REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
May 10, 2018	Master's of MIlitary Studies	SEP 2017 - MAY 2018

4. TITLE AND SUBTITLE

Advanced Education for the Cyber Workforce:
Addressing a Key Vulnerability in the Marine Corps

5a. CONTRACT NUMBER
N/A

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
N/A

6. AUTHOR(S)
Smith, Jason R., Major, USMC

5d. PROJECT NUMBER
N/A

5e. TASK NUMBER
N/A

5f. WORK UNIT NUMBER
N/A

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
USMC Command and Staff College
Marine Corps University
2076 South Street
Quantico, VA 22134-5068

8. PERFORMING ORGANIZATION REPORT NUMBER
N/A

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Approved for public release, distribution unlimited.

10. SPONSOR/MONITOR'S ACRONYM(S)
Benitez, Jorge, Ph.D.

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

12. DISTRIBUTION / AVAILABILITY STATEMENT

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The focus of this paper is to research the current cyber operation environment in which the Marine Corps is operating and determine if the established training systems provides the adequate depth of knowledge and understanding required for its senior cyber workforce. While there are many variables that go into cyber operations, this paper focuses specifically on what the Marine Corps is currently doing for training and where it needs to develop to meet the emerging threats and technological advancements within the cyber domain. This paper seeks to showcase where the Marine Corps can take advantage of lessons learned from its sister services and industry to develop an advanced education program focused on developing a cadre of well educated cyber professionals. Additionally, this paper points out unique capabilities and assets that are already available to the Marine Corps in order to establish an advanced cyber education program quickly.

15. SUBJECT TERMS

Cyber; education; Quantico; senior cyber managers; cyber wokforce

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
					USMC Command and Staff College
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**	UU	29	**19b. TELEPHONE NUMBER** *(include area code)*
Uncass	Uncass	Uncass			(703) 784-3330 (Admin Office)

United States Marine Corps
Command and Staff College
Marine Corps University
2076 South Street
Marine Corps Combat Development Command
Quantico, Virginia 22134-5068

MASTER OF MILITARY STUDIES

Advanced Education for the Cyber Workforce: Addressing a Key Vulnerability in the Marine Corps

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

AUTHOR: Major Jason Smith

AY 2017-18

Mentor and Oral Defense Committee Member: Jorge Benitez
Approved: Jorge Benitez
Date: 4/30/18

Oral Defense Committee Member: Matthew Flynn
Approved:
Date: 4/30/18

Oral Defense Committee Member: LtCol Pennella, B.S.
Approved: B.S.
Date: 4/30/18

LtCol Vega, R.J.
30 Apr 2018

Executive Summary

Title: Advanced Education for the Cyber Workforce: Addressing a Key Vulnerability in the Marine Corps

Author: Major Jason Smith

Thesis: In order for the Marine Corps to successfully operate in the complex cyber domain, it must improve the senior cyber workforce through the implementation of selective recruitment, development of an advanced cyber education program, and development of a cyber institute to manage the education and integration of cyber operations throughout the MAGTF.

Discussion:
The USMC's current defensive cyber security education for the senior cyber workforce is an *ad-hoc* system of individual initiative, individuals selected for advanced education programs through annual boards, and reliance on abbreviated certification courses that focus on passing a test rather than a comprehensive understanding of network management and defense. The current gap in education of the senior cyber workforce creates a substantial risk in the operation and management of Command, Control, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) platforms. The failure to address educational requirements for advanced network defense and cyber operations to the senior cyber workforce is a huge oversight that the current structure of training does not sufficiently answer.

Conclusion: Failure to establish a cohesive advanced cyber education program which meets the specific needs of the Marine Corps' senior cyber workforce will exacerbate the current critical vulnerability in network and will hamper the Marine Corps ability to operate within the increasingly contested cyber domain.

DISCLAIMER

Table of Figures

Table of Contents

Introduction

The cyber domain is a complex global environment made up of physical, logical, and the cyber-persona layers. Each of these layers consists of systems, interdependent network connections, software, information, and devices interacting with people in order to provide connectivity throughout the information environment. The Department of Defense (DoD) utilizes these interconnected systems of systems in order to transport network traffic that enables command and control. Specifically, the interconnected systems of systems allows the DoD to develop network architectures that utilize commercial and governmental network backbones in order to enable commanders the ability to conduct command and control throughout the world. The installation, operation, maintenance, and defense of these systems requires a thorough understanding of the fundamental principles on which the networks operate and transfer data.

The same vast interconnected systems that allows the DoD to communicate over great distances also open the DoD networks and command control systems up to vulnerabilities from malicious actors, misconfigurations, and poor security procedures that can lead to compromise of data, exfiltration of critical information, or denial of access to systems required for operational success. Mitigating these vulnerabilities requires advanced education in the underlying technologies, systems, and procedures utilized to counter threats to DoD networks. The Marine Corps is currently facing a gap in cyber education within its senior cyber workforce created by the inability to maintain pace with advancing cyber threats and complex, interconnected systems. In order to rectify this gap and meet the environmental challenges within the ever changing cyber domain, the Marine Corps must develop an advanced education program for the senior cyber workforce.

Explaining the Problem

The Department of Defense relies on data networked systems that operate in the cyber domain and are capable of carrying providing command and control across all domains. Land, sea, air, and space operations all rely on communications systems that operate within and through the cyber domain. Whether providing for command and control of critical satellite systems, ship navigation, or communications data for ground based units, cyber is pervasive within all domains. Department of Defense networks must provide confidentiality, integrity, and availability when forces require them for operations and the service components are task accordingly with developing a cyber workforce that can ensure that their portions of the Department of Defense networks are secure.

While the Department of Defense relies on United States Cyber Command (USCYBERCOM) to direct the defense of DoD Information Networks through its service component representatives, it is the responsibility of the services to ensure that the acquisition of systems, development of network operation frameworks, and education of the cyber workforce are established in a fashion that protects government data systems. As the Marine Corps looks to the future of cyber operations with the establishment of MARFORCYBER as the service component representative to USCYBERCOM, it also takes stock of the relative capabilities of our adversaries and the high probability that operations within cyberspace will spill over into the other domains.[1] Additionally, a hard look must be taken at current network defense strategies and educational requirements to ensure that the Marine Corps maintains competence within an ever changing networked environment.

As adversarial forces attempt to gain military parity with the United States through means other than conventional force, they will continue to look at low cost capabilities provided through cyber operations to establish an effective counter to military power. Cyber operations

provide a low cost, low risk capability with drastic implications for modern militaries. Disruption and destruction of government information systems and the embedding of remote access tools can allow adversaries the ability to create chaos during operations. Admiral Michael Rogers, Commander of USCYBERCOM and Director of the National Security Agency stated:

> Hardly a day has gone by during my tenure at Cyber Command that we have not seen at least one significant cybersecurity event occurring somewhere in the world. We face a growing variety of advanced threats from actors who operate with ever-more sophistication and precision.[2]

Attribution for cyber-attacks is particularly difficult and while claims from groups and reports from the cyber security industry can be dubious, they do express the potential capabilities of the nation's adversaries to carry out ever increasing lethal cyber-attacks against government agencies. CrowdStrike, an American cyber security firm, reported that cyber-attacks conducted by the Russian hacker organization FANCY BEAR from 2014 to 2016 against Ukrainian artillery units provided geographic location data to Russian military intelligence and allowed them to effectively target Ukrainian artillery forces.[3] While attribution of the attack source that compromised the geolocation data may complicate the claim regarding the accuracy of this report, the possible utilization of malware to locate individuals utilizing their personal communications devices is a realistic threat that spotlights the immediate impact that offensive cyber operations can have when fused with kinetic operations. The utilization of malware against mobile devices in a combat zone in order to gain geolocation data of enemy forces is a prime example of the changing role of adversarial tactics within the cyber domain.

Cyber-attacks are not just limited to countries currently in conflict. The United States Department of Homeland Security (DHS) and Federal Bureau of Investigation (FBI) released Joint Technical Alerts providing details concerning North Korean cyber-attacks on U.S. targets that have been occurring since 2016.[4] The attacks targeted everything from media outlets to

critical infrastructure sectors. The U.S. Computer Emergency Readiness Team provides multiple reports which show that even small countries with limited global influence and military might can affect much larger nations through the cyber domain.[5]

The transition from disruption to exploitation shows that there is an ever increasing need to provide robust security for systems utilized by military members and forces. As advanced cyber exploitation tools become easier to obtain and the sophistication require to operate them decreases, their use will continue to become increasingly popular with future adversaries. Additionally, as the Marine Corps looks to employ a wider range of command and control systems to the tactical edge of operations, it exposes network systems, software, and personnel to the risk of exploitation by cyber actors. The push of processing power to the tactical edge will require a robust defense, solid foundation on advanced network defense, and comprehensive risk mitigation processes to ensure that forces are protected from exploitation and risk. Operations within this complex domain required highly educated professionals with a thorough understanding of underlying languages and principles on which these systems operate as well as a knowledge of how best to manage the both network systems and the personnel that operate them.

Increased vulnerabilities:

The complex systems of systems involved in the creation of the modern communication networks has drastically increased the number of available vulnerabilities that cyber actors can utilize to subvert network defense systems and cyber security procedures. With the ever increasing amount of software, hardware, and code being introduced into military command and control systems, the Marine Corps' exposure to vulnerabilities drastically increased over the last ten years.

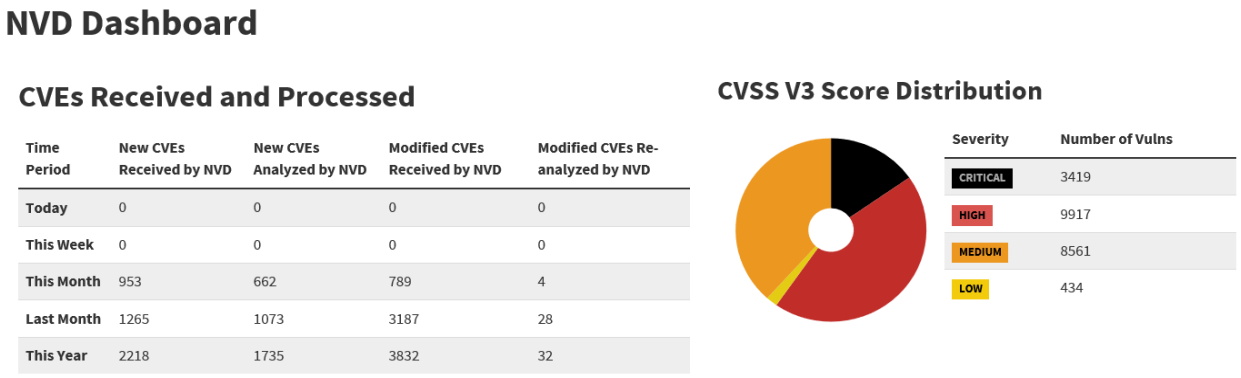
A Center for Strategic & International Studies 2018 study reported that there were 39 significant cyber incidents in 2016.[6] The same study reported that in 2017 there were 59 significant incidents, an increase of 51% in the course of one year.[7] While this report only captures significant cyber incidents, the increase in number shows an ever increasing utilization of cyber as a method of attacking resource capabilities and decision making systems of businesses and government agencies.[1]

Businesses are not the only organizations that are at risk from the increased number of vulnerabilities associated with complex communications systems. Major General Lori E. Reynolds, the Commanding General of Marine Forces Cyber Command (MARFORCYBEROM), testified before the Senate Armed Services Subcommittee on Cybersecurity that the Marine Corps Cyber Operations Group (MCCOG), the organization tasked with the defense of the Marine Corps Enterprise Network (MCEN), "responded to 4,050 events on the MCEN" between May, 2016 and May, 2017.[8] The 4,050 events included unauthorized network access, security vulnerabilities due to non-compliance with cyber security standards, network reconnaissance, and attributed configuration anomalies. The response to these events can range from patch management, systems audits, revocation of access, restriction of privileges, and active defensive measures to identify and deny future threat capabilities. Although these actions will likely increase the cyber hygiene of network systems, a new batch of vulnerabilities is already being exploited by adversarial cyber actors.

The National Institute of Standard and Technology reported over 2,000 Common Vulnerabilities and Exposures (CVE) on the National Vulnerability Database (NVD) between January and February of 2018.[9] The year 2017 was a record high for reported CVEs at over

[1] A detailed active cyber-attack map is available at: http://map.norsecorp.com/#/

14,000.[10] While not all of these vulnerabilities present a risk to DoD communications networks, they do show an increase in the number of reported cyber security vulnerabilities that could be utilized to compromise a Marine Corps command and control networks. The drastic rise in vulnerabilities highlights the complexity of implementing cyber defense in an ever changing environment and the potential for exposure to advancing adversarial cyber capabilities.



NVD Dashboard

CVEs Received and Processed

Time Period	New CVEs Received by NVD	New CVEs Analyzed by NVD	Modified CVEs Received by NVD	Modified CVEs Re-analyzed by NVD
Today	0	0	0	0
This Week	0	0	0	0
This Month	953	662	789	4
Last Month	1265	1073	3187	28
This Year	2218	1735	3832	32

Figure 1. National Vulnerability Dashboard (NVD) retrieved from NIST: https://nvd.nist.gov/general/nvd-dashboard

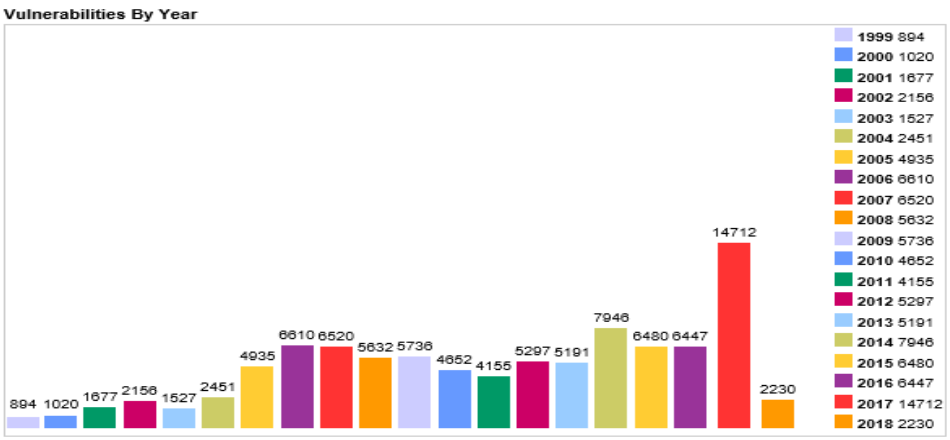


Figure 2. Common Vulnerability Exposure (CVE) by year list retrieve from: https://www.cvedetails.com/browse-by-date.php

Advanced Threat Capabilities

The use of intricate systems vulnerabilities and target based code to severely damage the Iranian nuclear program was a prominent example that the subversion of technology has become drastically more sophisticated. The advancement of cyber-attack tools and techniques poses a continually changing threat environment for DoD networks. The attacks that systems technicians faced in 1988 from the Morris Worm are considerably less advanced than those posed by threat actors in the modern cyber environment. Today's cyber threat actors have a litany of software, hardware, and systems vulnerabilities that are exploitable. Even obscure vulnerabilities in a portion of code can lead to the successful access to systems of the elevation to privileged access. A key example of this advancement in technical capabilities and effects on DoD systems can be seen in the Heartbleed vulnerability.

Far from an unintended replication of a computer virus like the Morris Worm, Heartbleed is a flaw in the OpenSSL encryption technology that enables secure communications over the internet through email, instant messaging, and virtual private networks. The vulnerability creates a buffer overflow due to a missing bounds check and allows cyber actors to steal information, communications, and credentials.[11] In 2014 when Heartbleed was reported, OpenSSL had been utilized as a secure connection method for internet transactions for two years without identification of the vulnerability. The detection of an attack from Heartbleed is very difficult due to the establishment of a legitimate connection and the cyber actor capturing data within the transaction. Usual Intrusion Detection Systems would not identify the activity as outside of the standard connection transaction. Once the Heartbleed vulnerability was identified and a fix was developed for the OpenSSL software, DoD was quick to mitigate the vulnerability, but the

advanced nature of the threat underpins the potential for sophisticated cyber-attacks and requirement for advanced understanding of threat capabilities.

Exponential Advancement of Technology

Cyber security professionals must have a comprehensive understanding of the information that they are responsible for and be capable of making security decisions that ensure the confidentiality, integrity, and availability of that data. This requires that the professional have an understanding of existing and emerging threats and how to best utilize the security tools that are available to them. Education is the key to being capable of making informed decisions concerning threat analysis and the development of a comprehensive security architecture.

During an Armed Forces Communication and Electronics Association's luncheon, John Zangardi, the Principle Deputy Chief Information Officer for the DoD, said "We can't solve today's complex problems with yesterday's thinking or technologies."[12] This is particularly important for service components within the Department of Defense. In many cases, education is limited to specific times during a member's career. Even within these limited opportunities, education competes with the high rate of deployments, changes in assignments, and requirement to fill key-billets for retention and promotion. Additionally, network infrastructure, defense systems, and software follow the similar stringent controls on acquisitions as other end items, such as tanks. This slow approach to acquisitions fails to recognize the exponential rate of development of systems and software within the communications sector. Network managers and technicians are required to utilize the equipment fielded to them that may not have the most capable cyber defense capabilities available and must contest with ever advancing technologies and threats. Although the senior cyber workforce may be facing a technological gap created by the exponential advancement of the technologies expressed in Ray Kurzweil's Law of

Accelerating Returns, this gap can be diminished by a well-educated cyber workforce that is able to identify key vulnerabilities and develop defense strategies that meet those requirements.[13] This ability to mitigate the gap requires continued advanced education and exposure to emerging technologies not currently prescribed in the USMC's senior cyber workforce training courses.

Marisa Viveros, Vice President in charge of leading Cyber Security innovation initiative for IBM Cooperation, explains that, "One important way to achieve enhanced security is to design it from the start, in new application development, in how data is managed, and in the construction of IT infrastructure. Employers should invest in IT employee's training, encouraging and supporting the pursuit of related certificates and degrees from graduate schools and other outside programs."[14] She proposes that cyber security experts are provided an opportunity to continue to receive education past the entry level to ensure that they understand the underlying principles, languages, and protocols as well as advancements in techniques and systems capabilities as they progress through their carriers. Through education in defensive cyber capabilities, network managers and technicians will understand how to build security into data networks and respond to the advancing complexities of communications networks. Additionally, in its FY 2017 Annual Report, Director, Operational, Test, and Evaluation (DOT&E) stressed the importance of human capital as the key to cyber operations, "DOT&E observations continue to highlight that human expertise is essential for effective cyber operations, including defensive cyberspace operations, offensive cyberspace operations, and cyber adversarial teams." [15]

The USMC's current defensive cyber security training for the senior cyber workforce is an *ad-hoc* system of individual initiative, individuals selected for advanced education programs through annual boards, and reliance on abbreviated certification courses that focus on passing a

test rather than a comprehensive understanding of network management and defense. The current gap in education of the senior cyber workforce creates a substantial risk in the operation and management of Command, Control, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) platforms. The failure to address educational requirements for advanced network defense and cyber operations to the senior cyber workforce, who are responsible for the management and defense of these networks, is a huge oversight that the current training curriculum does not sufficiently answer.

Cyber Workforce Vulnerabilities: Creating a Gap

USMC Introductory Training vs Education

As the senior members of the cyber workforce, communication officers are exposed to introductory communications training through the Basic Communications Officer Course (BCOC), a 21 week course designed to familiarize students with Marine Corps communications systems and techniques for employment. This introductory course provides an expedited training package that introduces junior officers to the capabilities and limitations of communications equipment utilized within the MAGTF. With the limited training timeline, junior officers are provided a large amount of information in a short period. Much of this information only provides a cursory amount of information pertaining to the basic of communications technology. Cyber security training is provided with the Data Package portion of the course and only touches on the topics of change management, vulnerability identification, and security.

Communication officers can, but are not required to, receive follow on training through the MAGTF Planner's Course (MCPC), a 10 week course that is designed to prepare Captains for assignments as Marine Expeditionary Unit S-6, Regimental S-6, Communications Battalion and Squadron Operations Officers, and Major Subordinate Command (MSC) G-6 level.[16] While

MCPC does provide training for the familiarization, planning, and employment of Department of Defense Information Network Operations (DODIN OPS), Offensive Cyber Operations (OCO), and Defensive Cyber Operations (DCO), the 10 week course does not provide an education specifically designed to develop advance network defense managers or cyber operations specialists. In many cases this course is a refresher for communications officers that have been in non-communications billets and are completing assignment to resident professional military education programs.

Neither BCOC nor MCPC are designed to make communications officers highly trained network defense professionals familiar with extensive cyber security techniques and procedures. Rather they serve as an introductory training curriculum providing communications officers with a wide breath of knowledge from satellite systems, telephony, radio, multiplex, video teleconferencing, data networking, and communications control.

Communication officer receive their first formal exposure to network defense and cyber security training through the completion of certification requirements. Although all communication officers are required to comply with the Department of Defense 8410 Information Assurance (IA) Workforce Improvement Program, completion of certification requirements does not provide advanced cyber defense training or an understanding of the DoD network defense structure.[17] Maintenance of currency in IA Workforce requirements does require the individual to seek out continued education to maintain relevancy within the communications field but follow on courses are not evaluated based on operational requirements. The relevance of the courses selected for training maintenance depends on the individual seeking continued education and is approved by the company that holds the certification, not the Marine Corps. Utilization of concepts learned during certification training must be merged with

operating techniques and procedures utilized within enterprise network operations and integrated with a thorough understanding of adversarial threat capabilities. Certification training, while a measure of baseline understanding of network security concepts, does not equate to a thorough understanding of network defense systems integration and cyber operations.

There is no established requirement for senior officer to receive any further training in communications outside of the Basic Communications Officer Course for advancement and little incentive exists for the individual to search out advanced cyber education. With no requirement and no incentive for officers to obtain advanced degrees in cyber security, the Marine Corps fails to ensure that the officer in charge of the installation, operation, management, and defense of data communications networks have the proper education to meet the needs of tomorrows precarious cyber environment.

Coupled with the gap in education for advanced information technology management and cyber security is an inconsistency in the exposure to commands that work within these environments. Since the preponderance of Marine Corps training involves on the job training (OJT), exposure to duties associated with a Marine's military occupation are usually dictated by which command levels and where within a command that individual is serving.

The inconsistency in training, in this case on-the-job and command level exposure, fails to create a cadre of experienced cyber security managers within the Marine Corps cyber workforce with a common baseline of education in the cyber domain. Additionally, this is complicated by the fact that only specific command levels operate network security tools, typically Communications Company and above for MCEN tactical communications and MAGTF IT Support Center Branches within Marine Corps Installations G-6s and above for MCEN garrison networks. The assignment of officers to specific commands that have a high

exposure rate to cyber operations and advanced network security is limited and the individual does not always have the opportunity to influence their assignments. Furthermore, assignment to one of these commands may not be advantageous to a Marine's career progression as there is no requirements for communications officers to serve in any of these specific commands for career advancement.

While the certification courses, BCOC, and MCPC courses provide entry based training concerning data networks and security, advanced network defense and cyber operations education is relegated to a system of personally sought courses and individuals selected for advanced degree programs. The reliance on self-motivated study and limited number of personnel that are accepted to advanced cyber degree programs cannot meet requirements for advanced senior cyber workforce and do not assist in providing education to the large number of senior cyber workforce personnel required by the Marine. Additionally, operation tempo and traditional Marine Corps Professional Military Education further constrain the time available for senior cyber workforce professionals to complete advanced cyber security and cyber education programs.

While the Marine Corps looks for a way to address gaps in the current advanced cyber workforce educational systems, it lags behind the other services that identified advanced cyber education as a key contributor to the development of a professional cyber workforce. By utilizing traits from the educational systems established by the Air Force, Army, Navy, and private industry cyber defense institutes, the Marine Corps can develop a framework for an educational program to meet its future force requirements.

Air Force

The Air Force training program for the 17X Cyberspace Operations Officer, as captured in the Career Field Education and Training Plan, provides a tiered training progression from entry to staff officer level. The tiered progression of education allows the Air Force to develop a cadre of Cyberspace Officers that complete continuing education courses at each level of their career while serving in positions that expose them to operational relevance between educational courses. The training progression is separated into four main levels: entry, initial, qualified, and staff level. Each of these levels has an associated educational requirement commiserate with the level of assignment within the cyberspace workforce. Entry level training requires that 17X Cyberspace Operation Officer attend an undergraduate cyber training. Beginning at the Captain rank, Cyberspace Operations Officers are required to complete the Air Forces Cyberspace 200 course. This course focuses on planning, directing, and executing offensive and defensive cyber operations. Additionally, beginning at the rank of Major, Cyberspace Operations Officers are required to complete the Cyberspace 300 course. The Cyberspace 300 course provides a "broad background in cyber concepts, including capabilities, limitations, and vulnerabilities and their associated application and employment in joint military operations."[18] Finally, Cyberspace Operations Officers are required to complete the Cyber 400 course beginning at the rank of Lieutenant Colonel focusing on policy implementation.

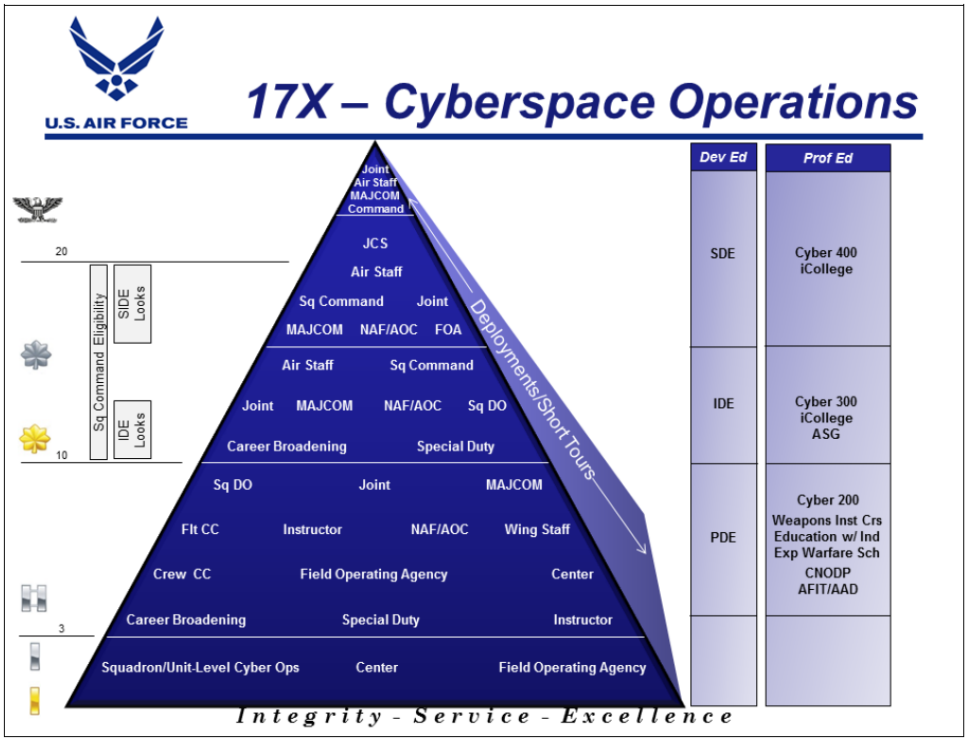


Figure 3. 17X Career Field Pyramid, US Air Force
Department of the Air Force

As with all Department of Defense Cyber Workforce, Cyberspace Operations Officers are also required to complete the appropriate level DoD 8140 certification and maintain currency. Further advanced educational opportunities are available through the Air Force Institute of Technology (AFIT).

The Air Force established the Center for Cyberspace Research at the Air Force Institute of Technology in March of 2002. As the Air Forces Cyberspace Technical Center of Excellence, the Center for Cyberspace Research faculty provide direction and education to graduate level students in cyber research with a focus on advanced defensive and protection capabilities development. AFIT offers two graduate level courses that provide for network defense and cyber operations education. AFIT's Master in Computer Science provides a graduate level course work focused on in six categories: Artificial Intelligence, Computer Networks, Database Systems, High Performance Computing, Cyber Security, and Software Engineering. AFIT's Graduate

Cyber Operations (GCO) Program is an eighteen month graduate level program that culminates with a Master of Science in Cyber Operations. Students can select from a wide variety of topics within the cyber realm to include both offensive and defensive cyber operations, data security, cyber forensics, and management. Concise and well structured, the Air Force's Cyberspace Operations Officer educational path is a focused model that the Marine Corps can utilize as a reference in the development of future network defense and cyber operations program.

Army

The United States Army established the Cyber Leader College at Fort Gordon on August 4, 2014. The college provides training and education of the Army's Cyber Soldiers to include: Defensive Cyberspace Operations (DCO), Offensive Cyber Operations (OCO), Electronic Warfare (EW), and the integration of cyber and electronic warfare capabilities.

Initial training for the 17A Cyber Officer is the Cyber Basic Officer Leadership Course (CyBOLC). The Cyber Basic Officer Leadership Course is a 37 week entry level course designed to provide Lieutenants with an introductory knowledge of planning and executing cyber operations. Included in the Cyber Basic Officer Leadership Course curriculum are 8140 certification courses for both CISCO Certified Network Associate Routing and Switching and (ISC)2 Certified Information Systems Security Professional.

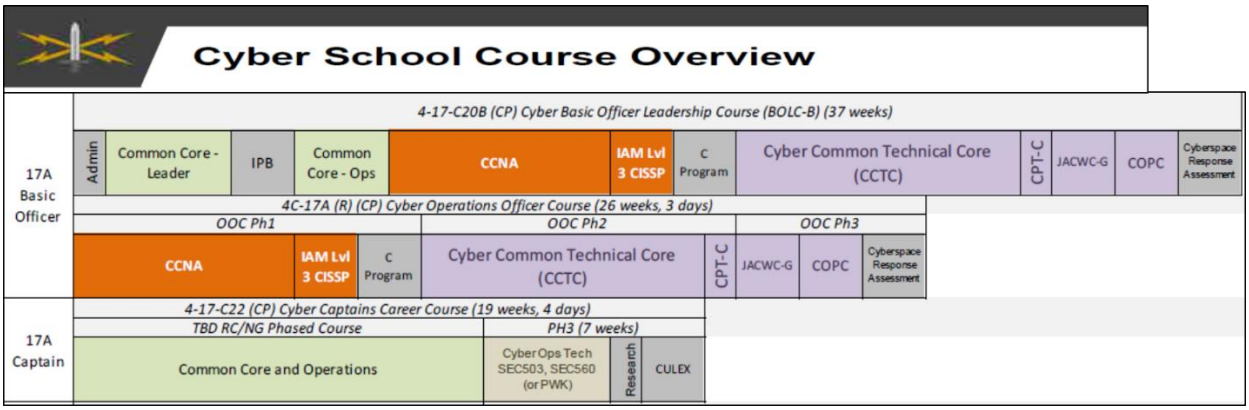


Figure 4. 17A Cyber Basic Officer Leadership Course and Cyber Captain Career Course Overview, US Army Department of the Army

The Cyber Leader College also offers the Cyber Captain Career Course (CCCC), a 13 week program designed to provide Captains with the skills to lead, plan, and direct defensive and offensive cyber operations.[19] In addition, the Army has integrated industry leading cyber training courses from SANS and Joint level cyber training into its Cyber Operations Officer education program. The utilization of select industry and Joint courses allows the Army to refine training relevant to its operational requirements into its educational program and ensures a well-trained cyber workforce. Additionally, it allows for the introduction of up-to-date training from top security institutes in the industry.

Navy

In October of 2016, the United States Navy broke ground on the Center for Cyber Security Studies. The facility, located at the Naval Academy (USNA) in Annapolis, Maryland, was established to provide cyber operations courses to midshipmen. The USNA provides both a cyber operations major as well as requires that all students take cyber security classes. This investment in the future of the Navy's cyber workforce as well as the development of an educated user base shows a commitment to the defense of Navy networks. Though the Center for Cyber Security Studies will not be complete until sometime in 2019, the undergraduate Cyber Operations Major and courses are already available for mid-shipmen.

Additional opportunities for midshipman with the Cyber Operations Major includes internships with the National Security Agency, Defense Information Agency, or Naval Research Labs. Graduates of the Cyber Operations Major are eligible to be selected for the Information Professional and Information Warfare career paths. By providing a direct educational path at the Naval Academy, the Navy has ensured that advanced education in defensive cyber operations are

constructed into the career path for future officers. Additionally, the Navy provides multiple advanced degree programs through the Naval Post Graduate Program related to defensive cyber operations and computer science.

The Naval Postgraduate School's Computer Science Department provides graduate certificate, Master of Science, and PhD programs in Computer Science and Cyber Security. The Master of Science in Computer Science (368) is an 18 to 24-month program broken into seven quarters. The course covers a wide breadth of advanced studies within computer science to include: programming, operating systems, computer architecture, artificial intelligence, and database systems.

Specialization can be completed in one of six areas: Cyber Security and Defense (CSD), Network and Mobility (N&M), Autonomous Systems and Data Science (ASDS), Software Engineering, Cyber Operations, or focus in modeling and simulation. Requirements for admission to the Masters of Science is substantial and requires "above-average grades in mathematics, (including differential and integral calculus)."[20] Additionally, preferred applicants will have undergraduate degrees in applied science or engineering.

In addition to the Master and PhD programs, NPS offers a number of Graduate Certificates through its departments and groups. The Computer Science Department provides three Graduate Certificates: Cyber Security Fundamentals, Cyber Security Defense, and Cyber Security Adversarial Techniques. The Cyber Academic Group provides two Graduate Certificate Programs: Cyber Operations Infrastructure (227/228) and Applied Cyber Operations (226). The Electronic and Computer Engineering Department offer Cyber Warfare and Cyber Systems graduate certificates while the Applied Mathematic Department provides Mathematics of Secure Communications. Graduate certificates are "a non-degree program designed to enable

participants to gain a foundational understanding of basic concepts and methods involved with computer network defense, vulnerabilities, and exploitations."[21] The graduate certificates offer an incredible opportunity to provide succinct, packaged education while providing graduate course credits to those that attend. Of the eight certificate programs offered only three require residence and the remaining five can be completed through distance learning.

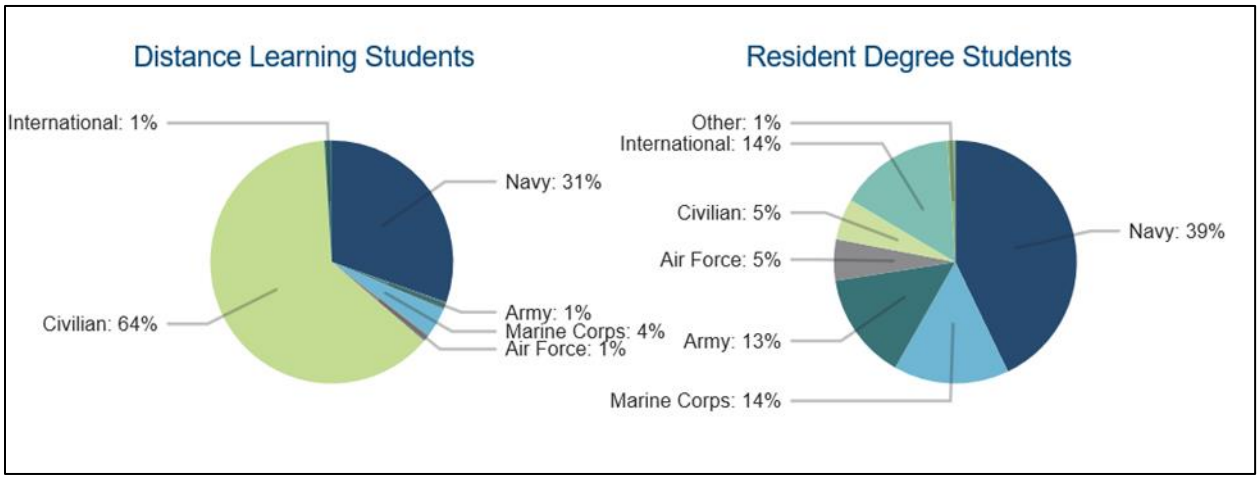


Figure 5. Attendance Statistics from Naval Post Graduate School. Retrieved from frhttps://my.nps.edu/academics

While Naval Post Graduate School offers an incredible educational opportunity for the senior cyber workforce member that can fit it into their career path and has the pre-requisite educational background to qualify for admission, current attendance numbers is not adequate to meet the higher education requirements to the entire senior cyber workforce throughout the Marine Corps. Marine Officers are typically selected to resident the Naval Postgraduate School through two annual boards, the Commandant's Professional Intermediate-Level Education Board (CPIB) or the Commandant's Career-Level Education Board (CCLEB). Additionally, individuals can apply through the Special Education Program (SEP). However, SEP is a competitive selection board with designated billet payback requirements that is limited to a handful of officers per fiscal year. On the other hand, the graduate certificate courses provide an example of

modular learning packages that can be provided over the course of a career in order to ensure a constant flow of education within the cyber domain and allow for the completion of continuing educational requirement for DoD 8140 certifications.

SANS Institute

The SANS Institute is a private company that provides industry leading information security training and certification. It also offers a multitude of modular education programs including cyber security, network security, forensics, auditing, security management, penetration testing, and application security. These modular courses are provided through graduate certificates or through a cyber security degree program. The modular nature of the courses allows the individual to enroll in blocks of courses that are digestible at the students pace. The programs are provided via live and virtual classroom courses, online at your own pace, or through webcast with instructors. This ability to push the educational courses in a modular fashion to be completed at the individuals own pace is ideal for military service members with high tempo operational assignments. Through the distributed education model, ensuring that education is available is less dependent on the location of a member's duty assignment and offers more opportunity to complete advanced education.[22]

Fixing the Problem

The Marine Corps Operating Concept 2016 states that future Marine Forces will be required to conduct Network Operations in a Contested Network Environment.[23] The operation and defense of DoD information systems is a critical task, but the Marine Corps is facing an educational gap in the cyber workforce that current military occupation specialty training is incapable of meeting.[24] Marine Corps command and control systems are at a higher risk than ever from attacks based on an advancing adversarial threat capability, increase in the number of

vulnerabilities, and the exponential advancement in technology. In order to mitigate these threats, it is critical that the Marine Corps develops an advanced cyber education program for its senior cyber workforce that provides a comprehensive understanding of these threats and understanding of how to mitigate them.

The future of combat operations by the Marine Corps hinges on professional education for senior cyber workforce in advanced defense, maintenance, and security of USMC networks. Without the development of a professional, capable senior cyber workforce, the Marine Corps risks significant failure of command and control systems in future conflicts. The Marine Corps must implement an advanced educational program with a curriculum focused on meeting cyber threats that will be faced as we move towards a more technologically interlaced future. An updated USMC education program needs to focus on three critical areas; selective recruitment, development of an advanced curriculum with a professional degree program, and establishment of an educational institute to manage the program.

Selective recruitment is an essential first step to producing high quality cyber Marines in sufficient numbers to meet the exponential growth in demand for their expertise. In order to improve the initial assignment of personnel to the cyber workforce and attract a cadre of well educated professionals, the Marine Corps must establish a tighter selection process and provide "cyber contracts" to persons with relevant educational backgrounds. The establishment of a specified contract to the cyber workforce is similar to the contracts offered to pilots, but would require a minimum of an undergraduate education in either computer science or information systems. Additionally, bonuses for coding language could be offered similar to foreign language competency. Finally, the advanced cyber education course completion must be tied to the promotion process and personnel must be provided adequate time in order to finish the

requirements within their career progression. Failure to incentivize advanced cyber education within the senior cyber workforce will prevent the Marine Corps from developing a robust cadre of capable personnel that can operate in the ever increasingly complex cyber environment.

In addition to producing a cyber workforce with more relevant education and experience, the curriculum and organization of their advanced education and training needs to be improved. The advanced education program should be developed similar to graduate level courses and certificate programs found in other higher education environments and focus on modular education packages that can be consumed in small bites. These modular courses would allow the student to complete a selected, focused education package with more flexibility. Modular course packages would need to be tiered, building on the education from the previous package and becoming more advanced as the student progressed. Additionally, this advanced education program should include a distance learning program in order to ensure the widest possible distribution. The development of an advanced education program will allow for the flexible inclusion of recent threats analysis, participation of industry leading defense specialists, and interactive discussions concerning the current state of cyber operations by senior cyber workforce personnel from within the Marine Corps. The interaction can assist in identifying trends, best practices, and assist in developing operational response packages that can be utilized throughout the Marine Corps and DoD.

A new cyber educational program for the United States Marine Corps should include the establishment of an advanced cyber school located in Quantico. Students benefit from hands on utilization of information attained through educational programs and cyber operations are no different. Most advanced education programs have a portion of their coursework that requires that the student utilize their newly acquired learning in a lab environment. A cyber school

located in Quantico, VA has the added benefit of proximity to the Department of Defense Cyber Range. Portions of the education packages would allow the student the opportunity to utilize their education in an interactive network environment that is segregated from "live" network environments, thus increasing their understanding of the operational uses of cyber operations.

Selective Recruitment

Complications of the assignment to military occupation specialties (MOS) begins at The Basic School, where Marines select and are assigned their MOS not on the merits of their previous education but through a selection process. Lieutenants are asked to rank all available MOS in order of priority. Once the graduating class is broken into thirds, the process begins assigning Marines based on their top selection. If the Marines number one choice is available he will be assigned that MOS, if not the process looks at the second and third choices respectively. Similarly process continues with the middle third and the bottom third. The process was developed in order to ensure quality distribution and give the greatest likelihood that a Marine will get an MOS in the top five on their list. Some consideration is given to prior background for Marines that were previously enlisted, but this is based on the Basic School staff conducting the selection process. This process, while exceptional for quality distribution and fairness, does not select individuals with degrees and special interest to MOS related positions within the cyber workforce.

Although not a direct solution for the advancement of senior cyber workforce education within the Marine Corps, actively recruiting and selecting Officer Candidates with Computer Science and Information Technology degree backgrounds for positions as Communications Officers and Cyber Operations Officers would assist in developing a cadre of educated entry level officers. Coupled with a well-developed, mature educational program directed at each

career level, the Marine Corps would be capable of establishing a qualified senior cyber workforce. Specific details for selection would be based on relevant degree and completion of program from an accredited school.

An Advanced Curriculum and Professional Degree Program

Utilizing lessons learned from the Air Force and the Army in the development of cyber operations training, the Marine Corps can quickly evaluate its operational cyber education requirements and develop a professional degree program that focuses advanced cyber education and integration of operations. Establishing a tiered program that creates a core competency in network defense, adversarial capabilities, DoD network infrastructure, and offensive operations will provide the Marine Corps with an educated cyber workforce able to plan, install, operate, and maintain robust, resilient command and control networks and reduce risk to personnel and systems.

Similar to the Air Force and the Army's tiered approach to cyber operations training, the Marine Corps must establish a comprehensive education program that builds on proven industry techniques for the development of cyber security professional. Integrated into this program should be courses covering the fundamentals of planning network security, network hardening techniques, auditing, penetration testing, intrusion detection, change management, and incident response. Courses should be structured to match the requisite skill required to operate at the appropriate level of command the officer is expected to serve. Initial educational focus should be given to theory and concepts of network defense, followed by technical implementation network defense systems, and integration of offensive and defensive cyber operations. As each Marine cyber expert advances, their education should progress to enterprise management and developing strategies for the implementation defensive cyber operations. In addition, introduction to

adversary threat capabilities and offensive cyber operations should be integrated throughout the education program. This seamless integration of education and operational context helps develop active thinkers that can apply what they have learned in the classroom to the battlefield.

By developing the education program in a modular construct, similar to the SANS Institute and NPS graduate certificate modules, the Marine Corps can capitalize on organized packets of education that allow the student to consume them in smaller sections without the requirement of lengthy commitments that would be hindered due to operational requirements. Utilization of techniques developed within distance education programs, such as the Graduate Certificate programs offered by Naval Post Graduate School, would allow cyber professionals the ability to space out the education modules throughout their careers and ensure that significant billet assignments and competing professional military education does not hinder their ability to complete the cyber educational modules. This will allow the service member to remain competitive within their career path through assignments while completing modular distance education programs that build solid network operations fundamentals.

The increasing value of cyber security within the corporate and private sectors creates a competition for experienced, educated professionals. With the private sector offering higher salaries and an increased stability in an individual's personal life verse the military, it is difficult to determine what incentives can be offered to keep highly educated professionals within the DoD. Additionally, military experience makes service members highly competitive due to their possession of security clearances and exposure to operational cyber operations that their civilian counterparts may not have. While this seems to insinuate that educating senior cyber workforce personnel will lead to an exodus of professionals to the more competitive pay within the private sector, further educational opportunities and assignment to specific cyber assignments may

counter this potential. Retention of highly educated cyber professionals can be tied to the incentives provided through continuing education and exposure to cyber operations. The more the individual works within the cyber domain with the military, the more lucrative a position they can obtain outside of service. This will create a natural equilibrium over time as personnel receive high levels of education and experience in operations and not the paycheck as the primary goal of their professional development. Additionally, the symbiotic environment where cyber professionals begin their careers in the military and transfer to the private sector is healthy and typically places those highly educated service member into contract and government positions filling jobs similar to the positions they left while in the service.

The incentive of receiving a highly prized education in cyber defense and exposure to cyber operations only functions if there is a requirement for completion within the career path of the individual. As the current system of career progression does not require that higher education levels are completed for continued progression, there is no incentive to complete advanced training. Cyber workforce members can continue to be promoted without receiving additional education other than that required as entry level and standard professional military education required for all members to be considered for promotion. Advanced cyber training for the cyber workforce must be tied to the promotion system as a requirement for further progression similar to the Air Force Cyber 200/300/400 coursework.

Development of USMC Cyber Institute

The development of an institution to manage and promote higher level cyber education for the Marine Corps does not require vast amounts of capital investment and organizational structure in order to accomplish. The Marine Corps University, as an establishment institute of higher education, would serve as an excellent location for the hosting of a Cyber School of

Excellence. Based on the Marine Corps University's proximity to the National Capitol Region, it benefits from being centrally located between resources already available at the Marine Corps Base Quantico as well other Department of Defense and industry partnership. Marine Corps units already located within the region such as Marine Forces Cyber Command (MARFORCYBER), Marine Corps Cyber Operations Group (MCCOG), Headquarters Marine Corps Command, Control, Communications, and Computers (C4), and Marine Corps Information Operations Center (MCIOC) have a wealth of knowledge and experience in operations in the information environment and cyber domain. Additionally, interagency organizations such as the Department of Homeland Security, Federal Bureau of Investigation, National Security Agency, and Defense Information Systems Agency (DISA) are located within the National Capitol Region and are a resource that can be tapped to assist in the development of a professional cyber course. Finally, there are numerous institutes of higher education located both on Quantico and within the region that provide a hard to match concentration of experts to facilitate and support the establishment of advanced cyber education program for the Marine Corps. The management of these resources and provisioning of educational course offerings would be the principle mission of a developed cyber institute.

Practical application of learned cyber fundamentals during the advanced education course could be achieved through the use of a laboratory environment located in close proximity to Marine Corps University. The Department of Defense Cyber Security Range, managed by Headquarters Marine Corps C4, Cyber Division, is located just off Marine Corps Base Quantico and offers a network environment that can serve as an educational laboratory at no cost to the service.[25] The range exists outside of the operational environment of production networks and thus can serve as both a testing laboratory for new concepts as well as a practical application

environment for educational courses. The range and the staff that operate it are familiar with Marine Corps cyber operations and have hosted the Marine Corps, Joint Services, and National Guards teams for exercise such as Cyber Flag and Cyber Guard. Additionally, the range can be accessed remotely through either a Remote Boundary Suite (RBS) or through the use of a virtual private network (VPN) making it capable of supporting interactive education throughout the globe. The ranges ability to support onsite and distance interactive education, as well as laboratory functions, enables students to exercise cyber operations in a network environment that can replicate the network architectures, tools, and attack vectors that they will be facing in the operational environment.

The most effective part of utilizing the Marine Corps University as the backbone for the development of an advanced cyber education course is that it can be started now. Cyber operations are not hypothetical, future activities. The Marine Corps is grappling with how to work within the information and cyber domain at this instance. The recent conversion of the Marine Expeditionary Force Headquarters Groups (MHG) to the Marine Expeditionary Force Information Groups (MIG) shows that there is a focus and significant investment on the development of operations within cyber, information, and electronic warfare. Additionally, the creation of the 17XX Cyberspace Operations military occupational specialty and changes to acquisition processes for cyber operations systems, software, and training provide a clear indication of the level of investment the Marine Corps is putting into cyber.[26]

There is an added benefit in the development of an advance cyber educational program within the Marine Corps. This benefit couples the education and advancement of the senior cyber workforce with the ability to provide an educational institute that can assist in tackling the operational use and integration of cyber, information operations, and electronic warfare. As the

Marine Corps looks to further integrate cyber operations, information operations, and electronic warfare capabilities to the tactical edge of deployment, the establishment of an advanced institution that can assist in fostering the development of capabilities in the information environment would be beneficial to future capabilities.

Conclusion

As adversarial cyber capabilities continue to advance, so does the requirement for the Marine Corps to ensure that the senior cyber workforce that plan, install, operate, and maintain the command and control networks are capable of providing advanced network defensive and cyber operations capabilities. For the Marine Corps to meet these requirements, it must invest in the education of its cyber workforce and institute an education program that incorporates multiple technical and managerial disciplines. The battlefield of tomorrow will provide a complex information environment ripe with security vulnerabilities and advanced cyber threats.

The Marine Corps' best tool in countering adversarial cyber threats is a well-educated cadre of cyber warriors armed with cutting edge training and capable of developing robust network defense structures and integrating cyber operations. The current model of education does not adequately prepare senior cyber workforce personnel for operations in a contested information environment. By adopting traits from the sister services and industry to develop an advance cyber education program, developing a cyber institute to manage the advanced educational program , and utilizing selective recruiting for entry level cyber professionals while incentivizing advanced education, the Marine Corps can ensure that it can meet the challenges of an ever changing cyber domain.

Endnotes

[1] U.S. Marine Corps Forces, Cyberspace Command (MARFORCYBER) organization and mission, accessed February 30, 2018, https://marinecorpsconceptsandprograms.com/organizations/operating-forces/us-marine-corps-forces-cyberspace-command-marforcyber.
[2] Cheryl Pellerin, "Cybercom: Pace of Cyberattacks Have Consequences for Military, Nation." *Defense Media Activity*, May 24, 2017.
[3] Adam Meyers. "Danger Close: Fancy Bear Tracking of Ukrainian Field Artillery Units," *Research & Threat Intel (blog*), December 22, 2016.
[4] Department of Homeland Security online, Public Affairs (blog), November 14, 2017. https://www.dhs.gov/blog/2017/11/14/dhs-and-fbi-release-joint-technical-alerts-malicious-north-korean-cyber-activity.
[5] United States Computer Emergency Readiness Team (US-CERT) online, Hidden Cobra – North Korean Malicious Cyber Activity, March 2018. https://www.us-cert.gov/HIDDEN-COBRA-North-Korean-Malicious-Cyber-Activity
[6] Center for Strategic & International Studies (CSIS), Significant Cyber Incidents Since 2006, Washington, DC, retrieved March 2018. https://www.csis.org/programs/cybersecurity-and-governance/technology-policy-program/other-projects-cybersecurity
[7] Ibid.
[8] *Cyber Posture: The Senate Armed Service Cybersecurity Subcommittee*, 115th Cong. (2017) (Statement by Major General Lori E. Reynolds, Commander Marine Forces CYBERSPACE Command*)*
[9] National Institute of Science and Technology, National Vulnerability Database Dashboard online, accessed February 12, 2018, https://nvd.nist.gov/general/nvd-dashboard.
[10] CVE Details: The ultimate security vulnerability datasource online, accessed February 14, 2018, https://www.cvedetails.com/browse-by-date.php.
[11] SYNOPSYS, Inc, April 29, 2014, http://heartbleed.com/.
[12] Lisa Ferdinando, "DoD Seeks to Stay Ahead of Cybersecurity Threats, Acting CIO Says." *Defense Media Activity*, June 15, 2017.
[13] Drake Baer, "Google's genius futurist has on theory that he says will rule the future – and it's a little terrifying." *Business Insider*, May 27, 2015. http://www.businessinsider.com/ray-kurzweil-law-of-accelerating-returns-2015-5
[14] Marisa Viveros. "Cyber Security Depends on Education." *Harvard Business Review*, June 24, 2013.
[15] Director, Operational Test and Evaluation FY 2017 Annual Report, 319.
[16] Director of Marine Corps Communication-Electronics School, Communication Training Battalion, *Officer/Advanced Enlisted Training School (BCOC, MOS 0602)(MCPC, NMOS 0603)*.
[17] United States Department of Defense, *Cyberspace Workforce Management.* Directive 8140.01, July 31, 2017.
[18] Air Force Institute of Technology, "Cyberspace 200/300 Courses," last modified November 2, 2017, https://www.afit.edu/ccr/programs.cfm?p=60&a=pd&page=162&tabname=Tab1A.
[19] Department of the Army, *Officer Professional Development and Career Management (DA PAM 600-3) 17A Army Cyber Officer Development Model (DRAFT),* US Army, 2015.
[20] Naval Post Graduate School Academic Catalog, December 27,2017, 206.
[21] Naval Postgraduate School online, accessed January 7, 2018, http://www.nps.edu/web/guest/-/certificate-offering-cybersecurity-fundamentals-open-for-applications.
[22] SANS Institute online, accessed January 12, 2018, https://www.sans.org/.
[23] Headquarters Marine Corps, *Marine Corps Operating Concept: How an Expeditionary Force Operates in the 21st Century*, Department of the Navy, Headquarters Marine Corps, Washington, D.C., September 2016, 17-18.
[24] Sean Gallagher, "DOD needs Cyberwarriors so badly it may let skilled recruits skip boot camp," arstechnica.com, May 9, 2017, https://arstechnica.com/information-technology/2017/05/dod-needs-cyberwarriors-so-bad-it-may-let-skilled-recruits-skip-boot-camp/?comments=1.
[25] Headquarters Marine Corps, Command, Control Communications, and Computers/Cybersecurity Division online, December 29, 2017, http://www.hqmc.marines.mil/Agencies/Command-Control-Communications-and-Computers/Cybersecurity-Division/DODCSR/.

[26] Commandant of the Marine Corps, *Establishment of the Cyberspace 1700 Occupational Field (OCCFLD),* MARADMIN 136/18, March 1, 2018. http://www.marines.mil/News/Messages/Messages-Display/Article/1454562/establishment-of-the-cyberspace-1700-occupational-field-occfld/

Bibliography

Baer, Drake. "Google's genius futurist has on theory that he says will rule the future – and it's a little terrifying." *Business Insider*, May 27, 2015. http://www.businessinsider.com/ray-kurzweil-law-of-accelerating-returns-2015-5

Commandant of the Marine Corps. *Establishment of the Cyberspace 1700 Occupational Field (OCCFLD)*. MARADMIN 136/18, March 1, 2018. http://www.marines.mil/News/Messages/Messages-Display/Article/1454562/establishment-of-the-cyberspace-1700-occupational-field-occfld/

Commandant of the Marine Corps. *Maine Corps Cybersecurity*. MCO 5239.2B, November 5, 2015. http://www.marines.mil/Portals/59/MCO%205239.2B.pdf

Center for Strategic & International Studies (CSIS). Significant Cyber Incidents Since 2006. Washington, DC, retrieved March 2018. https://www.csis.org/programs/cybersecurity-and-governance/technology-policy-program/other-projects-cybersecurity

Department of the Air Force. *Air Force Space Command: Career Field Education and Training Plan*, Washington, DC, June 1, 2015.

Department of Defense Chief Information Officer. *Department of Defense Strategic Network Operations Vision*, The Pentagon, Washington, DC, 2008.

Department of the Army. *Officer Professional Development and Career Management (DA PAM 600-3) 17A Army Cyber Officer Development Model (DRAFT).* US Army, 2015.

Director of Marine Corps Communication-Electronics School, Communication Training Battalion. *Officer/Advanced Enlisted Training School (BCOC, MOS 0602) (MCPC, NMOS 0603)*. http://www.trngcmd.marines.mil/Units/West/MCCES/MCCES-Schools/

Department of Defense, Director, *Operational Test and Evaluation*. FY 2017 Annual Report, Washington, DC, January, 2017.

Ferdinando, Lisa and Garamone, Jim. "DoD Initiates Process to Elevate U.S. Cyber Command to Unified Combatant Command" DoD News, *Defense Media Activity*, August 18, 2017.

Ferdinando, Lisa. "DoD Seeks to Stay Ahead of Cybersecurity Threats, Acting CIO Says" DoD News. *Defense Media Activity*, June 15, 2017.

Gallagher, Sean. "DOD needs Cyberwarriors so badly it may let skilled recruits skip boot camp," *Ars Technica*, May 9, 2017. https://arstechnica.com/information-technology/2017/05/dod-needs-cyberwarriors-so-bad-it-may-let-skilled-recruits-skip-boot-camp/?comments=1

Grove, Thomas, Julian E. Barnes, and Drew Hinshaw. "Russia Targets NATO Soldier Smartphones, Western Officials Say; Moscow Seeks Information on Operations and Troop Strength, According to Officials with NATO Countries." *Wall Street Journal (Online)*, Oct 4, 2017. https://search-proquest-com.lomc.idm.oclc.org/docview/1946238853?accountid=14746.

Headquarters Marine Corps. Marine Corps Operating Concept: *How an Expeditionary Force Operates in the 21st Century*. Department of the Navy, Headquarters Marine Corps, Washington, D.C., September 2016.

Kaplan, Fred M. *Dark Territory: The Secret History of Cyber War*. First Simon & Schuster Hardcover Edition. ed. New York: Simon & Schuster, 2016.

Major General Lori E. Reynolds, "Cyber Posture Statement," *The Senate Armed Service Cybersecurity Subcommittee*, 115th Cong. (2017).

Meyers, Adam. "Danger Close: Fancy Bear Tracking of Ukrainian Field Artillery Units," *Research & Threat Intel (blog*), December 22, 2016. https://www.crowdstrike.com/blog/danger-close-fancy-bear-tracking-ukrainian-field-artillery-units/

Pellerin, Cheryl. "Cybercom: Pace of Cyberattacks Have Consequences for Military, Nation." DoD News, *Defense Media Activity*, May 24, 2017.

Secretary of Defense. *The Department of Defense Cyber Strategy*, Washington, DC, April 2015.

Volz, Dustin. "Russian hackers tracked Ukrainian artillery units using Android implant: report." *Reuters*, December 2016. https://www.reuters.com/article/us-cyber-ukraine/russian-hackers-tracked-ukrainian-artillery-units-using-android-implant-report-idUSKBN14B0CU

United States Department of Defense. *Cyberspace Workforce Management.* Directive 8140.01, July 31, 2017.

Viveros, Marisa. "Cyber Security Depends on Education." *Harvard Business Review Online*, June 24, 2013. https://hbr.org/2013/06/cyber-security-depends-on-educ