Report GAO-17-39, pp. 62, 68.

188. U.S. Army Training and Doctrine Command, *Multi-Domain Battle: Combined Arms for the 21st Century*, Information Paper, Fort Eustis, VA: U.S. Army Training and Doctrine Command, February 24, 2017, pp. 1, 3.

189. *Multi-Domain Battle: Combined Arms for the 21st Century*, p. 2.

190. Ibid., pp. 3-4. The MDB information paper provides a context for the importance of CO:

> Multi-Domain Battle evolves combined arms methodology to include not only those capabilities of the physical domains, but also greater emphasis on space, cyberspace, and other contested areas such as the electromagnetic spectrum, the information environment, and the cognitive dimension of warfare. In executing this concept, air, ground and maritime forces project power from air, land, and sea into other domains and contested spaces to support U.S. freedom of action. Thus, U.S. forces strive to affect an adversary in both the physical and abstract domains creating dilemmas too numerous to counter. (p. 4)

191. Paul M. Nakasone and Charlie Lewis, "Cyberspace in Multi-Domain Battle," *Cyber Defense Review,* Vol.

2, No. 1, Spring 2017, p. 10, available from *https://cyberdefensereview.army.mil/Portals/6/Documents/CDR%20Journal%20Articles/Cyberspace%20in%20Multidomain_Nakasone_Lewis.pdf?ver=2018-07-31-093725-297,* accessed November 1, 2018.

192. *Joint Operational Access Concept (JOAC)*, Version 1.0, Washington, DC: Department of Defense, January 17, 2012, p. 12, available from *https://dod.defense.gov/Portals/1/Documents/pubs/JOAC_Jan%202012_Signed.pdf,* accessed November 1, 2018.

193. Nakasone and Lewis, "Cyberspace in Multi-Domain Battle," p. 20.

194. Director, Operational Test and Evaluation (DOT&E), *FY 2016 Annual Report*, Washington, DC: Department of Defense, December 2016, p. 444, available from *http://www.dote.osd.mil/pub/reports/FY2016/*, accessed September 8, 2017. Table 2 of the *FY 2016 Annual Report* lists the cyber test teams for each of the services.

195. Eric K. Fanning, Memorandum for Deputy Chief of Staff, G-3/5/7, Subject: Delegation of Authority for Department of Defense Executive Agency Responsibility for Cyber Training Ranges, Washington, DC: Secretary of the Army, August 25, 2016.

196. DOT&E, *FY 2016 Annual Report*, pp. 442, 444, 446. The report cautions against creating two separate Executive Agents for cyberspace testing and cyberspace training:

> The FY15 NDAA [National Defense Authorization Act] directed DOD to establish an Executive Agent for cyber training ranges and an Executive Agent for cyber testing ranges. In FY16, the DOD allocated funds separately for a Persistent Training Environment, and for cyber test ranges. As combined testing and training are necessary for efficient use of the ranges, and to help address the rapidly increasing demand for cyber range resources, the creation of two separate Executive Agents—with separate responsibilities and funding—may hinder the Department's ability to effectively respond to rapidly evolving and increasingly sophisticated cyber threats. The DoD should designate a single Executive Agent for cyber ranges with the authority to oversee funding and personnel for all DoD-funded ranges, and the authority to identify and certify commercial cyber range resources for DoD use, as appropriate. (p. 446)

197. Todd Arnold, Rob Harrison, Gregory Conti, and David Raymond, *Professionalizing the Army's Cyber Officer Force*, Report 1337.2, West Point, NY: U.S. Military Academy, Army Cyber Institute, November 23, 2013, available from *https://cyber.army.mil/Portals/3/Documents/publications/internal/Professionalizing%20the%20Army's%20Cyber%20Officer%20Force.pdf*, accessed September 4, 2017.

198. Gregory Conti, Michael Weigand, Ed Skoudis, David Raymond, Thomas Cook, Todd Arnold, and Daniel Ragsdale, *Towards a Cyber Leader Course: Not for the Weak or Faint Hearted*, Report 1337.3, West Point, NY: U.S. Military Academy, Army Cyber Institute, May 26, 2014, available from *http://www.gregconti.com/publications/201405_CyberRanger_ACI.pdf*, accessed August 21, 2017.

199. DOT&E, *FY 2016 Annual Report*, p. 441.

200. DOT&E, *FY 2015 Annual Report*, Washington, DC: Department of Defense, January 2016, p. 389, available from *http://www.dote.osd.mil/pub/reports/FY2015/*, accessed September 8, 2017. The use of PCO teams in USPACOM was described as:

> In FY15, U.S. Pacific Command (USPACOM) leadership approved year-round activities of a Persistent Cyber OPFOR [opposing forces] (PCO) in order to portray a more realistic cyber adversary in training and assessment events, and make the most efficient use of scarce Red Team personnel. The PCO employs DOD-certified Red Teams in longer-duration activities to be more representative of enduring threat actors than can be portrayed in a brief exercise period. This PCO has already helped USPACOM find and remediate mission-critical vulnerabilities that might have otherwise gone undetected.

201. DOT&E, *FY 2015 Annual Report*, p. 391.

202. "Defense Innovation Initiative (DII)," Defense Innovation Marketplace website, available from *https://defenseinnovationmarketplace.dtic.mil/innovation/dii/,* accessed November 1, 2018.

203. DOT&E, *FY 2016 Annual Report*, p. 441.

204. Ibid., p. 446.

205. Edward C. Cardon, "The Future of Army Maneuver-Dominance in the Land and Cyber Domains," *The Cyber Defense Review*, Vol. 1, No. 1, Spring 2016, pp. 15-20, available from *https://cyberdefensereview.army.mil/Portals/6/Documents/CDR-SPRING2016.pdf?ver=2016-09-14-122108-290*, accessed November 1, 2018.

206. Jan Kallberg, "Strategic Cyberwar Theory—A Foundation for Designing Decisive Strategic Cyber Operations," *The Cyber Defense Review*, Vol. 1, No. 1, Spring 2016, pp. 113-128, available from *https://cyberdefensereview.army.mil/Portals/6/Documents/CDR-SPRING2016.pdf?ver=2016-09-14-122108-290*, accessed November 1, 2018. Dr. Kallberg offers an initial theory of strategic cyberwar that challenges some of the tenets of traditional warfare:

> As stated, traditional military theory applied to cyber conflict with four challenges: anonymity, object permanence, measurable results, and rapid execution. In a Westphalian and Clausewitzian geopolitical world these challenges were non-existent. The lack of object permanence nullifies maneuver, which until now has been essential in military strategy, and it replaces object permanence with a rapidly evolving kaleidoscope of nodes and bits. The massive anonymity in digital interchanges removes the ability to clearly understand who is your enemy, and based on that assessment gauge their abilities. Finally, with no measurement of effectiveness a fighting nation is unaware of the actual impact of the interchanges in tactical time frames and the rapid execution is likely to create a battle of which only the machines are fully aware. These four unique cyber tenets evaporate the opportunity to use traditional military thinking in cyber. If traditional military thinking is utilized to formulate a strategy, it is likely that the result would aggregate spurious assumptions and remove the opportunity for decisive offensive cyber operations as a geopolitical toolset. (p. 125)

207. Cynthia E. Ayers, "Rethinking Sovereignty in the Context of Cyberspace," *The Cyber Sovereignty Workshop Series*, Carlisle, PA: U.S. Army War College, Center for Strategic Leadership, December 2016, pp. 126-129, available from *https://csl.armywarcollege.edu/usacsl/Publications/Rethinking%20sovereignty.*

pdf, accessed September 4, 2017. Findings and recommendations from this workshop related to cyberspace theory include:

> Pursue development of cyberspace theory which incorporates cognitive sciences and philosophy, and is independent of current operational requirements. In layman's terms: while we're busy trying to keep the alligators at bay, let's have someone focus on trying to drain the swamp. (p. 126)
>
> Develop a comprehensive and accepted definition of cyberspace and theory of cyber power including all aspects of sovereignty, security, and offensive cyberspace operations. (p. 127)
>
> Theory—where is it that we can make a unique contribution? Since most of the other issues listed are being worked on by other organizations, theory is where we could make a unique contribution. Right now, however, it's an area that is being pursued by only a very few. (p. 129)

208. Jeffrey L. Caton, "On the Theory of Cyberspace," in J. Boone Bartholomees, Jr., ed., *U.S. Army College Guide to National Security Issues, Volume I: Theory of War and Strategy*, Carlisle, PA: Strategic Studies Institute, U.S. Army War College, June 2012, pp. 325-343. The chapter provides some initial axioms and considerations from cyberspace theory as well as examines how CO may relate to the principles of joint operations.

209. James Stavridis and David Weinstein, "Time for a U.S. Cyber Force," *Proceedings*, Vol. 140, No. 1, January 2014, available from *http://www.usni.org/print/28551*, accessed September 14, 2017. See also Gregory Conti and John Surdu, "Army, Navy, Air Force, and Cyber—Is it Time for a Cyberwarfare Branch of Military?" *IAnewsletter*, Vol. 12, No. 1, Spring 2009, pp. 14-18, available from *https://www.csiac.org/wp-content/uploads/2016/02/Vol12_No1.pdf*, accessed September 4, 2017.

210. Stavridis and Weinstein.

211. Sean Charles Gaines Kern, "Expanding Combat Power Through Military Cyber Power Theory," *Joint Force Quarterly*, No. 79, 4th Quarter, 2015, pp. 88-95.

APPENDIX I
ACRONYMS AND ABBREVIATIONS

A2/AD	anti-access/area denial
ACOIC	Army Cyber Operations and Integration Center
AFCYBER	Air Force Cyber Command
AFIN	Air Force Information Network
AFNET	Air Force Network
ARCOG	Army Reserve Cyberspace Operations Group
ARCYBER	Army Cyber Command
ASCC	Army service component command
CCoE	U.S. Army Cyber Center of Excellence
CEMA	Cyber Electromagnetic Activities
CEWCC	Cyberspace & Electronic Warfare Coordination Cell
CGCYBERCOM	Coast Guard Cyber Command
C-ISR	cyberspace intelligence, surveillance, and reconnaissance
CMF	Cyber Mission Force
CMTs	Combat Mission Teams
CNMF	Cyber National Mission Force
CNO	Chief of Naval Operations
CO	cyberspace operations
COMMARFORCYBERCOM	Commander, Marine Corps Forces Cyberspace Command
CPB	Cyber Protection Brigade
CPG	Cyber Proving Ground
CPTs	Cyber Protection Teams
CROWS	Cyber Resiliency Office for Weapons Systems
CSCB	Cyber Support to Corps and Below

CSSP	cybersecurity service provider
CSTs	Combat Support Teams
CTC	Army Combat Training Center
DCO	defensive cyberspace operations
DHS	Department of Homeland Security
DISA	Defense Information Systems Agency
DoD	Department of Defense
DODI	DoD Instruction
DODIN	DoD information network
DOT&E	Director, Operational Test and Evaluation
ECT	Expeditionary Cyber Team
EMS	electromagnetic spectrum
EW	Electronic Warfare
FA	functional area
FBI	Federal Bureau of Investigation
FCC	Fleet Cyber Command
FCC/C10F	Fleet Cyber Command/U.S. 10th Fleet
FLTCYBERCOM	Fleet Cyber Command
FM	Field Manual
FSCC	fire support coordination center
FY	fiscal year
HQDA	Headquarters, Department of Army
IE	Information Environment
IO	information operations
IW	information warfare
JCAC	Joint Cyber Analysis Course
JFHQ-C	Joint Force Headquarters-Cyber
JFHQs	Joint Force Headquarters
JRSS	Joint Regional Security Stack

JS J6	Joint Staff Directorate for Command, Communications, and Computer/Cyber
JTF	Joint Task Force
MAGTF	Marine Air Ground Task Force
MARFORCYBER	U.S. Marine Corps Forces Cyberspace
MCCOG	Marine Corps Cyberspace Operations Group
MCCYWG	Marine Corps Cyberspace Warfare Group
MCEN	Marine Corps Enterprise Network
MCEN Ops	Marine Corps Enterprise Network Operations
MDB	Multi-Domain Battle
MI	military intelligence
MIG	Marine Expeditionary Force Information Group
NAVCOMTELSTA	Naval Computer & Telecommunications Station
NAVIFOR	Naval Information Forces Command
NAVSOC	Naval Satellite Operations Center
NCDOC	Navy Cyber Defense Operations Command
NCTAMS	Naval Communication & Telecommunication Area Master Station
NCWDG	Navy Cyber Warfare Development Group
NETCOM	Network Enterprise Technology Command
NETWARCOM	Naval Network Warfare Command

NIOC	Navy Information Operations Command
NIWDC	Naval Information Warfare Development Command
NMT	National Mission Team
NOSC	Coast Guard Network Operations and Security Center
NST	National Support Team
OCO	offensive cyberspace operations
OPE	operational preparation of the environment
OPFOR	opposing forces
PCTE	Persistent Cyberspace Training Environment
PMW	Program Manager, Warfare
RCC	regional cyber center
SDAP	Special Duty Assignment Pay
SIGINT	signals intelligence
TFCA	Task Force Cyber Awakening
TRADOC	Training and Doctrine Command
TT&P	tactics, techniques, & procedures
USCYBERCOM	U.S. Cyber Command
USPACOM	U.S. Pacific Command
USSTRATCOM	United States Strategic Command

APPENDIX II:
KEY ARMY CYBER-RELATED PERSONNEL

ARMY OFFICER PERSONNEL
17A - Cyber Operations Officer Cyber branch is a maneuver branch with the mission to conduct defensive and offensive cyberspace operations (DCO and OCO). Cyber is the only branch designed to directly engage threats within the cyberspace domain.
29A - Electronic Warfare Officer The electronic warfare officer is the principal staff officer responsible for cyber protection and integration. This officer is responsible for conducting and coordinating electronic attacks, facilitating electronic protection, and providing electronic warfare support.
25A - Signal Officer The signal officer leads the Signal Corps, which is responsible for the Army's entire systems of communication. Officers plan and execute all aspects of communication on a mission and are critical to the Army's continued success.
35 - Military Intelligence Officer The Army's military intelligence [MI] is responsible for all collected intelligence during Army missions. They provide essential information that often save the Soldiers fighting on front lines. Military Intelligence Officers specialize in these specific areas: Imagery intelligence: Collection and analysis of imagery using photogrammetry and terrain analysis. All-Source intelligence: Performs collection management/surveillance/reconnaissance and provides advice. Counterintelligence: Provides coordination and participation in counterintelligence investigations, operations and production. Human intelligence: Controlled collection operations and interviews. Signals intelligence/electronic warfare: Collects signal intelligence and engages in electronic warfare. All-source intelligence aviator: Performs duties as an aviator/MI officer and participates in special electronic mission aircraft missions. Job Duties: • Command and coordinate the military intelligence Soldiers and combined armed forces. • Assess risks associated with friendly/enemy courses of action and act to counter/neutralize intelligence threats. • Use intelligence systems and data to reduce uncertainty for a commander.

Table II-I. Position Title and Description of Key Army Cyber-Related Personnel[1]

ARMY WARRANT OFFICER PERSONNEL
170A - Cyber Operations Technician
Performs as the Subject Matter Expert and advisor to the Commander and staff regarding the employment of offensive and defensive cyber operations assets and personnel. Directs plans, administers, manages, integrates, and assesses cyberspace operations. Develops policy recommendations and provides technical guidance regarding the operation and management of Army, Joint, intergovernmental, interagency, and multi-national cyberspace assets and personnel. Integrates cyberspace effects into warfighting functions in an effort to optimize combat effectiveness. Protects the Department of Defense Information Network against foreign and domestic threat vectors in order to maintain network integrity and functionality. Leads, trains, and mentors Cyber personnel through individual and group instruction, as well as the establishment, direction, and evaluation of Standard Operating Procedures and Job Qualification Standards.
255A - Information Services Technician
Information Services Technicians establish and maintain the ability to collect, process, store, secure, search for and discover, retrieve and disseminate information utilizing the application layer environment of the Army's portion of the Cyberspace domain; they enable information dissemination management/content staging in order to perform the required information management/knowledge management functions supporting combat information superiority and decision dominance. They supervise and manage the systems, services and personnel in operation centers that ensure efficient and effective caching, compiling, cataloging, retrieval and distribution of information as an element of combat power. Information services technicians plan, install, administer, manage, maintain, operate, integrate, service, secure and troubleshoot information systems and services to include Mission command systems and various automation information systems enabling voice, video, data and imagery processing. They manage the training of personnel on the planning, installation, administration, management, maintenance, operation, integration, servicing, securing and troubleshooting of information systems and services.
255N - Network Management Technician
Network Management Technicians transport the voice, video and data networks establishing and maintaining the transport layer environment of Army's portion of the Cyberspace domain through network management/enterprise systems management (NM/ESM) functions to include fault management, configuration management, auditing and accountability measures, maintaining performance standards, and implementing security measures at all levels in support of combat information superiority and command and control. They supervise and manage the operation and internetworking of telecommunications networks, network systems equipment, network nodal transmission and transport systems, network management system platforms, networked information systems and associated personnel at both the local area and wide area network level. They plan, install, administer, manage, maintain, integrate, operate, service, secure, optimize and troubleshoot communications networks and networked systems connectivity and capacity in order to transmit information as an element of combat power. They supervise and oversee network security planning and the implementation and use of electronic keys and frequency management to support communications networks and networked-systems. They manage the training of personnel on the planning, installation, administration, management, maintenance, integration, operation, servicing, securing, optimization and troubleshooting of communications networks and networked-systems.

Table II-I. Position Title and Description of Key Army Cyber-Related Personnel (cont.)

ARMY WARRANT OFFICER PERSONNEL
290A - Electronic Warfare Technician
The electronic warfare specialist advises and assists the commander on electronic warfare operations. This person makes use of electromagnetic and directed energy to control the electromagnetic spectrum (EMS) and defeat the enemy through planning, coordination, integration, and execution of electronic attack (EA), electronic protection (EP), and electronic support (ES).
352N - SIGINT Analysis Technician
Manages personnel and equipment to collect, process, exploit, locate, identify, analyze and report on SIGINT [signals intelligence] information to support tactical, operational, and strategic requirements across all domains. Establishes priorities and provides guidance and oversight for collection, exploitation, analysis and reporting missions. Manages training for subordinates and peers on technical, operational, and tactical SIGINT skills required to perform the mission. Coordinates staff actions to fulfill all requirements in support of SIGINT mission activities and the Commander's intent. Advises the commander and staff with regard to tactical and technical SIGINT operations, activities, and personnel.
352S - Signals Collection Technician
Performs as the Subject Matter Expert (SME) and advisor to the Commander in regards to Signals Intelligence (SIGINT) collection, analysis. Manages personnel and equipment to collect, process, locate, identify, analyze and report on SIGINT information to support tactical, operational, and strategic requirements across all domains. Manages training for subordinates and peers on technical, operational, and tactical SIGINT skills required to perform the mission. Coordinates staff actions to fulfill all requirements in support of SIGINT mission activities and the Commander's intent.
ARMY ENLISTED PERSONNEL
17C - Cyber Operations Specialist
Cyber Operations Specialists conduct integrated and synchronized offensive cyberspace operations by targeting enemy and hostile adversary activities and capabilities. These specialists also conduct defensive operations to protect data, networks, net-centric capabilities, and other designated systems. They are responsible for detecting, identifying, and responding to attacks against friendly networks with other lethal and nonlethal actions that enable commanders to gain an advantage in cyberspace, across all domains.
25D - Cyber Network Defender
The cyber network defender performs specialized computer network defense duties, including infrastructure support, incident response, auditing and managing. The cyber network defender also protects against and detects unauthorized activity in the cyberspace domain and uses a variety of tools to analyze and respond to attacks.

Table II-I. Position Title and Description of Key Army Cyber-Related Personnel (cont.)

ARMY ENLISTED PERSONNEL
25U - Signal Support Systems Specialist Signal support systems specialists are primarily responsible for working with battlefield signal support systems and terminal devices. This equipment needs to consistently work in order for the Army to direct the movement of its troops.
29E - Electronic Warfare Specialist The electronic warfare specialist advises and assists the commander on electronic warfare operations. This person makes use of electromagnetic and directed energy to control the electromagnetic spectrum (EMS) and defeat the enemy through planning, coordination, integration, and execution of electronic attack (EA), electronic protection (EP), and electronic support (ES).
35N - Signals Intelligence Analyst A signals intelligence analyst examines foreign communications/activity and relays that information by producing combat, strategic and tactical intelligence reports.
35P - Cryptology Linguist A cryptologic linguist is primarily responsible for identifying foreign communications using signals equipment. Their role is crucial as the nation's defense depends largely on information that comes from foreign languages.
35Q - Cryptologic Network Specialist A Cryptologic Network Warfare Specialist performs initial cryptologic digital analysis to establish target identification and operational patterns; identifies, reports, and maintains Intelligence information in support of Commander's Intelligence Requirements and uses technical references to analyze information.
35S - Signals Collection Analyst The signals collector/analyst is primarily responsible for the detection, acquisition, location and identification of foreign electronic intelligence. They exploit nonvoice communications and other electronic signals to provide strategic/tactical intelligence.

Table II-I. Position Title and Description of Key Army Cyber-Related Personnel (cont.)

ENDNOTES – APPENDIX II

1. Officer and enlisted information was taken verbatim from the specific position webpages available from *http://goarmy.com/careers-and-jobs/browse-career-and-job-categories.html,* accessed September 3, 2017. Warrant officer information was taken verbatim from the specific position webpages available from *http://www.usarec.army.mil/hq/warrant/,* accessed November 1, 2018.

APPENDIX III:
KEY MARINE CORPS CYBER-RELATED PERSONNEL

MARINE CORP OFFICER PERSONNEL
0605 - Cyber Network Operations Officer
The Cyber Network Operations Officer develops, plans, and implements the overall tactical and strategic goals of the MAGTF [Marine Air Ground Task Force] computer network systems. Evaluates and recommends changes to current and future network requirements to meet the operational needs. They are responsible for the implementation of IA, CND, and NetOps in support of cyber operations. The duties include: providing technical and administrative support to the commander and higher headquarters staff during the identification, resolution, and tracking of computer security incidents or events; provide long-term and near-term CND analysis and planning for resolving systemic and enterprise computer events and/or intrusions across the MAGTF networks; and develop, research, publish, test and update related SOPS methodologies, and tools, techniques and procedures. They provide liaison to the T/S-3 within the MAGTF to synchronize the activities among CND [Computer Network Defense], CNO [Computer Network Operations], CNE [Computer Network Exploitation], and CNA [Computer Network Attack].
MARINE CORP WARRANT OFFICER PERSONNEL
0650 - Cyber Network Operations Engineer
Cyber Network Operations Engineer Officers supervise and manage the security, planning, and operation of Information Technology (IT) Systems. With a primary focus in the functional areas of Internet Protocol based Local and Wide Area Networks, they plan and supervise the installation and management of IT systems. They provide technical direction in conjunction with the overall communications control effort relating to the security, installation and performance of IT systems within MAGTF, Joint, and coalition networks. Additionally, they provide technical guidance required to procure and integrate enterprise IT systems in the development of Marine Corps plans and policy for current and future operations.

Table III-I. Position Title and Description of Key Marine Corps Cyber-Related Personnel[1]

MARINE CORP ENLISTED PERSONNEL
0651 - Cyber Network Operator
Cyber Network Operators are responsible for the installation, configuring and management of cyber network systems in both stand alone and client-server environments including Microsoft based curriculum and MS Exchange/Server, CISCO Certified Network Associate (CCNA) modules 1-4 as well as other authorized cyber network systems. They install, configure and maintain cyber services, both hardware and software. They also plan and execute the integration of multiple information systems to include Data Distribution System-Replacement/Modular (DDS-M), in a network environment, evaluate and resolve customer information system problems and effect hardware upgrades and repair to maintain mission capability. Skill progression for Staff Sergeant through Corporal is the Cyber Network Supervisor Course.
0659 - Cyber Network Systems Chief
Cyber Network Systems Chiefs perform advanced systems installation, operation, integration and troubleshooting in order to maintain optimum secure cyber communication systems. They plan and supervise the installation, configuration and maintenance of all cyber communication systems and network services in both a garrison and deployment environment. Cyber Network Systems Chiefs plan and design local and wide area networks and link heterogeneous networks through the application of appropriate cyber and telecommunication hardware and software. Skill progression training for Gunnery Sergeants and Staff Sergeants is the Cyber Systems Chief Course.

Table III-I. Position Title and Description of Key Marine Corps Cyber-Related Personnel (cont.)

MARINE CORP ENLISTED PERSONNEL
0681 - Information Security Technician
Provide day-to-day operation of the DoN's [Department of the Navy] COMSEC Material Control System (CMCS). The duties include: coordinate for the provisioning of symmetric and asymmetric key products to support C4 and C2 systems while work[ing] in collaboration with communications planners for the development of communications instructions and support for elements of the Marine Air Ground Task Force (MAGTF) or other authorized elements requiring authorized support, provide information regarding new or revised COMSEC policies and procedures and their impact on the command, train and inspect COMSEC users within the command, monitors and maintains the command COMSEC material allowances, performs spot checks of users to assess adherence to prescribed instructions. Also may serve as a Central Office of Record (COR) Auditor for COMSEC account inspections. Entry-level input to this MOS may be from any MOS at the grade of Staff Sergeant.
0689 - Cyber Security Chief
Cyber Security Chiefs are responsible for all aspects of ensuring Marine Corps information systems data availability, integrity authentication, confidentiality, and non-repudiation. Computer network defense specialists implement and monitor security measures for USMC communication information systems networks, and advise the commander that systems and personnel adhere to established security standards and governmental requirements for security on these systems. Duties include assisting in the development and execution of security policies, plans, and procedures; design and implementation of data network security measures; network intrusion detections and forensics; information system security incident handling; and certification of Marine Corps systems and networks. The skill progression training for Master Gunnery Sergeant through Staff Sergeant is the Information Assurance Managers Course (IAM) and Cyber Security Chiefs Course.

Table III-I. Position Title and Description of Key Marine Corps Cyber-Related Personnel (cont.)

ENDNOTES – APPENDIX III

1. Officer information was taken verbatim from Marine Corps Order 1200.17E, *Military Occupational Specialties Manual*, Washington, DC: Commandant of the Marine Corps, August 8, 2013, available from *https://www.marines.mil/Portals/59/MCO%201200.17E.pdf,* accessed November 1, 2018. Enlisted information was taken verbatim from the specific position webpages, see the MOS dropdown under "Find & Select Related Credentials," Marine Corps COOL: Credentialing Opportunities On-Line, available from *https://www.cool.navy.mil/usmc/*, accessed September 24, 2017.

APPENDIX IV:
KEY NAVY CYBER-RELATED PERSONNEL

NAVY OFFICER PERSONNEL
1810 - Cryptologic Warfare . . . directly involved in every aspect of Naval operations—delivering information to decision-makers by attacking, defending and exploiting networks to capitalize on vulnerabilities in the information domain. As a CWO [Cryptologic Warfare Officer], you will employ a thorough understanding of sensors and weapons, strategy and tactics, as well as national systems' capabilities and limitations.[1]
1820 - Information Professional . . . plan, acquire, secure, operate and maintain the Naval network and the systems that support Navy operations and business processes.[2]
1830 - Intelligence Supervise the collection, analysis and dissemination of critical information. . . .Provide intelligence support to US Naval forces and multinational military forces. . . . Advise executive-level decision makers in US government. . . . Lead Enlisted personnel in gathering and analyzing mission-sensitive intelligence.[3]
1840 - Cyber Warfare Engineer Provide defense against attacks and deliver tactical advantages. Develop tools and techniques in the information environment that ensure situational awareness.[4]
NAVY CHIEF WARRANT OFFICER PERSONNEL
781X (744X) - Information Warfare Technician . . . serve as officer technical leaders and managers in the field of cryptology, versed in all facets of Signals Intelligence, Computer Network Operations and Electronic Warfare. Perform functions of electronic maintenance, communications, CMS [Combat Management System], and technical research in support of the operating forces and the national cryptologic effort. They plan and manage the employment of resources, equipment and manpower; operation and maintenance of electrical, electromechanical equipment and the conduct of communications, administration of CMS functions.[5]
782X (742X) - Information Systems Technician . . . serve as an officer technical specialist in the field of informations [sic] systems, communications (fixed/mobile) suites, satellite communications systems, knowledge management and information assurance. They plan and direct the installation of equipment and administer the operations and maintenance of data processing installations.[6]

Table IV-I. Position Title and Description of Key Navy Cyber-Related Personnel

NAVY CHIEF WARRANT OFFICER PERSONNEL
783X (745X) - Intelligence Technician
Serve as an officer technical specialist in the following intelligence discipline: Human Intelligence (HUMINT), Operational Intelligence (OPINTEL), and Carrier Air Wing (CVW) Targeting. They supervise and direct intelligence personnel in assembling and analyzing HUMINT reports, multi-source OPINTEL of surface, sub-surface, and air activity and CVW strike missions in support of intelligence analysis, reporting, and briefing. Intelligence CWOs [chief warrant officers] supervise and direct intelligence personnel in the following: interviewing and preparation of various HUMINT reports; preparation of intelligence material utilized in planning strike and photographic reconnaissance missions; preparation of graphics including annotated photographs, plot sheets, mosaics and overlays; plotting and preparing multi-sensory imagery and OPINTEL reports; providing input to and receiving data from various computerized intelligence systems afloat and ashore; and maintenance of intelligence files including digital photographs, maps, and charts and soft/hard copy libraries.[7]
784X - Cyber
. . . operate, analyze, plan and direct full-spectrum cyber operations.[8]
NAVY ENLISTED PERSONNEL
Cryptologic Technician Interpretive (CTI)
CTIs serve as experts in linguistics (including Arabic, Chinese, Korean, Persian-Farsi, Russian and Spanish) and deciphering information in other languages. Their responsibilities include: • Collecting, analyzing and exploiting foreign language communications of interest • Transcribing, translating and interpreting foreign language materials • Providing cultural and regional guidance in support of Navy, Joint Force, national and multinational needs.[9]
Cryptologic Technician Maintenance (CTM)
CTMs serve as experts in the preventive and corrective maintenance of sophisticated cryptologic equipment, networks and systems. Their responsibilities include: • Installing, testing, troubleshooting, repairing or replacing cryptologic networks, physical security systems, electronic equipment, antennas, personal computers, auxiliary equipment, digital and optical interfaces, and data systems • Configuring, monitoring and evaluating Information Operations (IO), Information Warfare (IW) systems and Information Assurance (IA) operations.[10]

Table IV-I. Position Title and Description of Key Navy Cyber-Related Personnel (cont.)

NAVY ENLISTED PERSONNEL
Cryptologic Technician Networks (CTN) CTNs serve as experts in communication network defense and forensics. Their responsibilities include: • Monitoring, identifying, collecting and analyzing information • Providing computer network risk mitigation and network vulnerability assessments and incident response/reconstruction • Providing network target access tool development • Conducting computer network operations worldwide in support of Navy and Department of Defense missions.[11]
Cryptologic Technician Collection (CTR) CTRs serve as experts in intercepting signals. Their responsibilities include: • Analyzing and reporting on communication signals using computers, specialized computer-assisted communications equipment, video display terminals and electronic/magnetic tape recorders • Exploiting signals of interest to identify, locate and report worldwide threats • Providing tactical and strategic signals intelligence, technical guidance, and information warfare support to surface, subsurface, air and special warfare units.[12]
Cryptologic Technician Technical (CTT) CTTs serve as experts in airborne, shipborne and land-based radar signals. Their responsibilities include: • Operating electronic intelligence-receiving and direction-finding systems, digital recording devices, analysis terminals, and associated computer equipment • Operating systems that produce high-power jamming signals used to deceive electronic sensors and defeat radar-guided weapons systems • Providing technical and tactical guidance in support of surface, subsurface, air and special warfare operations.[13]
Intelligence Specialist (IS) Intelligence Specialists play no small part in the success of America's Navy. [Their responsibilities include]: • Collect, process, analyze, organize and disseminate information • Prepare detailed materials that communicate findings • And, ultimately, help generate insight that has strategic and tactical implications all over the world.[14]

Table IV-I. Position Title and Description of Key Navy Cyber-Related Personnel (cont.)

NAVY ENLISTED PERSONNEL
Information Systems Technician (IT)
. . . [ITs] engage in a broad range of responsibilities including network administration, database management and computer hardware and software implementation. Their responsibilities include: • Operating and maintaining Navy global satellite telecommunications systems • Serving as admin on mainframe computers and local and wide area networks • Implementing micro-computer systems throughout the Fleet[15]

Table IV-I. Position Title and Description of Key Navy Cyber-Related Personnel (cont.)

ENDNOTES – APPENDIX IV

1. See "Responsibilities," under the "More Information," section in "Cryptologic Warfare Careers," available from *https://www.navy.com/index.php/careers/cryptologic-warfare*.

2. Ibid.

3. See "Responsibilities," under the "More Information," section in "Information Professionals Careers," available from *https://www.navy.com/careers/information-professional*.

4. See "About," in "Military Intelligence Careers," available from *https://www.navy.com/careers/military-intelligence*.

5. See "About," in "Cyber Warfare Engineer Careers," available from *https://www.navy.com/careers/cyber-warfare-engineer*.

6. See "781X - Cryptological Warfare Technician," under "CWO DESIGNATOR CAREER PATTERN SHEETS," Navy Personnel Command, last modified September 6, 2018, available from *http://www.public.navy.mil/bupers-npc/officer/communitymanagers/active/ldo_cwo/Pages/Career%20Path%20Sheets.aspx*.

7. See "782X – Information Systems Technician," under "CWO DESIGNATOR CAREER PATTERN SHEETS,"

Navy Personnel Command, last modified September 6, 2018, available from *http://www.public.navy.mil/bupers-npc/officer/communitymanagers/active/ldo_cwo/Pages/Career%20Path%20Sheets.aspx*.

8. See "783X - INTELLIGENCE TECHNICIAN," under "CWO DESIGNATOR CAREER PATTERN SHEETS," Navy Personnel Command, last modified September 6, 2018, available from *http://www.public.navy.mil/bupers-npc/officer/communitymanagers/active/ldo_cwo/Pages/Career%20Path%20Sheets.aspx*.

9. See Andrea Perez, "Cyber Warrant Officer Program Broadens Eligibility," Navy News, Story Number: NNS131025-05, October 25, 2013, available from *https://www.navy.mil/submit/display.asp?story_id=77266*, accessed September 24, 2017.

10. See "Responsibilities," under the "More Information," section in "Cryptologic Technician Careers," available from *https://www.navy.com/index.php/careers/cryptologic-technician*.

11. Ibid.

12. Ibid.

13. Ibid.

14. Ibid.

15. See under heading "Intelligence Specialist," archived page available from *https://web.archive.org/web/20170511000237/https://www.navy.com/careers/information-and-technology/intelligence-specialist.html#ft-key-responsibilities*.

APPENDIX V:
KEY AIR FORCE CYBER-RELATED PERSONNEL

AIR FORCE OFFICER PERSONNEL
17DX – Network Operations **17SX – Cyber Warfare Operations** Executes cyberspace operations and information operations functions and activities. Plans, organizes, directs and executes cyberspace and information operations such as, Defensive Cyber Operations (DCO), Offensive Cyber Operations (OCO), Department of Defense (DoD) Information Network [DODIN] Operations and Mission Assurance for Air Force weapons systems and platforms. Such operations cover the spectrum of mission areas within the cyberspace domain.[1]
AIR FORCE ENLISTED PERSONNEL
1B4X1 – Cyberspace Warfare Operations Performs duties to develop, sustain, and enhance cyberspace capabilities to defend national interests from attack and to create effects in cyberspace to achieve national objectives. Conduct Offensive Cyberspace Operations (OCO) and Defensive Cyberspace Operations (DCO) using established tactics, techniques and procedures (TTPs) to achieve Service, CCMD, and national objectives. Executes command and control (C2) of assigned cyberspace forces and de-conflicts cyberspace operations across the kinetic and non-kinetic spectrum. Supports cyberspace capability development, testing and implementation. Partners with Joint, Interagency, Intergovernmental, and Multinational forces to detect, deny or manipulate adversarial access to sovereign national cyberspace systems.[2]

Table V-I. Position Title and Description of Key Air Force Cyber-Related Personnel

AIR FORCE ENLISTED PERSONNEL
D0X1 – Knowledge Management
Develop, govern, and monitor processes, technologies, and practices that support organizations to identify, capture, organize, and employ information in both fixed and deployed environments. These information assets comprise of raw data, documents, practices, policies, and individual expertise. Core competencies of Knowledge Managers include: professional networking, social collaboration, Communities of Practice (CoP), enterprise information systems technology, business continuity, cross-functional data sharing, and process-improvement.[3]
3D0X2 – Cyber Systems Operations
Installs, supports and maintains server operating systems or other computer systems and the software applications pertinent to its operation, while also ensuring current defensive mechanisms are in place (IAVA Patches, etc.), and responding to service outages and interruptions to network operations. Administers server-based networked systems, distributed applications, network storage, messaging, and application monitoring required to provision, sustain, operate and integrate cyber networked systems and applications in garrison and at deployed locations. Core competencies include: server operating systems, database administration, web technologies, systems-related project management and supervising computer operators. Supports identification, reconnaissance and remediation of vulnerabilities while enhancing capabilities within cyber environments to achieve desired affects.[4]

Table V-I. Position Title and Description of Key Air Force Cyber-Related Personnel (cont.)

AIR FORCE ENLISTED PERSONNEL
3D0X3 – Cyber Surety
Performs risk management framework security determinations of fixed, deployed and mobile information systems (IS) and telecommunications resources to monitor, evaluate and maintain systems, policy and procedures to protect clients, networks, data/voice systems and databases from unauthorized activity. Identifies potential threats and manages resolution of communications security incidents. Enforces national, DoD and Air Force security policies and directives to ensure Confidentiality, Integrity and Availability (CIA) of IS resources. Administers and manages the overall cybersecurity program to include Communications Security (COMSEC), Emissions Security (EMSEC) and Computer Security (COMPUSEC) programs.[5]
3D0X4 – Computer Systems Programming
Supervises and performs as computer analyst, coder, tester and manager in the design, development, maintenance, testing, configuration management, and documentation of application software systems, client-server, and web-enabled software and relational database systems critical to warfighting capabilities.[6]
3D1X1 – Client Systems
Deploys, sustains, troubleshoots, and repairs standard voice, data, desktop video and network client devices in fixed and deployed environments. Sustains and operates systems through effective troubleshooting, repair, and system performance analysis. Manages client user accounts and organizational client device accounts.[7]
3D1X2 – Cyber Transport Systems
Deploys, sustains, troubleshoots, and repairs standard voice, data, and video network infrastructure systems, IP detection systems and cryptographic equipment. Performs, coordinates, integrates, and supervises network design, configuration, operation, defense, restoration, and improvements. Analyzes capabilities and performance, identifies problems, and takes corrective action. Fabricates, terminates, and interconnects wiring and associated network infrastructure devices.[8]

Table V-I. Position Title and Description of Key Air Force Cyber-Related Personnel (cont.)

AIR FORCE ENLISTED PERSONNEL
3D1X3 – RF Transmission Systems
Deploys, sustains, troubleshoots, and repairs standard radio frequency wireless, line-of-sight, beyond line-of-sight, wideband, ground-based satellite, and encryption transmission devices in a fixed and deployed environment. Included are multiple waveform systems operating across the spectrum, keying and signal devices; telemetry and instrumentation systems. Establishes and maintains circuits, configures and manages system and network connectivity.[9]
3D1X4 – Spectrum Operations
The Spectrum Operations technician analyzes requirements and requests frequencies to support terrestrial, aircraft and space systems and coordinate radio, radar, land, and other electromagnetic radiating or receiving requirements. They possess a solid understanding of wireless communications systems technologies and configurations and provide guidance to program offices, developers, and potential users of radiating and receiving equipment planned for introduction into the Air Force inventory and for modification to existing equipment.[10]

Table V-I. Position Title and Description of Key Air Force Cyber-Related Personnel (cont.)

ENDNOTES – APPENDIX V

1. "AFSC 17X Cyberspace Operations Officer," CFETP 17X, Washington, DC: Headquarters, Department of the Air Force, June 1, 2015, p. 11, available from *http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/cfetp17x/cfetp17x.pdf*.

2. "AFSC 1B4X1 Cyber Warfare Operations," CFETP 1B4X1, Washington, DC: Headquarters, Department of the Air Force, July 15, 2018, p. 12, available from *http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/cfetp1b4x1/cfetp1b4x1.pdf*.

3. "AFSC 3D0X1 Knowledge Management," CFETP 3D0X1, Washington, DC: Headquarters, Department of the Air Force,

September 1, 2014, p. 14, available from *http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/cfetp3d0x1/cfetp3d0x1.pdf*.

4. "AFSC 3D0X2 Cyber Systems Operations," CFETP 3D0X2, Washington, DC: Headquarters, Department of the Air Force, June 1, 2015, p. 15, available from *http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/cfetp3d0x2/cfetp3d0x2.pdf*.

5. "AFSC 3D0X3 Cyber Surety," CFETP 3D0X3, Washington, DC: Headquarters, Department of the Air Force, December 15, 2014, p. 16, available from *http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/cfetp3d0x3/cfetp3d0x3.pdf*.

6. "AFSC 3D0X4 Computer Systems Programming," CFETP 3D0X4, Washington, DC: Headquarters, Department of the Air Force, August 1, 2013, p. 11, available from *http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/cfetp3d0x4/cfetp3d0x4.pdf*.

7. "AFSC 3D1X1 Client Systems," CFETP 3D1X1, Washington, DC: Headquarters, Department of the Air Force, April 1, 2015, p. 16, available from *http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/cfetp3d1x1/cfetp3d1x1.pdf*.

8. "AFSC 3D1X2 Cyber Transport Systems," CFETP 3D1X2, Washington, DC: Headquarters, Department of the Air Force, September 1, 2014, p. 18, available from *http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/cfetp3d1x2/cfetp3d1x2.pdf*.

9. "AFSC 3D1X3 Radio Frequency (RF) Transmissions Systems," CFETP 3D1X3, Washington, DC: Headquarters, Department of the Air Force, May 15, 2015, p. 18, available from *http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/cfetp3d1x3/cfetp3d1x3.pdf*.

10. "AFSC 3D1X4 Spectrum Operations," CFETP 3D1X4, Washington, DC: Headquarters, Department of the Air Force, March 1, 2015, p. 15, available from *http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/cfetp3d1x4/cfetp3d1x4.pdf*.

U.S. ARMY WAR COLLEGE

Major General John S. Kem
Commandant

*****

STRATEGIC STUDIES INSTITUTE
AND
U.S. ARMY WAR COLLEGE PRESS

Director
Professor Douglas C. Lovelace, Jr.

Director of Research
Dr. Steven K. Metz

Author
Jeffrey L. Caton

Editor for Production
Dr. James G. Pierce

Publications Assistant
Ms. Denise J. Kersting

*****

Composition
Mrs. Jennifer E. Nevil

FOR THIS AND OTHER PUBLICATIONS, VISIT US AT
https://www.armywarcollege.edu/

ISBN 1-58487-797-9

9 781584 877974 90000 >

This Publication

SSI Website

USAWC Website