BUILDING JOINT, MULTI-DOMAIN UNITED STATES AIR FORCE CYBERSPACE OPERATIONS OFFICERS:
A COMPARATIVE ANALYSIS OF UNITED STATES MILITARY CYBERSPACE OFFICER FORCE DEVELOPMENT MODELS

BY

ANDREW C. MILLER

A THESIS PRESENTED TO THE FACULTY OF

THE SCHOOL OF ADVANCED AIR AND SPACE STUDIES

FOR COMPLETION OF GRADUATION REQUIREMENTS

SCHOOL OF ADVANCED AIR AND SPACE STUDIES

AIR UNIVERSITY

MAXWELL AIR FORCE BASE, ALABAMA

JUNE 2018

APPROVAL

The undersigned certify that this thesis meets master's-level standards of research, argumentation, and expression.

DR. STEPHEN E. WRIGHT 17 May 2018

DR. DAVID C. BENSON 17 May 2018

DISCLAIMER

The conclusions and opinions expressed in this document are those of the author. They do not reflect the official position of the US Government, Department of Defense, the United States Air Force, or Air University.

ABOUT THE AUTHOR

Lieutenant Colonel Andrew C. Miller is a United States Air Force cyberspace operations officer with 15 years of total service, and he is currently attending the School of Advanced Air and Space Studies, Maxwell Air Force Base, Alabama. In his previous assignment, he served as the Commander, 690th Cyberspace Operations Squadron, 67th Cyber Wing, Joint Base Pearl Harbor - Hickam, Hawaii. There he commanded 162 military personnel providing network operations and defense for more than 850,000 users on unclassified and classified USAF networks.

Lieutenant Colonel Miller commissioned through the Reserve Officer Training Corps at the Pennsylvania State University in 2002. He has served in a variety of leadership and staff positions at the squadron, group, wing, warfighting headquarters, major command, and joint task force levels. Lieutenant Colonel Miller deployed multiple times in support of Operation Enduring Freedom and Operation Iraqi Freedom. He attended the US Army's Command and General Staff College and holds a master's degree in Information Technology from the University of Maryland University College. Lieutenant Colonel Miller's next assignment is to command the 333d Training Squadron at Keesler Air Force Base, Mississippi.

Lieutenant Colonel Miller is married with children.

ACKNOWLEDGMENTS

I owe a debt of gratitude to many people who inspired, motivated, and encouraged me throughout the year.

Thank you to my thesis advisor and reader:

Dr. Stephen “Wilbur” Wright provided a herculean effort to advise me while simultaneously being the course director for the final SAASS seminar. He provided expert advice on how to narrow my research and helped me construct a deliberate framework to approach this project. Though my thesis topic morphed over time, the original framework proved so tight that it never changed. Finally, his exceptional patience, editing skills, and dedicated efforts resulted in a much more polished final product than I could have hoped to achieve on my own.

Dr. David Benson for his patience in reading a double-length thesis at the end of the year. While my thesis may have been a bit long, he understood my personal desire for the included content and focused his efforts on ensuring I had a tight argument.

Thank you to my brothers and sisters in arms from the US Marine Corps, US Army, US Cyber Command, and the US Air Force who aided in my research and understanding of their services. You all know what you did but I would be remiss without mentioning you by name.

From the USMC I would like to thank Karl Schlegel, Matthew Knopp, Patrick Skehan, William Hochrine, Michael Ronza, Paul Stokes, Anthony Johnson, Joshua Chang, and Aaron Ellis. From the USA I would like to thank Benjamin Sangster, Nathan Saul, John Williams, Thomas Founders, Jason Allen, Jim Beck, Chan Ho Lee, Derrick Smith, and Thomas Barnes. From USCC, Steven Naylor, Leslie Overmyer, and Matthew Isnor. From the USAF I would like to thank Jeffrey Blankenship, Joseph Wingo, Nathaniel Huston, Angela Waters, Gilberto Perez, Molly Braun, Kimber Nettis, Andrew Day, Robert Patt, Vic Ashdown, and Kyle Dye. You are all truly testaments to your respective services and I can only hope to return the favor ten-fold someday. Any mistakes or misinterpretations of provided information are solely the fault of the author.

Thank you to all my friends and peers with whom I continually commiserate how to resolve the challenges facing our community. My research confirmed previous thoughts and discussions, however hopefully provides the proverbial meat to our arguments as we attempt to shape our community into the future.

Finally, thank you to my wife and children for their infinite patience throughout this year. There were many long nights of reading and writing, but we still found time to recharge as a family. Even more importantly, I am thankful that they willingly sacrificed a three-year duty extension in Hawaii to come to Alabama. As my wife likes to remind me, not only did we volunteer to leave Hawaii, but I had to write several essays to do so.

ABSTRACT

If the USAF cyberspace operations community desires to build joint, multi-domain warfighting leaders, it should examine and integrate aspects of its sister-service force development models. Through a comparative analysis of the current US Air Force, US Army, and US Marine Corps cyberspace-related officer force development models, this thesis identifies how each service develops its officers to meet joint officer requirements, satisfy internal service institutional requirements, to be occupationally-proficient, and to ultimately be joint leaders. The research finds that while all three services dedicate significant efforts to training cyberspace-related occupational competencies, the USMC and USA cyberspace officer force development models invest significantly more effort towards developing institutional competencies through training, education, and reinforcing duty experience. Based upon the assumption that the USMC and USA models produce more effective joint leaders, their developmental focus on institutional competencies serves as the primary difference compared to the USAF model. Thus, for the USAF cyberspace operations community to effectively develop joint, multi-domain warfighting leaders, it must re-focus and re-balance career-field training and educational opportunities to resolve institutional competency gaps in USAF professional military education while deliberately reinforcing the competencies through deliberate, practical duty experience.

CONTENTS

Chapter Page

Illustrations

Tables

Figure

Introduction

The United States Air Force cyberspace officer career field finds itself at the center of a maelstrom of complementary and competing challenges. The Chief of Staff of the Air Force (CSAF), and many in the service, does not feel that the service's officer force development model effectively builds joint, multi-domain leaders.[1] Furthermore, the USAF cyberspace community amid an on-going, multi-year culture shift. The Air Force cyber community is attempting to "operationalize" itself and respond to an external command entity (US Cyber Command) that dictates how the Air Force will organize, train, and equip its cyberspace forces. Meanwhile, the USAF cyberspace community retains the responsibility for traditional service responsibilities; such as providing garrison and expeditionary communications and services, as well as serving as joint enablers. Finally, the Air Force faces the challenge that most of its mid- and senior-level cyberspace officers grew up under a mission support and maintenance construct, and thus lack a force-developed understanding of what it means to be *operational*. These multiple challenges create a force development conundrum for the USAF cyberspace officer community. Does the current USAF cyberspace officer force development model effectively build joint, multi-domain warfighting leaders while satisfying internal service expectations and external developmental requirements?

Thesis of this Paper

Through a comparative analysis of the current US Air Force, US Army, and US Marine Corps cyberspace-related officer force development models, this thesis seeks to identify how and why each service develops its officers to meet joint officer requirements, to be occupationally-proficient, and to be joint function and multi-domain leaders. The desired outputs are recommendations for USAF cyberspace leaders to consider as they evolve their force development models to include evolving training,

[1] David Goldfein, "CSAF Focus Area: Strengthening Joint Leaders and Teams," October 2016, http://www.af.mil/Portals/1/documents/csaf/letters/16%2010%2013%20Focus%20Area%20II.pdf?ver=2016-10-13-105649-460&timestamp=1476371621707; David Goldfein, "CSAF Focus Area: Enhancing Multi-Domain Command and Control...Tying It All Together," March 2017, http://www.af.mil/Portals/1/documents/csaf/letter3/CSAF_Focus_Area_CoverPage.pdf. The CSAF focus areas outline three priority areas he wants to focus on to improve the USAF. Strengthening Joint Leaders and Teams focuses on developing personnel and teams that understand combined arms and can lead in joint, multi-domain environments.

education, and experience. This paper provides two overarching recommendations for USAF cyberspace operations officer development:

1) The USAF cyber community should integrate identified aspects of joint, sister-service force development models to best build capable service and joint cyberspace leaders within the current USAF officer force development construct.

2) The USAF cyberspace operations community should re-focus and re-balance career-field training and educational opportunities to incorporate institutional competency gaps in USAF Professional Military Education (PME) and deliberately reinforce the competencies across all types of units through repeatable, practical experience.

Origins of the Research Topic

The reader may ask why I decided to write a paper on the oft-studied subject of officer development, even if pared down to officer occupational fields in the cyberspace realm. In the Fall of 2017, I was surprised to find out that upon completion of the School for Advanced Air and Space Studies, the USAF selected me for a second opportunity for squadron command. This new command will be the 333d Training Squadron at Keesler Air Force Base, Mississippi. This unit provides cyberspace-related initial training programs from enlisted cyberspace warfare operators and initiatial occupational training for all USAF cyberspace officers. It is the officer element that brought me to the desire to focus on this thesis topic. Initially, this research sought to compare initial "cyberspace" officer training across the services to find best practices, opportunities for partnership, and so on. I saw this project as a means to understand better the training business before stepping into command. However, what started as journey to compare these initial training programs illustrated how much context matters in the determination of competencies and experiences the services value, and how those skill sets influence officer development.

As I started looking for service-specific institutional competencies that would influence officer development and cyberspace officer development in particular, I found largely general and holistic concepts in the Army and Marine Corps; only the USAF had a detailed list of competencies. Thus, I had no meaningful way to tie service-emphasized competencies to cyberspace officer training. I also understand that Federal law, the

Department of Defense, and United States Cyber Command also influence cyberspace officer developmental priorities. Therefore, I decided the best way to determine what the services value in cyber officer development was to look at the entire officer force developmental model for each entity.

The comparative analysis of the force development models includes institutional and cyberspace-specific occupational training and education, as well as key developmental experiences. The weight of effort each service puts towards developing certain knowledge, skills, and abilities will illustrate what each service deems important to the growth of their cyberspace officers. Significant differences in force development models will provide insights into mechanisms that contribute to or detract from effectively building joint, multi-domain leaders.

Chapter 1

Scope, Concepts, Methodology

The following chapter provides scoping, methodology, and concepts for this thesis. Scoping includes the intended audience, assumptions, and limitations of the research. The methodology includes an overview of the framework for the paper, the variables utilized, and the primary types of research sources. Finally, this chapter concludes with an overview of the foundational terms and concepts used in subsequent chapters.

Scope and Audience

Audience. The primary intended audience for this paper are leaders within the USAF cyberspace operations community, both those who directly influence cyberspace officer force development as well as all officers who will mentor and influence junior officers. While this paper will define certain concepts and lexicon to aid the reader, the paper assumes the reader has a fundamental understanding of the military, force development, and military cyberspace operations. However, the author intends this paper to be approachable enough for non-cyberspace practitioners.

While the primary audience is the USAF cyberspace officer community, the findings of this paper apply more broadly across the USAF and other services. The comparative analysis of officer force development may prove of interest to those in the USAF focused on institutional officer development, to include those trying to solve the CSAF’s joint, multi-domain challenge. Other USAF occupational communities may glean some insights into opportunities to modify their own force development models. Finally, sister services and especially their cyberspace-related occupational fields may discover some findings and implications within this paper relevant and useful.

What this thesis is not. The purpose of this thesis is not to cure the woes of officer development nor judge the output quality of the various training and education courses. In addition, this paper is not a history or origin story of cyberspace operations or the associated development of its officers within the Department of Defense. Instead, this paper is a non-judgmental examination of the current state of affairs with regards to cyberspace officer development. It attempts to illuminate similarities and differences between the services to inform conversations on how the USAF might consider better-developing its cyberspace officer force.

Concepts and Terms

In order to understand the analysis within this paper, the reader must first understand several foundational concepts and terms. The primary concepts relate to *cyberspace* and subordinate concepts within *cyberspace operations*, *officer force development* and *force development models*, *institutional* versus *occupational*, and *joint* and *multi-domain*. Numerous other military-centric terms will be used throughout the paper, however they will not be defined in this chapter as the intended audience are members of the US Department of Defense who should have a working understanding of the concepts.

As mentioned in the introduction, this paper uses the term cyberspace in both generic and specific terms. This paper will utilize the current DoD definitions for cyberspace, cyberspace operations, Department of Defense Information network operations, defensive cyberspace operations, and offensive cyberspace operations.

> *Cyberspace* – "A global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[1]
>
> *Cyberspace operations* – "The employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace."[2]
>
> *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."[3]
>
> *Department of Defense information network operations (DoDIN Operations)* – "Operations to design, build, configure, secure, operate, maintain, and sustain Department of Defense networks to create and preserve information assurance on the Department of Defense information networks."[4]

[1] Joint Chiefs of Staff, *DOD Dictionary of Military and Associated Terms*, April 2018, 59, http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf?ver=2018-03-27-153248-110.

[2] Ibid., 60.

[3] Ibid., 64.

[4] Ibid., 66.

> *Offensive cyberspace operations* – "Cyberspace operations intended to project power by the application of force in or through cyberspace."[5]

Force development is the deliberate use of training, education, and experience (through positional assignments) to build the personnel the military requires to execute specific missions or roles across the span of a career.[6] Thus, *officer force development* focuses on how a given military service builds its officers from pre-commissioning and continues throughout a career. An *officer force development model* is the preferred method and roadmap of force development for officers generically as well as occupational field. The military services document their force development models in regulations and often create easy-reference visualizations as the reader will see in Chapters 3-5 of this paper. Few individuals' careers precisely follow the outlined force development models, but the models serve as a guidepost to how the services manage their folks as well as illustrates the institutional and occupational experiences the service values in development their force.

The military uses the terms *institutional* and *occupational* to describe specific knowledge, skills, and abilities desired for a given demographic, which in this paper will be officers. *Institutional* refer to what a given service values and expects for all officers (e.g. all officers must be able to lead), whereas *occupational* refers to the knowledge, skills, and abilities unique to a given occupational field (e.g. a pilot may need to know how to drop a bomb whereas a cyberspace officer may need to understand how a router works).[7] The reader may hear or use terms like *technical* or *functional* used in the place of occupational, but assume they are roughly analogous for purpose of this paper. In practice, certain knowledge, skills, and abilities such as planning overlap both occupational and institutional lenses, however the institutional versus occupational construct provides useful delineation for what the service values for all vice what additional values it has for a specific occupational field.

[5] Ibid., 169.

[6] Curtis E. Lemay Center for Doctrine Development and Education, *Annex 1-1 Force Development Appendix, Institutional Competency List*, 17 April 2017, 1, http://www.doctrine.af.mil/Portals/61/documents/Annex_1-1/1-1-D06-Appendix-1-Competency.pdf.

[7] Ibid.

This paper will use the terms *joint* and *multi-domain* relating to the desired knowledge, skills, and abilities for its officers. The DoD Dictionary of Military and Associated Terms defines joint as "activities, operations, organizations, etc., in which elements of two or more Military Departments participate."[8] The author's use of joint in this paper will further expand beyond this definition to incorporate *joint functions*. The *joint functions* are the "related capabilities and activities placed into six basic groups of command and control, intelligence, fires, movement and maneuver, protection, and sustainment to help joint force commanders synchronize, integrate, and direct joint operations."[9] Thus, the use of joint in this paper will refer both multi-service as well as multi-function. Finally, the term *multi-domain* is a term referring to and encompassing the air, land, sea, space, and cyberspace warfighting domains.

Methodology

Group Analyzed. This paper focuses on the category of officers that includes active duty, line/unrestricted officers within the United States Air Force, United States Army, and United States Marine Corps. The line/unrestricted designator excludes health professionals, lawyers, and chaplains and active duty precludes analysis of reserve and guard officers. The primary analysis within the line/unrestricted officer category focuses on the cyberspace occupational fields which include the single occupational specialty in the USAF, two within the USA, and two within the USMC.

This paper focuses on officers in the grades of O-1 through O-5 and does not cover the portions of a career and associated force development for officers at the O-6 and the General/Flag Officer ranks. This is deliberate for scoping reasons, but also due to the fact that the foundational experiences, skills, and knowledge required to make an effective joint, multi-domain leader generically, and specifically within cyberspace occupational fields, occur during the first 18-20 years leading up to O-6.

A final caveat on the study group is that the paper does not delve into the nuances of below-the-zone promotions nor talent management of these proverbial *fast-burners*. The described force development models still apply to these individuals, however their

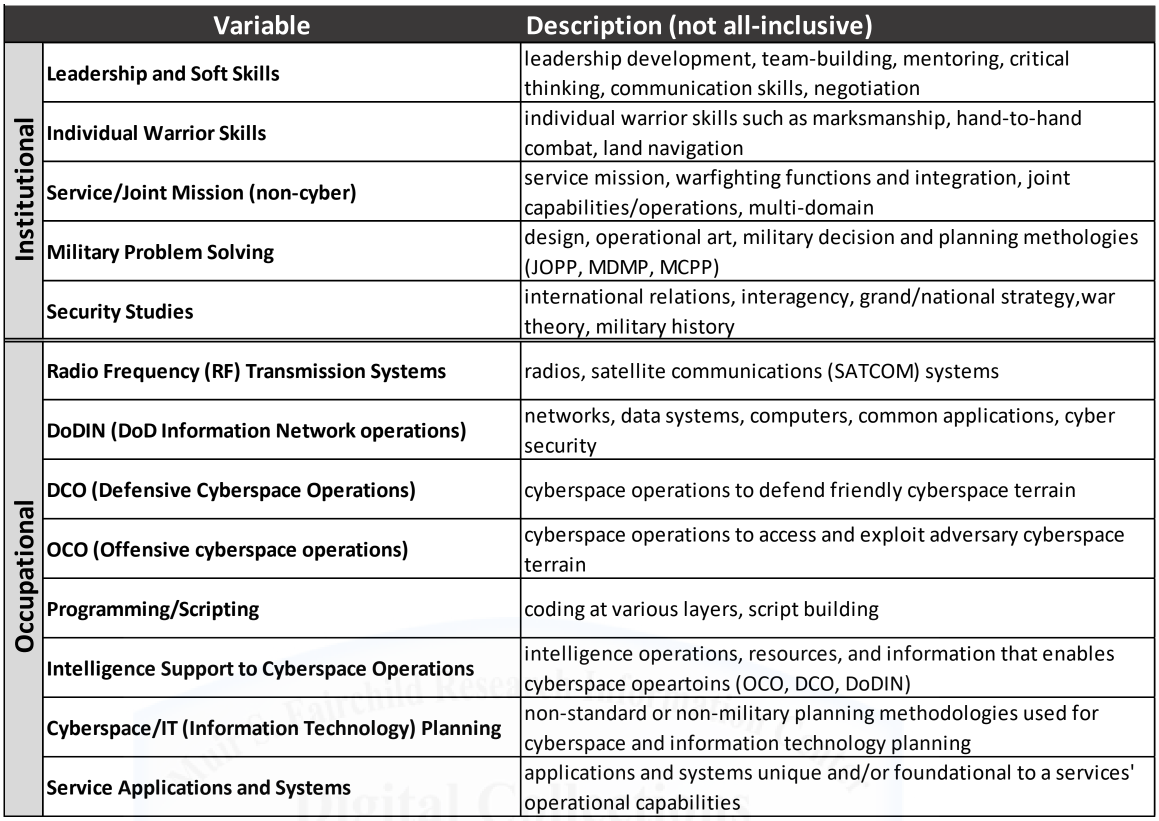
[8] Joint Chiefs of Staff, *DOD Dictionary of Military and Associated Terms*, 121.
[9] Ibid., 125.

timelines to hit specific milestones may be faster or sooner than described in the standard force development models.

Variables. The examined variables in this paper derive from the underlying components included within military force development. The two macro-level variables are *training/education* and *experience* (positions/assignments). Within the training and education area of analysis, the paper uses thirteen variables to analyze formal (cyberspace) officer training and education. These thirteen variables allow the codification of course curriculum into "like" measurable values. Table 1 identifies the thirteen variables and descriptions, aligned in two broad categories labelled *institutional* and *occupational.*

The term *institutional* refers to the knowledge, skills, and abilities that a given service prioritizes and values for its officers, regardless of occupational specialty. The first five training/education variables fall into the institutional category. The term *occupationa*l refers to knowledge, skills, and abilities unique to cyberspace occupational fields. The remaining eight training/education variables fall into this occupational category. This paper will codify the curriculum within each analyzed formal training and education course into these thirteen variables by hour. Table 2 provides an example of the analysis data presented in this thesis.

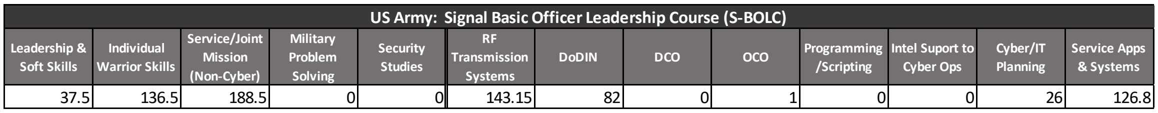
Table 1. Training/Education Curriculum Variables (unit = hours)



	Variable	Description (not all-inclusive)
Institutional	**Leadership and Soft Skills**	leadership development, team-building, mentoring, critical thinking, communication skills, negotiation
	Individual Warrior Skills	individual warrior skills such as marksmanship, hand-to-hand combat, land navigation
	Service/Joint Mission (non-cyber)	service mission, warfighting functions and integration, joint capabilities/operations, multi-domain
	Military Problem Solving	design, operational art, military decision and planning methologies (JOPP, MDMP, MCPP)
	Security Studies	international relations, interagency, grand/national strategy,war theory, military history
Occupational	**Radio Frequency (RF) Transmission Systems**	radios, satellite communications (SATCOM) systems
	DoDIN (DoD Information Network operations)	networks, data systems, computers, common applications, cyber security
	DCO (Defensive Cyberspace Operations)	cyberspace operations to defend friendly cyberspace terrain
	OCO (Offensive cyberspace operations)	cyberspace operations to access and exploit adversary cyberspace terrain
	Programming/Scripting	coding at various layers, script building
	Intelligence Support to Cyberspace Operations	intelligence operations, resources, and information that enables cyberspace opeartoins (OCO, DCO, DoDIN)
	Cyberspace/IT (Information Technology) Planning	non-standard or non-military planning methodologies used for cyberspace and information technology planning
	Service Applications and Systems	applications and systems unique and/or foundational to a services' operational capabilities

Source: Author's Original Work

Table 2. Example Course Curriculum Analysis (hours)



US Army: Signal Basic Officer Leadership Course (S-BOLC)												
Leadership & Soft Skills	Individual Warrior Skills	Service/Joint Mission (Non-Cyber)	Military Problem Solving	Security Studies	RF Transmission Systems	DoDIN	DCO	OCO	Programming /Scripting	Intel Suport to Cyber Ops	Cyber/IT Planning	Service Apps & Systems
37.5	136.5	188.5	0	0	143.15	82	0	1	0	0	26	126.8

Source: Author's Original Work

Assumptions and Limitations

Assumptions. The analysis in this paper rests on three key assumptions. First, this paper assumes that the by-law requirements to build joint qualified officers are insufficient to reliably build effective and credible joint leaders. A perfect example is that the USAF continually produces joint qualified officers, yet the USAF is historically underrepresented in commanding geographic combatant commands and filling key joint staff positions.[10] As Lieutenant Colonel (Dr.) Daniel Magruder argues, the USAF "does not sufficiently develop FGOs for joint leadership roles."[11] The second assumption is that, due to the preponderance of USA and USMC officers in key leadership positions across the defense establishment, the USA and USMC officer force development models effectively build joint, multi-domain leaders (regardless of occupational specialty).[12] Even if these models do not produce the perfect joint, multi-domain leader, the assumption is that the models produce officers who are generally more effective and qualified than those the current USAF model produces. The third assumption is that the analyzed training and education courses effectively convey the curriculum from instructor to student. The analysis and conclusions found in this paper focus solely on the content and time spent on topics within these courses, not on the quality of actual instruction or student absorption of the material.

Limitations. This paper has six major limitations. First, the research is a snapshot in time. Second, new and evolving cyberspace officer force development models will not have evidence of their effectiveness for years. Third, the services view cyberspace occupational fields and the role of cyberspace officers slightly differently. Fourth, each service's pre-commissioning differs to include training and associated academic education. Fifth, very few officers' careers perfectly follow a documented force development model. Sixth, this paper does not evaluate the United States Navy nor reserve and guard development.

The first stated limitation of this paper is that it focuses on a snapshot in time. While institutional-level officer force development changes relatively slowly, cyberspace officer force development remains in a constant state of evolution due to an ever-changing domain and evolving military role within it. For example, three months into research for this paper, the USMC announced that it would be establishing a new cyberspace operations occupational field separate from its communications officer field.

[10] Lee, Caitlin, Bart E. Bennett, Lisa M. Harrington, and Darrell D. Jones, "Air Force Senior Leader Representation in the Joint Community" (RAND Corporation, 2017), 2, https://www.rand.org/pubs/research_briefs/RB9970.html.

[11] Daniel L. Magruder, "Developing Air Force Field Grade Officers for Joint Leadership," *Air & Space Power Journal* 32, no. 1 (Spring 2018): 53.

[12] Lee, et al., 2

Additionally, the curriculum within cyberspace training and education from every service are constantly changing, in some cases from one academic class to the next.

Another challenge to a comparative analysis of officers across the three examined services is that each service views the cyberspace domain slightly differently. The USAF separates cyberspace and electronic warfare into separate functions and occupational fields while the USA includes electronic warfare within the basket of skills its cyberspace officers' must have. Discussions of information warfare and psychological operations even further blur the lines. Thus, this paper attempts to focus on the largest commonalities between services. The commonalities emphasize the current DoD definition of cyberspace coupled with the USAF lens of what cyberspace officers are since the focus on this thesis are implications for USAF cyberspace officer development.

A fourth limitation is that this paper does not focus on pre-commissioning training and education. New officers may have different undergraduate (technical) backgrounds and the various pre-commissioning programs train and educate cadets on different knowledge, skills, and abilities (e.g. Army teaches land navigation which is immediately applicable on active duty). Despite these differences, each service's initial active duty training and education courses assume the officers have dissimilar backgrounds and must bring their knowledge, skills, and abilities into rough parity. Therefore, this paper does not focus on pre-commissioning training and education as part of its analysis.

The fifth primary limitation is that there are always exceptions to any rule due to the nature of the military organization and industrial-age personnel systems. While the analysis of officer force development focuses on an ideal or desired path, individual officers or individual occupational fields may evince different developmental paths milestones. Additionally, certain officers promote at advanced rates compared to their peers, resulting in their developmental milestones moving farther to the chronological left. These differences and outliers should not detract from the general analysis and takeaways from the forthcoming comparative analysis.

Finally, the reader may note that this paper does not analyze the United States Navy (USN). This is a recognized shortfall of this research, but the author made the decision for scoping reasons largely due to the increased complexity of analysis as the USN has three distinct cyberspace officer occupational fields. Furthermore, many of the findings in this paper may apply to varying degrees to the Navy, total force partners (Reserves and National Guard), and other categories of officers found in the services (Limited Duty Officers, Warrant Officers). However, to narrow down the comparison required selecting a specific subset of “like” officers.

Despite the stated assumptions and limitations, the value of this snapshot-in-time research is to discern the aspects of force development across the services that remain relatively steady and could inform USAF cyberspace officer development today and in the near future. Finally, examining how each service currently develops their cyberspace officers can foster understanding on what each service currently values and how they are each trying to tackle the evolving nature of cyberspace and their officers role within it.

Sources and Framework

The material for this research comes from five primary source types: Federal Law, military regulations and doctrine, training and educational curriculum, interviews, and documents from individuals in positions within their respective cyberspace officer force development organizations. The laws and military regulations serve as the formal codification of force development and associated national, defense, and service values. The training and educational curriculum illustrate exactly what within institutional and occupational courses each service emphasizes, thus values. Finally, several interviews and documents from individuals in force development positions within their services add further context to the what, how, and why of each service’s cyberspace occupational field force development.

The analysis portion of this paper begins with an examination of *extra-service* (outside the service) echelons and influences on cyberspace officer development, three chapters each looking at a given service cyberspace officer force development model, followed by comparative analysis across the services leading to implications and recommendations in the conclusion. Chapter two provides details on the externally-derived requirements placed upon the services for officer and cyberspace occupational field. Chapter three through chapter five describe the force development models by military service (USAF, USA, USMC respectively). Each of these three chapters begins by providing service-specific context to include descriptions of service-level and cyberspace organizational constructs and cyberspace occupational fields. These chapters then outline the force development of officers in chronological blocks: years 0-4, years 4-10, years 10-15, and then years 15-20. Each chronological block breaks down the aforementioned force development variables both institutionally and occupationally to provide a clear picture of each service's cyberspace officer force development model.

Chapter six and seven bring the focused research together. Chapter six provides a comparative analysis of service cyberspace officer force development models based upon the data and context presented in chapters three through five. Chapter seven, the conclusion, takes the findings from the comparative analysis and derives conclusions and recommendations for the USAF cyberspace operations community.

Chapter Summary

In this chapter, the discussion sought to provide the reader an understanding of the scoping, foundational terms, and methodology used throughout this paper. Of the various concepts included, three concepts are most important to understand. Unless otherwise specified, the term *cyberspace officer* serves an umbrella term covering all flavors of cyberspace-related officer occupational fields across the services. The concept of *joint, multi-domain* expands to include the knowledge, skills, and abilities associated with the six joint functions. Finally, the services leverage *force development* models to build officers. These models include both *institutional* (all officers) and *occupational* (specific specialty) competencies that span subordinate force development components of training/education and experience.

Despite the identified scoping, assumptions, and research limitations, the reader can still derive from this paper useful implications and actionable recommendations for evolving USAF cyberspace officer development. The proceeding chapter will build upon the foundation built here by expanding the overarching by-law and Department of Defense requirements to influencing the building of joint officers, both for officers writ-large as well as cyberspace officers.

Chapter 2

Extra-Service Force Development Standards/Requirements

This chapter will examine the force development standards and requirements placed upon the services by both US Federal Law and other joint standards for all military officers and those specific to cyberspace officers. The chapter will first examine the by-law and associated joint requirements for all officers (i.e. specialty-independent) and will then focus in on the additional unique standards for cyberspace officers. At the end of this chapter, the reader will have a foundational understanding of the primary extra-service requirements that influence how military services internally build institutional and occupational (cyberspace) officer force development models.

Joint Officer Management

Section 401-406 of the Goldwater-Nichols Act of introduced into law the requirement for the Secretary of Defense to establish "policies, procedures, and practices for the effective management of officers of the Army, Navy, Air Force, and Marine Corps on the active-duty list who are particularly trained in, and oriented toward, joint matters."[1] Federal law specifically defines the requirements that for the services to develop joint qualified officers which includes duty experience in joint matters, joint professional education, and requirements for joint qualified officer promotions to certain grades.[2]

Experience. Federal law dictates that for officers to be designated as joint qualified officers, the officers must have duty experience relating to joint matters. *Joint matters* refers to the "development or achievement of strategic objectives through the synchronization, coordination, and organization of integrated forces in operations conducted across domains, such as land, sea, or air, in space, or in the information environment."[3] For officers from any service to complete the joint duty requirement,

[1] "Goldwater-Nichols Department of Defense Reorganization Act of 1986," Pub. L. No. 99–433 (1986), 35, http://history.defense.gov/Portals/70/Documents/dod_reforms/Goldwater-NicholsDoDReordAct1986.pdf.
[2] "10 USC Ch. 38: Joint Officer Management," 10 USC Ch. 38 § §661, accessed February 28, 2018, http://uscode.house.gov/view.xhtml?path=/prelim@title10/subtitleA/part2/chapter38&edition=prelim.
[3] "10 USC Ch. 38: Joint Officer Management," 10 USC Ch. 38 § §668, accessed February 28, 2018, http://uscode.house.gov/view.xhtml?path=/prelim@title10/subtitleA/part2/chapter38&edition=prelim.

each must both hold the grade of O-3 or higher while filling a joint designated position for no less than two years.[4]

Federal law and CJCS policy do not dictate the nature of the duty, only that the duty must be in a joint-duty validated billet. The Joint Staff maintains lists of joint duty authorized positions within joint organizations. Unlike within the specific military services, this duty need not be a key leadership position. The preponderance of positions fall within staff functions.

Training and Education. CJCS 1800.01E outlines standards and requirements for officer joint professional military education (JPME) from pre-commissioning through Flag/General Officer levels. JPME "…provides the body of knowledge to enhance performance of duties consistent with Joint Matters and in the context of joint functions (command and control, intelligence, fires, movement and maneuver, protection and sustainment)."[5] Figure 1, an excerpt from CJCS 1800.01E, illustrates the continuum of officer professional military education and associated requirements.

The introduction to, and expanding awareness of, joint matters and functions occurs during each services' officer pre-commissioning and primary military educations schools. While many junior officers' early years are focused on becoming proficient at their military occupation and tactical leadership abilities, this exposure to joint matters in primary PME, and through the course of their duties, provides an opportunity to expand their horizons into different levels of war, domains, military services, and warfighting functions and how their occupation fits into the larger picture. Subsequent chapters three thru five will highlight how, and to what degree, the individual services incorporate these *joint* topics into their force development models for company grade officers.

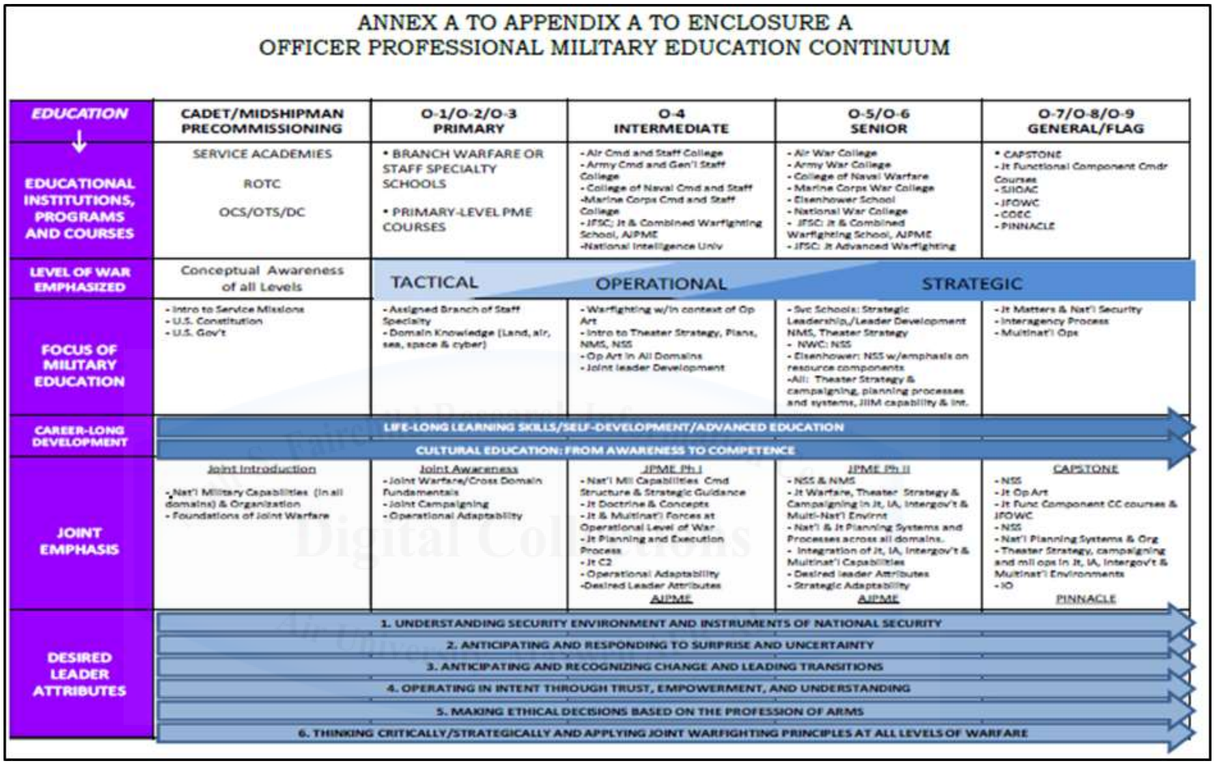
Joint Professional Military Education (JPME) Phase I and II programs become extremely important as officers must complete both to become joint qualified officers.[6] Title 10, U.S.C., chapter 107 and CJCS 1800.01E define the curriculum requirements for

[4] "10 USC Ch. 38: Joint Officer Management," 10 USC Ch. 38 § §664, accessed February 28, 2018, http://uscode.house.gov/view.xhtml?path=/prelim@title10/subtitleA/part2/chapter38&edition=prelim.

[5] Chairman Joint Chiefs of Staff Instruction (CJCSI) 1800.01E, *Officer Professional Military Education Policy*, 29 May 2015, A-1, http://www.jcs.mil/Portals/36/Documents/Doctrine/education/cjcsi1800_01e.pdf?ver=2017-12-29-142206-877.

[6] "10 USC Ch. 38: Joint Officer Management," 10 USC Ch. 38 § §661, accessed February 28, 2018, http://uscode.house.gov/view.xhtml?path=/prelim@title10/subtitleA/part2/chapter38&edition=prelim.

JPME Phase I/II-awarding programs. All JPME-awarding schools including those internal to the specific military services, must include in their curriculum the joint emphasis topics listed in Figure 1 below.[7] While officers may attend specific JPME I or II courses whenever assigned to a designated joint organization, the services typically target Field Grade Officers to complete JPME I and II, thus include the requisite topics in their intermediate and senior developmental education schools.



ANNEX A TO APPENDIX A TO ENCLOSURE A
OFFICER PROFESSIONAL MILITARY EDUCATION CONTINUUM

EDUCATION ↓	CADET/MIDSHIPMAN PRECOMMISSIONING	O-1/O-2/O-3 PRIMARY	O-4 INTERMEDIATE	O-5/O-6 SENIOR	O-7/O-8/O-9 GENERAL/FLAG
EDUCATIONAL INSTITUTIONS, PROGRAMS AND COURSES	SERVICE ACADEMIES ROTC OCS/OTS/DC	• BRANCH WARFARE OR STAFF SPECIALTY SCHOOLS • PRIMARY-LEVEL PME COURSES	- Air Cmd and Staff College - Army Cmd and Gen'l Staff College - College of Naval Cmd and Staff -Marine Corps Cmd and Staff College - JFSC; Jt & Combined Warfighting School, AJPME -National Intelligence Univ	- Air War College - Army War College - College of Naval Warfare - Marine Corps War College - Eisenhower School - National War College - JFSC: Jt & Combined Warfighting School, AJPME - JFSC: Jt Advanced Warfighting	• CAPSTONE - Jt Functional Component Cmdr Courses - SJIOAC - JFOWC - COEC - PINNACLE
LEVEL OF WAR EMPHASIZED	Conceptual Awareness of all Levels	TACTICAL	OPERATIONAL		STRATEGIC
FOCUS OF MILITARY EDUCATION	- Intro to Service Missions - U.S. Constitution - U.S. Gov't	- Assigned Branch of Staff Specialty - Domain Knowledge (Land, air, sea, space & cyber)	- Warfighting w/in context of Op Art - Intro to Theater Strategy, Plans, NMS, NSS - Op Art in All Domains - Joint leader Development	- Svc Schools: Strategic Leadership,/Leader Development NMS, Theater Strategy - NWC: NSS - Eisenhower: NSS w/emphasis on resource components -All: Theater Strategy & campaigning, planning processes and systems, JIIM capability & int.	- Jt Matters & Nat'l Security - Interagency Process - Multinat'l Ops
CAREER-LONG DEVELOPMENT	LIFE-LONG LEARNING SKILLS/SELF-DEVELOPMENT/ADVANCED EDUCATION CULTURAL EDUCATION: FROM AWARENESS TO COMPETENCE				
JOINT EMPHASIS	Joint Introduction - Nat'l Military Capabilities (in all domains) & Organization - Foundations of Joint Warfare	Joint Awareness - Joint Warfare/Cross Domain Fundamentals - Joint Campaigning - Operational Adaptability	JPME Ph I - Nat'l Mil Capabilities Cmd Structure & Strategic Guidance - Jt Doctrine & Concepts - Jt & Multinat'l Forces at Operational Level of War - Jt Planning and Execution Process - Jt C2 - Operational Adaptability -Desired Leader Attributes AJPME	JPME Ph II - NSS & NMS - Jt Warfare, Theater Strategy & Campaigning in Jt, IA, Intergov't & Multi-Nat'l Envirnt - Nat'l & Jt Planning Systems and Processes across all domains. - Integration of Jt, IA, Intergov't & Multinat'l Capabilities - Desired leader Attributes - Strategic Adaptability AJPME	CAPSTONE - NSS - Jt Op Art - Jt Func Component CC courses & JFOWC - NSS - Nat'l Planning Systems & Org - Theater Strategy, campaigning and mil ops in Jt, IA, Intergov't & Multinat'l Environments - IO PINNACLE
DESIRED LEADER ATTRIBUTES	1. UNDERSTANDING SECURITY ENVIRONMENT AND INSTRUMENTS OF NATIONAL SECURITY 2. ANTICIPATING AND RESPONDING TO SURPRISE AND UNCERTAINTY 3. ANTICIPATING AND RECOGNIZING CHANGE AND LEADING TRANSITIONS 4. OPERATING IN INTENT THROUGH TRUST, EMPOWERMENT, AND UNDERSTANDING 5. MAKING ETHICAL DECISIONS BASED ON THE PROFESSION OF ARMS 6. THINKING CRITICALLY/STRATEGICALLY AND APPLYING JOINT WARFIGHTING PRINCIPLES AT ALL LEVELS OF WARFARE				

Figure 1. Joint Officer Professional Military Education Continuum. (Reprinted from Chairman Joint Chiefs of Staff (CJCSI) 1800.01E, Officer Professional Military Education Policy, 29 May 2015, A-A-A-1.)

Advancement/Promotion. One of the most powerful driving factors for the services to build large pools of joint qualified officers resides in the realm of promotions to higher grades. Federal Law relating to joint officer matters influences internal service promotion policy for the grades of O-4 through O-6 and establishes requirements for promotion to the Flag/General Officer grades (O-7 thru O-10). Federal law mandates the

[7] "10 USC Ch 107: Professional Military Education," 10 USC § §2151, §2155, accessed February 27, 2018, http://uscode.house.gov/view.xhtml?path=/prelim@title10/subtitleA/part3/chapter107&edition=prelim; CJCSI 1800.01E, *Officer Professional Military Education Policy*.

military services promote officers in the grades of O-3 to O-5 who are filling joint duties or who are already joint qualified at least an equal rate to their competitive peer group not in joint duties. For promotion to the Flag/General Officer ranks, competing officers must be joint officer qualified.[8] These two promotion requirements serve as great motivators for the services to build deliberate force development models that ensure sufficient numbers of their officers complete JMPE and joint duty experience requirements.

The intent of the joint officer management components of the Goldwater-Nichols Act are to create a robust cadre of joint-minded officers across the services in order to enhance the abilities of the services to integrate and warfight across domains and functions. However, federal law does not dictate the numbers or percentage of joint qualified officers each service must generate. The promotion requirements to flag/general officer serve as a tangible forcing function on the services to train, assign, and promote officers in alignment with these standards. Even though only a small percentage of officers in any occupational field (especially cyberspace) will achieve flag or general officer rank, each occupational field must incorporate these requirements in their internal service officer force development methodology to ensure a sufficient pool of qualified personnel. The result are cyberspace officer force development models that include completion of Joint Professional Military Education and joint duty qualification assignments.

Cyberspace Officer Unique

US military cyberspace officers must fulfill additional cyber-related extra-service requirements beyond the aforementioned joint officer qualification standards. The intent of these additional requirements is two-fold. First, due to the inter-networked nature of military weapon systems and cyberspace capabilities, any cyberspace professional with elevated network privileges or their supervisory decision-makers (e.g. officers) can introduce vulnerability and risks into the larger DoD infrastructure. Thus, the DoD desires a common certification standard for these members. Second, for those members assigned to National and Cyber Mission Force teams, the US Cyberspace Command

[8] "10 USC Ch. 38: Joint Officer Management," 10 USC Ch. 38 § §662, accessed February 28, 2018, http://uscode.house.gov/view.xhtml?path=/prelim@title10/subtitleA/part2/chapter38&edition=prelim.

desires to establish common knowledge, skill, ability, and associated proficiency standards for any service member serving within these standardized team constructs.

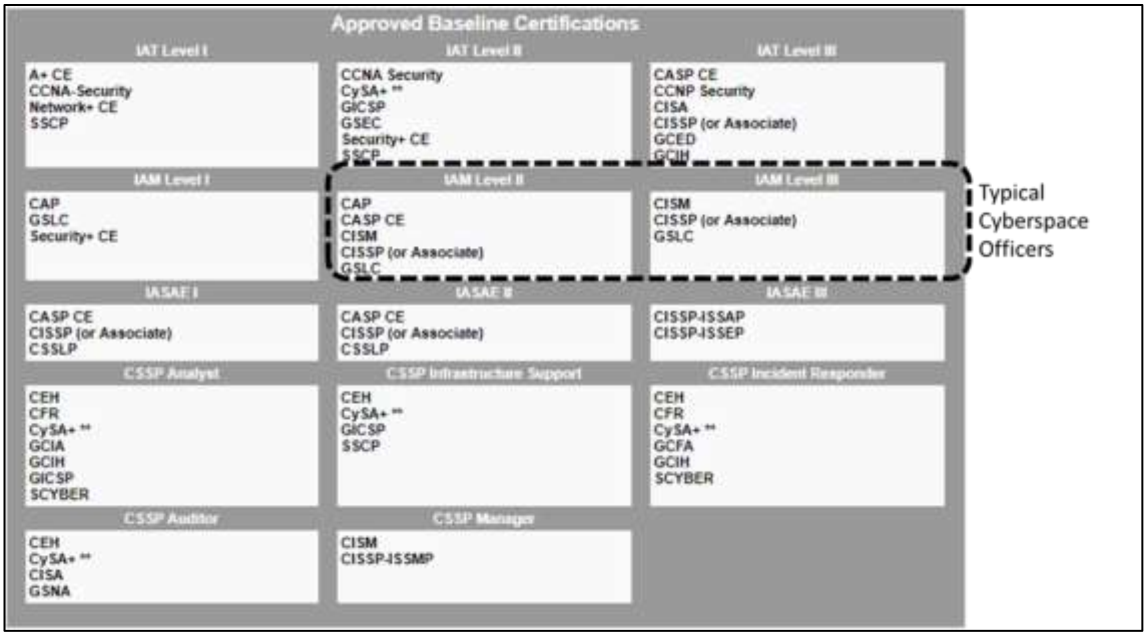
The requirements for cyberspace professionals come from two primary sources respectively: Department of Defense Directive 8140/8570 and United States Cyber Command (USCYBERCOM) Joint Cyberspace Training and Certification Standards (JCT&CS).[9] The first applies to all cyberspace officers while the second applies specifically to officers fulfilling roles on Cyber Mission Forces.

Certification, Training, and Education for All Cyberspace Officers. Department of Defense Directive 8140/8570 (DoDD 8140/8570) dictates specific commercial Information Technology certification requirements for DoD cyberspace professionals, including officers. The type of certification depends upon the level of responsibility of the member, but cyberspace officers typically have Information Assurance Manager Level II or III designated certifications as seen in Figure 2.[10]

DoDD 8140/8570 directs the services to manage these certifications and their members. Each service approaches initial and continuing training and education requirements and procuring the certification for their members in different ways as will be briefly discussed in chapters three through five. While the types and levels of certifications themselves are not relevant to this thesis, it is important that the reader understand that the services must account for the standards into their force development models for cyberspace officers.

[9] Defense Information Systems Agency, “DoD Approved 8570 Baseline Certifications,” IASE: Information Assurance Support Environment, accessed 20 January 2018, https://iase.disa.mil/iawip/Pages/iabaseline.aspx; “Joint Cyberspace Training and Certification Standards” (US Cyber Command, 14 October 2016).

[10] Defense Information Systems Agency, “DoD Approved 8570 Baseline Certifications.”



Approved Baseline Certifications

IAT Level I	IAT Level II	IAT Level III
A+ CE CCNA-Security Network+ CE SSCP	CCNA Security CySA+ ** GICSP GSEC Security+ CE SSCP	CASP CE CCNP Security CISA CISSP (or Associate) GCED GCIH
IAM Level I	**IAM Level II**	**IAM Level III**
CAP GSLC Security+ CE	CAP CASP CE CISM CISSP (or Associate) GSLC	CISM CISSP (or Associate) GSLC
IASAE I	**IASAE II**	**IASAE III**
CASP CE CISSP (or Associate) CSSLP	CASP CE CISSP (or Associate) CSSLP	CISSP-ISSAP CISSP-ISSEP
CSSP Analyst	**CSSP Infrastructure Support**	**CSSP Incident Responder**
CEH CFR CySA+ ** GCIA GCIH GICSP SCYBER	CEH CySA+ ** GICSP SSCP	CEH CFR CySA+ ** GCFA GCIH SCYBER
CSSP Auditor	**CSSP Manager**	
CEH CySA+ ** CISA GSNA	CISM CISSP-ISSMP	

Typical Cyberspace Officers

Figure 2. DoDD 8140/8570 Approved Certifications. (Adapted from Defense Information Systems Agency, "DoD Approved 8570 Baseline Certifications," IASE: Information Assurance Support Environment, accessed 20 January 2018, https://iase.disa.mil/iawip/Pages/iabaseline.aspx.)

Training & Education for National and Cyber Mission Forces. Cyberspace professionals assigned to National and Cyber Mission Force teams fall under additional training and qualification requirements. For those assigned to National Mission Forces, the supported agency required training, qualification, and experience requirements are extensive (years vice months) and USCYBERCOM typically classifies the desired training knowledge, skills, and abilities to protect tradecraft. Therefore, this essay will not provide details as what is important to the reader is to understand there are significant technical/occupational training requirements for members assigned to these teams.

For cyberspace professionals assigned to Cyber Mission Force teams, the USCYBERCOM Joint Cyberspace Training and Certification Standards (JCT&CS) direct specific knowledge, skills, abilities (KSAs) and their associated proficiency levels for members assigned to operational positions. It does not dictate service-unique training requirements but does prescribe specific, service-agnostic standards to servicemembers serving on N/CMF teams.[11] The JCT&CS outlines 48 *work roles* across the six different

[11] "Joint Cyberspace Training and Certification Standards," 1.

types of CMF teams, of which cyberspace officers typically hold one of a subset of 19 work roles.[12] Officers may fill roles as an actual tactical operator through various levels of element and team leadership.

Meeting the N/CMF knowledge, skill, and ability proficiency standards is the responsibility of both USCYBERCOM and the individual services. While the focus and balance of training responsibilities continues to evolve, the current model is that the military services provide foundational cyberspace training and members assigned to CMF work through various service and USCYBERCOM-provided courses. The training pipeline alone for a brand-new cyberspace officer can take anywhere from 26 weeks to 100 weeks depending upon the individual service approach and type of N/CMF team role.[13] This time duration does not include subsequent experiential and mission-specific requirements. The duration of training also changes for cyberspace officers in subsequent tours who become qualified for new work roles or positions.

The intent of the DoD and N/CMF training and certification standards are to ensure common standards expectations across the DoD and its individual military services for cyberspace professionals. Joint personnel managers may assign cyberspace professionals, including officers, from any service to joint organizations or joint service providers like the Defense Information Systems Agency. Likewise, the National Security Agency and/or USCYBERCOM may task members assigned to National or Cyber Mission Force teams to conduct missions outside of their own service mission set or domains. Therefore, the individual military service institutional and occupational force development models must take into account these unique occupational requirements for cyberspace officers.

Chapter Summary

The purpose of this chapter was to highlight the external influences on the individual military services as they build and execute force development models their cyberspace officers. Specifically, this chapter examined the experiential, training and education, and promotion requirements dictated by federal law and CJCS policy for all

[12] “Joint Cyberspace Training and Certification Standards,” 7.
[13] Ibid.

officers, as well as DoD and USCYBERCOM training and certification standards for cyberspace officer.

Primarily, from the joint officer perspective, Joint Officer Professional Military Education throughout the PME continuum provides a wider understanding of Joint Matters and joint functions. Federal law is highly prescriptive in the curriculum requirements for JPME Phase I and II and that officers (including cyberspace officers) require this education to become joint officer qualified. In addition to JPME Phase I and II completion requirements, officers must also complete a joint duty experience for a minimum of two years to become joint officer qualified. Finally, law dictates that eligibility for promotion to Flag or General officer requires the officers to hold joint qualification.

In addition to the requirements of joint officer qualification, cyberspace officer development also entails its own unique requirements. Most military cyberspace officers must earn and maintain commercial certifications of appropriate levels as dictated by DoDD 8140/8570. Furthermore, officers assigned to National and Cyber Mission Forces require additional training and qualification standards as dictate by NSA and USCYBERCOM policy. These additional National or Cyber Mission Force requirements can add months to years of training and experience that officer force development models must account for.

The challenge for the individual military services is devising institutional and subordinate cyberspace (occupational) officer force development models that can account for by-law/joint and cyberspace-unique requirements, while still meeting internal service missions and developmental requirements. This is no mean feat. The next three chapters will specifically illustrate how the US Marine Corps, Army and Air Force currently tackle this problem.

US Air Force Cyberspace Operations Officer Development

This chapter examines how the US Air Force (USAF) develops its officers with a specific focus on cyberspace operations officers. This chapter will first provide an overview of the USAF organization and service mission to provide context to how and why the USAF develops their officers in the manner it does. The chapter will then focus on USAF officer development followed by an examination of the specific nuances of this development model for USAF cyberspace operations officers. At the end of this chapter, the reader will have a foundational understanding of how the USAF develops its cyberspace operations officers to satisfy extra-service and internal USAF developmental priorities, allowing comparative analysis with the USMC and USA in Chapter 6.

USAF Organization

This section will provide service-related context including the USAF mission, organization, and overview of occupational specialty framework. This discussion will provide the reader a working understanding of the USAF as the chapter progresses into a detailed analysis of the USAF officer development model. The contextual overview will not be a full "Air Force 101" but will hit major points relevant to the rest of the chapter and thesis.

It is important to understand the USAF mission and how it organizes itself as this directly relates to the focus, roles, and units to which the USAF assigns its officers. The stated mission of the USAF is to "fly, fight and win in air, space and cyberspace."[1] The USAF is an air- and space-focused military service.

USAF Service Organizational Construct. The USAF primarily organizes units, in descending echelon, into: major commands, numbered air forces, wings, groups, squadrons/detachments, and flights. At the number air force level and higher, USAF organizations generally follow the standard joint staff construct (A1-A10).[2] USAF officers hold positions at any echelon within this organizational construct dependent upon their grade, experience, and military occupational specialty.

The USAF generally does not forward deploy entire units (flying units being the primary exception), but instead tailors deployable capabilities to satisfy combatant

[1] "U.S. Air Force," U.S. Air Force, 2018, https://www.airforce.com/mission.
[2] Air Force Instruction (AFI) 38-101, *Air Force Organization*, 31 January 2017, 75.

commander requirements as efficiently as possible. The USAF uses Unit Type Codes (UTC) to quantify and measure smaller-than-unit capabilities. Some UTCs are squadron-size are larger, while others are to an individual airman.[3] For scoping, the USAF currently has over 32,200 different cyberspace capability UTCs.[4]

For example, a fighter squadron and their associated aircraft maintenance squadron may deploy from one fighter wing, but the USAF typically sources supporting logistics, personnel, civil engineering, and communications (cyberspace) UTCs piecemeal from many different units and installations. The USAF uses this *Air Expeditionary Force* model for two main reasons. First, tailoring the deployable force down to the individual unit type code level maximizes resource efficiency. Second, the majority of mission support capabilities in the USAF a full-time garrison mission in addition to a deployed mission. Therefore, if the USAF deployed an entire base communications squadron, no one would remain at their home installation to provide communications capabilities to the remaining organizations on base.

The discussion of how the USAF deploys is important to the discussion of cyberspace operations officer force development. USAF cyberspace officers must be flexible to waxing and waning garrison personnel due to deployments, as well as will deploy with other cyber UTCs to create new cyberspace units and teams who have not previously known or trained together. To further complicate matters, the mission sets, and organizations the cyberspace officer may deploy with can span the range of AF core mission through other joint missions and functions. Thus, USAF cyberspace officer development must make flexible officers as the potential training requirements are extremely broad.

USAF Cyberspace Organizational Constructs. Understanding the specific roles of USAF cyberspace operations officers requires a more detailed examination of how the USAF organizes cyberspace units and personnel. USAF cyberspace operations officers may hold positions across all echelons and organizations across the USAF. USAF cyberspace operations officers may lead and command various types of service

[3] Air Force Instruction (AFI) 10-403, *Deployment Planning and Execution*, 6 October 2016, 66.
[4] Lt Col David Canady (former SAF CIO/A6 staff officer), interview by the author, September 29, 2015.

cyberspace-related organizations, serve in staff positions, or serve in roles on National and Cyber Mission Forces similar to its sister services.

To further clarify the types of roles a cyberspace operations officer within the USAF may hold, we will examine the actual types of cyberspace units/echelons within the USAF, followed by an examination of cyberspace units/echelons within US Air Force Cyber Command (AFCYBER). USAF cyberspace organizations generally align to the standard USAF organizational construct of numbered air force, wings, groups, and squadrons. The USAF has a single dedicated cyberspace numbered Air Force (24 AF), two cyberspace wings (67 CW and 688 CW), several cyberspace/communications groups, and 147 O-5 or O-4 commanded squadrons.

The 147 squadrons are not mirror images of each other as each varies in size and mission. The majority of USAF cyberspace-related squadrons are base *communications squadrons*, aligned to an installation's host wing and tasked to conduct DoDIN operations to provide communications and information technology capabilities to the local installation units. Squadrons also specialize depending upon specific mission sets. Several of the more common specialized squadrons include cyberspace operations squadrons (introduced in the AFCYBER discussion below), combat communications and contingency response units who provide expeditionary communications capabilities, and Air and Space Communications Squadrons provide mission systems and networks to Air Operations Centers. USAF cyberspace officers at the O-3 and O-2 level may also lead smaller flight and smaller echelon communications capabilities embedded in other operational squadrons such as Special Tactics Squadrons, Air Support Operations Squadrons, and Air Control Squadrons.

The USAF's Air Forces Cyberspace Command (AFCYBER) serves as the service's dedicated component and numbered Air Force (24 AF) that provides USAF global enterprise DoDIN operations, defensive cyberspace operations, offensive cyberspace operations, cyberspace capability test and development, and expeditionary communications (combat communications) for the USAF as well as a force provider to USCYBERCOM and other Combatant Commands. AFCYBER/24 AF is comprised of a command element, the 624th Operations Center, 67th Cyber Wing, 688th Cyber Wing, and 5th Combat Communications Group.[5] The AFCYBER/24 AF subordinate wings, groups, and squadrons will undergo a realignment in the summer of 2018, with all National-Cyber Mission Force teams (within cyberspace operations squadrons) aligning under the 67th Cyber Wing. The USAF-focused defensive and DoDIN operations and several other one-off squadrons align under the 688th Cyber Wing.[6]

One final cyberspace-related organizational construct, the *mission defense team* (MDT), needs examination. In the past 3 years, the USAF started a pilot program to energize defensive cyberspace operations at the lower echelons and focused on defending critical USAF mission threads and weapons systems. Full USAF-wide implementation details for MDTs remain limited at this time, but the USAF will embed the MDTs in existing base communications squadrons to be tasked by host installation/wing commander or Air Forces Cyber (AFCYBER) to actively defend the mission systems and networks deemed most critical to USAF core missions.[7] AFCYBER retains a larger defensive cyberspace and cyber security capability overseeing USAF enterprise networks, but the MDTs will be more tactically and mission focused force multipliers.

Similar to the other US military services, USAF cyberspace operations officers also fill roles across the institutional and operational Air Force. USAF cyberspace officer positions exist in virtually every Air Force and Joint staff organization. Typically, these positions reside within the Directorate of Communications (J6 or A6), but also a growing number in the Operations (J3/A3) and Plans and Programming (J5/J8 or A5/A8) due to the evolution of cyber as an operational warfighting domain. Outside the USAF, its USAF cyberspace operations officers fulfill roles in joint tactical units like the Joint Signal Support Element (JCSE).

USAF Cyberspace Occupational Specialties

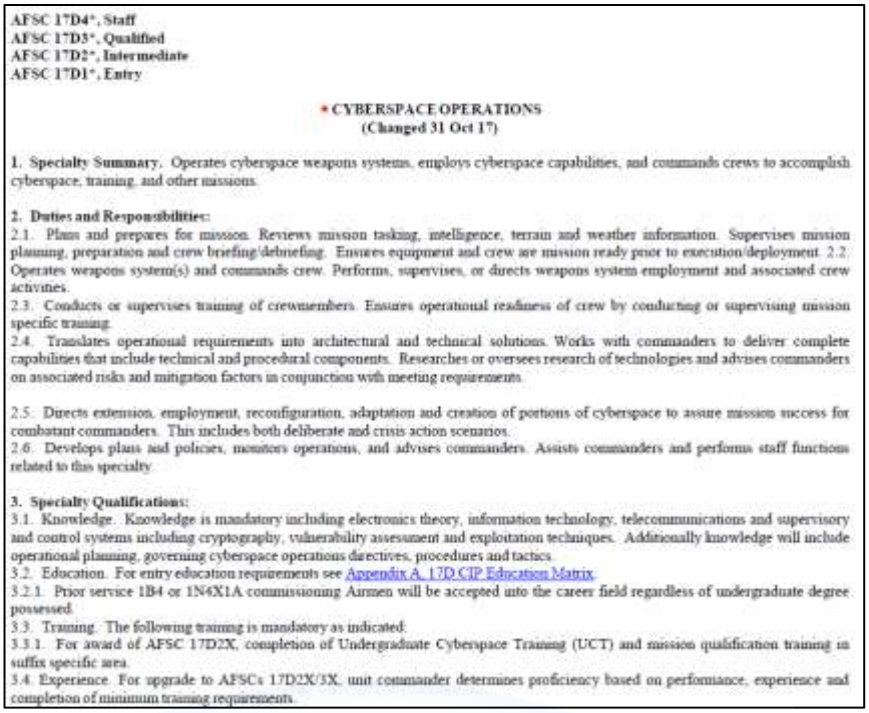
The USAF officer corps are 100% commissioned officers. The USAF does not have limited duty officers or warrant officer constructs as found in other services. As of the writing of this thesis, the United States Air Force has a single core officer Air Force Specialty Code (AFSC) for cyberspace, the *17XX*. Recognizing the need to

[5] "24th Air Force," Air Forces Cyber, 6 February 2017, http://www.afcyber.af.mil/About-Us/Fact-Sheets/Display/Article/458567/24th-air-force-afcyber/.
[6] Bradley L. Pyburn (commander, 67th Cyberspace Wing), interview by the author, 7 March 2018.
[7] Steven T. Wieland, "Cyber Squadron Enabling Concept" (SAF CIO/A6, 15 March 2018), 10, 23.

operationalize its communications force, in 2010 the USAF converted its entire traditional 33SX *Communications and Information Officer* military occupational specialty into the operational 17XX Cyberspace Officer specialty. The "XX" portion of this specialty code denotes a placeholder for sub-specialties based upon the position the member holds. The *17DX* specialty code refers to the *Cyberspace Operations* officer specialty while those members in positions coded *17SX Cyberspace Warfare Operations* for the duration of time in the position.[8] While holding specific positions may require specialized or additional qualification training or to meet selection criteria, current policy provides that any 17XX officer may fill a 17DX or 17SX position. To reduce confusion and unless otherwise specified, the remainder of this thesis will use *Cyberspace Operations Officer* as an umbrella term to denote any officer within the USAF 17XX specialty.

USAF Cyberspace Operations officers fill a plethora of operational, staff, acquisition, and training duties. The official specialty description states *17DX* officers "operate cyberspace weapons systems, employs cyberspace capabilities, and commands crews to accomplish cyberspace, training, and other missions."[9] The majority 17XX officer positions across the USAF are 17DX positions while the remaining positions fall into the 17SX realm and frequently reside in cyber mission force units and/or units within AFCYBER. The official USAF specialty description for officers holding 17SX positions is not substantively different than 17DX, therefore, this chapter will only use the nomenclature *cyberspace operations officer*. For further details on the 17XX specialties, please see figures 3 and 4.

[8] Air Force Officer Classification Directory (AFOCD), Air Force Personnel Center, 31 October 2017, 80-81.
[9] Air Force Officer Classification Directory (AFOCD), 80.



AFSC 17D4*, Staff
AFSC 17D3*, Qualified
AFSC 17D2*, Intermediate
AFSC 17D1*, Entry

*** CYBERSPACE OPERATIONS**
(Changed 31 Oct 17)

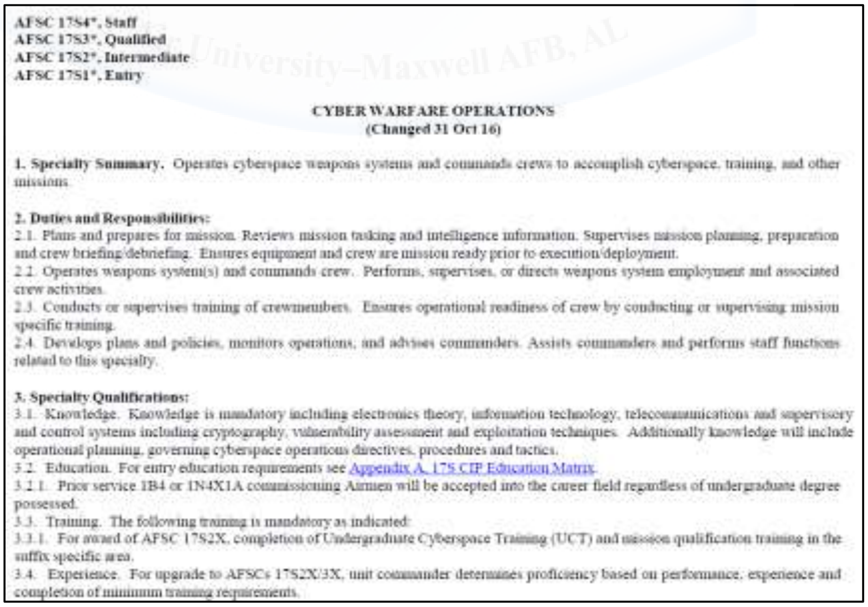
1. Specialty Summary. Operates cyberspace weapons systems, employs cyberspace capabilities, and commands crews to accomplish cyberspace, training, and other missions.

2. Duties and Responsibilities:
2.1. Plans and prepares for mission. Reviews mission tasking, intelligence, terrain and weather information. Supervises mission planning, preparation and crew briefing/debriefing. Ensures equipment and crew are mission ready prior to execution/deployment. 2.2. Operates weapons system(s) and commands crew. Performs, supervises, or directs weapons system employment and associated crew activities.
2.3. Conducts or supervises training of crewmembers. Ensures operational readiness of crew by conducting or supervising mission specific training.
2.4. Translates operational requirements into architectural and technical solutions. Works with commanders to deliver complete capabilities that include technical and procedural components. Researches or oversees research of technologies and advises commanders on associated risks and mitigation factors in conjunction with meeting requirements.

2.5. Directs extension, employment, reconfiguration, adaptation and creation of portions of cyberspace to assure mission success for combatant commanders. This includes both deliberate and crisis action scenarios.
2.6. Develops plans and policies, monitors operations, and advises commanders. Assists commanders and performs staff functions related to this specialty.

3. Specialty Qualifications:
3.1. Knowledge. Knowledge is mandatory including electronics theory, information technology, telecommunications and supervisory and control systems including cryptography, vulnerability assessment and exploitation techniques. Additionally knowledge will include operational planning, governing cyberspace operations directives, procedures and tactics.
3.2. Education. For entry education requirements see Appendix A, 17D CIP Education Matrix.
3.2.1. Prior service 1B4 or 1N4X1A commissioning Airmen will be accepted into the career field regardless of undergraduate degree possessed.
3.3. Training. The following training is mandatory as indicated:
3.3.1. For award of AFSC 17D2X, completion of Undergraduate Cyberspace Training (UCT) and mission qualification training in suffix specific area.
3.4. Experience. For upgrade to AFSCs 17D2X/3X, unit commander determines proficiency based on performance, experience and completion of minimum training requirements.

Figure 3. USAF Cyberspace Operations Officer Occupational Specialty Description. (Reprinted from Air Force Officer Classification Directory (AFOCD), Air Force Personnel Center, 31 October 2017, 80.)



AFSC 17S4*, Staff
AFSC 17S3*, Qualified
AFSC 17S2*, Intermediate
AFSC 17S1*, Entry

CYBER WARFARE OPERATIONS
(Changed 31 Oct 16)

1. Specialty Summary. Operates cyberspace weapons systems and commands crews to accomplish cyberspace, training, and other missions.

2. Duties and Responsibilities:
2.1. Plans and prepares for mission. Reviews mission tasking and intelligence information. Supervises mission planning, preparation and crew briefing/debriefing. Ensures equipment and crew are mission ready prior to execution/deployment.
2.2. Operates weapons system(s) and commands crew. Performs, supervises, or directs weapons system employment and associated crew activities.
2.3. Conducts or supervises training of crewmembers. Ensures operational readiness of crew by conducting or supervising mission specific training.
2.4. Develops plans and policies, monitors operations, and advises commanders. Assists commanders and performs staff functions related to this specialty.

3. Specialty Qualifications:
3.1. Knowledge. Knowledge is mandatory including electronics theory, information technology, telecommunications and supervisory and control systems including cryptography, vulnerability assessment and exploitation techniques. Additionally knowledge will include operational planning, governing cyberspace operations directives, procedures and tactics.
3.2. Education. For entry education requirements see Appendix A, 17S CIP Education Matrix.
3.2.1. Prior service 1B4 or 1N4X1A commissioning Airmen will be accepted into the career field regardless of undergraduate degree possessed.
3.3. Training. The following training is mandatory as indicated:
3.3.1. For award of AFSC 17S2X, completion of Undergraduate Cyberspace Training (UCT) and mission qualification training in the suffix specific area.
3.4. Experience. For upgrade to AFSCs 17S2X/3X, unit commander determines proficiency based on performance, experience and completion of minimum training requirements.

Figure 4. USAF Cyberspace Warfare Officer Occupational Specialty Description. (Reprinted from Air Force Officer Classification Directory (AFOCD), Air Force Personnel Center, 31 October 2017, 81.)

USAF Cyberspace Operations Officer Development

This section will examine the training/education and experiential expectations and milestones over a "typical" USAF cyber officer's career. While no two officers' career paths are identical, each USAF officer occupational community produces career development path charts outlining a typical/desired career path or pyramid. Figures 6 and 7 illustrate the USAF officer and cyber operations officer career paths that this section will dissect. Not explicitly written into policy, the USAF evolved the current overall officer developmental path around the requirements, milestones, and requirements for rated aircrew (e.g. required flight hours, etc.), ensuring a relatively common baseline of expectations and duties for all USAF officers.

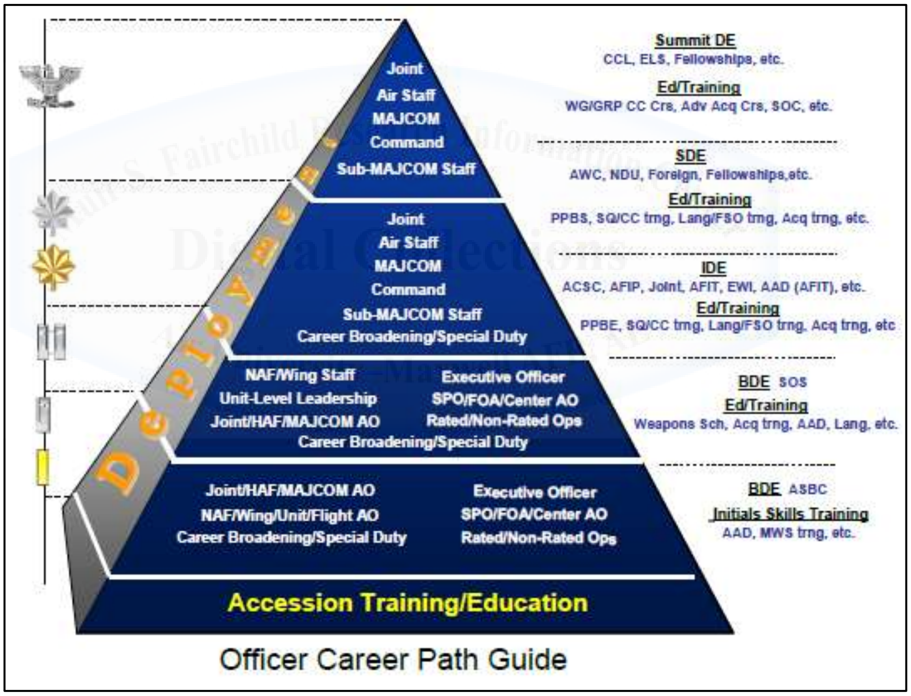

Joint
Air Staff
MAJCOM
Command
Sub-MAJCOM Staff
Joint
Air Staff
MAJCOM
Command
Sub-MAJCOM Staff
Career Broadening/Special Duty
NAF/Wing Staff
Unit-Level Leadership
Joint/HAF/MAJCOM AO
Executive Officer
SPO/FOA/Center AO
Rated/Non-Rated Ops
Career Broadening/Special Duty
Joint/HAF/MAJCOM AO
NAF/Wing/Unit/Flight AO
Career Broadening/Special Duty
Executive Officer
SPO/FOA/Center AO
Rated/Non-Rated Ops
Accession Training/Education
Deployments
Summit DE
CCL, ELS, Fellowships, etc.
Ed/Training
WG/GRP CC Crs, Adv Acq Crs, SOC, etc.
SDE
AWC, NDU, Foreign, Fellowships,etc.
Ed/Training
PPBS, SQ/CC trng, Lang/FSO trng, Acq trng, etc.
IDE
ACSC, AFIP, Joint, AFIT, EWI, AAD (AFIT), etc.
Ed/Training
PPBE, SQ/CC trng, Lang/FSO trng, Acq trng, etc
BDE SOS
Ed/Training
Weapons Sch, Acq trng, AAD, Lang, etc.
BDE ASBC
Initials Skills Training
AAD, MWS trng, etc.
Officer Career Path Guide

Figure 5. USAF Officer Career Pyramid. (Reprinted from Air Force Instruction (AFI) 36-2640, Executing Total Force Development, 29 December 2011, 33.)

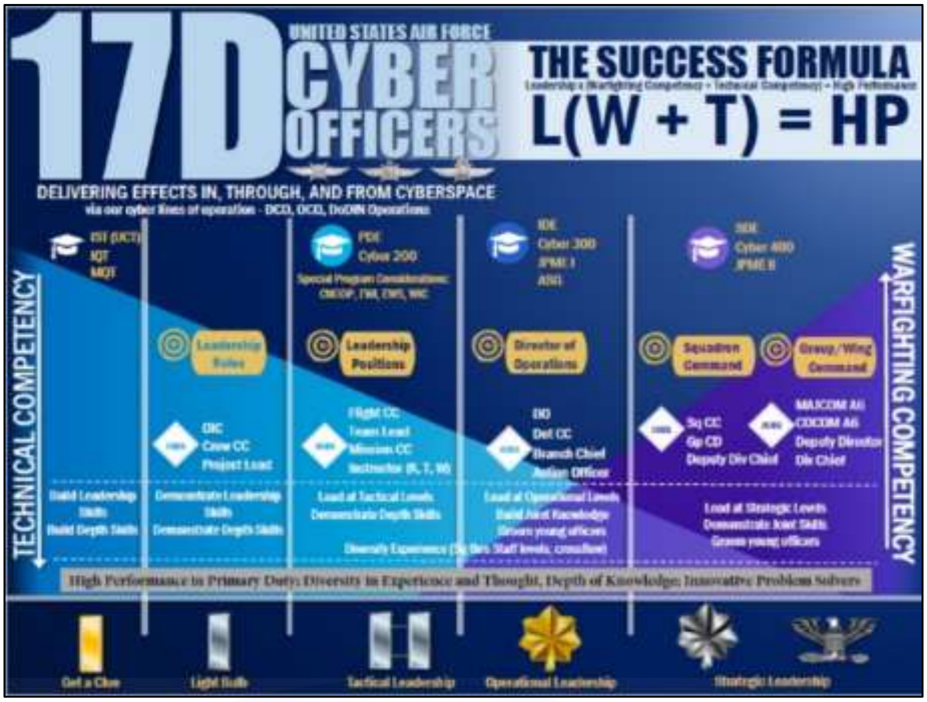
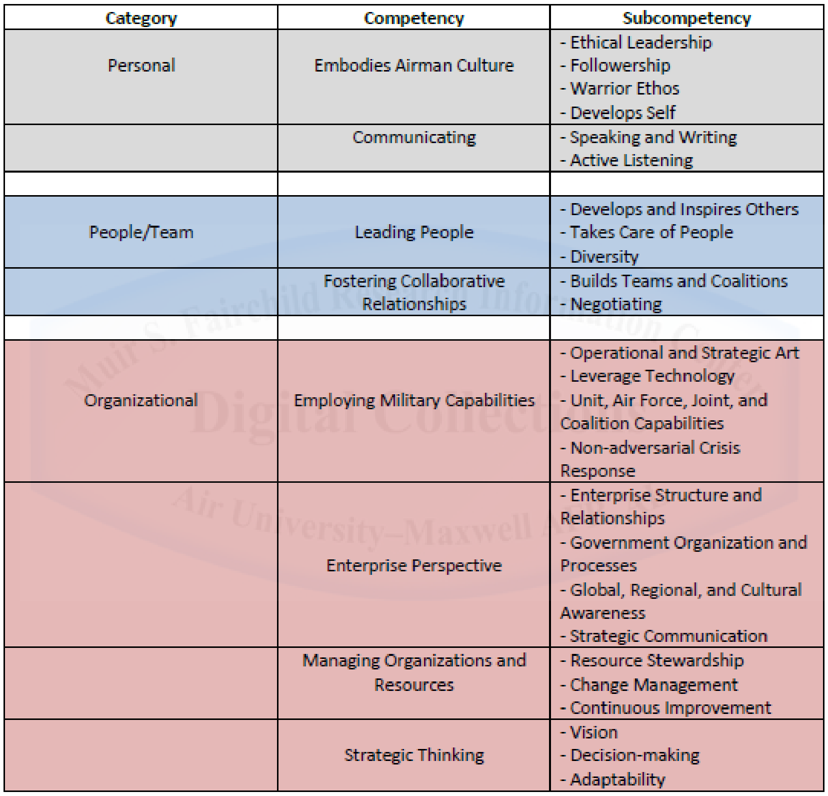


Figure 6. USAF Cyberspace Officer Career Path Chart. (Reprinted from Patrick C. Higby, "USAF Cyberspace Operations Officers Mentoring and Development" (USAF Cyberspace Force Development Team, 20 March 2017), 5.)

This section will divide the first 20 years of an officer's career into four chronological blocks: 0-4 years, 4-10 years, 10-15 years, and 15-20 years. Each chronological block will review the primary institutional and occupational training/education requirements followed by deliberate experience (i.e. key duty positions, employment of capabilities). A complete review of all training, education, and experimental opportunities for USAF officers is outside the scope of this paper, thus it will focus on relatively standard developmental factors and opportunities.

USAF Developmental Focus. Before proceeding into an analysis of the USAF cyberspace operations officer force developmental model, the reader needs to understand some overall developmental goals and themes within the USAF writ-large as well as in the USAF cyberspace community. The USAF utilizes defined institutional competencies to "…enhance leadership performance, set behavioral standards of leadership for all levels of the Total Force and translate requirements and values into behavioral indicators."[10] These competencies, listed in Table 3, emphasize what the USAF expects from its personnel. The proficiency levels in each sub-competency depends upon the grade of the individual (i.e. higher proficiency as member advances through the ranks).[11] Specific to officer development, these competencies drive curriculum requirements for USAF Professional Military Education: from pre-commissioning sources through Air War College.[12]

Table 3. USAF Institutional Competencies



Category	Competency	Subcompetency
Personal	Embodies Airman Culture	- Ethical Leadership - Followership - Warrior Ethos - Develops Self
	Communicating	- Speaking and Writing - Active Listening
People/Team	Leading People	- Develops and Inspires Others - Takes Care of People - Diversity
	Fostering Collaborative Relationships	- Builds Teams and Coalitions - Negotiating
Organizational	Employing Military Capabilities	- Operational and Strategic Art - Leverage Technology - Unit, Air Force, Joint, and Coalition Capabilities - Non-adversarial Crisis Response
	Enterprise Perspective	- Enterprise Structure and Relationships - Government Organization and Processes - Global, Regional, and Cultural Awareness - Strategic Communication
	Managing Organizations and Resources	- Resource Stewardship - Change Management - Continuous Improvement
	Strategic Thinking	- Vision - Decision-making - Adaptability

Source: Reprinted from Curtis E. LeMay Center for Doctrine Development and Education, Annex 1-1 Force Development, Appendix, Institutional Competency List, 1.

In 2016, senior leaders within the USAF cyberspace operations officer community decided that the USAF institutional competencies sufficiently covered the

[10] Air Force Manual (AFMAN) 36-2647, *Institutional Competency Development and Management*, 15 September 2016, 3, http://static.e-publishing.af.mil/production/1/af_a1/publication/afman36-2647/afman36-2647.pdf.
[11] Ibid., 12–20.
[12] Ibid., 20–21.

expertise they believe USAF cyberspace officers.[13] In addition, several other documents govern the occupational standards, tasks, and proficiency levels for USAF cyberspace operation officers, nominally tasks and standards within these documents align with the *Employing Military Capabilities* and *Enterprise Perspective* institutional competencies. These governing directives are the 17X Career Field Education and Training Plan (CFETP) and the 17-2 series Air Force Instructions.[14]

Years 0-4 (2nd Lieutenant – 1st Lieutenant)

The first four years of an USAF officer's career varies significantly between occupational specialties. For example, pilots, navigators, and air battle managers undergo extensive occupational training during their first four-plus years, and the USAF expects them to focus on developing their occupational proficiency at the individual level. Contrast that experience with a logistics readiness or aircraft maintenance officer who, as a lieutenant, may supervise more than 100 enlisted airmen, in addition to his personal development. Similarly, lieutenants in cyberspace operations face a myriad of potential experiences during their first four years.

Training & Education (0-4 years). The USAF currently provides no institutional training or education courses for officers prior to the four-year point of their career. The USAF experimented with a 6-8-week Lieutenant-level Professional Military Education course similar to the USMC Basic Course for several years in the 2000s, but eliminated it in 2011 due to fiscal reasons.[15] Therefore, the USAF relies on its commissioned sources and in-unit professional development to provide sufficient institutional competency training and education for its most junior officers.

USAF officers do receive occupational training during their first four years. All cyberspace operations officers first attend Undergraduate Cyberspace Training (UCT) at Keesler AFB, Mississippi. This training, currently a six-month course, is very technically focused, emphasizing foundational cyber and information technology knowledge and skillsets as outlined in the 17X CFETP. UCT contains 13 major blocks of instruction

[13] Jeffrey Blankenship (former duty with Air Force Senior Leader Matters Office), interview by the author, 29 September 2017.

[14] "AFSC 17X Cyberspace Operations Officer Career Field Education and Training Plan" (Department of the Air Force, 15 August 2014).

[15] Kevin E. Blanchard, "Air and Space Basic Course: A Cost-Effective Contribution to Air Force Officer Professional Development?" (Air University, 16 February 2011), 5.

aligned in two phases. UCT Phase One focuses on cyberspace fundamentals instructed in five blocks: Introduction to Cyberspace Operations (67 hours), Operating Systems (72 hours), Scripting (72 hours), Network Fundamentals (56 hours), and Network Configuration (93 hours).[16] UCT Phase Two focuses on more advanced cyberspace and operational concepts instructed in eight blocks: Attacking and Exploiting Cyber Networks (124 hours), Defensive Cyberspace Operations and Department of Defense Information Network (115 hours, Industrial Control Systems (34 hours), Telephony Networking (36.5 hours), Strategic Network Warfare (70 hours), Law and Ethics (16 hours), Fighting Through a Cyber Attack capstone (79 hours), and DoDD 8570.1M Boot Camp and Certification (85.5 hours).[17]

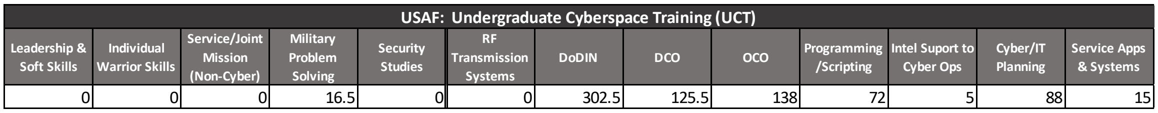
Table 4 depicts the content of the UCT blocks of instruction by thematic variable. The course primarily focuses on the occupational aspects of cyberspace operations balanced between the three cyber lines of effort (DoDIN, defensive, and offensive cyberspace operations).[18] USAF cyberspace officers can fill a multitude of roles within and across the three cyberspace lines of effort, thus the balanced approach within the curriculum. Interestingly, UCT includes little foundational training or education on RF transmission systems and theory (radio and SATCOM). And yet, the USAF's core missions rely heavily on RF transmission systems as aircraft, space assets, battlefield airmen, base defenders and first responders, wing operations centers, and air operations centers which all use transmission systems to communicate and operate.

Two additional items of note in UCT involve commercial information assurance certification and a tailored focus on cyberspace-enabled capabilities important to the USAF mission. Cyberspace operations officers receive commercial Security+ certification during the final block of UCT instruction, satisfying DoDD 8140/8570 information assurance requirements. Additionally, officers receive training on the supporting cyberspace architectures for space systems, integrated air defense systems,

[16] Robert D. Patt, "Undergraduate Cyberspace Training (Phase 1) Course Chart" (333d Training Squadron, 28 September 2016), 2.
[17] Robert D. Patt, "Undergraduate Cyberspace Training (Phase 2) Course Chart" (333d Training Squadron, 22 September 2016), 2-3.
[18] "Undergraduate Cyberspace Training (Phase 1) Plan of Instruction" (333d Training Squadron, 28 September 2016); "Undergraduate Cyberspace Training (Phase 2) Plan of Instruction" (333d Training Squadron, 22 September 2016).

ballistic missile defense systems, tactical air control systems, tactical datalinks, and industrial control systems.[19]

Table 4. USAF Undergraduate Cyberspace Training Curriculum Content (hours)

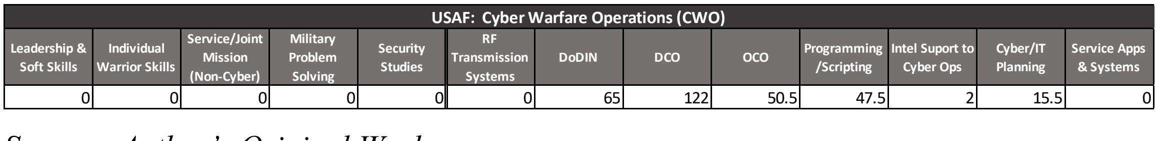


USAF: Undergraduate Cyberspace Training (UCT)												
Leadership & Soft Skills	Individual Warrior Skills	Service/Joint Mission (Non-Cyber)	Military Problem Solving	Security Studies	RF Transmission Systems	DoDIN	DCO	OCO	Programming /Scripting	Intel Suport to Cyber Ops	Cyber/IT Planning	Service Apps & Systems
0	0	0	16.5	0	0	302.5	125.5	138	72	5	88	15

Source: Author's Original Work

Following UCT and dependent upon follow-on duty assignment, certain cyberspace officers will attend additional specialized cyberspace training. The 39th Information Operations Squadron at Hurlburt Field, Florida provides much of the training courses for officers heading to cyber mission force teams. The most common 39 IOS course that many cyberspace officers complete is the Cyber Warfare Operations course. This 9.5-week course focuses on increasing students offensive and defensive. The curriculum contains 9 blocks of instruction: Windows Operating System Foundations (29.5 hours), Linux Operating System Foundations (28 hours), Programming/Scripting Fundamentals (47.5 hours), Networking and Protocols (7.5 hours), SANS Advanced Digital Forensics and Incident Response (69 hours), Network Forensics (15.5 hours), Forensics and Malware (37.5 hours), Offensive Cyber Operations and Methodologies (50.5 hours), and Mission Analysis and Plan, Brief, Execution, Debrief Model (17.5 hours).[20] Table 5 depicts the content of these blocks of instruction by thematic variable. CWO students earn a commercial Global Information Assurance Certification (GIAC) Certified Forensic Analyst certification, yet another certification that satisfies DoDD 8140/8570 certification requirements.[21]

Table 5. USAF Cyber Warfare Operations Curriculum Content (hours)



USAF: Cyber Warfare Operations (CWO)												
Leadership & Soft Skills	Individual Warrior Skills	Service/Joint Mission (Non-Cyber)	Military Problem Solving	Security Studies	RF Transmission Systems	DoDIN	DCO	OCO	Programming /Scripting	Intel Suport to Cyber Ops	Cyber/IT Planning	Service Apps & Systems
0	0	0	0	0	0	65	122	50.5	47.5	2	15.5	0

Source: Author's Original Work

[19] Robert D. Patt, "Undergraduate Cyberspace Training (Phase 2) Course Chart," 3.
[20] "Cyber Warfare Operations (CWO) Training" (39th Information Operations Squadron, January 2017), 5.
[21] "Cyber Warfare Operations (CWO) Training," 6.

Key Duties/Experience (0-4 years). Upon completion of UCT and other en-route training courses, USAF cyberspace operations officers flow to their first duty assignment. The USAF does not identify any key duty positions in the first 4 years as the units and experiences of junior officers greatly varies by occupational specialty and duty assignment.

Cyberspace operations officer duty experience during these years varies greatly. Ideally, the USAF desires to send new lieutenants to one of the 147 cyberspace-related squadrons to build tactical and leadership experience. Members initially assigned to a cyber mission force team or cyber weapon system unit may hold the duty title and positional qualification as a weapon system operator and/or crew commander.[22] This experience aligns more to the rated aircrew developmental experience in their first four years of service. On the contrary, junior officers assigned to a base communications squadron or combat communications squadron may hold leadership duty titles such as "Officer in Charge" or "Chief of XXXX", leading significant numbers of enlisted airmen. This latter experience aligns more to the examples of the logistics readiness and maintenance officer experience.

Years 4-10 (Captain)

At the end of these first four years of service, USAF developmental expectations of its officers start to align across occupational specialties, to include key duty experience and education. Years 4-10 of an USAF officer's career will typically involve at least two duty assignments and includes a 6.5-week PME. These 6 years focus on higher levels of leadership (flight command), potentially breadth in a staff position,6.5-week PME called Squadron Officer School (SOS), and advanced occupational training for certain occupational specialties to include cyberspace.

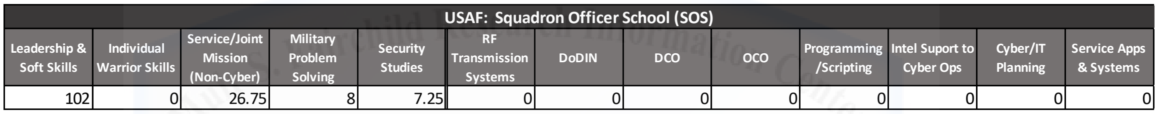
Training & Education (4-10 years). The first post-commissioning institutional USAF Professional Military Education, Squadron Officer School (SOS), occurs during this period of a member's career (years 4-7). Squadron Officer School is currently 6.5 weeks long, focuses on "four primary areas (1) leadership, (2) building highly-effective teams, (3) logical and ethical reasoning in decision making, and (4) multi-domain joint

[22] "AFSC 17X Cyberspace Operations Officer Career Field Education and Training Plan."

warfare (SOC website). SOS accomplishes these objectives through four blocks of instruction: Leadership (45 hours), Team building (24 hours), Reasoning (33 hours), and Joint Warfare (34 hours).[23]

Table 6 depicts the content of SOS blocks of instruction by thematic variable. SOS is the first common institutional PME any USAF officer receives, thus it deliberate focus on reinforcing the commonalities between all USAF occupational specialties. Most of the 6.5 weeks focus on leadership (including team-building) and a knowledge-level understanding of core USAF missions and joint capabilities. Students return to their assigned duty units with an "enhanced understanding of institutional competencies, leadership actions, and key elements of reasoning required to fly, fight, and win in the 21st century."[24]

Table 6. USAF: USAF Squadron Officer School Curriculum Content (hours)



USAF: Squadron Officer School (SOS)												
Leadership & Soft Skills	Individual Warrior Skills	Service/Joint Mission (Non-Cyber)	Military Problem Solving	Security Studies	RF Transmission Systems	DoDIN	DCO	OCO	Programming /Scripting	Intel Suport to Cyber Ops	Cyber/IT Planning	Service Apps & Systems
102	0	26.75	8	7.25	0	0	0	0	0	0	0	0

Source: Author's Original Work

The USAF offers several additional highly selective courses to officers during this period. Too few cyberspace operations officers attend these courses to include them as part of the overall curriculum analysis in this project. However, these courses are important to the USAF and cyberspace community and the concluding thesis chapter will highlight the import of these courses in charting a way-forward.

The USAF officers a highly-selective course for USAF officers in operational (1X-series) career fields: the Weapons Instructor Course (WIC). WIC, established as the "Fighter Weapons School" in 1954, "trains tactical experts and leaders to control and exploit air, space and cyber on behalf of the joint force."[25] Each occupational specialty

[23] "Squadron Officer School (SOS) In-Resident Course Catalog" (Air University Squadron Officer College, 24 August 2017), 5.

[24] "Welcome to Squadron Officer School," Air University, 5 April 2018, http://www.airuniversity.af.mil/SOS/.

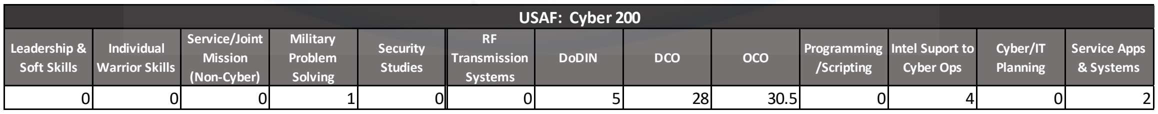
[25] "United States Air Force Weapons School," Nellis Air Force Base, 10 May 2016, http://www.nellis.af.mil/About/Fact-Sheets/Display/Article/284156/united-states-air-force-weapons-school/.

at WIC follows a specified occupational tactical-level training track, including practical experience and integration across occupations and capabilities. The USAF established the “Cyber WIC” in 2012, affording cyberspace operations officers to attend WIC.[26]

From the occupational side, the USAF affords its cyberspace operations officers one mandatory and three primary competitive educational opportunities. The required education course is Cyber 200, a course owned and provided by the Air Force Institute of Technology’s Center for Cyberspace Research at Wright-Patterson AFB, Ohio.[27] Cyberspace 200 is a 3-week course focused at the tactical and operational level of warfare. The four blocks of instruction at Cyber 200 are: Fundamentals (12 hours), Offensive Cyber Operations (16.5 hours), Defensive Cyber Operations (14 hours), and DoDIN (5 hours), Perspectives (12.5), and a Capstone event (36.5 hours).[28]

Table 7 depicts the content of Cyber 200 blocks of instruction by thematic variable. The course primarily focuses on tactical offensive and defensive cyberspace operations, but the newest curriculum includes a lesson on operational design. For many USAF cyberspace officers, this may be their first exposures to military design and how it can inform problem solving and planning.

Table 7. USAF Cyber 200 Curriculum Content (hours)



USAF: Cyber 200												
Leadership & Soft Skills	Individual Warrior Skills	Service/Joint Mission (Non-Cyber)	Military Problem Solving	Security Studies	RF Transmission Systems	DoDIN	DCO	OCO	Programming /Scripting	Intel Suport to Cyber Ops	Cyber/IT Planning	Service Apps & Systems
0	0	0	1	0	0	5	28	30.5	0	4	0	2

Source: Author’s Original Work

Amongst the many optional courses available to officers in these grades, the three primary competitively selected programs are Engineering with Industry (EWI), the USMC’s Expeditionary Warfare School (EWS), and the Computer Network Operations Development Program (CNODP). EWI is an opportunity for a handful of USAF cyberspace operations (and other AFSC) captains to spend a year-long internship with a

[26] Ken Lustig, “Weapons School Integrates Cyber Warfare,” Nellis Air Force Base, 30 May 2012, http://www.nellis.af.mil/News/Article/284777/weapons-school-integrates-cyber-warfare.
[27] “AFSC 17X Cyberspace Operations Officer Career Field Education and Training Plan,” 12.
[28] Kimber Nettis, “Cyberspace 200 Course Guide (FY18)” (Air Force Institute of Technology, 15 March 2018).

commercial corporation, typically within the technological and communication realm.[29] The USMC Expeditionary Warfare School is the same school covered in Chapter 5 and USAF cyberspace operations officers are the only USAF officers afforded this opportunity (six attend annually).[30] Computer Network Operations Development Program is a National Security Agency developmental program that produces "technical Computer Network Operations (CNO) leaders in the areas of CNO defense, exploitation and attack."[31] Though there are limited opportunities to attend, each program brings valuable knowledge, skillsets, and follow-on assignment opportunities for a select group of USAF cyberspace officers.

Key Duties/Experience (4-10 years). The primary key developmental position for a USAF officer in this career window is *flight commander*.[32] The flight, the immediate subordinate echelon to the squadron, may range in size from ten personnel into the hundreds. Flight command is typically the first time the average USAF officer leads a significant number of people. The duties and mission of the flights depends the occupational community as well as the type of unit. A rated aircrew member typically only executes ADCON of their flights as OPCON/TACON during mission execution (i.e. flying operations) falls within separate C2 channels. A cyber operations officer may lead 100 personnel, executing ADCON as well as OPCON/TACON of their mission execution. On the counter a USAF cyber operations officer holding "Flight Command" of a CMF unit may or may not have TACON/OPCON during mission execution as USCYBERCOM retain C2 authority (not the USAF). Thus, while the position of flight commander is a key development duty across the institutional USAF, the actual leadership experience and expectations vary greatly across occupations and units.

Years 10-15 (Major – Lieutenant Colonel)

After reaching the 10-year mark in their careers, the USAF promotes most USAF officers to the rank of major which is the first field-grade rank. Like its sister service

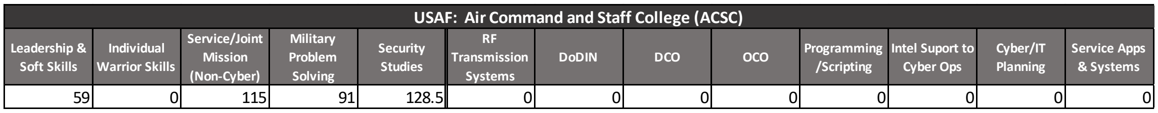
[29] "2019 Advanced Academic Degree (AAD) and Special Experience Exchange Duties Selection Process Guide" (Air Force Personnel Center, 4 April 2018), 23.
[30] "2019 Advanced Academic Degree (AAD) and Special Experience Exchange Duties Selection Process Guide," 26.
[31] "National Security Agency Development Programs," Intelligence Careers, 2018, https://www.intelligencecareers.gov/nsa/nsadevprograms.html.
[32] "Air Force Instruction (AFI) 36-2640, *Executing Total Force Development*, 33.

counterparts, field grade officers (FGOs) begin focusing on higher levels of leadership (and larger organizations), furthering broadening experience at the headquarters staff level or in the joint realm. The institutional Professional Military Education expectations focus on completing Intermediate Developmental Education (IDE) either in residence or by distance education.

Training & Education (10-15 years). Many of those competitively selected for in-residence IDE attend the USAF Air Command and Staff College at Maxwell AFB, Alabama. However, a percentage of officers can attend fellowships or attend sister-service or international equivalent developmental education opportunities such as the Army Command and General Staff College or Marine Corps Command and Staff College, which the study will cover in more detail in succeeding chapters.

Air Command and Staff College (in-residence and distance education) fulfills Joint Professional Military Education I (JPME I) requirements and also awards an accredited Master's of Military Operational Art and Science degree.[33] ACSC's major blocks of instruction include Leadership (58 hours), War Theory (42 hours), International Security I and II (96 hours), Airpower I and II (83 hours), and Joint Warfighting (133 hours).[34] Table 8 depicts the content of these blocks of instruction by thematic variable.

Table 8. USAF Air Command and Staff College Curriculum Content (hours)



USAF: Air Command and Staff College (ACSC)												
Leadership & Soft Skills	Individual Warrior Skills	Service/Joint Mission (Non-Cyber)	Military Problem Solving	Security Studies	RF Transmission Systems	DoDIN	DCO	OCO	Programming /Scripting	Intel Suport to Cyber Ops	Cyber/IT Planning	Service Apps & Systems
59	0	115	91	128.5	0	0	0	0	0	0	0	0

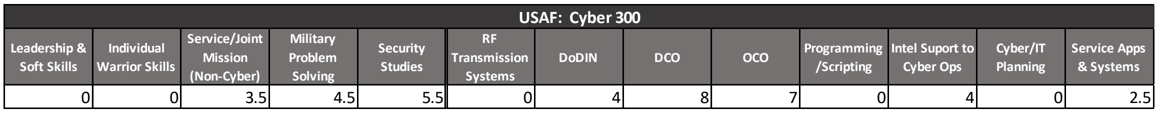
Source: Author's Original Work

[33] "Air Command and Staff College Resident Curriculum," Air University, 5 October 2017, http://www.airuniversity.af.mil/ACSC/Display/Article/922353/resident-curriculum/.

[34] Trevor D. Albertson, "Airpower I: Capabilities and Limitations in American Airpower Syllabus AY 18" (United States Air Force Air Command and Staff College, 2018); Heather P. Venable, "Airpower II: Integrating Air, Cyber, and Space into Multi-Domain Operations Syllabus AY 18" (United States Air Force Air Command and Staff College, 2018); Brent A. Lawnicsak, "Joint Warfighting: 'How We Fight' Syllabus AY 18" (United States Air Force Air Command and Staff College, 2018); Fil Arenas, "Leadership Syllabus AY 18" (United States Air Force Air Command and Staff College, 2018); J. Wesley Hutto, "International Security I: The Context of International Security Syllabus AY 18" (United States Air Force Air Command and Staff College, 2018); Ann Mezzell, "International Security II: The Conduct of National Security Syllabus AY 18" (United States Air Force Air Command and Staff College, 2018); Kelly A. Grieco, "War Theory: The Evolution of War and Military Thought Syllabus AY 18" (United States Air Force Air Command and Staff College, 2018).

Occupationally, USAF cyberspace officers attend the Cyber 300 provided by the Air Force Institute of Technology's Center for Cyberspace Research at Wright-Patterson AFB, Ohio. Cyberspace 300 is a 2-week course focused at the operational and strategic level. The seven blocks of instruction include: Strategy (12.5 hours), Mission Assurance (6 hours), DoDIN operations (4 hours), Defensive Cyberspace Operations (8 hours), Offensive Cyberspace Operations (7 hours), Joint (10 hours), and Industry (4 hours).[35] Table 9 depicts the contents of these blocks of instruction by thematic variable.

Table 9. Cyber 300 Curriculum Content (hours)



USAF: Cyber 300												
Leadership & Soft Skills	Individual Warrior Skills	Service/Joint Mission (Non-Cyber)	Military Problem Solving	Security Studies	RF Transmission Systems	DoDIN	DCO	OCO	Programming /Scripting	Intel Suport to Cyber Ops	Cyber/IT Planning	Service Apps & Systems
0	0	3.5	4.5	5.5	0	4	8	7	0	4	0	2.5

Source: Author's Original Work

Key Duties/Experience (10-15 years). Experientially, during the 10-15-year period of a career, the key duties USAF officers complete are squadron Director of Operations (or equivalent) and in some cases, Squadron Command. Certain USAF occupational areas such as cyberspace are able to command as a major or lieutenant colonel, while the vast majority of other operational career fields command as a lieutenant colonel around the 15-18-year points in their career.[36] Apart from key developmental duties, USAF officers may have the opportunity to complete staff duty within the USAF (numbered air force, major command, or headquarters air force) or externally in a joint staff billet to complete joint duty experience requirements.[37]

Years 15-20 (Lieutenant Colonel – Colonel)

The final chronological block of career analysis covers years 15-20. Around the 15-year mark in their careers, USAF officers compete for the rank of lieutenant colonel. A small percentage of high performing officers reach colonel and O-6 level commands during this window, however these outliers are outside the scope of this thesis. Like its

[35] Andrew Day, "Cyberspace 300 Course Syllabus (FY18)" (Air Force Institute of Technology, 12 February 2018).

[36] Patrick C. Higby, "USAF Cyberspace Operations Officers Mentoring and Development" (USAF Cyberspace Force Development Team, 20 March 2017), 5.

[37] Air Force Instruction (AFI) 36-2640, *Executing Total Force Development*, 33.

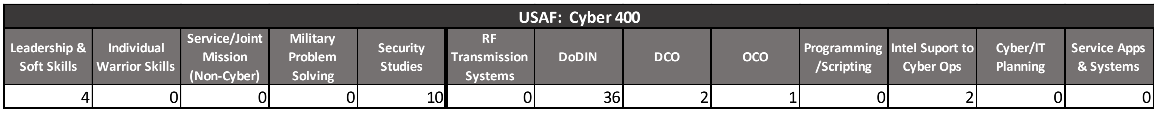
sister service counterparts, field grade officers in this period of their career continue to focus on higher levels of leadership (and larger organizations), furthering broadening experience at the headquarters staff level or in the joint realm. Additionally, USAF officers complete another level of professional military education (resident or correspondence), with this senior level education satisfying the requirements for Joint Professional Military Education Level II.

Training & Education (15-20 years). The primary institutional USAF professional military education during this part of a career is Senior Developmental Education (SDE). The USAF's SDE program is the Air War College (AWC) held at Maxwell AFB, Alabama. Like the previous intermediate-level developmental education, competitively selected officers may attend in-residence SDE (AWC, joint/sister service equivalents, or other fellowships) while all USAF lieutenant colonels may complete AWC by distance education. The other primary education opportunity at this level is completing a JPME II course taught by the National Defense University (often a pre-requisite for those assigned to joint organizations who have not previously completed JMPE II requirements in a SDE program).

Occupationally, USAF cyberspace operations officers must complete the 1-week resident Cyber 400 course during this point in their career.[38] Cyber 400 focuses at the strategic level of cyberspace and is comprised of two major instructional components. As a prerequisite to attend the resident portion of Cyber 400, officers must complete the National Defense University's Chief Information Officer Roles and Responsibilities 2.0 course (~34 hours residence or distance education). The second component of Cyber 400 is the resident Cyber 400 course in Washington D.C. The course curriculum changes, but the instruction typically divides into the following blocks of instruction: Senior Leader Challenges (8-12 hours), Cyberspace Force Management and Development Initiatives (18-22 hours), Interagency Partnership in Cyberspace (10 hours), and a Capstone Problem (4-6 hours).[39] Table 10 depicts the content of these blocks of instruction by thematic variable.

[38] "AFSC 17X Cyberspace Operations Officer Career Field Education and Training Plan," 12.
[39] Vic L. Ashdown, "Cyber 400 Schedule - 18002" (333d Training Squadron, 20 April 2018).

Table 10. Cyber 400 Curriculum Content (hours)



USAF: Cyber 400												
Leadership & Soft Skills	Individual Warrior Skills	Service/Joint Mission (Non-Cyber)	Military Problem Solving	Security Studies	RF Transmission Systems	DoDIN	DCO	OCO	Programming /Scripting	Intel Suport to Cyber Ops	Cyber/IT Planning	Service Apps & Systems
4	0	0	0	10	0	36	2	1	0	2	0	0

Source: Author's Original Work

Experience (15-20 years). The key developmental duty required of competitive officers in this timeframe is successful completion of squadron command. During this window, competitive USAF officers also gain broadening in various levels of staffs, centers, or agencies. The USAF also ensures officers competitive for O-6 and beyond begin or complete Joint Duty staff tours to fulfill Joint Qualified Officer requirements to be competitive for promotion beyond O-6.[40]

Chapter Summary

This chapter sought to provide the reader a foundational understanding of how the US Air Force develops cyberspace operations officers within the larger context of USAF officer development and DoD/joint officer requirements. Due to the nature of the USAF mission, the USAF warfighting/deployment construct relies on fixed installations to project airpower. Furthermore, several core AF Missions such as space, intelligence, and offensive cyberspace operations execute much of their warfighting mission from garrison locations. The result is USAF personnel executing their different warfighting functions without training or exercising together, and yet deploying or executing missions together. Furthermore, the installation support echelons retain a full-time garrison installation mission and yet their personnel and resources continue a deployable resource for expeditionary air operations.

Experience during the first four years of service varies widely across USAF military occupational specialty and assigned units. Likewise, cyberspace operations officers garner varied experience within the occupational field. Certain officers will immediately lead airmen in a unit aligned with DoDIN operations, while others will spend their first four-plus years on keyboard executing cyber missions. Beyond the first

[40] Air Force Instruction (AFI) 36-2640, *Executing Total Force Development*, 33; Higby, "USAF Cyberspace Operations Officers Mentoring and Development," 5.

four years, cyberspace operations officer key developmental positions and experience through the 20-year point of the career largely mirror rest of the operational air force. Flight command and squadron command (or their equivalents) serve as the two primary key developmental duties through the O-5 grade. The USAF also ensures competitive field grade officers complete their joint duty experience at some point during the 10-20-year portion of their careers.

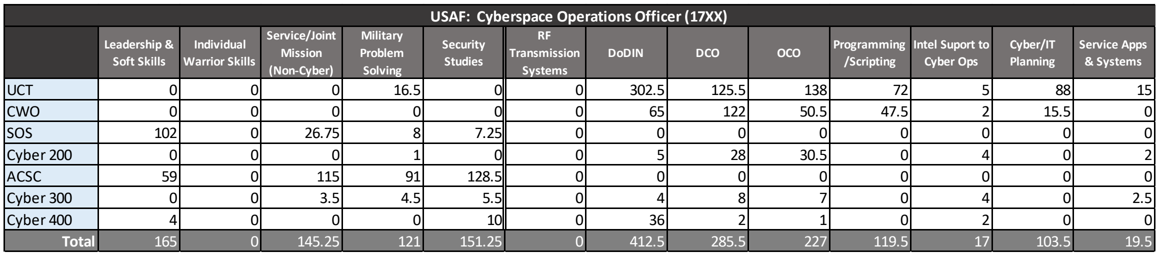
Air Force institutional training and education begins at the O-3 grade with Squadron Officer School. Cyberspace occupational training and education begins within the first year after commissioning and continues through every chronological block of a career. The primary and commonly-required cyberspace occupational courses all cyberspace operations officers take are Undergraduate Cyberspace Training, Cyber 200, Cyber 300, and Cyber 400. Many officers also experience Cyber Warfare Operations, thus the inclusion of the course in this analysis.

Table 11 provides the summary of thematic content of formal training and education courses a notional USAF cyberspace officer experiences through their twentieth year of commissioned service. A seasoned USAF cyberspace officer may note that Table 11 below leaves out dozens of specialized or “just-in-time” cyberspace-related courses. These courses are essential to training the USAF cyberspace force but, other than the Air Operations Center Initial Qualification Training, many of the courses are less than 7 years old. Also, the preponderance of the USAF cyberspace courses are part of the pipeline for cyberspace officers heading to very specific CMF units and/or cyberspace weapons system units, thus the vast majority of USAF cyberspace officers do not have deliberate and ready access to the educational opportunities. Even the CWO course included in this chapter does not apply to all cyberspace officers. Due to the relatively limited penetration of these courses into the larger USAF cyberspace operations officer population, this thesis focused on the cyberspace training and education courses that the majority of USAF cyberspace officers attend (CWO being the exception).

An initial look at Table 11 may show that over the span of a career, the USAF cyberspace officer force development model provides a balance between institutional and occupational competencies in training and education. However, this table can be misleading as truly the majority of training and education within the formative first 12 years of service focuses on the occupational vice institutional. The USAF cyberspace operations officer force development model generates at most 102 hours leadership, 26.75 hours service/joint mission focus, 25.5 hours military problem-solving methodologies, and 7.25 hours security studies. Of note is that the majority (17.5 hours of 26.75) of military problem-solving training come in occupational training opportunities vice Air Force-wide institutional courses. Compare these 161.5 hours of institutional training in the first 12 years to 1,118 hours of occupational training and education: a 1:14 hour ratio. Thus, it appears that the USAF values occupational competency development in the formative first half of a career over formal institutional competency development. This lack of institutional competency focus coupled with disparate duty experiences results in a cyberspace officer corps with a unpredictable and varied understanding of how the USAF executes its core missions. The result is an entire occupational field that may be occupationally brilliant, but many who do not understand how they should enable and/or execute AF and joint warfighting across all domains.

With this foundational understanding of USAF cyberspace officer development, the next chapter will examine the USA's signal and cyberspace operations officer force development models.

Table 11. USAF Cyberspace Officer Career Education/Training (hours)



USAF: Cyberspace Operations Officer (17XX)												
	Leadership & Soft Skills	Individual Warrior Skills	Service/Joint Mission (Non-Cyber)	Military Problem Solving	Security Studies	RF Transmission Systems	DoDIN	DCO	OCO	Programming /Scripting	Intel Suport to Cyber Ops	Cyber/IT Planning	Service Apps & Systems
UCT	0	0	0	16.5	0	0	302.5	125.5	138	72	5	88	15
CWO	0	0	0	0	0	0	65	122	50.5	47.5	2	15.5	0
SOS	102	0	26.75	8	7.25	0	0	0	0	0	0	0	0
Cyber 200	0	0	0	1	0	0	5	28	30.5	0	4	0	2
ACSC	59	0	115	91	128.5	0	0	0	0	0	0	0	0
Cyber 300	0	0	3.5	4.5	5.5	0	4	8	7	0	4	0	2.5
Cyber 400	4	0	0	0	10	0	36	2	1	0	2	0	0
Total	165	0	145.25	121	151.25	0	412.5	285.5	227	119.5	17	103.5	19.5

Source: Author's Original Work

US Army Signal & Cyberspace Operations Officer Development

This chapter examines United States Army (USA) officer force development and specific nuances for the Army's two primary cyberspace-related officer occupational fields: signal officers and cyberspace operations officers. The chapter will first provide an overview of the Army organization and service mission to provide context to how and why the Army develops their officers in the manner it does. The chapter will then focus on Army officer development followed by an examination of the specific nuances of this development model for Army signal and cyber officers. At the end of this chapter, the reader will have a foundational understanding of how the Army develops its signal and cyberspace operations officers to satisfy extra-service and internal Army developmental priorities, allowing comparative analysis with the USMC and USAF in Chapter 6.

USA Organization

This section will provide service-related context including the Army mission, organization, and overview of occupational specialty framework. This discussion will provide the reader a working understanding of the Army as the chapter progresses into a detailed analysis of the Army officer development model. The contextual overview will not be a full "Army 101" but will hit major points relevant to the rest of the chapter and thesis.

It is important to understand the Army mission and how it organizes itself as this directly relates to the focus, roles, and units to which the Army assigns its officers. The stated mission of the United States Army is to "fight and win our Nation's wars by providing prompt, sustained land dominance across the full range of military operations and spectrum of conflict in support of combatant commanders."[1] The Army is inherently land-centric focused military service, however relies heavily on organic and sister service capabilities in other domains (air, maritime, space, etc.) to execute its mission.

Army Service Organizational Construct. The Army divides its active duty force and units into two large functional bins: the Operational Army and the Institutional Army. The Operational Army consists of soldiers and associated units that execute the operational/warfighting mission of the Army. The operational Army organizes its warfighting organizations into numbered armies, corps, divisions, brigades, battalions,

[1] "U.S. Army Organization: Who We Are," U.S. Army, 2018, https://www.army.mil/info/organization.

companies, and platoons. Operational Army units train and deploy as one. For example, a Brigade Combat Team will typically deploy in its entirety vice pieces of multiple brigades packaged together to forward-deploy. The institutional Army exists to support the operational Army. The institutional Army will "raise, train, equip, deploy, and ensure the readiness of all Army forces."   This tasking includes operating Army installations on which the operational Army organizations reside and trains when not deployed.[2]

Army units generally follow the standard US land component organizational model in both its operational and institutional Army. In increasing size order, the Army organizes its units into platoons, companies (3-4 platoons), battalions/squadrons (3-5 companies), brigades (4-6 battalions), divisions (2 or more brigades), corps (2 or more divisions), and numbered Armies (2 or more corps).[3] At each echelon from battalion and higher, the unit has a staff that aligns with the J-staff construct. Army officers hold positions at any echelon within this organizational construct dependent upon their grade, experience, and military occupational specialty. Army signal and cyberspace operations officers fill various roles in the operational and institutional Army.

Army Signal Organizational Constructs. Understanding the specific roles of Army signal and cyberspace operations officers requires a more detailed examination of how the Army organizes these units and personnel. Army signal and cyberspace operations officers may hold positions across all echelons and organizations within the operational and institutional Army. Army signal officers may command signal units, serve in S/G-6 positions on staffs, or serve in roles on National and Cyber Mission Forces like their sister services.

To further clarify the types of roles a signal or cyberspace operations officer within the Army may hold, we will examine the actual types of signal and cyberspace units/echelons within the main operating Army, followed by an examination of signal and cyberspace units/echelons within USA Cyber Command (ARCYBER). The primary role of Army signal units within the operational Army is to provide expeditionary communications capabilities across the range of military operations in peace and war.

[2] "U.S. Army Organization: Who We Are."
[3] Ibid.

When not on operational missions, these signal echelons train and prepare with their supported operational Army commands.

The Army aligns signal organizations into *signal commands* (division-equivalent), *signal brigades*, *signal battalions*, *signal companies*, and *signal platoons*. Each signal echelon consists of subordinate echelons in line with the standard operational Army construct (e.g. signal brigade contains signal battalions and so forth). Outside of the major dedicated signal organizations, the Army aligns signal organizations within its Corps and subordinate operational echelons to provide dedicated, expeditionary communications capabilities within their parent unit. Starting at the lowest, companies and battalions such as infantry, armor, and artillery will have an S-6 section. Brigade Combat Teams contain an O-3 commanded signal company aligned under the Brigade Special Troops Battalion.[4]

Army Cyberspace Organizational Constructs. The Army organizes its cyberspace operations forces under Army Cyber Command (ARCYBER) and in Cyber and Electromagnetic Activities (CEMA) cells. ARCYBER is the USA's organization responsible for defensive cyberspace operations (DCO) and offensive cyberspace operations (OCO) in support of both the Army and as a force provider to USCYBERCOM.[5] ARCYBER is comprised of a command element, Network Command (NETCOM), the 1st Information Operations Brigade (Land), 780th Military Intelligence Brigade (Cyber), and Cyber Protection Brigade.[6] Except for the 1st IOB, the three remaining organizations functionally align to Department of Defense Information Network (DoDIN) operations, offensive cyberspace operations, and defensive cyberspace operations. NETCOM primarily focuses on executing DoDIN operations for the global Army enterprise network.[7] The 780th MIB (Cyber) focuses on signal intelligence and

[4] Field Manual (FM) 3-90.6, *Brigade Combat Team*, 14 September 2010, 1–8, https://usacac.army.mil/sites/default/files/misc/doctrine/CDG/cdg_resources/manuals/fm/fm3_90x6.pdf.
[5] Army Regulation (AR) 10-87, *Army Commands, Army Service Components, and Direct Reporting Units*, 11 December 2017, 17. https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/ARN2541_AR10-87_WEB_Final.pdf.
[6] "U.S. Army Cyber Command," U.S. Army Cyber Command, http://www.arcyber.army.mil/.
[7] "NETCOM: U.S. Army Network Enterprise Technology Command," U.S. Army, http://www.netcom.army.mil.

offensive cyberspace operations while the Cyber Protection Brigade focuses on defensive cyberspace operations.[8]

The cyberspace and electronic activity (CEMA) cells are a new Army-devised construct to embed cyberspace and electronic warfare capabilities within several echelons of its operational Army. Implementation details are limited at this time; however, cyberspace operations officers will likely lead these cells at certain echelons.[9]

Like the other US military services, both Army signal and cyberspace operations officers also fill roles in Institutional Army organizations. Some serve in roles that align with their specialty such as service on Headquarters Army staffs or subordinate Army Commands such as Training and Doctrine Command (doctrine, training, education) or Army Logistics Command (acquisitions and major logistics).[10] Outside the Army, its signal and cyberspace operations officers fulfill roles in joint organizations such as the Joint Staff, Combatant Commands, and joint tactical units like the Joint Signal Support Element (JCSE).

Army Cyberspace Occupational Specialties

This section will illustrate the two cyberspace-related officer military occupational fields within the Army: signal and cyberspace operations. However, the reader must first understand unique officer force management dynamics within the Army. The Army divides its active duty officer corps into commissioned officers and warrant officers. Commissioned officers are what one thinks of as a traditional military officer: their role is to become proficient in their core specialty, lead, and command personnel, and can rise to the grade of O-6 and beyond. The intent the Warrant Officer program is to retain a cadre of specialized and technically proficient officers within a given occupational specialty. The remainder of this section and chapter will focus on commissioned officers as the comparable officer pool across the USA and US Air Force.

The Department of the Army Pamphlet 600-3 *Officer Professional Development and Career Management* outlines the approved military occupational specialties (MOS)

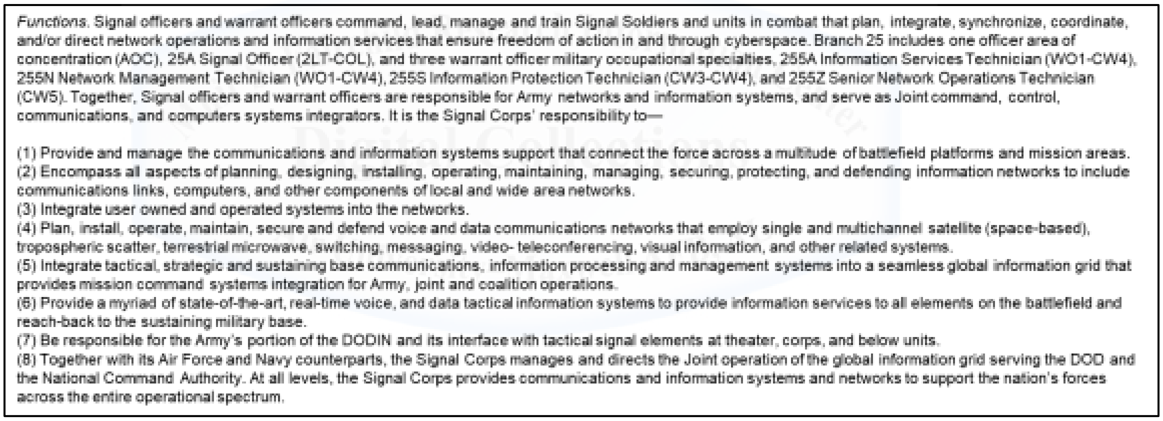
[8] "780th Military Intelligence Brigade," 780th Military Intelligence Brigade, https://www.inscom.army.mil/msc/780mib/.

[9] Mark Pomerleau, "Here's How the Army Wants to Integrate Cyber, EW into Operational Formations," Fifth Domain, 2 October 2017, https://www.fifthdomain.com/dod/army/2017/10/02/heres-how-the-army-wants-to-integrate-cyber-ew-into-operational-formations/.

[10] "U.S. Army Organization: Who We Are."

for Army officers, warrant officers, and enlisted. Effective 1 September 2014, the Army has had two primary military occupational specialties in the cyberspace field: the *signal* (25-series) and the *cyberspace operations* (17-series).[11] The following sections will provide details on the 25A signal officer and 17A/B cyberspace operations officers occupational specialties. The Army directly assesses second lieutenants into both specialties out of their commissioning source.

Occupational Specialty: Signal Officer (25A). The Army military occupational specialty for signal corps officers is 25A. The signal branch of the Army focuses on service DoDIN operations ranging from enterprise information technology at garrison bases through providing mobile communications to forward-deployed fighting Army forces.[12] Figure 7 is an excerpt from the Department of the Army Pamphlet 600-3 that provides a detailed and an authoritative description of the 25A signal officer function.



Functions. Signal officers and warrant officers command, lead, manage and train Signal Soldiers and units in combat that plan, integrate, synchronize, coordinate, and/or direct network operations and information services that ensure freedom of action in and through cyberspace. Branch 25 includes one officer area of concentration (AOC), 25A Signal Officer (2LT-COL), and three warrant officer military occupational specialties, 255A Information Services Technician (WO1-CW4), 255N Network Management Technician (WO1-CW4), 255S Information Protection Technician (CW3-CW4), and 255Z Senior Network Operations Technician (CW5). Together, Signal officers and warrant officers are responsible for Army networks and information systems, and serve as Joint command, control, communications, and computers systems integrators. It is the Signal Corps' responsibility to—

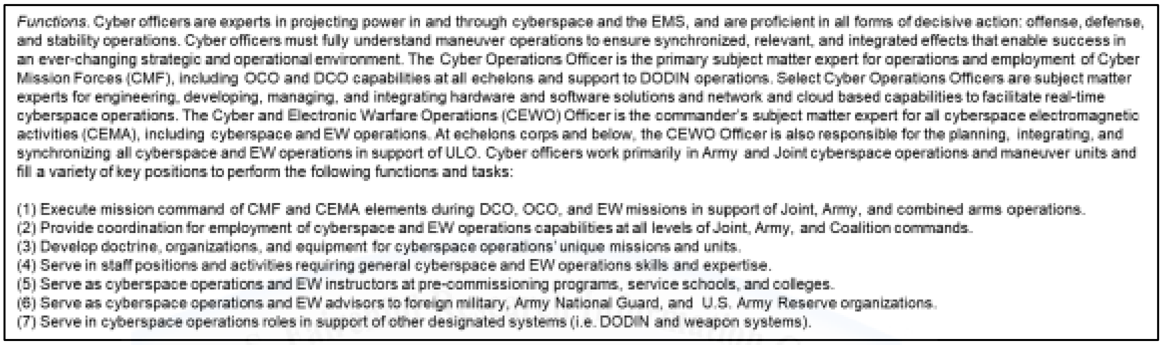
(1) Provide and manage the communications and information systems support that connect the force across a multitude of battlefield platforms and mission areas.
(2) Encompass all aspects of planning, designing, installing, operating, maintaining, managing, securing, protecting, and defending information networks to include communications links, computers, and other components of local and wide area networks.
(3) Integrate user owned and operated systems into the networks.
(4) Plan, install, operate, maintain, secure and defend voice and data communications networks that employ single and multichannel satellite (space-based), tropospheric scatter, terrestrial microwave, switching, messaging, video- teleconferencing, visual information, and other related systems.
(5) Integrate tactical, strategic and sustaining base communications, information processing and management systems into a seamless global information grid that provides mission command systems integration for Army, joint and coalition operations.
(6) Provide a myriad of state-of-the-art, real-time voice, and data tactical information systems to provide information services to all elements on the battlefield and reach-back to the sustaining military base.
(7) Be responsible for the Army's portion of the DODIN and its interface with tactical signal elements at theater, corps, and below units.
(8) Together with its Air Force and Navy counterparts, the Signal Corps manages and directs the Joint operation of the global information grid serving the DOD and the National Command Authority. At all levels, the Signal Corps provides communications and information systems and networks to support the nation's forces across the entire operational spectrum.

Figure 7. USA Signal Officer Occupational Specialty Description. (Reprinted from Department of the Army Pamphlet 600-3, Commissioned Officer Professional Development and Career Management, Signal Corps Branch, 1 June 2017.)

Occupational Specialty: Cyberspace Operations Officer (17A/B). The Army established its Cyber Branch on 1 September 2014.[13] The Army designates

[11] John M. McHugh, "General Order No. 2014-63: Establishment of the United States Army Cyber Branch" (Headquarters, Department of the Army, August 21, 2014); Department of the Army Pamphlet 600-3, *Commissioned Officer Professional Development and Career Management*, *Signal Corps Branch*, 1 June 2017; Department of the Army Pamphlet 600-3, *Commissioned Officer Professional Development and Career Management*, *Cyber Branch*, 17 January 2018.
[12] Department of the Army Pamphlet 600-3, *Commissioned Officer Professional Development and Career Management: Signal Corps Branch*, 1.
[13] McHugh, "General Order No. 2014-63: Establishment of the United States Army Cyber Branch."

commissioned officer within the cyber branch as 17A cyberspace operations officers or 17B cyber and electronic warfare operations officers. All cyberspace branch commissioned officers begin as a 17A, but the Army sends select 17As to its electronic warfare units to earn the 17B MOS. The cyber branch focuses on offensive cyberspace operations, defensive cyberspace operations, and electronic warfare operations.[14] Figure 8 is a direct excerpt from the Department of the Army Pamphlet 600-3 that provides a detailed and authoritative description of a cyberspace operations officer functions.



Functions. Cyber officers are experts in projecting power in and through cyberspace and the EMS, and are proficient in all forms of decisive action: offense, defense, and stability operations. Cyber officers must fully understand maneuver operations to ensure synchronized, relevant, and integrated effects that enable success in an ever-changing strategic and operational environment. The Cyber Operations Officer is the primary subject matter expert for operations and employment of Cyber Mission Forces (CMF), including OCO and DCO capabilities at all echelons and support to DODIN operations. Select Cyber Operations Officers are subject matter experts for engineering, developing, managing, and integrating hardware and software solutions and network and cloud based capabilities to facilitate real-time cyberspace operations. The Cyber and Electronic Warfare Operations (CEWO) Officer is the commander's subject matter expert for all cyberspace electromagnetic activities (CEMA), including cyberspace and EW operations. At echelons corps and below, the CEWO Officer is also responsible for the planning, integrating, and synchronizing all cyberspace and EW operations in support of ULO. Cyber officers work primarily in Army and Joint cyberspace operations and maneuver units and fill a variety of key positions to perform the following functions and tasks:

(1) Execute mission command of CMF and CEMA elements during DCO, OCO, and EW missions in support of Joint, Army, and combined arms operations.
(2) Provide coordination for employment of cyberspace and EW operations capabilities at all levels of Joint, Army, and Coalition commands.
(3) Develop doctrine, organizations, and equipment for cyberspace operations' unique missions and units.
(4) Serve in staff positions and activities requiring general cyberspace and EW operations skills and expertise.
(5) Serve as cyberspace operations and EW instructors at pre-commissioning programs, service schools, and colleges.
(6) Serve as cyberspace operations and EW advisors to foreign military, Army National Guard, and U.S. Army Reserve organizations.
(7) Serve in cyberspace operations roles in support of other designated systems (i.e. DODIN and weapon systems).

Figure 8. USA Cyberspace Operations Officer Occupational Specialty Description. (Reprinted from "Department of the Army Pamphlet 600-3 Commissioned Officer Professional Development and Career Management: Cyber Branch" [Headquarters, Department of the Army, January 17, 2018].)

Army Signal and Cyberspace Operations Officer Development

This section will examine the training/education and experiential expectations and milestones over a "typical" Army cyber officer's career. While no two officers' career paths are identical (even within a single occupational field), each Army officer occupational community produces career development path charts outlining a typical/desired career path or pyramid. Figures 10, 11, and 12 provide the Army's official career models for 25A signal, 17A cyberspace operations, and 17B cyberspace and electronic warfare operations officers respectively. The reader may find it useful to reference back to these charts as they proceed through the remainder of this chapter.

[14] Department of the Army Pamphlet 600-3, *Commissioned Officer Professional Development and Career Management: Cyber Branch*, 1.

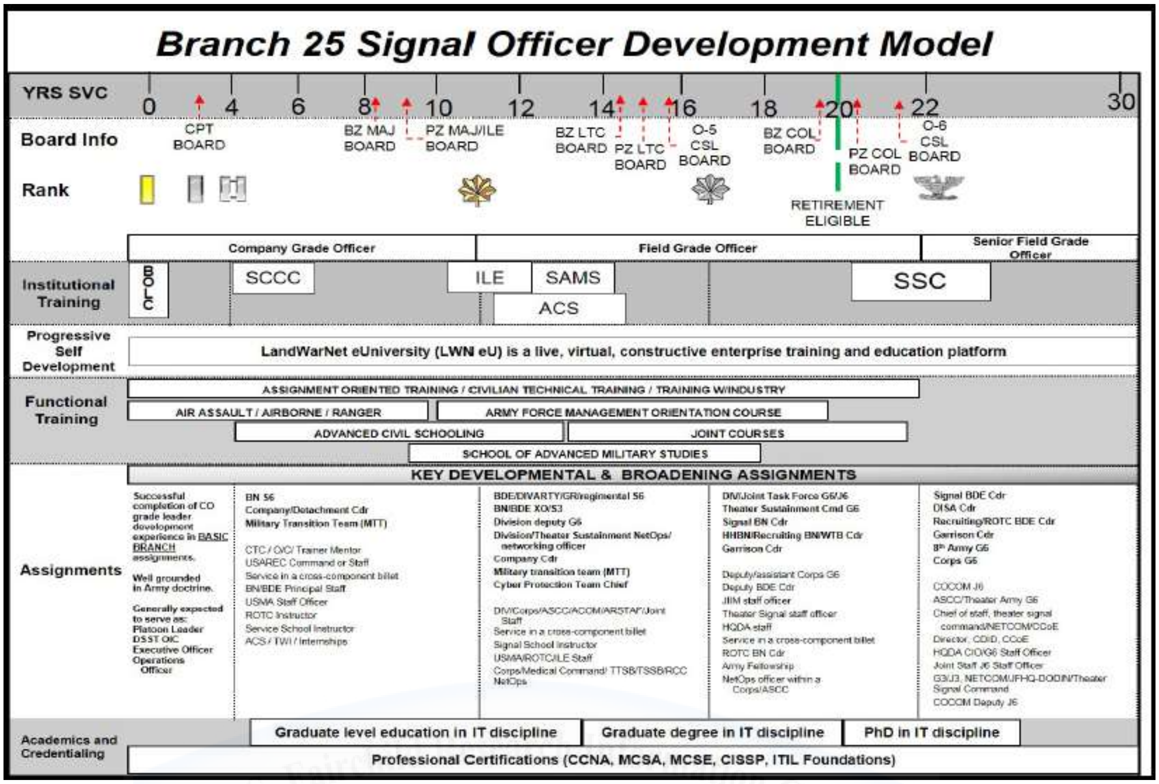

Branch 25 Signal Officer Development Model
YRS SVC
0
4
6
8
10
12
14
16
18
20
22
30
Board Info
CPT BOARD
BZ MAJ BOARD
PZ MAJ/ILE BOARD
BZ LTC BOARD
PZ LTC BOARD
O-5 CSL BOARD
BZ COL BOARD
PZ COL BOARD
O-6 CSL BOARD
Rank
RETIREMENT ELIGIBLE
Company Grade Officer
Field Grade Officer
Senior Field Grade Officer
Institutional Training
BOLC
SCCC
ILE
SAMS
ACS
SSC
Progressive Self Development
LandWarNet eUniversity (LWN eU) is a live, virtual, constructive enterprise training and education platform
Functional Training
ASSIGNMENT ORIENTED TRAINING / CIVILIAN TECHNICAL TRAINING / TRAINING W/INDUSTRY
AIR ASSAULT / AIRBORNE / RANGER
ARMY FORCE MANAGEMENT ORIENTATION COURSE
ADVANCED CIVIL SCHOOLING
JOINT COURSES
SCHOOL OF ADVANCED MILITARY STUDIES
KEY DEVELOPMENTAL & BROADENING ASSIGNMENTS
Assignments
Successful completion of CO grade leader development experience in BASIC BRANCH assignments.
Well grounded in Army doctrine.
Generally expected to serve as:
Platoon Leader
DSST OIC
Executive Officer
Operations Officer
BN S6
Company/Detachment Cdr
Military Transition Team (MTT)
CTC / O/C/ Trainer Mentor
USAREC Command or Staff
Service in a cross-component billet
BN/BDE Principal Staff
USMA Staff Officer
ROTC Instructor
Service School Instructor
ACS / TWI / Internships
BDE/DIVARTY/GR/regimental S6
BN/BDE XO/S3
Division deputy G6
Division/Theater Sustainment NetOps/ networking officer
Company Cdr
Military transition team (MTT)
Cyber Protection Team Chief
DIV/Corps/ASCC/ACOM/ARSTAF/Joint Staff
Service in a cross-component billet
Signal School Instructor
USMA/ROTC/ILE Staff
Corps/Medical Command/ TTSB/TSSB/RCC NetOps
DIV/Joint Task Force G6/J6
Theater Sustainment Cmd G6
Signal BN Cdr
HHBN/Recruiting BN/WTB Cdr
Garrison Cdr
Deputy/assistant Corps G6
Deputy BDE Cdr
JIIM staff officer
Theater Signal staff officer
HQDA staff
Service in a cross-component billet
ROTC BN Cdr
Army Fellowship
NetOps officer within a Corps/ASCC
Signal BDE Cdr
DISA Cdr
Recruiting/ROTC BDE Cdr
Garrison Cdr
8th Army G6
Corps G6
COCOM J6
ASCC/Theater Army G6
Chief of staff, theater signal command/NETCOM/CCoE
Director, CDID, CCoE
HQDA CIO/G6 Staff Officer
Joint Staff J6 Staff Officer
G3/J3, NETCOM/JFHQ-DODIN/Theater Signal Command
COCOM Deputy J6
Academics and Credentialing
Graduate level education in IT discipline
Graduate degree in IT discipline
PhD in IT discipline
Professional Certifications (CCNA, MCSA, MCSE, CISSP, ITIL Foundations)

Figure 9. USA Signal Officer Career Model. (Reprinted from Department of the Army Pamphlet 600-3, Commissioned Officer Professional Development and Career Management, Signal Branch, 1 June 2017, 7.)

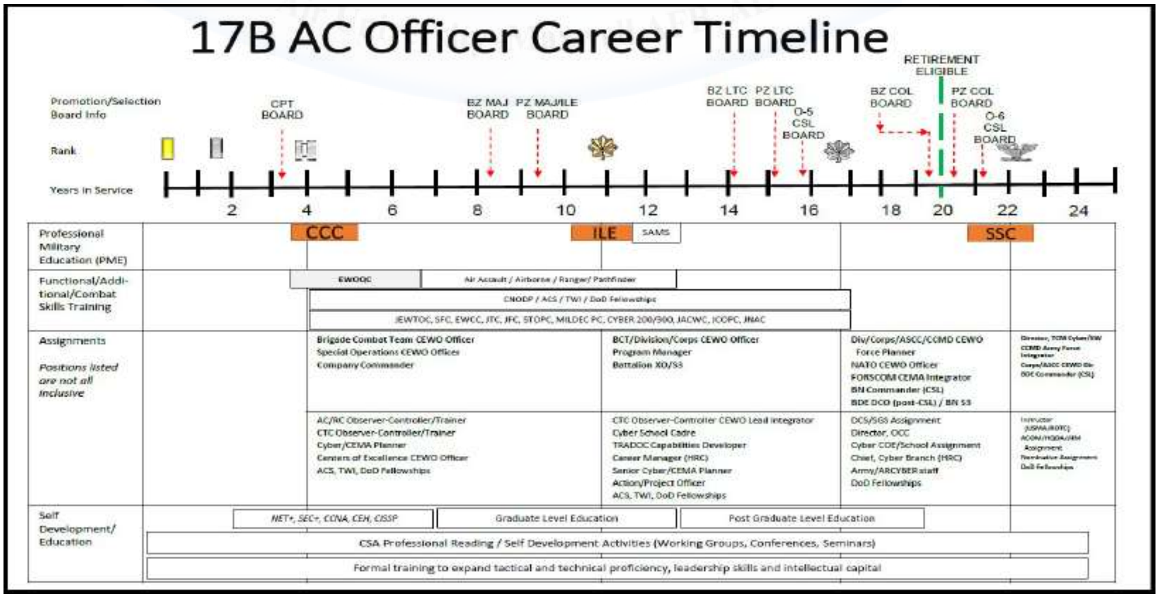
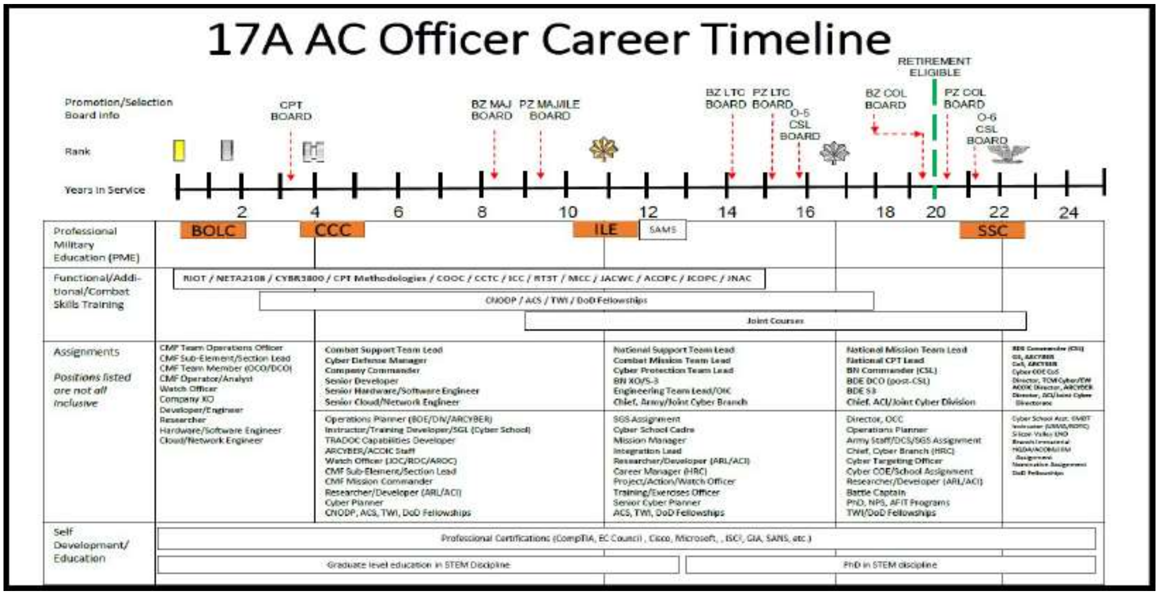

17B AC Officer Career Timeline
RETIREMENT ELIGIBLE
Promotion/Selection Board Info
CPT BOARD
BZ MAJ BOARD
PZ MAJ/ILE BOARD
BZ LTC BOARD
PZ LTC BOARD
O-5 CSL BOARD
BZ COL BOARD
PZ COL BOARD
O-6 CSL BOARD
Rank
Years in Service
2
4
6
8
10
12
14
16
18
20
22
24
Professional Military Education (PME)
CCC
ILE
SAMS
SSC
Functional/Additional/Combat Skills Training
EWOQC
Air Assault / Airborne / Ranger/ Pathfinder
CNODP / ACS / TWI / DoD Fellowships
JEWTOC, SFC, EWCC, JTC, JFC, STOPC, MILDEC PC, CYBER 200/300, JACWC, JCOPC, JNAC
Assignments
Positions listed are not all inclusive
Brigade Combat Team CEWO Officer
Special Operations CEWO Officer
Company Commander
BCT/Division/Corps CEWO Officer
Program Manager
Battalion XO/S3
Div/Corps/ASCC/CCMD CEWO Force Planner
NATO CEWO Officer
FORSCOM CEMA Integrator
BN Commander (CSL)
BDE DCO (post-CSL) / BN S3
Director, TCM Cyber/EW
CCMD Army Force Integrator
Corps/ASCC CEWO Div BDE Commander (CSL)
AC/RC Observer-Controller/Trainer
CTC Observer-Controller/Trainer
Cyber/CEMA Planner
Centers of Excellence CEWO Officer
ACS, TWI, DoD Fellowships
CTC Observer-Controller CEWO Lead Integrator
Cyber School Cadre
TRADOC Capabilities Developer
Career Manager (HRC)
Senior Cyber/CEMA Planner
Action/Project Officer
ACS, TWI, DoD Fellowships
DCS/SGS Assignment
Director, OCC
Cyber COE/School Assignment
Chief, Cyber Branch (HRC)
Army/ARCYBER staff
DoD Fellowships
Instructor (USMA/ROTC)
ACOM/HQDA/JIIM Assignment
Nominative Assignment
DoD Fellowships
Self Development/ Education
NET+, SEC+, CCNA, CEH, CISSP
Graduate Level Education
Post Graduate Level Education
CSA Professional Reading / Self Development Activities (Working Groups, Conferences, Seminars)
Formal training to expand tactical and technical proficiency, leadership skills and intellectual capital

Figure 10. USA Cyberspace Operations Officer Career Model. (Reprinted from Department of the Army Pamphlet 600-3, Commissioned Officer Professional Development and Career Management, Cyber Branch, 17 January 2018, 11.)



Professional Military Education (PME)	BOLC	CCC	ILE SAMS		SSC
Functional/Additional/Combat Skills Training	RIOT / NETA2108 / CYBR3800 / CPT Methodologies / COOC / CCTC / ICC / RT3T / MCC / JACWC / ACOPC / JCOPC / JNAC CNODP / ACS / TWI / DoD Fellowships Joint Courses				
Assignments *Positions listed are not all inclusive*	CMF Team Operations Officer CMF Sub-Element/Section Lead CMF Team Member (OCO/DCO) CMF Operator/Analyst Watch Officer Company XO Developer/Engineer Researcher Hardware/Software Engineer Cloud/Network Engineer	Combat Support Team Lead Cyber Defense Manager Company Commander Senior Developer Senior Hardware/Software Engineer Senior Cloud/Network Engineer	National Support Team Lead Combat Mission Team Lead Cyber Protection Team Lead BN XO/S-3 Engineering Team Lead/OIC Chief, Army/Joint Cyber Branch	National Mission Team Lead National CPT Lead BN Commander (CSL) BDE DCO (post-CSL) BDE S3 Chief, ACI/Joint Cyber Division	BDE Commander (CSL) G3, ARCYBER CoS, ARCYBER Cyber COE CoS Director, TCM Cyber/EW ACOIC Director, ARCYBER Director, ACI/Joint Cyber Directorate
		Operations Planner (BDE/DIV/ARCYBER) Instructor/Training Developer/SGL (Cyber School) TRADOC Capabilities Developer ARCYBER/ACOIC Staff Watch Officer (JOC/ROC/AROC) CMF Sub-Element/Section Lead CMF Mission Commander Researcher/Developer (ARL/ACI) Cyber Planner CNODP, ACS, TWI, DoD Fellowships	SGS Assignment Cyber School Cadre Mission Manager Integration Lead Researcher/Developer (ARL/ACI) Career Manager (HRC) Project/Action/Watch Officer Training/Exercises Officer Senior Cyber Planner ACS, TWI, DoD Fellowships	Director, OCC Operations Planner Army Staff/DCS/SGS Assignment Chief, Cyber Branch (HRC) Cyber Targeting Officer Cyber COE/School Assignment Researcher/Developer (ARL/ACI) Battle Captain PhD, NPS, AFIT Programs TWI/DoD Fellowships	Cyber School Asst. CMDT Instructor (USMA/ROTC) Silicon Valley LNO Branch Immaterial HQDA/ACOM/JTF/M Assignment Nominative Assignment DoD Fellowships
Self Development/ Education	Professional Certifications (CompTIA, EC Council , Cisco, Microsoft, , ISC², GIA, SANS, etc.) Graduate level education in STEM Discipline			PhD in STEM discipline	

Figure 11. USA Cyber and Electronic Warfare Operations Officer Career Model. (Reprinted from Department of the Army Pamphlet 600-3, Commissioned Officer Professional Development and Career Management, Cyber Branch, 17 January 2018, 12.)

This section will divide the first 20 years of an officer's career into four chronological blocks: 0-4 years, 4-10 years, 10-15 years, and 15-20 years. Though an officer's career may go beyond 20 years, this is outside the scope of this paper. Each chronological block will review the primary institutional and occupational training/education requirements followed by deliberate experience (i.e. key duty positions, employment of capabilities). A complete review of all training, education, and experimental opportunities for Army officers is outside the scope of this paper, thus this analysis will focus on the major and relatively common items.

USA Developmental Focus. Before proceeding into the chronological development model, the reader must understand some overall developmental goals and themes within the Army to include the signal and cyberspace community. The Army uses the *Army Development Model* illustrated in figure 13 to guide officer development. The goal of this model is to "create the training, education, and experience conditions that produce agile, innovative, and adaptive leaders of unimpeachable integrity, character, and competence who act to achieve decisive results and who understand and are able to exploit the full potential of current and future Army doctrine."[15]

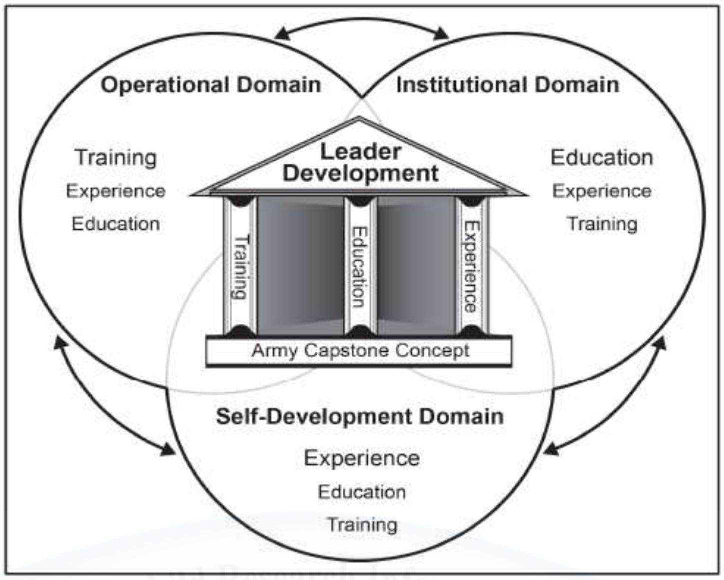


Figure 12. The Army Leader Development Model. (Reprinted from Army Doctrine Reference Publication 7-0, Training Units and Developing Leaders, 23 August 2012, 1-2.)

This thesis primarily focuses on the institutional and operational domains of the Army Leader Development model. The institutional domain focuses on the deliberate education and training courses an Army officer traverses at deliberate times in their career. The operational domain focuses on the deliberate developmental positions the Army identifies for officers to build desired experience. The Army ideally assigns officers who complete institutional training and education directly into leadership positions within the operational Army in order to apply and reinforce newly gained knowledge, skills, and abilities.

Four doctrinal publications underpin the Army Leader Development model. The extract below from Army Pamphlet DA PAM 600-3 summarizes these four publications for the reader, stating:

> Leader development is based on ADP 1 [The Army], providing the foundation for our warfighting doctrine. It articulates the constitutional

[15] "Department of the Army Pamphlet 600-3, *Officer Professional Development and Career Management*, 26 June 2017, 6.

> and legal basis for our being, the national security objectives, the spectrum of warfare and our beliefs concerning the profession of arms to include the professional Army ethic and values. ADP 3–0 [Unified Land Operations] is our keystone warfighting doctrine for subordinate and tactical-level doctrine, professional education and individual and unit training. ADP 7–0 [Training Units and Leaders] tells us how we should train, including the senior leader's role. ADP 6–22 [Army Leadership] outlines the core dimensions of leadership and the basis for leadership excellence. Together, these references provide the foundation needed to develop competent, confident leaders capable of assuming positions of greater responsibility and creating the conditions for sustained organizational success.[16]

Aside from the leadership development, the Army specifically expects its officers to be effective military planners, which includes becoming leaders and practitioners of the Military Decision-Making Process (MDMP). MDMP is very similar to Joint Operational Planning Process (JOPP) and Marine Corps Planning Process (MCPP), with utility for planning from the tactical through operational and campaign levels of warfare.

As stated, Army officer force development gives primacy to leadership, operations, and planning within the operational Army to build warfighters no matter their occupation. This section will dive deeper into examining how the Army builds its signal and cyberspace operations officers within the larger context of Army officer development over the first 20 years of a career. This study will not cover unit-specific institutional and/or occupational qualification training in its survey treatment of officer development across the Army. (Airborne School, Ranger School, specialized cyberspace or electronic warfare training, Advanced Civilian Academic Degrees, etc.)

Years 0-4 (2nd Lieutenant – 1st Lieutenant)

The Army focuses the first four years of an Army officer's career heavily on institutional and occupational training, building a foundational understanding of Army warfighting, and developing leadership experience at the tactical-level. Upon commissioning, Army officers proceed to their respective occupational field Basic Officer Leadership Course (BOLC). BOLC serves as both institutional and occupational training. The Army Combined Arms Center establishes common core tasks for each branch schoolhouse to instruct during their respective BOLC. While these are early

[16] Ibid., 7.

"learning" years for Army officers, performance in these training and leadership positions during these four years can significantly affect the following four to ten years.

Training & Education (0-4 years). The Army invests considerable time to train institutionally and occupationally its new officers not only in their primary occupational field, but in common core Army competencies. Upon commissioning, officers designated to enter the signal corps or cyber branch proceed to their respective Basic Officer Leadership Courses (BOLC). Both courses instruct the Army Combined Arms Center-generated common core tasks which include tasks such as marksmanship, land navigation, convoy operations, and small unit leadership.[17] While common core task training is similar across the two courses, the courses diverge significantly in specific occupational training.

Army officers selected to become 25A signal officers attend the Signal Basic Officer Leadership Course (BOLC) at Fort Gordon, Georgia. Signal BOLC is a 16-week course focuses on "specialized Signal skills, doctrine, tactics and techniques designed to complement Warrior Tasks and Battle Drills and enable them to lead Soldiers in the Unified Land Operational environment."[18] Signal BOLC contains five major blocks of instruction: Warrior Leader Training (Common Core Tasks) (175 hours), Warfighter Information Network – Tactical (89.95 hours), Combat Network Radio (158 hours), Mission Command Information Systems (40 hours), Information Technology (82 hours), and a Capstone event (145.05 hours).[19]

Table 12 depicts the content of Signal BOLC blocks of instruction by thematic variable. Aside from the significant concentration on common core tasks in the left side of the table, S-BOLC heavily focuses on transmissions systems (radios and SATCOM) and Army-unique applications and systems. Other than an 80-hour block on DoDIN operations, S-BOLC contains little instruction on defensive or cyberspace operations (DCO/OCO). The decision by S-BOLC course directors to not focus on DCO or OCO is

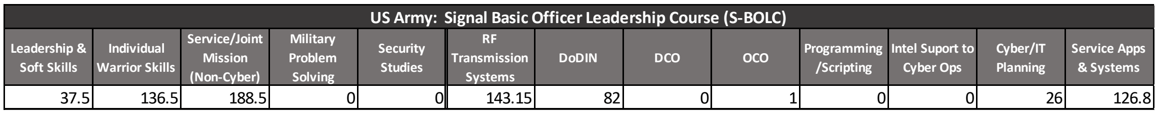
[17] James Beck, "FY15 Approved BOLC Common Core Task List" (US Army Combined Arms Center, 29 January 2016), 15.

[18] "Signal Basic Officer Leaders Course (SBOLC)," The Official Homepage of the U.S. Army Signal School, March 30, 2016, https://signal.army.mil/index.php/organizations/15th-regimental-signal-brigade/442nd-signal-battalion/25-courses/93-sbolc.

[19] John Williams, "Master Training Schedule: Signal Basic Officer Leader - Branch" (Signal School, U.S. Army Cyber Center of Excellence, 15 February 2018).

likely due to the Army expecting its young signal officers to become proficient on the configuration, operations, and maintenance of key warfighting applications, systems, and radios used by the operational Army units. Based upon the signal officer development model (Figure 9), most signal officers will not deal with DCO or OCO early in their careers.

Table 12. USA Signal Basic Officer Leadership Course Curriculum Content (hours)



US Army: Signal Basic Officer Leadership Course (S-BOLC)												
Leadership & Soft Skills	Individual Warrior Skills	Service/Joint Mission (Non-Cyber)	Military Problem Solving	Security Studies	RF Transmission Systems	DoDIN	DCO	OCO	Programming /Scripting	Intel Suport to Cyber Ops	Cyber/IT Planning	Service Apps & Systems
37.5	136.5	188.5	0	0	143.15	82	0	1	0	0	26	126.8

Source: Author's Original Work

Two additional items of note in Signal BOLC involve commercial information assurance certification and a tailored focus on cyberspace-enabled capabilities vital the Army's warfighting mission. Cyberspace operations officers receive their commercial Security+ certification during the final block of S-BOLC instruction, satisfying DoD 8570/8140 information assurance manager level I requirements. Additionally, signal officers receive significant training on the core communications capabilities supporting the operational Army's maneuver forces: Warfighter Information Network-Tactical (WIN-T), Force XXI Battle Command Brigade and Below (FBCB2) platform, and Mission Command Information Systems (MCIS).[20]

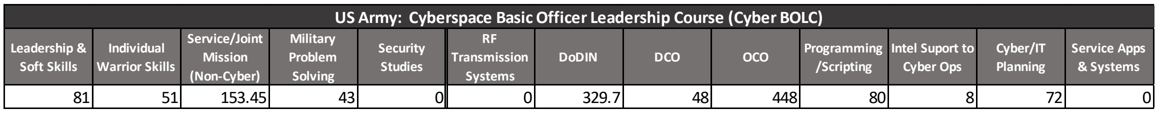
Army officers accessed as 17A signal officers attend the Cyberspace Basic Officer Leadership Course (BOLC) at Fort Gordon, Georgia. The Cyberspace BOLC is a 40-week course containing two primary instructional components: Army common core and the Cyber Operations Officers Course (COOC). The 7-week common core instruction covers the Army-mandated curriculum for all lieutenants, divided into small-unit leadership (4 weeks) and tactical operations and planning (3 weeks). The Cyber Operations Officer Course component, the majority of Cyberspace BOLC, contains six major blocks of instruction completed over a 33-week period. The blocks of instruction are Cisco Certified Network Associate (7 weeks), Certified Information Systems Security

[20] Williams, "Master Training Schedule," 7–9.

Professional (2 weeks), Programming (1 week), Army Cyberspace Operations Planners course (2 week), and Cyber Common Technical Core (9 weeks), Cyber Protection Team Methodologies, Intelligence (2 weeks), and Research (1 week). Cyberspace BOLC provides officers both Cisco Certified Network Associate (CCNA) and Certified Information Systems Security Professional (CISSP) certifications, satisfying the DoD 8570/8140 information assurance certification requirement.[21]

Table 13 depicts the content of Cyber BOLC blocks of instruction by thematic variable. From the occupational curriculum lens, Cyber BOLC curriculum emphasizes completely opposite themes than Signal BOLC; focusing on cyberspace operations (OCO/DCO/DoDIN) over transmission systems and service applications. Granted Cyber BOLC is three times as long as S-BOLC (40 versus 16 weeks), however Cyber BOLC does not include any curriculum on transmission systems or core service-unique applications and systems.[22] This difference in focus likely on commercially-provided and joint-provided instructors and curriculum for certain blocks of instruction, but also by the fact that the Army established this cyberspace career field to specifically specialize in offensive and defensive cyberspace operations vice providing traditional Army communications capabilities.

Table 13. USA Cyber Basic Officer Leadership Course Curriculum Content (hours)



US Army: Cyberspace Basic Officer Leadership Course (Cyber BOLC)												
Leadership & Soft Skills	Individual Warrior Skills	Service/Joint Mission (Non-Cyber)	Military Problem Solving	Security Studies	RF Transmission Systems	DoDIN	DCO	OCO	Programming /Scripting	Intel Suport to Cyber Ops	Cyber/IT Planning	Service Apps & Systems
81	51	153.45	43	0	0	329.7	48	448	80	8	72	0

Source: Author's Original Work

Key Duties/Experience (0-4 years). Upon completion of their respective Basic Officer Leadership Courses, Army lieutenants typically proceed to their first duty assignment. Signal officers proceed to their first duty assignment. Cyberspace officers proceed to their first duty assignment, although some continue to further advanced cyberspace training, depending the unit to which they will be assigned.

[21] "Cyber Technical College" (Cyber School, U.S. Army Cyber Center, 15 September 2016).
[22] "US Army Cyber Basic Officer Leadership Course B Weekly Training Schedule," 15 July 2016.

The first key developmental position for commissioned officers (excluding Chaplains, Judge Advocate Generals, and Medical/Veterinary services) within the Army is as a Platoon Leader, ideally within the operational Army.   Within the first 36 months of service post-training, the Army developmental aim is for its Lieutenants to serve at least one year as Platoon Leader. This includes signal officers; however, key developmental duties for signal officer may also include Commander of a Special Forces Group Signal Detachment, Direct Signal Support Team OIC, or Company Executive Officer/Operations Officer.[23] The Army values these leadership positions as they provide tactical leadership experience for their junior officers. Platoon Leadership within the operational Army provides the additional bonus by providing the Army lieutenant the opportunity to execute their occupational specialty within the primary Army warfighting construct. As a result, they develop a foundational understanding of how and why the Army operates and how their specific occupation integrates with the whole.

Platoon leader positions are not always available for every signal lieutenant when they first arrive at their first duty station. Thus, the gaining units assign these lieutenants to other duties such as Assistant Platoon Leader or Assistant Battalion S6. These other duties afford the signal lieutenants opportunities to further hone understanding and skill with their primary occupational field as well as further develop their institutional competencies such as Army warfighting and planning.

Cyberspace operations lieutenants may complete their 12 months of key developmental duty in a variety of positions. Cyberspace operations lieutenants do not have the opportunity for platoon leadership, but instead primarily complete key developmental duty in the many cyber mission force positions. Some of these positions are leadership positions, but many are team member positions in which the lieutenant is directly executing cyberspace missions "on keyboard."[24] Department of the Army Pamphlet 600-3 (Cyber) contains a full list of key developmental positions for 17A lieutenants.

[23] Department of the Army Pamphlet 600-3, *Commissioned Officer Professional Development and Career Management, Signal Corps Branch*, 3.

[24] Department of the Army Pamphlet 600-3, *Commissioned Officer Professional Development and Career Management, Cyber Branch*, 4.

As illustrated in this section, the goal of Army officer development within the first four years of service focuses on tactical and leadership expertise, understanding Army and/or cyberspace operations, and occupational proficiency. Signal lieutenants follow a more traditional “Army” path, leading platoons and serving on operational unit staffs. A signal lieutenant’s ability to dual-hat as Battalion S6’s and experience non-platoon leader duties within these first years provides direct exposure and experience to Army planning processes, multi-domain operations, and associated joint warfighting function integration. Cyberspace operations lieutenants, on the other hand, have significantly more training than signal officers and spend much of their first four years more heavily focused on occupational (technical) skill development within ARCYBER either in a service-retained unit or in the Army’s Cyber, or National Mission Force teams. These cyberspace operations lieutenants build more experience with joint and cyber-specific planning and operational processes.

Years 4-10 (Captain)

At the end of these first four years of service, the Army starts looking to provide developmental breadth while still reinforcing core warfighting concepts. Years 4-10 of an Army officers’ career will typically involve at least two duty assignments and may include an multi-month PME opportunity. These six years focus on higher levels of leadership (company command), expansion of the officer’s breadth of experience in an institutional Army organization, and PME called the *Captain’s Career Course*. Opportunities also exist for work on higher echelon staffs within the Operating Force (Brigade, Division, and Corps G-6).

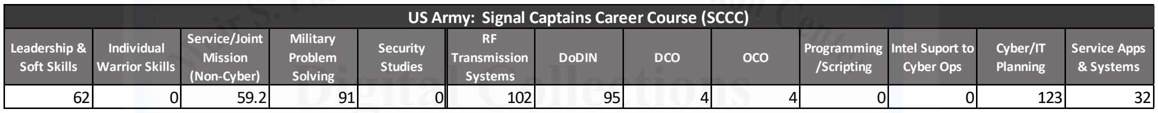
Training & Education (4-10 years). During this part of a career, Army captains complete a multi-month long professional military education (PME) resident (or distance education) program that incorporates common core tasks developed by the Army Combined Arms Center and occupational field specific training. The Captains Career Courses are branch specific, thus signal officers attend the Signal Captains Career Course (SCCC) and cyberspace operations officers attend the Cyberspace Captains Career Course (CyCCC).

The Signal Captains Career Course (SCCC) is a 20-week in-resident course at Fort Gordon, Georgia. The course begins with a block of mid-grade common core tasks

(360 hours) followed by signal corps-specific training. The signal blocks of instruction include: Introduction to Signal Operations (40 hours), Cyberspace Electromagnetic Activities (32 hours), Network Essentials (76 hours), Lower Tactical Internet (88 hours), Upper Tactical Internet (96 hours), and Mission Command Information Systems (48 hours), Professional Development (20 hours), and a Capstone event (40 hours).[25]

Table 14 depicts the content of Signal CCC blocks of instruction by thematic variable. From an institutional lens, this course is the first formal course where Army signal officers gain exposure to the military decision-making process (MDMP). This course also continues the trend established in Signal BOLC focusing on RF transmission systems and Army applications and systems. However, the course does introduce more focus on defensive and offensive cyber operations, as well as continues a considerable focus on DoDIN operations.

Table 14. USA Signal Captains Career Course Curriculum Content (hours)



US Army: Signal Captains Career Course (SCCC)												
Leadership & Soft Skills	Individual Warrior Skills	Service/Joint Mission (Non-Cyber)	Military Problem Solving	Security Studies	RF Transmission Systems	DoDIN	DCO	OCO	Programming /Scripting	Intel Suport to Cyber Ops	Cyber/IT Planning	Service Apps & Systems
62	0	59.2	91	0	102	95	4	4	0	0	123	32

Source: Author's Original Work

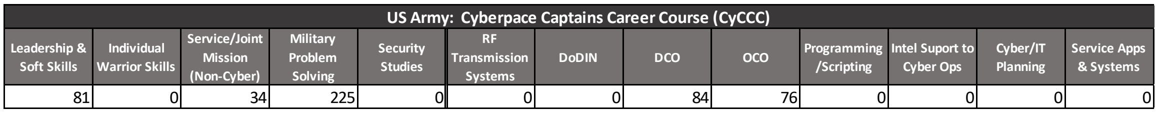
The Cyberspace Captains Career Course (CyCCC) is a 25-week in-resident course at Fort Gordon, Georgia focusing on the Army's mid-grade common core tasks and cyberspace occupational-specific training and education. The core instructional blocks of CyCCC are Common Core (2 weeks), Tactics and Troop Leading Procedures (5 weeks), Operations and the Military Decision-Making Process (6 weeks), Cyber Operations Technical (4 weeks), Research Project (2 weeks), and a Culminating Exercise (3 weeks). During CyCCC, the officers complete two commercial certifications that align with DoD 8570/8140 information assurance requirements: GCIA Certified Intrusion Analysis (GCIA) and GIAC Penetration Tester (GPEN).[26]

[25] Pete Jones, "Master Training Schedule: Signal Captains Career Course" (442nd Signal Battalion, U.S. Army Signal Center, 5 February 2018).

[26] "Cyber Technical College," 8.

Table 15 depicts the content of Cyber CCC blocks of instruction by thematic variable. This course continues the trend established in Cyber BOLC focusing on offensive and defensive cyberspace operations. Interestingly, Cyber CCC also includes a heavy focus on military decision-making process (MDMP), dedicating almost two and half times to the topic as the Signal Captains Career Course.[27] The difference may merely lie in the fact that CyCCC is five weeks longer than SCCC, providing more time to focus on MDMP.

Table 15. USA Cyberspace Captains Career Course Curriculum Content (hours)



US Army: Cyberpace Captains Career Course (CyCCC)												
Leadership & Soft Skills	Individual Warrior Skills	Service/Joint Mission (Non-Cyber)	Military Problem Solving	Security Studies	RF Transmission Systems	DoDIN	DCO	OCO	Programming /Scripting	Intel Suport to Cyber Ops	Cyber/IT Planning	Service Apps & Systems
81	0	34	225	0	0	0	84	76	0	0	0	0

Source: Author's Original Work

Key Duties/Experience (4-10 years). Besides the captain-level PME and occupational training, the Army aims to provide key developmental duties to its officers. The key developmental experience during the 4-10-year career point is to serve as a company commander. The Army values company command as it provides the next-higher tactical leadership experience above the platoon level and is the first opportunity Army Officers are given UCMJ authority over their subordinates.

Signal officers largely mirror the Army in development experience during the 4-10-year career block. To remain competitive for future advancement, Army signal captains must successfully complete signal company command or battalion S6 duty (ideally in a combat arms battalion). While awaiting a key developmental duty position to become available or after completion of key duty, signal captains may hold a variety of other positions to include serving on a Brigade, Division, or Corps staff.[28]

Cyberspace operations and CEWO captains may complete their 24 months of key developmental duty in a variety of positions. Cyberspace operations (17A) and CEWO (17B) officers can complete key developmental duty in company command similar to the

[27] Derrick J. Smith, "Cyber CCC Course Map" (U.S. Army Cyber School, Cyber Center of Excellence, 26 January 2018).

[28] "Department of the Army Pamphlet 600-3, *Commissioned Officer Professional Development and Career Management, Signal Corps Branch*, 3.

other Army branches. However, the Army has very few of these positions within cyberspace organizations forcing the cyber branch to identify other equivalent key developmental positions. Cyberspace operations officers complete key developmental duty as Cyber Support Team Lead, Cyber Defense Manager, and several other development and engineering positions. CEWO officer unique key developmental duty positions include Brigade Combat Team CEWO officer and Special Operations CEWO officer.[29] Department of the Army Pamphlet 600-3 (Cyber) contains a full list of key developmental positions for 17A and 17B captains.

Years 10-15 (Major – Lieutenant Colonel)

After reaching the 10-year mark in their careers, the Army promotes most of its officers to the field grade ranks. Like its sister service counterparts, Army field grade officers (FGOs) begin to focus on higher levels of leadership (and larger organizations), furthering broadening experience at the headquarters staff level or in the joint realm. Additionally, Army officers complete another level of Professional Military Education, the intermediate level education, while also satisfying the requirements for JPME Level I.

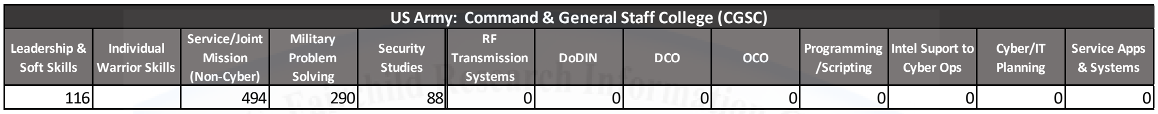
Training & Education (10-15 years). The Army requires no formal occupational training for its signal or cyberspace operations officers during the 10-15-year timeframe of their career. However, Army Professional Military Education expectations applicable to signal and cyberspace operations officers focus on completing intermediate-level education, either in residence or by distance education. Most of the Army officers (of all specialties) competitively selected for in-residence developmental education attend the Army Command and Staff Course in Fort Leavenworth, Kansas. However, a smaller percentage of officers could attend fellowships, sister-service schools, or international programs of equivalent developmental education.

Army Command and General Staff College (CGSC) fulfills Joint Professional Military Education I (JPME I) requirements and awards an accredited Masters of Military Art and Science for those students desiring to complete a Master's thesis during the

[29] "Department of the Army Pamphlet 600-3 Commissioned Officer Professional Development and Career Management: Cyber Branch," 5.

program.[30] Army CGSC "educates, trains and develops leaders for Unified Land Operations in a Joint, Interagency, Intergovernmental, and Multinational operational environment; and advances the art and science of the profession of arms in support of Army operational requirements."[31] CGSC's major blocks of instruction include Foundations, Strategic Context of Operational Art, Unified Action, Army Doctrine and Planning, CFLCC Planning, Decisive Action Division Operations, Decisive Action Brigade Operations, Ethics, Leadership, History, and Managing Army Change, and 192 hours of electives.[32] Table 16 depicts the content of CGSC blocks of instruction by thematic variable. Of note, CGSC curriculum heavily focuses on Army core missions, joint warfighting functions, and military problem solving.[33]

Table 16. USA Command and General Staff College Curriculum Content (hours)



US Army: Command & General Staff College (CGSC)												
Leadership & Soft Skills	Individual Warrior Skills	Service/Joint Mission (Non-Cyber)	Military Problem Solving	Security Studies	RF Transmission Systems	DoDIN	DCO	OCO	Programming /Scripting	Intel Suport to Cyber Ops	Cyber/IT Planning	Service Apps & Systems
116		494	290	88	0	0	0	0	0	0	0	0

Source: Author's Original Work

Key Duties/Experience (10-15 years). Experientially, during the 10-15-year period of a career, the key duties Army officers complete are serving as a battalion/brigade *executive officer* (XO) or *operations officer* (S-3). Individual occupational communities may also identify other key duty positions at different echelons or other organizations as identified by the occupational field's leaders. The signal corps aligns similarly with the overall Army key developmental model. However, the cyberspace branch may need to introduce alternate and equivalent key duty positions due to extra-service mandated organizing principles such as the CMF team constructs.

The Battalion Executive Officer (XO) is the second in command behind only in the Battalion Commander. They must be prepared to assume battalion command, if

[30] "CGSC Circular 350-1: U.S. Army Command and General Staff College Catalog" (U.S. Army Command and General Staff College, January 2016), 3–1.
[31] "CGSC Circular 350-1: U.S. Army Command and General Staff College Catalog," 1–2.
[32] "CGSC Circular 350-1: U.S. Army Command and General Staff College Catalog," 7–3.
[33] "AY2014-02 and CGSOC Class 2015 Combined Strawman" (U.S. Army Command and General Staff College, November 21, 2014); "U.S. Army Command and General Staff College Curriculum Class 2015," August 2014.

required; however, their primary day-to-day duty focuses on leading the Battalion's staff functions (S1-S6) in the planning and execution of the battalion commander orders and intent. Closely aligned with the XO, the battalion operations officer position (S-3) focuses on managing the execution of current and future operations, to include in-garrison training. Neither the XO or S3 position is a command position, however the positions require formal and informal leadership and synchronization across different staff functional areas as well as working with subordinate company commanders who work for the Battalion Commander and execute battalion orders. They must also become experts not only of the Military Decision-Making Process (MDMP), but of leading planning teams. They are responsible for leading the staff to translate higher headquarters operational orders and commander's vision/intent into operational orders for the battalion commander to provide for execution by subordinate echelons.

The primary key developmental duties for signal officers are completing 24 months as a Battalion/Brigade Executive Officer or Operations Officer like the other Army branches. However, the signal corps also recognizes several other key developmental duties to include brigade or equivalent S6, Division deputy G6, Division/Theater Sustainment Command Network Operations Officer, or Company Command if the member has yet to complete one.[34] When not holding one of the key developmental positions and like previous chronological career blocks, Army signal officer serve in various other staff elements. As Field Grade Officers, staff duty may include everything from serving in a Department of the Army or Army Command staff positions, to serving in a joint organization to satisfy the 36-month duty requirement to become a joint qualified officer in accordance with the Goldwater-Nichols Act.

Cyberspace operations and CEWO majors may complete their 24 months of key developmental duty during this block in a myriad of positions. Cyberspace operations (17A) officers can complete key developmental duty in the standard Battalion/Brigade Executive Officer or Operations Officer positions like the other Army branches. However, the Army has very few of these positions within cyberspace organizations so the cyber branch adds other key duties such as national support team lead, cyber mission

[34] Department of the Army Pamphlet 600-3, *Commissioned Officer Professional Development and Career Management, Signal Corps Branch*, 4.

team lead, cyber protection team lead, or two identified duty positions on USCYBERCOM staff. For 17B CEWO officers, unique key developmental duty positions include Brigade/Division/Corps CEWO officer and Program Manager.[35] Department of the Army Pamphlet 600-3 (Cyber) contains a full list of key developmental positions for 17A and 17B majors.

Years 15-20 (Lieutenant Colonel – Colonel)

Around the 15-year mark in their careers, Army officers compete for the rank of lieutenant colonel. Like its sister service counterparts, field grade officers in this period of their career continue to focus on higher levels of leadership (and larger organizations), furthering broadening experience at the headquarters staff level or in the joint realm. Additionally, Army officers complete another level of professional military education (resident or correspondence), with this intermediate level education satisfying the requirements for Joint Professional Military Education Level II.

Training & Education (15-20 years). The Army requires no formal occupational training for its signal or cyberspace operations officers at the 15-20-year points of their career. However, Army Professional Military Education expectations applicable to signal and cyberspace operations officers focus on completing Senior Developmental Education (SDE) either in residence or by distance education. Most of those Army officers (of all specialties) competitively selected for in-residence SDE attend the Army War College in Carlisle Barracks, Pennsylvania. However, a percentage of officers can attend fellowships or attend sister-service or international equivalent senior developmental education opportunities. From the residence developmental education opportunity or via distance learning, Army officers complete Joint Professional Military Education II (JMPE II) requirements, satisfying all necessary educational requirements required for Joint Qualified Officer categorization.

Key Duties/Experience (15-20 years). Experientially, during the 15-20-year period of a career, the Army force development models focuses on completing two requirements: 24 months of battalion command and 24-36 months joint duty. Battalion command is the foundational O-5 command opportunity afforded deserving Lieutenant

[35] Department of the Army Pamphlet 600-3, *Commissioned Officer Professional Development and Career Management, Cyber Branch*, 7.

Colonels. The battalion commander, informed by his/her staff, must be able to take higher echelon orders and direction through leadership and operational art and science. When not operationally deployed, battalion commanders focus on the administration and operational training of the battalion and ensuring subordinate companies/Soldiers have the equipment required to execute their mission.

The primary key developmental duties for signal officers during the 15-20-year career block are completing 24 months as a Battalion Commander like the other Army branches. However, the signal corps also recognizes several other key developmental duties. These duties include garrison (installation) command, Division/JTF G6/J6, Theater Sustainment Command G6, or an out-of-branch command such as headquarters or recruiting battalion.[36] Department of the Army Pamphlet 600-3 (Signal) contains a full list of key developmental positions for 25A officers.

The primary key developmental duties for cyberspace operations and CEWO lieutenant colonels during the 15-20-year career block are completing 24 months as a battalion commander similar to the other Army branches. However, the cyber corps also recognizes numerous other key developmental duties. For 17A cyberspace operations lieutenant colonels these positions include National Mission Team or National Cyber Protection Team Lead, Brigade Deputy Commanding Officer (post battalion command), and Brigade Operations Officer. For 17B cyberspace and electronic warfare operations (CEWO) officers, unique key developmental duty positions include Division/Corps or equivalent CEWO Force Planner, NATO CEWO Officer and Army FORSCOM CEMA Integrator.[37] Department of the Army Pamphlet 600-3 (Cyber) contains a full list of key developmental positions for 17A and 17B lieutenant colonels.

When not holding one of the key developmental positions, Army signal and cyberspace operations officers serve in various other staff elements such as Department of the Army or Army Commands. Army officers who have yet to complete their 24-36 months joint duty will complete this requirement during the 15-20-year career block.

[36] “Department of the Army Pamphlet 600-3, *Commissioned Officer Professional Development and Career Management, Signal Corps Branch*, 5.
[37] “Department of the Army Pamphlet 600-3 *Commissioned Officer Professional Development and Career Management, Cyber Branch*, 8.

Toward the end of this 15-20-year period, Army officers have their first opportunity to compete for promotion to Colonel (O-6).

Chapter Summary

The purpose of this chapter was to provide the reader a foundational understanding of how the Army develops its signal and cyberspace operations officers within the larger context of Army officer development and DoD/joint officer requirements. Primarily, the Army views itself and its soldiers as warfighters, prioritizing tactical and operational leadership experience within the operating Army. This understanding serves as a foundation to understanding why the Army emphasizes its doctrine and warfighting skills focused on unified land operations in all levels of institutional and occupational training and education.

The Army uses two different classifications of active duty officer within its signal and cyberspace occupational fields to ensure sufficient expertise to have officers on command/leadership tracks (commissioned officers) and officers who focus upon becoming technical subject matter experts (Warrant Officers). The commissioned officers, the focus of this chapter, developmentally alternate between leadership and staff assignments in the operational Army and gain breadth in institutional Army organizations and joint duty.

Signal officer key duty positions and experience through the 20-year point of the career largely mirror the combat arms branches: platoon leader, company commander, battalion/brigade executive officer and/or operations officer, and battalion commander. However, the signal corps does recognize other key developmental signal positions across the Army.

Cyberspace operations (17A) and cyberspace and electronic warfare operations officers (17B) mirror some of the larger Army and signal corps key developmental positions. However, due to heavy focus of these officers in organizations driven by extra-service organizational constructs such as the cyber mission forces, the cyber branch identifies other key development duties on cyber mission force teams and even on US Cyber Command staff. One key difference is that signal officers lead soldiers as lieutenants while many cyber operations lieutenants serve in positions where they are the soldiers tactically executing cyberspace missions and effects.

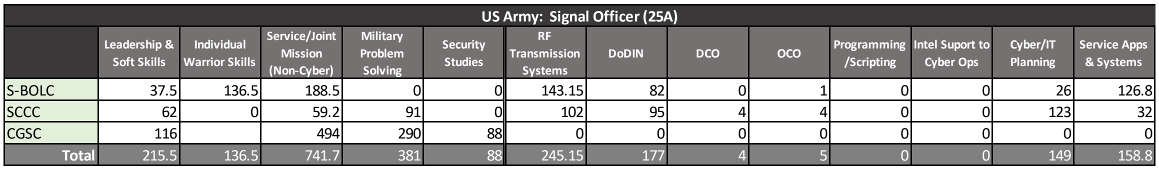
The Army deliberately ensures its signal and cyberspace operations branch officers meet all extra-service requirements. The Army provides commercial certifications during formal training (BOLC and Captains Career Courses) to satisfy the DoD 8570/8140 information assurance certification requirements. Furthermore, the Army deliberately ensure its deserving officers are eligible to compete for general officer by mandating JPME and assigning officers to joint duty experience in alignment with the Goldwater Nichols Act.

The Army expects its officers, regardless of occupational field, to understand and contribute to Army operations and planning processes in the execution of unified land operations. They, have a working knowledge and experience of individual warrior skills and military problem-solving methodologies such as MDMP and JOPP. This skill is evident in that the Army emphasizes and reinforces these competencies during its institutional and occupational training and education.

Signal officers typically receive 247.7 hours of in-resident Army warfighting competencies and 91 hours of military problem solving during their Basic Officer Leadership and Captains Career Courses. For those signal officers competitively selected for resident CGSC, the educational hours increase to 741.7 hours Army unified land and joint warfighting and 381 hours of military problem-solving education alone. Cyberspace officers receive a minimum of 187.45 hours of in-resident Army warfighting competencies and 268 hours of military problem solving during their Basic Officer Leadership and Captains Career Courses. For those officers competitively selected for CGSC, the educational hours increase to 681.45 hours Army unified land and joint warfighting and 558 hours of military problem-solving education alone. Tables 17 and 18 provide the summary of thematic content from formal training and education courses a notional USAF signal and cyberspace operations officer experiences through their 20th year of commissioned service.

The heavy training and educational focus on Army and joint core missions/competencies and military problem solving is not solely an academic exercise. The Army expects the officers to use this knowledge and planning methodologies immediately and frequently within their assigned duty organizations to maximize combat effects. This allows Army officers not only to have an academic understanding, but to build true skillsets that will carry through their career. With this foundational understanding of Army cyberspace officer development, the next chapter will examine the US Marine Corps communication and cyberspace officer force development models.

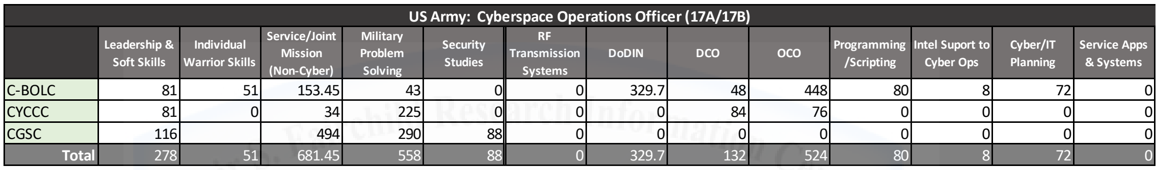
Table 17. USA Signal Officer Career Education/Training (hours)



US Army: Signal Officer (25A)													
	Leadership & Soft Skills	Individual Warrior Skills	Service/Joint Mission (Non-Cyber)	Military Problem Solving	Security Studies	RF Transmission Systems	DoDIN	DCO	OCO	Programming /Scripting	Intel Suport to Cyber Ops	Cyber/IT Planning	Service Apps & Systems
S-BOLC	37.5	136.5	188.5	0	0	143.15	82	0	1	0	0	26	126.8
SCCC	62	0	59.2	91	0	102	95	4	4	0	0	123	32
CGSC	116		494	290	88	0	0	0	0	0	0	0	0
Total	215.5	136.5	741.7	381	88	245.15	177	4	5	0	0	149	158.8

Source: Author's Original Work

Table 18. USA Cyberspace Officer Career Education/Training (hours)



US Army: Cyberspace Operations Officer (17A/17B)													
	Leadership & Soft Skills	Individual Warrior Skills	Service/Joint Mission (Non-Cyber)	Military Problem Solving	Security Studies	RF Transmission Systems	DoDIN	DCO	OCO	Programming /Scripting	Intel Suport to Cyber Ops	Cyber/IT Planning	Service Apps & Systems
C-BOLC	81	51	153.45	43	0	0	329.7	48	448	80	8	72	0
CYCCC	81	0	34	225	0	0	0	84	76	0	0	0	0
CGSC	116		494	290	88	0	0	0	0	0	0	0	0
Total	278	51	681.45	558	88	0	329.7	132	524	80	8	72	0

Source: Author's Original Work

US Marine Corps Communications & Cyberspace Officer Development

This chapter will examine United States Marine Corps (USMC) officer force development and specific nuances for the Marines two cyberspace-related officer occupational fields: communications officers and the newly-established cyberspace officer. The chapter will first provide an overview of the USMC organization and service mission to provide context to how and why the USMC develops their officers in the manner it does. The chapter will then focus on USMC officer development followed by an examination of the specific nuances of this development model for USMC communications and cyber officers. At the end of this chapter, the reader will have a foundational understanding of how the USMC develops its communications and cyberspace officers to satisfy extra-service and internal USMC developmental priorities, allowing comparative analysis against the USA and USAF in Chapter 6.

USMC Organization

This section will provide service-related context including the USMC mission, organization, and overview of occupational specialty framework. This discussion gives the reader a working understanding of the Corps as the chapter progresses into a detailed analysis of the USMC officer development model. The contextual overview will not be a full “USMC 101” but will hit major points relevant to the rest of the chapter and thesis.

It is important to understand the USMC mission and how it organizes itself as this directly relates to the focus, roles, and units to which the Corps assigns its officers. The mission of the United States Marine Corps is to “win our nation’s battles swiftly and aggressively in times of crisis. We [Marine Corps] fight on land, sea, and air, as well as provide forces and detachments to naval ships and ground operations.[1] The USMC is inherently a multi-domain focused military service as it organizes, trains, and equips organic air, land, sea (and growing space and cyber) as an integrated whole to execute its warfighting mission.

USMC Service Organizational Construct. The USMC divides its active duty force and units into two large functional bins: the Operating Forces and the Supporting Establishment. The Operating Forces are the Marines and associated units that execute

[1] “Who We Are: Our Purpose,” Marines, 2018, https://www.marines.com/who-we-are/our-purpose.html.

the operational/warfighting mission of the USMC. Operating Force units include: Marine Air Ground Task Forces (MAGTF), Service Component Commands, Chemical/Biological Incident Response Force (CBIRF), Marine Corps Security Force Regiment, Marine Corps Embassy Security Group, HMX-1 Presidential (Helicopter) Support Squadron, Marine Special Operations Command (MARSOC), and Marine Forces Cyber Command (MARFORCYBER). The standing operating force organizations train and deploy together, and typically deploy from the same MEF. For example, a standing brigade will deploy as a Marine Expeditionary Brigade. The Supporting Establishment includes Marines and organizations that enable the Operating Force. Supporting Establishment organizations include: Headquarters USMC (HQMC); Recruiting, Educating, Training, and Equipping units; and those entities responsible for sustaining the various USMC bases and stations.[2] The common Marine parlance for positions within the Supporting Force is "B-billet."[3]

The Marine Air Ground Task Force (MAGTF) is the primary warfighting construct that the Marine Corps designs itself around. Figure 13 illustrates the types of MAGTFs. The Corps tailors MAGTFs for a given operational or mission requirement; however, the USMC does have standing organizations such as I, II, and III Marine Expeditionary Force (MEF). Each type of MAGTF may have a Command Element (MAGTF leadership), Ground Combat Element, Aviation Combat Element, and Logistics Combat Element. Each of these elements will consist of actual USMC units.[4]

[2] "United States Marine Corps: America's Expeditionary Force in Readiness," Headquarters United States Marine Corps, 21 April 2015, 2, http://www.hqmc.marines.mil/Portals/61/Docs/20150420_SIG_USMC%20101Brief_FINAL.pdf.

[3] Patrick Skehan (0600 and 1700 Captain Monitor, United States Marine Corps), interview by the author, 28 February 2018.

[4] "Types of MAGTFs," U.S. Marine Corps Concepts & Programs, 23 January 2015, https://marinecorpsconceptsandprograms.com/organizations/marine-air-ground-task-force/types-magtfs; "United States Marine Corps: America's Expeditionary Force in Readiness."

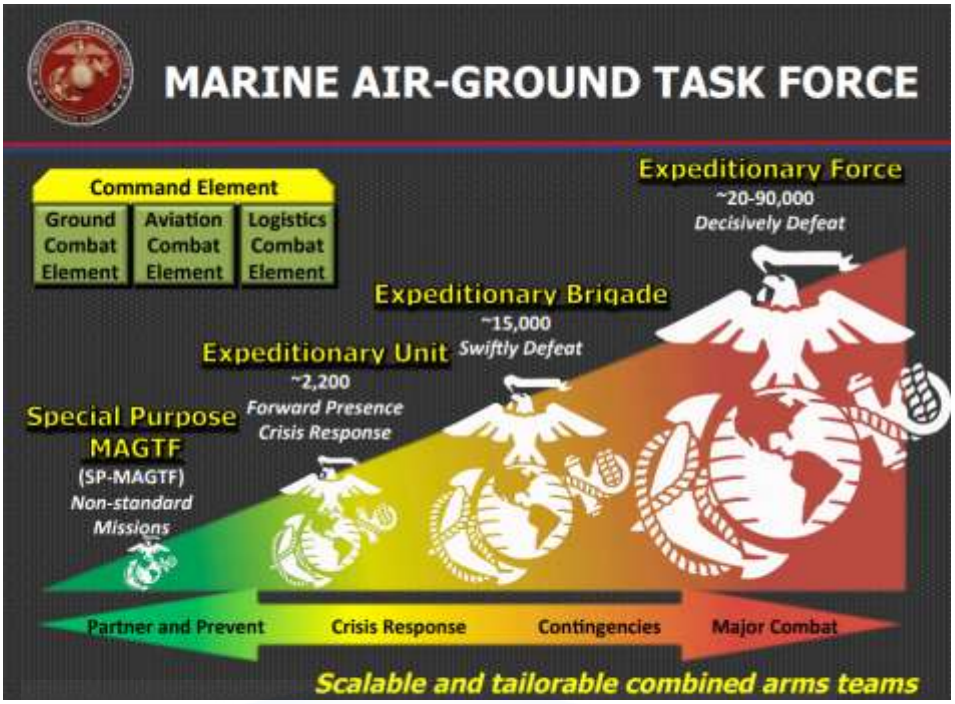


Figure 13. The Marine Air-Ground Task Force. (Reprinted from "Types of MAGTFs," U.S. Marine Corps Concepts & Programs, 23 January 23 2015, https://marinecorpsconceptsandprograms.com/organizations/marine-air-ground-task-force/types-magtfs; "United States Marine Corps: America's Expeditionary Force in Readiness.")

USMC units generally follow the standard US land component organizational model in both its Operating Forces and Supporting Establishment. In increasing size order, the Corps organizes its units into platoons, companies (3-4 platoons), battalions/squadrons (3-5 companies), regiments (for infantry and armor), brigades, divisions, and MEF (a la "Corps"). At each echelon from battalion and higher, the unit has a staff that aligns with the J-staff construct. Marine officers hold positions at any echelon within this organizational construct dependent upon their grade, experience, and military occupational specialty. USMC communications and cyberspace officers fill various roles within these operating forces and supporting establishment.[5]

USMC Communications Organizational Constructs. Understanding the specific roles of Marine communications and cyberspace officers requires a more detailed

[5] Karl W. Schlegel (Communications Officer, United States Marine Corps), interview by the author, 13 November 2017.

examination of how the USMC organizes these units and personnel. Marine Corps communications and cyberspace officers may hold positions across all echelons and organizations within the Operating Forces and Supporting Establishment. USMC communications officers may command communications units, serve in S/G-6 positions on staffs, or serve in roles on National and Cyber Mission Forces like their sister services.[6]

To further clarify the types of roles a communication or cyberspace officer within the USMC may hold, we will examine the actual types of communications units/echelons within the MAGTF construct, followed by an examination of MARFORCYBER. The primary role of USMC communications units within the MAGTF and the majority of other Operating Forces is to provide expeditionary communications capabilities to the MAGTF over the range of military operations in peace and war. When not on operational missions, these communications echelons train and prepare with their supported MEF echelon.

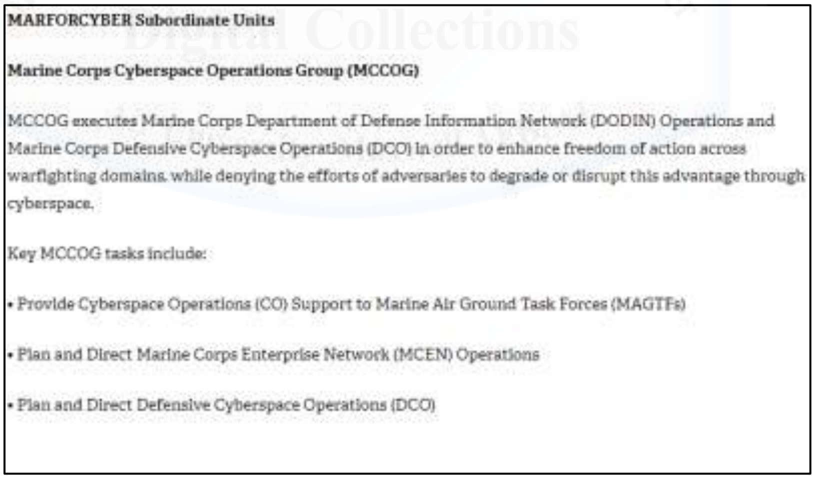
The USMC currently has six O-5 level commands within the MAGTF: three *Communications Battalions* and three *Communications Squadrons*. Each of the three Communications Battalions falls under the MEF Information Group (MIG) which reports directly to the MEF command element. The *Marine Wing Communications Squadrons* is the designation for the communications units under the Marine Air Control Group assigned to each of the three Marine Air Wings (MAW). These units provide expeditionary communications for the Aviation Combat Element to include its Marine Air Command and Control System. Each Battalion/Squadron contains *Communications Companies* (O-3-level command) and subordinate *Communications Platoons (O-2)*.[7]

Outside of the dedicated communications battalion or squadron, each other type of Marine battalion (i.e. infantry, logistics, etc.) also rates an O-2 led *Communications Platoon* that reports directly to the Battalion command element. In these instances, the Communications Platoon Commander wears a dual-hat as the Battalion Communications Officer (S-6). Outside of the MAGTF/MEF organizations, Marine Communications

[6] Skehan, interview.
[7] Ibid.

Officers may also fulfill similar roles in non-MAGTF/MEF operating forces, especially MARFORCYBER.

USMC Cyberspace Organizational Constructs. Marine Forces Cyber Command (MARFORCYBER) serves as the USMC's organization responsible for Marine Corps Department of Defense Information Network (DoDIN) operations (enterprise-level), defensive cyberspace operations (DCO), and offensive cyberspace operations (OCO) in support of both the USMC and as a force provider to USCYBERCOM. MARFORCYBER is comprised of a command element and two subordinate groups: the Marine Corps Cyber Operations Group (MCCOG) and the Marine Corps Cyberspace Warfare Group (MCCYWG). The MCCOG primarily focuses on Marine Corps (service) enterprise network operations and associated defensive cyberspace operations. The MCCYWG is the USMC's force provider to USCYBERCOM.[8] Figures 15 and 16 below present excerpts from the *Marine Corps Concepts and Programs* website provides more specifics on these two groups.



MARFORCYBER Subordinate Units

Marine Corps Cyberspace Operations Group (MCCOG)

MCCOG 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.

Key MCCOG tasks include:

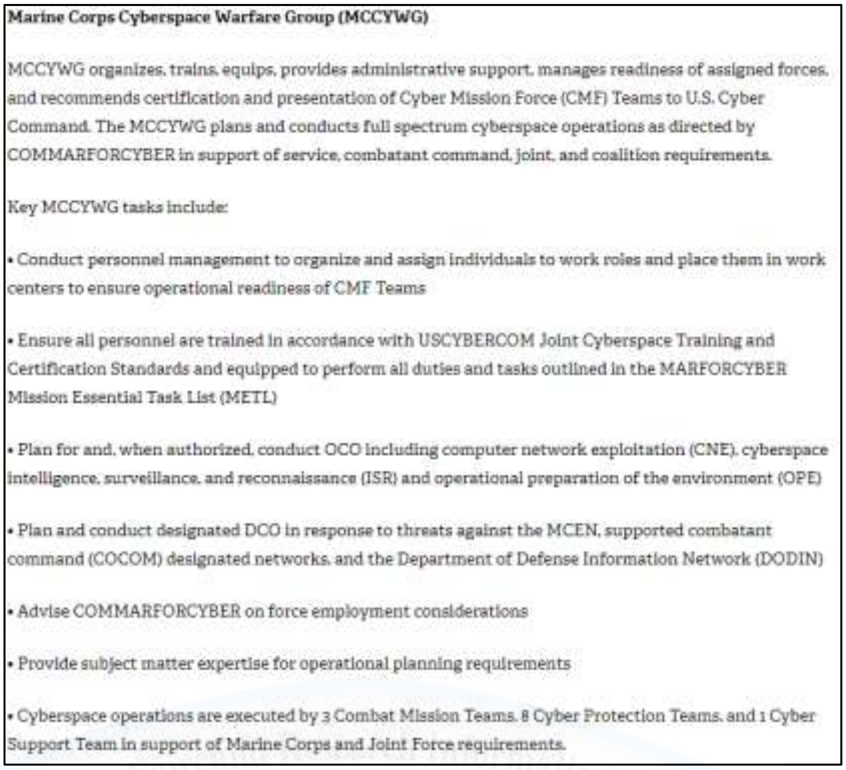
- Provide Cyberspace Operations (CO) Support to Marine Air Ground Task Forces (MAGTFs)

- Plan and Direct Marine Corps Enterprise Network (MCEN) Operations

- Plan and Direct Defensive Cyberspace Operations (DCO)

Figure 34. USMC Cyberspace Operations Group (MCOOG) Description. (Reprinted from "U.S. Marine Corps Forces, Cyberspace Command [MARFORCYBER]," U.S. Marine Corps Concepts & Programs, 12 February 2018, https://marinecorpsconceptsandprograms.com/organizations/operating-forces/us-marine-corps-forces-cyberspace-command-marforcyber.)

[8] "U.S. Marine Corps Forces, Cyberspace Command (MARFORCYBER)," U.S. Marine Corps Concepts & Programs, 12 February 2018, https://marinecorpsconceptsandprograms.com/organizations/operating-forces/us-marine-corps-forces-cyberspace-command-marforcyber.



Marine Corps Cyberspace Warfare Group (MCCYWG)

MCCYWG 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.

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 (METL)
- Plan for and, when authorized, conduct OCO including computer network exploitation (CNE), cyberspace intelligence, surveillance, and reconnaissance (ISR) and operational preparation of the environment (OPE)
- Plan and conduct designated DCO in response to threats against the MCEN, supported combatant command (COCOM) designated networks, and the Department of Defense Information Network (DODIN)
- Advise COMMARFORCYBER on force employment considerations
- Provide subject matter expertise for operational planning requirements
- Cyberspace operations are executed by 3 Combat Mission Teams, 8 Cyber Protection Teams, and 1 Cyber Support Team in support of Marine Corps and Joint Force requirements.

Figure 15. USMC Cyberspace Warfare Group (MCCYWG) Descriptions. (Reprinted from "U.S. Marine Corps Forces, Cyberspace Command [MARFORCYBER]," U.S. Marine Corps Concepts & Programs, 12 February 2018, https://marinecorpsconceptsandprograms.com/organizations/operating-forces/us-marine-corps-forces-cyberspace-command-marforcyber.)

Like the other US military services, USMC communications and cyberspace officers also fill roles in Supporting Establishment organizations. Some serve in roles that align with their specialty such as service on Headquarters Marine Corps G-6 staff or in acquisitions, while other roles such as recruiting, training and education instructors, and recruit training leadership roles are agnostic to occupational specialty.   Outside the USMC, its communications and cyberspace officers fulfill roles in joint organizations such as the Joint Staff, Combatant Commands, and joint tactical units like the Joint Communications Support Element (JCSE).

USMC Cyberspace Occupational Specialties

This section will illustrate the two cyberspace-related officer military occupational fields within the USMC to include requirements to enter them. However, the reader must first understand unique officer force management dynamics within the USMC.

The USMC divides its officer occupational fields into three primary categories (excluding professionals such as medical, lawyers, etc.) and three sub-divisions. The three primary categories of occupational groups are Ground (Infantry, Light Armor, Artillery), Air (Aviator, Naval Flight Officer, Unmanned Aircraft pilot), and Combat Services Support (Logistics, Communications, etc.). Each category is further sub-divided into specific occupational fields with specific military occupational specialty codes (MOS).

The USMC has three classifications of active duty officer spanning across the three abovementioned categories of officer. These divisions are *Unrestricted Officers, Restricted Officers (aka Limited Duty Officers)*, and *Warrant Officers*. Unrestricted Officers are what one thinks of as a traditional military officer: their role is to become proficient in their core specialty, lead, and command personnel and can rise to the grade of O-6 and beyond. The intent of the Limited Duty Officer (LDO) and Warrant Officer programs are to retain a cadre of specialized and technically proficient officers within a given occupational specialty. Limited Duty Officers are commissioned officers within the USMC who can rise to the grade of O-5, however do not hold command positions. While LDOs share the same occupational specialty code as the unrestricted officers and may lead personnel, they do not hold "command" positions and their force development emphasis does not as strongly align to all extra-service or intra-service requirements. Similarly, Warrant Officers are officers, but their primary role is to provide deep technical expertise within their specialty (even more so than the LDOs).[9] The understanding of three classifications of USMC officers is important during the comparative analysis across the services. Thus, with this understanding of the three classifications of Marine Corps officers, the remainder of this section and chapter will focus on Unrestricted Officers as the comparable officer pool to the USA and USAF.

Navy Marine Corps Order 1200.1D – *Military Occupational Specialties Manual*, outlines the approved military occupational specialties (MOS) for USMC officers,

[9] Marine Corps Order (MCO) P1400.31C, *Marine Corps Promotion Manual, Volume 1, Officer Promotions*, 9 August 2006.

warrant officers, and enlisted. Effective March of 2018, the USMC stated they will have two primary military occupational specialties in the cyberspace field: the *communications officer* (600-series) and the *cyberspace officer* (1700-series).[10] Historically, the USMC had a single occupational field in this realm: the 600-series communication officer. The USMC is still working out details on the 1700-series cyber operations career field (first designation Fiscal Year 2019) to include what the force development pipeline will look like and what 600-series billets and/or units will transition to 1700-series.[11] Therefore, we will discuss the current state of affairs, but with the understanding things will change in the near future.

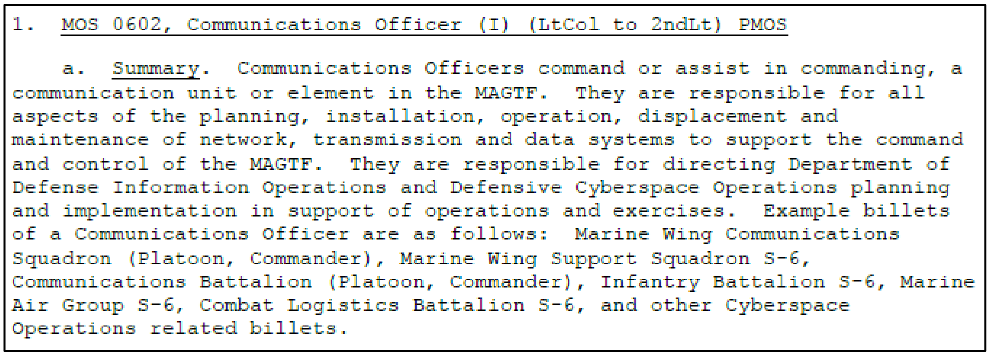
The 600-series *Communications Officer* occupational field falls under the Combat Service Support designation. Officers holding 600-series military occupational specialties primarily serve in the MAGTF/MEF, while the newly-established 1700-series occupational field will assume many of the Cyber Mission Force responsibilities within the MARCYBERFOR Marine Cyberspace Warfare Group and MEF Information Group

Occupational Specialty: Communications Officer (600-Series). The 600-series occupational field has one primary (permanent) officer occupational specialty and two temporary, duty-specific occupational specialties. The primary (permanent) MOS within the 600-series is the *602 Communications Officer*. An officer earns the 602 MOS after completing their primary occupational training and may retain this MOS through the grade of O-5. A 602 officer primarily focuses on the tactical and operational level of warfare within the Operating Force. Figure 16 provides a summary of the duties and responsibilities of a USMC communications officers. A Marine Communications Officer may also temporarily hold a *603 MAGTF Communications Planner* MOS or *691 Communications Training Instructor* MOS when assigned to designated positions. The 603 officers must complete the 12-week MAGTF Communications Planner Course and 691 officers must complete the Communications Training Instructors Course.[12]

[10] Navy Marine Corps (NAVMC), *1200.1D Military Occupational Specialties Manual (DRAFT)*, 2018.

[11] Skehan, interview; Matthew A Knopp, operations officer, Communications Training Battalion, United States Marine Corps, to the author, e-mail, 9 April 2018.

[12] Navy Marine Corps (NAVMC) 1200.1D, 1-39, 1-46.



```
1.  MOS 0602, Communications Officer (I) (LtCol to 2ndLt) PMOS

    a.  Summary.  Communications Officers command or assist in commanding, a
communication unit or element in the MAGTF.  They are responsible for all
aspects of the planning, installation, operation, displacement and
maintenance of network, transmission and data systems to support the command
and control of the MAGTF.  They are responsible for directing Department of
Defense Information Operations and Defensive Cyberspace Operations planning
and implementation in support of operations and exercises.  Example billets
of a Communications Officer are as follows:  Marine Wing Communications
Squadron (Platoon, Commander), Marine Wing Support Squadron S-6,
Communications Battalion (Platoon, Commander), Infantry Battalion S-6, Marine
Air Group S-6, Combat Logistics Battalion S-6, and other Cyberspace
Operations related billets.
```

Figure 4. USMC Communications Officer Occupational Specialty Description. (Reprinted from Navy Marine Corps [NAVMC] 1200.1D Military Occupational Specialties Manual [DRAFT], 1-39.)

Occupational Specialty: Cyberspace Officer (1700-Series). The 1700-series *Cyberspace Operations* occupational field is a split from the 600-series career field. Certain roles, primarily in the Offensive and Defensive Cyberspace Operations realms transition from the 600-series into the 1700-series. Becoming a 1700-series officer is significantly different than the 600-series in two key ways. First, while a Marine Officer can become a 600-series officer as their first MOS, the primary method an officer can become 1700-series is by a lateral move from another MOS (primarily from 602) and after attaining at least O-3 (captain) rank.[13] The USMC is actively also looking at direct accession into the 1700-series from their commissioning source, however these plans are preliminary.[14] The second major requirement is that the officer must be career designated, which is a significant milestone in the lifecycle of an officer desiring to make the USMC a career.[15] We will discuss the career designation concept in the Promotion/Advancement section later in this chapter. The reason the USMC made the 1700-series a lateral move into specialty as the USMC wants its Marine Officers to first build operational experience and prove themselves within the MAGTF/MEF or other Operating Force prior to "specializing" in the cyberspace operations realm.[16]

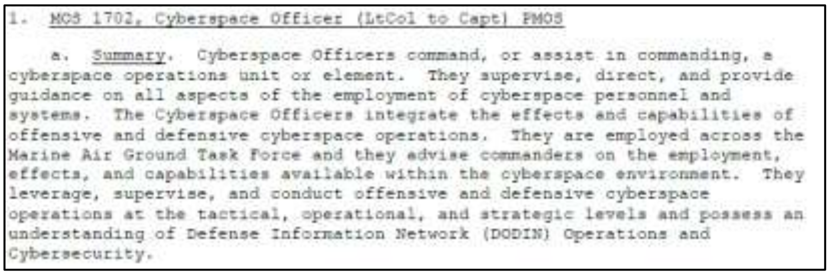
[13] "Navy Marine Corps (NAVMC) 1200.1D, 1–60.

[14] Matthew A Knopp, executive officer, Communications Training Battalion, United States Marine Corps, to the author, e-mail, 9 April 2018.

[15] "Navy Marine Corps (NAVMC) 1200.1D, 1–60.

[16] Skehan, interview.

The 1700-series occupational field will be comprised of a single primary commissioned officer MOS, the *1702 Cyberspace Officer*, and an additional *1705 Cyberspace Warfare Development Officer* designation. The 1702 Cyberspace Officer is the core 1700-series MOS and focuses at the tactical level of offensive and defensive cyberspace operations while understanding DoDIN operations. Officers in the grades of O-3 through O-5 may hold this MOS.[17] Figure 17 provides a summary of the duties and responsibilities of a USMC cyberspace officer.



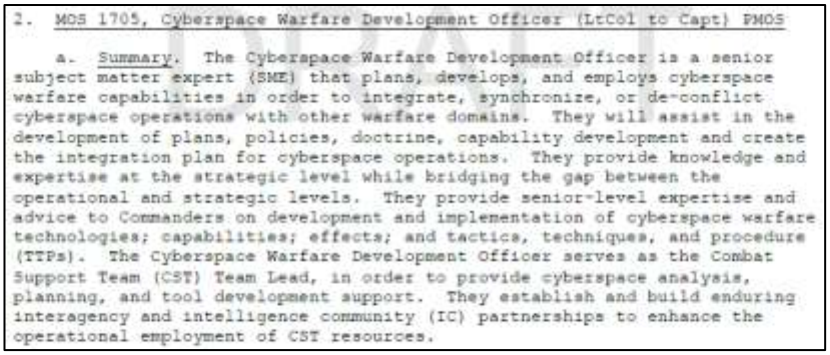
1. MOS 1702, Cyberspace Officer (LtCol to Capt) PMOS

a. Summary. Cyberspace Officers command, or assist in commanding, a cyberspace operations unit or element. They supervise, direct, and provide guidance on all aspects of the employment of cyberspace personnel and systems. The Cyberspace Officers integrate the effects and capabilities of offensive and defensive cyberspace operations. They are employed across the Marine Air Ground Task Force and they advise commanders on the employment, effects, and capabilities available within the cyberspace environment. They leverage, supervise, and conduct offensive and defensive cyberspace operations at the tactical, operational, and strategic levels and possess an understanding of Defense Information Network (DODIN) Operations and Cybersecurity.

Figure 5. USMC Cyberspace Officer Occupational Specialty Description.
(Reprinted from Navy Marine Corps [NAVMC] 1200.1D Military Occupational Specialties Manual [DRAFT],” 2018, 1-60.)

The 1705 Cyberspace Warfare Development Officer may be an O-3 through O-5, and are expected to be a SME who leads, plans, integrates, and advises at the operational and strategic level. Figure 18 provides a summary of the duties and responsibilities of a USMC cyberspace warfare development officer. They focus on the integration of warfighting effects. The USMC codes its single Combat Support Team Lead position as a 1705. A 1702 may become a 1705 or a 600-series officer may laterally move into the 1705 MOS, if approved.[18]

[17] Navy Marine Corps (NAVMC) 1200.1D, 1–60.
[18] Navy Marine Corps (NAVMC) 1200.1D, 1–61.



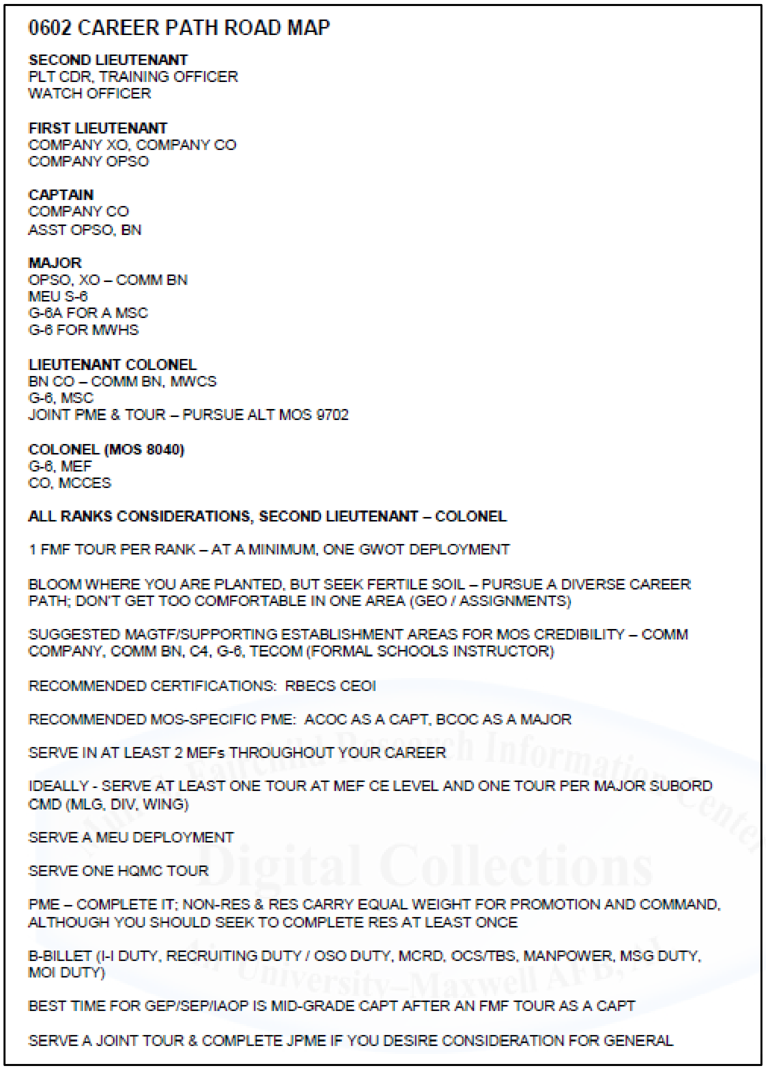
2. MOS 1705, Cyberspace Warfare Development Officer (LtCol to Capt) PMOS

a. Summary. The Cyberspace Warfare Development Officer is a senior subject matter expert (SME) that plans, develops, and employs cyberspace warfare capabilities in order to integrate, synchronize, or de-conflict cyberspace operations with other warfare domains. They will assist in the development of plans, policies, doctrine, capability development and create the integration plan for cyberspace operations. They provide knowledge and expertise at the strategic level while bridging the gap between the operational and strategic levels. They provide senior-level expertise and advice to Commanders on development and implementation of cyberspace warfare technologies; capabilities; effects; and tactics, techniques, and procedure (TTPs). The Cyberspace Warfare Development Officer serves as the Combat Support Team (CST) Team Lead, in order to provide cyberspace analysis, planning, and tool development support. They establish and build enduring interagency and intelligence community (IC) partnerships to enhance the operational employment of CST resources.

Figure 18. USMC Cyber Warfare Development Officer Occupational Description. (Reprinted from Navy Marine Corps [NAVMC] 1200.1D Military Occupational Specialties Manual [DRAFT], 2018, 1-61.)

USMC Communications and Cyberspace Officer Development

This section will examine the training/education and experiential expectations and milestones over a “typical” USMC cyber officer’s career. While no two officers’ career paths are identical (even within a single occupational field), each USMC officer occupational community produces career development path charts outlining a typical/desired career path or pyramid. Figure 19 illustrates a notional career path for a Communications Officer. A similar document for the 1700-series cyberspace officer is not yet available.



0602 CAREER PATH ROAD MAP

SECOND LIEUTENANT
PLT CDR, TRAINING OFFICER
WATCH OFFICER

FIRST LIEUTENANT
COMPANY XO, COMPANY CO
COMPANY OPSO

CAPTAIN
COMPANY CO
ASST OPSO, BN

MAJOR
OPSO, XO – COMM BN
MEU S-6
G-6A FOR A MSC
G-6 FOR MWHS

LIEUTENANT COLONEL
BN CO – COMM BN, MWCS
G-6, MSC
JOINT PME & TOUR – PURSUE ALT MOS 9702

COLONEL (MOS 8040)
G-6, MEF
CO, MCCES

ALL RANKS CONSIDERATIONS, SECOND LIEUTENANT – COLONEL

1 FMF TOUR PER RANK – AT A MINIMUM, ONE GWOT DEPLOYMENT

BLOOM WHERE YOU ARE PLANTED, BUT SEEK FERTILE SOIL – PURSUE A DIVERSE CAREER PATH; DON'T GET TOO COMFORTABLE IN ONE AREA (GEO / ASSIGNMENTS)

SUGGESTED MAGTF/SUPPORTING ESTABLISHMENT AREAS FOR MOS CREDIBILITY – COMM COMPANY, COMM BN, C4, G-6, TECOM (FORMAL SCHOOLS INSTRUCTOR)

RECOMMENDED CERTIFICATIONS: RBECS CEOI

RECOMMENDED MOS-SPECIFIC PME: ACOC AS A CAPT, BCOC AS A MAJOR

SERVE IN AT LEAST 2 MEFs THROUGHOUT YOUR CAREER

IDEALLY - SERVE AT LEAST ONE TOUR AT MEF CE LEVEL AND ONE TOUR PER MAJOR SUBORD CMD (MLG, DIV, WING)

SERVE A MEU DEPLOYMENT

SERVE ONE HQMC TOUR

PME – COMPLETE IT; NON-RES & RES CARRY EQUAL WEIGHT FOR PROMOTION AND COMMAND, ALTHOUGH YOU SHOULD SEEK TO COMPLETE RES AT LEAST ONCE

B-BILLET (I-I DUTY, RECRUITING DUTY / OSO DUTY, MCRD, OCS/TBS, MANPOWER, MSG DUTY, MOI DUTY)

BEST TIME FOR GEP/SEP/IAOP IS MID-GRADE CAPT AFTER AN FMF TOUR AS A CAPT

SERVE A JOINT TOUR & COMPLETE JPME IF YOU DESIRE CONSIDERATION FOR GENERAL

Figure 19. USMC Communications Officer Career Path Road Map. (Reprinted from Patrick Skehan,“0602 Career Path Road Map,” 5 March 2018.)

This section will divide the first 20 years of an officer’s career into four chronological blocks: 0-4 years, 4-10 years, 10-15 years, and 15-20 years. Though an officer’s career may go beyond 20 years, this is outside the scope of this paper. Each chronological block will review the primary institutional and occupational training/education requirements followed by deliberate experience (i.e. key duty positions, employment of capabilities). A complete review of all training, education, and experimental opportunities for USMC officers is outside the scope of this paper, thus this analysis will focus on the major and relatively common items.

USMC Developmental Focus. Before proceeding into the chronological development model, the reader must understand some overall developmental goals and themes within the USMC writ-large as well as in the communications and cyberspace community. The USMC specifies a framework for leader development aligned into six areas. The six areas are fidelity, fighter, fitness, family, finances, future. The *fighter* area applies to Marine officer development within this paper and refers to "the cumulative skill-sets and knowledge that make Marines well-rounded warriors." This area addresses Professional Military Education (PME), as well as the classifications of duties, such as Military Occupational Specialty, and corresponding standards of performance, interpersonal communication skills, and on and off-duty education. This area also helps focus training of both individuals and the team.[19]

The US Marine Corps values officers who demonstrate leadership in its operating forces (warfighting), which inherently includes understanding multi-domain operations and associated planning. Over a career, the USMC expects its officers to demonstrate these abilities in succeeding levels command and staff. Furthermore, the USMC attempts to build breadth for many of its officers by alternating duty assignments between Operating Forces and Supporting Establishment. For communications officers, the USMC attempts to create depth in warfighting (MAGTF) operations while building breadth across different mission sets by assigning communications officers to different types of units within Operating Forces throughout a career: Combat Arms (Ground) Division, Marine Logistics Group, Marine Aviation Wing, MARSOC, or MARCYBERFOR (for communications and cyberspace officers).[20]

The USMC also expects its officers to be effective military planners, which includes becoming practitioners of the Marine Corps Planning Process (MCPP). MCPP is very similar to Joint Operational Planning Process (JOPP) and USA's Military Decision-Making Process (MDMP) with utility for planning from the tactical through operational and campaign levels of warfare. Marine communications officers must annually demonstrate their ability to function and provide products as part of the Marine

[19] Marine Corps Order (MCO) 1500.61, *Marine Leader* Development, 28 July 2017, 3.
[20] Skehan, interview.

Corps Planning Process.[21] Marine communications officers in 603 MAGTF Communications Planner Billets are expected to be especially proficient with MCPP as their primary duty is planning. They must demonstrate building of a MAGTF Communications Plan annually.[22]

Now, with a wavetop-level understanding that USMC officer force development gives primacy to leadership and staff experience (planning and execution) within the MAGTF to build warfighters no matter their occupation, this paper will dive deeper into examining exactly how the Corps builds its communications and cyberspace officers within the larger context of USMC officer development over the first 20 years of a career. One specific caveat is that the following analysis will focus on the "ideal" and generic Marine (communication/cyberspace) officer development. This study will not cover unit-specific institutional and/or occupational qualification training (Airborne School, etc.) in its survey treatment of officer development across the service.

Years 0-4 (2nd Lieutenant – 1st Lieutenant)

The Corps focuses the first four years of a Marine officer's career heavily on institutional and occupational training, building a foundational understanding of USMC warfighting, and developing leadership experience at the platoon-level. While these are early "learning" years for Marine officers, performance in these training and leadership positions during these four years can significantly affect the following four to ten years.

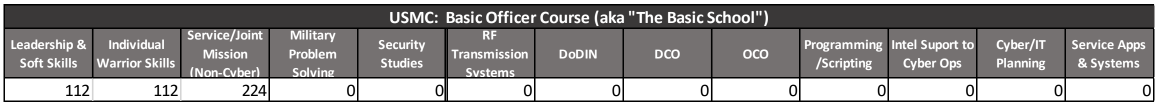
Training & Education (0-4 years). The Corps invests considerable time to train institutionally and occupationally its new officers, dedicating upwards of the first 12 months of an officer's active duty service solely to training. The USMC's motto is that "every Marine is a rifleman" and the Corps believes that all its officers must understand (and experience) the core Marine mission and be able to lead troops in combat. Thus, upon commissioning, all USMC officers attend six months of training named the *Basic Officer Course*, but more affectionately referred to as *The Basic School* (TBS). The Basic School deliberately trains all unrestricted active duty officers to be Provisional

[21] Navy Marine Corps (NAVMC) 3500.56C, *Communications Training and Readiness Manual*, 2 November 2016, 5-6, 5-8.

[22] Navy Marine Corps (NAVMC) 3500.56C, 6-4.

Rifle Platoon Commanders through four phases of instruction.[23] The four phases of instruction start with individual marine skills and build through subsequent echelons of team skills: rifle squad-level, rifle platoon-level, and to finally an introduction to MAGTF operations.[24] The end-result is that every Marine officer forms a warfighting skillset useful throughout their career, but they also built insight into how the experiences of younger Marine rifleman and squad leaders. Table 19 depicts the content of these blocks of instruction by thematic variable.

Table 19. USMC Basic Officer Course Content (hours)



USMC: Basic Officer Course (aka "The Basic School")												
Leadership & Soft Skills	Individual Warrior Skills	Service/Joint Mission (Non-Cyber)	Military Problem Solving	Security Studies	RF Transmission Systems	DoDIN	DCO	OCO	Programming /Scripting	Intel Suport to Cyber Ops	Cyber/IT Planning	Service Apps & Systems
112	112	224	0	0	0	0	0	0	0	0	0	0

Source: Author's Original Work

With exceptions (some aviation, law, etc.), most Marine officers receive their occupational specialty only at the end of TBS. Thus, Marine communications officers receive practical training on the core warfighting function of the Marine Corps prior to ever receiving any training in their primary occupational specialty.[25] As stated previously in this chapter, Marine officers do not currently assess directly into the 1700-series Cyberspace occupational field. Therefore, the occupational focus for this 0-4 Year section will focus solely on the 600-series Communications Officers. Upon completion of TBS, Marine officers proceed to their occupational training courses.

USMC officers selected to become 600-Communications Officers attend the Basic Communications Officer Course (BCOC) in Twentynine Palms, California. BCOC is a 11-week course focuses on "the mastery of fundamental techniques and skills required for the planning and employment of Marine Corps communications systems in both the tactical and garrison environment…covering the duties and responsibilities of

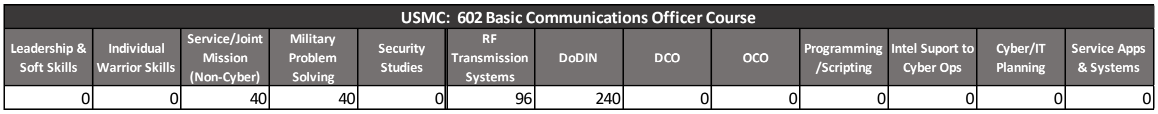
[23] W.R. Speigle II, "The Basic School: Continuing to Successfully Prepare Second Lieutenants to Be Officers", United States Marine Corps Command and Staff College, 17 April 2008), 1–4, http://www.dtic.mil/dtic/tr/fulltext/u2/a491616.pdf.
[24] "The Basic School Training Command: Phase 0-IV Student Materials," http://www.trngcmd.marines.mil/Units/Northeast/The-Basic-School/Academics/FY16-PHASE-0/.
[25] Skehan, interview.

the Communications Platoon Commander and S-6 Staff Officer to include the preparation of command and control plans and orders used by the Marine Air Ground Task Forces."[26]

BCOC has five major blocks of instruction: doctrinal use of communications within the Marine Air Ground Task Force (40 hours), Marine Corps Transmissions systems (60 hours), Networking Concepts (120 hours), Data Systems (120 hours), and the Marine Corps Planning Process (40 hours). The 51 days represent in-classroom time; the remaining 53 days of BCOC involve practical experience using this knowledge and skills in the field as well as other group instruction. BCOC does not provide Marine communications officers with a certification to satisfy DoDD 8140/8570 Information Assurance requirements.[27]

Table 20 depicts the content of BCOC blocks of instruction by thematic variable. BCOC not only trains the officers in their technical specialty, but also dedicates 10% of its classroom time specifically focusing on how the MAGTF leverages communications in warfighting and another 10% of to the Marine Corps Planning Process. This 20% of training illustrates how the USMC continually focuses its instruction to ensure officers understand how what they are learning applies to how the Marine corps plans and executes its operational (warfighting) mission.

Table 20. USMC Basic Communications Officer Course Curriculum Content (hours)



USMC: 602 Basic Communications Officer Course												
Leadership & Soft Skills	Individual Warrior Skills	Service/Joint Mission (Non-Cyber)	Military Problem Solving	Security Studies	RF Transmission Systems	DoDIN	DCO	OCO	Programming /Scripting	Intel Suport to Cyber Ops	Cyber/IT Planning	Service Apps & Systems
0	0	40	40	0	96	240	0	0	0	0	0	0

Source: Author's Original Work

As shown, the Marine Communications Officer spends most of the first year of active duty service in training (TBS and BCOC). Upon completion of this first year of training, Marine communications officers arrive at their first duty assignment.

[26] "Communications Training Battalion (CTB): CTB Courses 2017," United States Marine Corps Communications Training Battalion, 2017. http://www.trngcmd.marines.mil/Portals/207/Docs/MCCES/CTB/CTB%20COURSES%202017-%20Enclosure%20(2).docx?ver=2017-11-22-171439-797.
[27] Joshua D. Chang, course director, Basic Communications Officer Course, Communications Training Battalion), to the author, e-mail, 12 April 2018.

Key Duties/Experience (0-4 years). The first key developmental position for unrestricted officers within the USMC is as a Platoon Commander within the Operating Force (primarily MAGTF/MEF). Within the 36 months of service post-training, the USMC developmental aim is for its Lieutenants to serve at least one year as Platoon Commander. This includes communications officers. The USMC values platoon leadership as it provides direct tactical leadership experience for their junior officers. Platoon leadership within the MEF provides the additional bonus by providing the Marine lieutenant the opportunity to execute their occupational specialty within the primary Marine Corps warfighting construct.[28] As a result, officers develop a foundational understanding of how and why the USMC operates and how their specific occupation integrates with the whole.

For communications officer, platoon command ideally occurs within a combat arms battalion (infantry, light armor, artillery). However, what matters most is that the communications platoon gains platoon leadership experience in the operating force. One unique aspect of communications platoon leadership that differs from combined arms platoon leadership (e.g. infantry platoon) is that the Communications Platoon Commander holds a secondary duty as the Battalion S6. Thus, not only does the communications lieutenant can lead as a tactical Marine communicator, he or she also is a critical part of the planning and execution staff of the Battalion.[29] Thus, Marine communications lieutenants build experience with the Marine Corps Planning Process (MCPP) as part of a tactical warfighting echelon, experience that often requires, and reinforces, multi-domain understanding and integration of joint warfighting functions.

Platoon Commander positions are not always immediately available for every communications lieutenant as they arrive at their first duty station. While awaiting their platoon leadership opportunity, marine communications officers may hold a variety of other positions that may include Assistant Platoon Leader, Assistant Battalion S6, etc., affording opportunities to further hone understanding and skill with Marine warfighting and planning.[30]

[28] Patrick Skehan, “0602 Career Path Road Map,” 5 March 2018; Skehan, interview.
[29] Skehan, interview.
[30] Ibid.

As Marine lieutenants, including communications officers, approach their 4-year point of service, three primary developmental events occur. If not previously career-designated, the lieutenants meet the career designation board. Lieutenants also compete for promotion to Captain. Third, the USMC screens these senior lieutenants for the next level of developmental education: USMC Expeditionary Warfare School (EWS) or Naval Postgraduate School (NPS).[31] In addition to these three USMC-wide boards, communications officers can also apply for lateral transfer to the 1700-series Cyberspace Officer occupational field at this point.[32] Therefore, the results of these various boards directly influence a marine officer's next assignment, which we will discuss in the next 4-10-year development section.

As illustrated in this section, the goal of USMC basic and subsequent communications officer development within the first four years of service focuses on tactical and leadership expertise, understanding MAGTF operations, and occupational proficiency. Additionally, the ability of a communications lieutenant to dual-hat as Battalion S6s and experience non-platoon leader duties within these first years provides direct exposure and experience to Marine planning processes, multi-domain operations, and associated joint warfighting function integration. Not only have communications officers received over 28 weeks training in Marine warfighting and 40-hour hours on military problem-solving processes, but also the majority can leverage and build experience with service concepts during their first Operating Force tour. Finally, Marine communications officers do not yet satisfy the external DoDD 8140/8570 information assurance requirements unless they do so on their own time.

Years 4-10 (Captain)

At the end of these first four years of service, the Marine Corps starts looking to provide developmental breadth while still reinforcing core warfighting concepts. Years 4-10 of a USMC officers' career will typically involve at least two duty assignments and may include a 10-month long PME. These six years focus on higher levels of leadership (company command), breadth in a Supporting Establishment organization, and 10-month PME (USMC Expeditionary Warfare School, Naval Postgraduate School, or Army-

[31] Ibid.
[32] Navy Marine Corps (NAVMC) 1200.1D, 1-60.

equivalent Captain's Career Course). Opportunities also exist for work on higher echelon staffs within the Operating Force (Brigade, Division, and Corps G-6). The USMC evaluates Marine officers not previously career-designated during this window, assuming the officers are still in their initial active duty service commitment. The remainder of this chapter assumes that the communication/cyberspace officer is career designated by the service.

This paper assumes that the 1700-series cyberspace officer developmental model for years four through twenty will closely align to existing Marine Corps and 600-series communication officer developmental paths. We make this assumption for two reasons. First, as the 1700-series MOS is so new, not all force development regulations and materials for this occupational field exist yet, so there is nothing to analyze. Therefore, as cyberspace officers compete for promotion across all occupational fields like communications officers, we assume their developmental model will likely closely align to the USMC and, specifically, the communication officer models.[33] Therefore, unless otherwise noted, this and subsequent chronological sections will heavily focus on the Marine 600-series communications officer.

Training & Education (4-10 years). During this part of a career, Marine captains complete a 10-month long professional military education (PME) resident (or distance education) program as well as occupational-specific training courses. The two primary PME programs for USMC officers are its Expeditionary Warfare School and the Naval Postgraduate School. Some officers have the option to attend the USA Captains Career Courses for their given occupational specialty (details in chapter four). However, the Corps has not authorized its communications and cyberspace officers to attend the equivalent Army Captains Career Courses (in this case, Signal or Cyberspace Captains Career Courses).[34]

As discussed in the earlier section, the Corps initially screens officers for the Expeditionary Warfare School and Naval Postgraduate School around the 4-year career point. Their only "look" for NPS is during that first screening. For officers not selected for either program during their first screening, the USMC conducts additional screening

[33] Knopp to the author, e-mail.

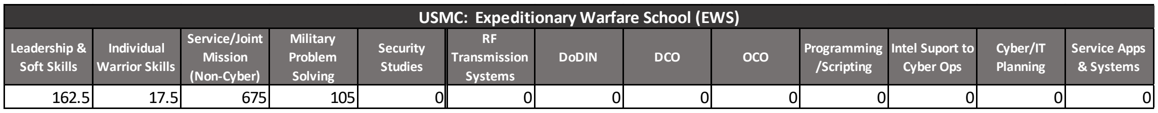
[34] Marine Corps Order (MCO) 1533.4B, *Professional Military Education*, 25 January 2008, 1-6.

boards annually; however, these follow-on boards only screen for the Expeditionary Warfare School.[35]

This thesis will focus on two resident programs available to communications and cyberspace officers: the USMC Expeditionary Warfare School (EWS) and the US Naval Postgraduate School. EWS is a 41-week program that covers six named themes: Profession of Arms (240 hours), Warfighting (140 hours doctrine/140 hours planning), MAGTF Operations Ashore (320 hours), MAGTF Operations Afloat (440 hours), Occupational Field Expansion Course (160 hours), and Future Operating Environment (throughout).[36] The Occupational Field Expansion Course is the primary occupational field-specific education Marine officers receive during the 4-10 year block of a career. In addition, Marine 602 officers receive additional occupational training in the 603 MAGTF Planners Course presented in the next section.

Table 21 depicts the content of EWS blocks of instruction by thematic variable. Of note, this course spends most of the academic year forcing Marine occupational specialties to come together and learn how operate, plan, and function as a part of a MAGTF ashore or afloat. However, the course also invests considerable time on leader development.

Table 21. USMC Expeditionary Warfare School Curriculum Content (hours)



USMC: Expeditionary Warfare School (EWS)												
Leadership & Soft Skills	Individual Warrior Skills	Service/Joint Mission (Non-Cyber)	Military Problem Solving	Security Studies	RF Transmission Systems	DoDIN	DCO	OCO	Programming /Scripting	Intel Suport to Cyber Ops	Cyber/IT Planning	Service Apps & Systems
162.5	17.5	675	105	0	0	0	0	0	0	0	0	0

Source: Author's Original Work

The US Navy's Naval Postgraduate School is a graduate institution within the US Department of the Navy that offers 75 different types of graduate degrees to US commissioned officers, DoD civilians, and international partners.[37] Communications

[35] Skehan, interview.

[36] "Expeditionary Warfare School," Marine Corps University, https://www.usmcu.edu/ews; "USMC Expeditionary Warfare School AY18 Curriculum Timeline" (Marine Corps University Expeditionary Warfare School); Maj Gilberto Perez, former EWS student, interview by the author, 18 April 2018.

[37] "Naval Postgraduate School Academics," Naval Postgraduate School, http://www.nps.edu/web/guest/academics.

officers attend NPS to work on a degree and research relevant to their occupation and/or interest area. This essay did not analyze this course by thematic variable as a relatively small population of Marine communications officers attend this course and the Navy is outside the scope of analysis.

Aside from the Occupational Field Enhancement Course during Expeditionary Warfare School, Marine 600-series communications officers also attend the 16-week 603 MAGTF Communications Planner Course. The course director aims to educate all captains and majors returning to the Operating Force after a tour in the Supporting Establishment. According to the course director, the "primary focus of the course was developed around creating a resilient C4 architecture through gaining a better understanding of key terrain in cyberspace, space, and electromagnetic spectrum operations: capable of being operationalized against the peer threats we would face in the future fight. We [Course Directors] also tie in discussions on intel gain loss and targeting boards to ensure the students understand how the information environment is shaping how we do business in the future."[38] The course presents instruction in 11 blocks: Project Management Professional commercial certification (42 hours), Planning (77 hours lecture), Command and Control Systems (70 hours), Cyberspace Operations (77 hours), Space (70 hours), Network Planning (42 hours), Data Systems Planning (42 hours), SPMAGTF/MEU/MEB and State Department Communications (21 hours), and three Capstone events (182 hours).[39]

Table 22 depicts the content of MCPC blocks of instruction by thematic variable. Of note, the USMC communications field includes the Project Management Professional (PMP) block in this course not as a replacement or parallel planning process to the Marine Corps Planning Process. Instead, they view PMP as a subordinate planning competency under MCPP; largely used for in-garrison project management and/or when working with contractors or other projects with the commercial sector.[40] At the end of this course, communications officers are better prepared to return to the Operating Force

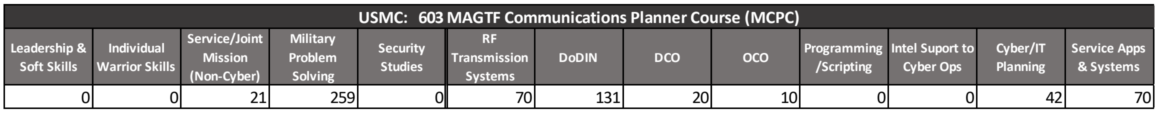
[38] William A. Hochrine, course director, MAGTF Communications Planner Course, to the author, e-mail, 16 April 2018.

[39] William A. Hochrine, "MAGTF Communications Planners Course Syllabus" (U.S. Marine Corps Communications Electronics School, 2018).

[40] William A. Hocrhine to the author, e-mail.

as they have additional education and experience with Marine Corps planning and their own occupational competencies.

Table 22. USMC MAGTF Comm Planner Course Curriculum Content (hours)



USMC: 603 MAGTF Communications Planner Course (MCPC)												
Leadership & Soft Skills	Individual Warrior Skills	Service/Joint Mission (Non-Cyber)	Military Problem Solving	Security Studies	RF Transmission Systems	DoDIN	DCO	OCO	Programming /Scripting	Intel Suport to Cyber Ops	Cyber/IT Planning	Service Apps & Systems
0	0	21	259	0	70	131	20	10	0	0	42	70

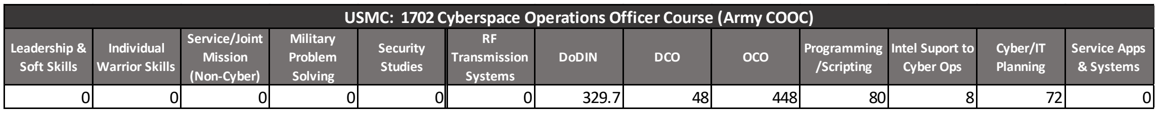
Source: Author's Original Work

During this 4-10-year timeframe, officers selected for lateral move in the 1700-series cyberspace officer occupational field undergo basic 1702 occupational training. Over the near term, the USMC does not intend to have its own 1702-level cyberspace training course. Instead, officers will attend the 27-week portion of the USA's cyberspace officer training known as Cyberspace Operations Officer Course (COOC). COOC is Army cyberspace basic officer training course (CBOLC), minus the Army-required common core training tasks. The Cyber Operations Officer Course contains six major blocks of instruction: Cisco Certified Network Associate (7 weeks), Certified Information Systems Security Professional (2 weeks), Programming (1 week), Army Cyberspace Operations Planners course (2 week), and Cyber Common Technical Core (9 weeks), Cyber Protection Team Methodologies, Intelligence (2 weeks), and Research (1 week). The Cyberspace Operations Officer Course provides officers both Cisco Certified Network Associate (CCNA) and Certified Information Systems Security Professional (CISSP) certifications, satisfying the DoD 8140/8570 information assurance certification requirement.[41]

Table 23 depicts the content of COOC blocks of instruction by thematic variable. As noted in the Cyber BOLC analysis in chapter four, COOC curriculum emphasizes cyberspace operations (OCO/DCO/DoDIN) over transmission systems and service applications. After completing COOC, Marine 1702 cyberspace officers will move to their first operating force cyberspace duty.

[41] "Cyber Technical College" (Cyber School, U.S. Army Cyber Center, September 15, 2016), 3–4.

Table 23. USMC Cyberspace Operations Officer Course (hours)



USMC: 1702 Cyberspace Operations Officer Course (Army COOC)												
Leadership & Soft Skills	Individual Warrior Skills	Service/Joint Mission (Non-Cyber)	Military Problem Solving	Security Studies	RF Transmission Systems	DoDIN	DCO	OCO	Programming /Scripting	Intel Suport to Cyber Ops	Cyber/IT Planning	Service Apps & Systems
0	0	0	0	0	0	329.7	48	448	80	8	72	0

Source: Author's Original Work

Key Duties/Experience (4-10 years). Besides a 10-month PME and occupational training, Marine officers will typically have two duty assignments: one within the Operating Force and one within the Supporting Establishment or joint organization. The key developmental position within the USMC during the 4-10-year career point is to serve at least one year as a *Company Commander* (desired within MAGTF/MEF).[42] The USMC values company command as it provides the next-higher tactical leadership experience above the platoon level and is the first opportunity Marine Officers are given UCMJ authority over their subordinates (aka given "G-series" orders).

A duty assignment within the supporting establishment is a key part of deliberate officer development as it provides experiential breadth outside of the officer's primary occupation. Or, if the duty remains within the occupational field, it provides a different lens than the USMC-centric tactical and operational warfighting side. After Marine officers complete this duty, they return to the operating force with a broader understanding about how the Marine Corps institutionally organizes, trains, and equips its force.

The 600-series Communications Officer occupational field mirrors the USMC in development experience. To remain competitive for future advancement, Marine communications captains must successfully complete Communications Company Command within the Operating Force. Company command opportunities exist across the MEF; with primary opportunities as the Communications Company Commander within one of the Marine Divisions, within the Communications Battalions under the MEF, and within a Marine Air Wing Communications Squadron. Company commands also exist across other non-MAGTF operating forces to include the two cyber groups under MARFORCYBER. When not in a company command position, Marine

[42] Skehan, "0602 Career Path Road Map"; Skehan, interview.

communications captains may hold a variety of other operational unit positions to include serving on a G-6 staff (MEF or Division Level).[43]

For 1700-series cyberspace officers, duty experience within six-year block will slightly differ. While details on force development during this period are slim, available information highlights that this period will include up to 27 weeks to 2 years of occupational training in their new field in addition to the possibility of attending 10-month institutional training (EWS/NPS). They will spend time in MARCYBERFOR with includes duty on National and Cyber Mission forces, on service-retained cyberspace protection teams (CPTs) or other cyberspace-focused units within the Cyber Operations Group supporting MAGTFs or embedded within the newly-established MEF Information Groups (MIG) providing direct cyber support to their assigned MEF.[44]

This section illustrated that during the 4-10-year career block, Marine communications or cyberspace officers have expanded their leadership experience and understanding of USMC operations. They have typically completed key duty as a company commander and built staff experience in the Operating Force, as well as fulfilled a broadening tour in the Supporting Establishment. The laterally-created cyberspace officer has undergone a minimum of 27 weeks training in their new occupational field and have completed at least one duty assignment as part of the Cyber Mission Force and/or Marine Information Group.

Through the Expeditionary Warfare School (and the 603 MAGTF Planners course for 600-series officers), communications and cyberspace officers furthered their knowledge, skills, and abilities in MAGTF operations and planning. The combination of experience and training/education creates the foundation for a soon-to-be Field Grade Officers. As a Field Grade Officer, the Marine Corps (communications/cyberspace) officer force development model shifts from a focus on direct tactical leadership within warfighting organizations, to a focus on the training/education and experience required to build proficiency in higher-echelon tactical and operational-level planning and execution.

[43] Skehan, interview.

[44] Skehan, interview; Knopp to the author, e-mail.

Years 10-15 (Major – Lieutenant Colonel)

After reaching the 10-year mark in their careers, the Corps promotes most of its officers to the field grade ranks. Like its sister service counterparts, USMC field grade officers (FGOs) begin to focus on higher levels of leadership (and larger organizations), furthering broadening experience at the headquarters staff level or in the joint realm. Additionally, USMC officers complete another level of Professional Military Education, the intermediate level education, while also satisfying the requirements for Joint Professional Military Education Level I.

Training & Education (10-15 years). The Corps requires no formal occupational training for its communications or cyberspace officers during the 10-15-year timeframe of their career.[45] However, USMC Professional Military Education expectations applicable to communications and cyberspace officers focus on completing intermediate-level education development, either in residence or by distance education. Most of the Marine officers (of all specialties) competitively selected for in-residence developmental education attend the USMC Command and Staff Course in Quantico, Virginia. However, a smaller percentage of officers have the opportunity to attend fellowships, sister-service schools, or international programs of equivalent developmental education.

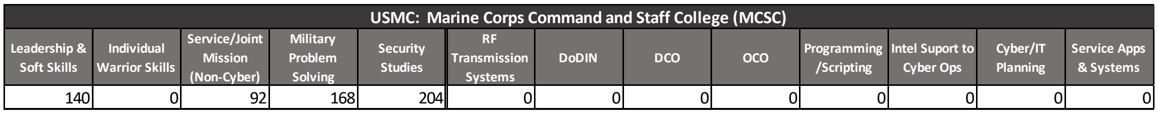
Marine Corps Command and Staff College (CSC) (in-residence and distance education) fulfills Joint Professional Military Education I (JPME I) requirements and awards an accredited Masters of Military Studies. Marine Corps CSC "provides graduate level education and training in order to develop critical thinkers, innovative problem solvers, and ethical leaders who will serve as commanders and staff officers in service, joint, interagency, intergovernmental, and multinational organizations confronting complex and uncertain security environments."[46] CSC's major blocks of instruction include Think/Decide/Communicate (40 hours), Leadership in the Profession of Arms I/II (100 hours), Evolution of Warfare to 1945 (64 hours), Evolution of Warfare Since 1945 (60 hours), National Security Affairs and the International System (64 hours), Evolving

[45] Skehan, interview.

[46] "United States Marine Corps Command and Staff College Curriculum" (United States Marine Corps Command and Staff College, 2017), 2.

National Security Concepts and Operations (64 hours), Joint and Marine Corps Operations (52 hours), The Marine Corps Planning Process (60 hours), Complex Operational Problem Solving and Design (60 hours), Theater Campaign Planning (48 hours), and an elective program.[47] (curriculum pg. 4-6). Table 24 depicts the content of these blocks of instruction by thematic variable.

Table 24. USMC Command and Staff College Curriculum Content (hours)



USMC: Marine Corps Command and Staff College (MCSC)												
Leadership & Soft Skills	Individual Warrior Skills	Service/Joint Mission (Non-Cyber)	Military Problem Solving	Security Studies	RF Transmission Systems	DoDIN	DCO	OCO	Programming /Scripting	Intel Suport to Cyber Ops	Cyber/IT Planning	Service Apps & Systems
140	0	92	168	204	0	0	0	0	0	0	0	0

Source: Author's Original Work

Key Duties/Experience (10-15 years). Experientially, during the 10-15-year period of a career, the key duties USMC officers complete are serving as a Battalion/Squadron Executive Officer (XO) or Operations Officer (S-3) within the Operating Forces. Individual occupational communities may also identify other key duty positions at different echelons or other organizations as identified by the occupational field's leaders. The 600-series communications field usually aligns with the overall USMC key developmental model. However, the 1700-series cyberspace field may need to introduce alternate and equivalent key duty positions due to extra-service mandated organizing principles such as the CMF team constructs.[48]

The Battalion Executive Officer (XO) is the second in command behind the Battalion Commander. The Marine Corps prepares them to assume battalion command, if required; however, their primary day-to-day duty focuses on leading the Battalion's staff functions (S1-S6) in the planning and execution of the battalion commander orders and intent. Closely aligned with the XO, the battalion operations officer position (S-3) focuses on managing the execution of current and future operations, to include overseeing in-garrison training. Neither the XO or S3 position is a command position,

[47] "United States Marine Corps Command and Staff College Curriculum," 4–6; "USMC CSC AY17-18 First Semester Calendar" (United States Marine Corps Command and Staff College, August 3, 2017); "USMC CSC AY17-18 Second Semester Calendar" (United States Marine Corps Command and Staff College, August 3, 2017).
[48] Skehan, "0602 Career Path Road Map"; Skehan, interview.

however the positions require formal and informal leadership and synchronization across different staff functional areas as well as working with subordinate company commanders who work for the Battalion Commander and actually execute battalion orders. They must also become experts not only of the Marine Corps Planning Process, but of leading planning teams. The Corps expects them to lead their staffs to translate higher headquarters operational orders and commander's vision/intent into operational orders for the battalion commander to provide for execution by subordinate echelons.

When not holding one of the key developmental positions and like previous chronological career blocks, Marine officers serve in various other staff elements at their duty locations. For 600 or 1700-series officers, this may include working as a staff officer within the G-6 at a higher echelon staff. Outside of the key developmental duty of XO or S3 and developmental education, Marine Corps officers during the 10-15-year points in their career typically also serve in another B-billet tour. As Field Grade Officers, this may include everything from serving in an acquisition or HQ Marine Corps staff position, to serving in a joint organization to satisfy the 36-month duty requirement to become a joint qualified officer in accordance with the Goldwater-Nichols Act.[49]

Years 15-20 (Lieutenant Colonel – Colonel)

After reaching the 15-year mark in their careers, USMC officers compete for the rank of lieutenant colonel. Like its sister service counterparts, Field Grade Officers in this period of their career continue to focus on higher levels of leadership (and larger organizations), furthering broadening experience at the headquarters staff level or in the joint realm. Additionally, USMC officers complete another level of Professional Military Education, with this intermediate level education satisfying the requirements for Joint Professional Military Education Level II.

Training & Education (15-20 years). The USMC requires no formal occupational training for its communications or cyberspace officers at the 15-20-year points of their career. However, USMC Professional Military Education expectations applicable to communications and cyberspace officers focus on completing Senior Developmental Education (SDE) either in residence or by distance education. Many of those Marine officers (of all specialties) competitively selected for in-residence SDE

[49] Skehan, interview.

attend the USMC War College in Quantico, Virginia. However, a percentage of officers have the opportunity to attend fellowships or attend sister-service or international equivalent senior developmental education opportunities. From the residence developmental education opportunity or via distance learning, Marine Corps officers complete Joint Professional Military Education II (JMPE II) requirements, satisfying all necessary educational requirements required for Joint Qualified Officer categorization.

Key Duties/Experience (15-20 years). Experientially, during the 15-20-year period of a career, the USMC force development models focuses on completing two requirements: battalion command and joint duty. Battalion command is the O-5 command opportunity afforded deserving Lieutenant Colonels. The battalion commander, informed by his/her staff, must be able to take higher echelon orders and direction and execute through leadership and operational art and science. When not operationally deployed, battalion commanders focus on the administration and operational training of the battalion and ensuring subordinate companies/Marines have the equipment required to execute their mission.

As mentioned earlier in this chapter, the USMC has six O-5 command opportunities within the Marine Expeditionary Force. Three battalions report directly to the MEF Commander and three communications squadrons reporting to one of three Marine Air Wings.[50] Thus far, the author has not seen anything official on the USMC coding specific MARCYBERFOR billets for 1700-series, however informed conjecture leads to the believe that, at a minimum, O-5 leadership within the MCYWG will be a 1700-series officer.

Marine lieutenant colonel communications and cyberspace officers not filling battalion command positions hold staff positions in the Operating Forces (e.g. G-6 staffs) or alternate in on Supporting Establishment B-billets. Of the B-billet opportunities, the USMC aims to assign officers to joint organizations to complete their joint duty qualification (if they have not already completed it).[51] Toward the end of this 15-20-year period, Marine Corps officers have their first opportunity to compete for promotion to Colonel (O-6).

[50] Skehan, interview.
[51] Ibid.

Chapter Summary

The purpose of this chapter was to provide the reader a foundational understanding of how the USMC develops its communications and cyberspace officers within the larger context of USMC officer development and DoD/joint officer requirements.   First and foremost, the Marine Corps views itself and its Marines as warfighters, valuing tactical and operational leadership experience within the MAGTF/MEF. This understanding serves as a foundation to understanding why the Marine Corps emphasizes warfighting skills and multi-domain MAGTF operations in all levels of institutional and occupational training and education. As a precursor, the USMC sends most of its newly-commissioned officers to The Basic School, graduating qualified Marine Rifle Platoon Commanders. Subsequent institutional PME and formal training reinforces these values as it focuses curriculum on leadership, integration of warfighting functions, and planning MAGTF operations…which are inherently multi-domain and span the joint warfighting functions.

The Marine Corps uses three different “divisions” of officer within its communications/cyberspace occupational field to ensure sufficient expertise to have officers on command/leadership tracks (unrestricted officers) and officers who focus upon becoming technical subject matter experts (Limited Duty Officers and Warrant Officers). The unrestricted officers, the focus of this chapter, developmentally alternate between leadership and staff assignments in the Operating Force and “B-billets” in the Supporting Establishment or joint duty. Unrestricted communications officer key duty positions and experience through the 20-year point of the career largely mirror the combat arms branches: Platoon Leader, Company Commander, Battalion Executive Officer and/or Operations Officer, and Battalion Commander. The USMC communications occupation has limited O-5 command opportunities; thus, officers must be true masters of leadership, warfighting, and their occupational field.

The Marine Corps also fulfills its DoD-directed obligations to support joint cyber operations. The Marine Corps decided to create a new cyberspace operations-focused occupational field and associated MOS in March 2018: the 1700-series Cyberspace Officer. Entry into this field as currently envisioned primarily occur at a minimum of O-3 as a lateral move from another occupational field (typically 600 Communications

Officers). While details on this new occupational field are currently sparse, nominally these officers will spend the much of the rest of their career working in cyberspace organizations both inside and outside the traditional USMC warfighting organizations.

Tables 25 and 26 at the end of this chapter provide the summary of content from formal training and education courses a notional USMC communications and cyberspace officer experiences through their twentieth year of commissioned service.

The Marine Corps expects its officers, regardless of occupational field, to be multi-domain leaders, have a working knowledge and experience of Marine warfighting (inherently multi-domain) and military problem-solving methodologies such as MCPP and JOPP. This is evident in that the USMC emphasizes these competencies during its institutional and occupational training and education.

At a minimum, communications officers receive 285 hours of in-resident USMC warfighting competencies (TBS, BCOC, and MCPC) and 299 hours education in the Marine Corps Planning process (BCOC and MCPC). For those communications officers competitively selected for EWS and MCSC, the educational hours leap to 1,052 hours USMC multi-domain warfighting and 572 hours of military problem-solving education. Likewise, Marine cyberspace officers receive a minimum of 264 hours of in-resident USMC warfighting competencies (TBS and BCOC) and 40 hours education in the Marine Corps Planning process (BCOC). For those cyberspace officers competitively selected for EWS and MCSC, the educational hours leap to 1,031 hours USMC multi-domain warfighting and 313 hours of military problem-solving education.

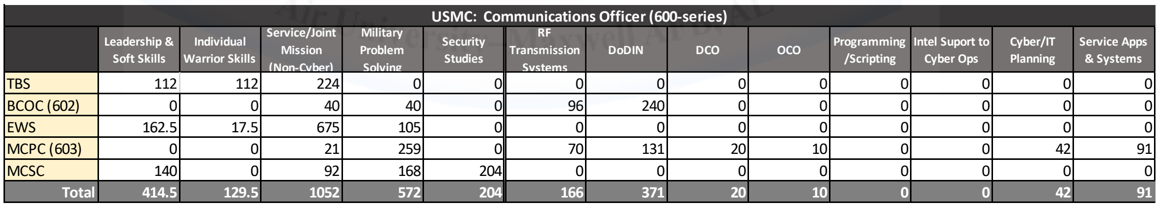
Nor is this heavy training and educational focus solely an academic exercise. The USMC expects the officers to use this knowledge and planning methodologies frequently within their assigned duty organizations to maximize combat effects. This allows Marine officers not only to have an academic understanding, but to build true skillsets that will carry through their career.

The Marine Corps deliberately ensures its communications and cyberspace operations officers meet all extra-service requirements. The USMC provides opportunities for its officers to earn commercial certifications to satisfy the DoDD 8140/8570 information assurance certification requirements. Cyberspace officers acquire the requisite certifications while attending their initial occupational training at the Army

Cyber Operations Officer Course. Communications officers may acquire certifications in an as-needed basis depending upon their desire and/or duty position. Finally, the USMC deliberately ensure its deserving officers are eligible to compete for general officer by mandating JPME and assigning officers to joint duty experience in alignment with the Goldwater Nichols Act.

To close, we will reiterate possibly the ultimate example of what the Marine Corps values in officer development. Only after demonstrated success tour in the Operating Force, serving in another occupational field, will the USMC consider an officer for entry into the 1700-series cyberspace field. Even though it requires upwards of two years of training to be a qualified cyberspace officer, the USMC places foundational primacy on MAGTF/MEF operations, reinforcing the fact that MAGTF warfighting is THE core competency all its officers will have. The Marine Corps values experience such that they will accept risk on losing upwards of four years of potential return on investment over the career of an officer by waiting until officers are Captains before allowing them to become cyberspace officers.

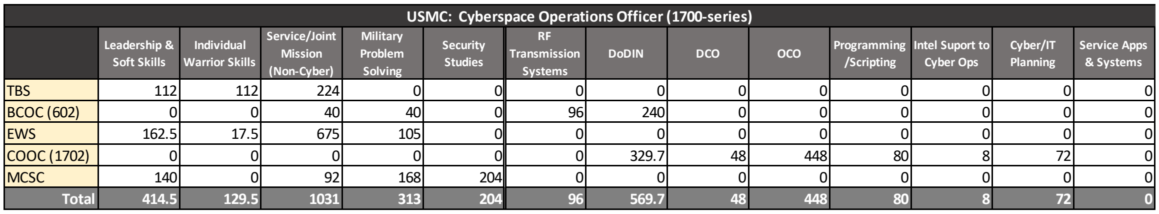
Table 25. USMC Communications Officer Career Education/Training (hours)



USMC: Communications Officer (600-series)													
	Leadership & Soft Skills	Individual Warrior Skills	Service/Joint Mission (Non-Cyber)	Military Problem Solving	Security Studies	RF Transmission Systems	DoDIN	DCO	OCO	Programming /Scripting	Intel Suport to Cyber Ops	Cyber/IT Planning	Service Apps & Systems
TBS	112	112	224	0	0	0	0	0	0	0	0	0	0
BCOC (602)	0	0	40	40	0	96	240	0	0	0	0	0	0
EWS	162.5	17.5	675	105	0	0	0	0	0	0	0	0	0
MCPC (603)	0	0	21	259	0	70	131	20	10	0	0	42	91
MCSC	140	0	92	168	204	0	0	0	0	0	0	0	0
Total	414.5	129.5	1052	572	204	166	371	20	10	0	0	42	91

Source: Author's Original Work

Table 26. USMC Cyberspace Officer Career Education/Training (hours)



USMC: Cyberspace Operations Officer (1700-series)													
	Leadership & Soft Skills	Individual Warrior Skills	Service/Joint Mission (Non-Cyber)	Military Problem Solving	Security Studies	RF Transmission Systems	DoDIN	DCO	OCO	Programming /Scripting	Intel Suport to Cyber Ops	Cyber/IT Planning	Service Apps & Systems
TBS	112	112	224	0	0	0	0	0	0	0	0	0	0
BCOC (602)	0	0	40	40	0	96	240	0	0	0	0	0	0
EWS	162.5	17.5	675	105	0	0	0	0	0	0	0	0	0
COOC (1702)	0	0	0	0	0	0	329.7	48	448	80	8	72	0
MCSC	140	0	92	168	204	0	0	0	0	0	0	0	0
Total	414.5	129.5	1031	313	204	96	569.7	48	448	80	8	72	0

Source: Author's Original Work

Chapter 6

Comparative Analysis of Cyberspace Officer Force Development

The previous three chapters examined how the United States Air Force, Army, and Marine Corps organize and develop their cyberspace officers within the context of their specific service institutional constructs. This chapter will examine the similarities and differences between service approaches to cyberspace officer development and suggest some reasons for why the similarities or differences exist. This chapter will especially focus on how the similarities and differences effect or apply to USAF cyberspace operations officers.

This chapter will follow the same analytical framework utilized in the previous three chapters: organizational, occupational specialties, service developmental focus, and chronological officer force development (subdivided into training/education and experience). The final analytical section of this chapter will present overarching themes and conclusions arising from this research. The results of this chapter's comparative analysis will inform implications and recommendations for the United States Air Force cyberspace office development in the conclusion chapter.

Organizational Constructs

The USA and USMC similarly organize as compared to the USAF. The differences in internal service organizational constructs directly influence officer cyberspace occupational field force development from a training and experiential lens. The two major ways the services differ involve alignment of their operational and sustaining organizations, and the organization of *staffs* within their services.

The USA and USMC both internally divide their services into operating (aka warfighting) and sustaining organizations. This division is not based upon occupational specialty, but on the purposes of the forces (e.g. an Army signal officer may serve in an assignment in the operating or sustaining organizations). The division between operating and sustaining forces allows the Army and Marines to better focus on their primary warfighting missions. The USA and USMC operating force home-station mission is primarily to train. The sustaining organizations focus on everything that provides the operating forces what they need: from acquisitions and professional military education through installation/garrison services and support.

Within the Air Force, flying squadrons and certain other expeditionary units' primary focus is training, similar to the Army and USMC's operating forces. However, the USAF treats installation support as part of its deployable capability. This difference is due to how the Air Force fights from installations due to the requirements to launch, recover, and maintain aircraft, to include hosting all supporting functions. The challenge is that many of these supporting organizations within the USAF do not have the luxury of a 100% training mission. They have a home-station mission to provide installation capabilities. This dual-duty requirement is a challenge for the majority of USAF cyberspace organizations that must balance their roles as part of the operational air force (train and prepare to deploy) with their role as a sustaining force (installation support).

A second key difference between Army and USMC organizational constructs as compared to the USAF is how they organize staff functions at the tactical echelon. The USA and USMC provide their battalion echelons and higher with full S/G-staffs in the standard J-staff model. Thus, tactical/operational staff duty in a battalion involves many of the same functions and operational and planning processes found in every higher echelon. The only major difference is in scope and scale of each ascending staff.

A Marine officer can look at an Army operating force organizational chart and understand the roles and responsibilities of each staff and command echelon and vice versa Army for the USMC. Both can also look at a J-staff organization chart for a joint organization and completely understand the roles, responsibilities, and interplay between J-staff functions as they have experience in nearly identical organizational constructs during their own tactical staff duty time. The Army's planning methodology, MDMP, and USMCs planning methodology, MCPP, are virtually the same as JOPP.

The USAF organizes its tactical staffs differently than the USMC and USA numbered staff structure. The USAF organizes differently between wing staff agencies, group staff functions, and dissimilar squadron-level organizations with differing organizations and processes depending upon type of squadron.[1] The internal operational and planning processes differ not only between echelons, but between same-echelon units with different missions.

[1] Air Force Instruction (AFI) 38-101, *Air Force Organization*, 31 January 2017, 38.

Despite all the differences in service organizational constructs, similarities exist between services in certain types of cyberspace organizational constructs.   The three services each have a general officer led cyberspace-focused command with subordinate cyberspace operations-focused missions. Secondly, the national and cyber mission force team constructs mirror across services.   USCYBERCOM establishes the standard organizational constructs of these teams across all services, thus an Army cyber protection team appears identical to a USAF team. The only major organizational differences in these cyberspace operations-focused organizational constructs are higher than the team level: a given service may wrap the team or teams in more common service organizational constructs. For example, the USAF places its cyber mission teams within USAF squadrons for organize, train, and equipping purposes.   With this contextual understanding of the differences of service organizational constructs; the next section analyzes the services' stated developmental focus areas.

Occupational Specialties

The major differences in cyberspace occupational specialties between the services align along the categorization of officers and the military occupational specialties themselves. The categorizations include line, unrestricted, restricted (limited duty officers), and warrant officers. The latter discussion focuses on the occupational specialties within the cyberspace-related fields.

The three services use different categorizations for its active duty officers within cyberspace-related fields. The USAF only uses the line, commissioned officer categorization. The United States Army utilizes two categorizations: regular commissioned officers and warrant officers. The USMC uses three categorizations: unrestricted, restricted (limited duty officers), and warrant officers.

The USA and USMC utilize the limited duty officer and warrant officer programs to enable officers to focus on their occupational specialty for an entire career, while the regular/unrestricted/line officer career paths include progression to higher echelons of command and leadership. The "technical" officer programs present advantages to the USA and USMC as their officers build deep tactical, operational, and occupational/technical skills, knowledge, and abilities in a domain (cyberspace) that constantly evolves. This focus does not mean the regular/unrestricted officers do not maintain proficiency in their primary occupation, however the service expects these officers to balance and broaden their scope to include larger institutional challenges and leadership positions over a career. The USAF's institutional lack of another "technical" categorization such as limited duty officers or warrant officers generates implications covered in the conclusion of this paper.

Aside from officer categorization differences, the three services have different cyberspace-related officer military occupational specialties. The USAF currently has a single officer cyberspace occupational field: the 17DX *cyberspace operations* officer. The USAF does have a 17SX *cyberspace warfare* specialty designator for those officers actively serving in positions aligned to offensive and defensive cyberspace operations; however, this distinction does not require a separate occupational field. Since 2014, the USA utilizes two officer occupational specialties: 25A *signal officer* and 17A *cyberspace operations officer*. The USMC uses the 600-series *communications officer* specialty, but in 2018, the Corps initiated the establishment of an additional 1700-series *cyberspace officer* specialty.

The different cyberspace occupational specialties influence the comparison of officer force development models. The multiple officer occupational career fields explain why the USA and USMC focus their traditional signal and communications officer force development on providing communications capabilities to their operational warfighting arms to include DoDIN operations, RF transmission systems, and service applications and systems. Likewise, the newer cyberspace specialties focus specifically on offensive and defensive cyberspace operations both aligned to USCYBERCOM and to support service-specific missions.   These different focuses explain why occupational training and education emphasize certain themes in their curriculum and provides insight into how the USAF balances providing the full scope of cyberspace capabilities in one force development model.

Developmental Focus Areas

All three services state relatively-generic concepts of what they value institutionally (and occupationally) for their officer development. Chapters three through five included research on the service developmental focus areas to provide context for their officer force developmental models. However, the broad generality of the concepts does not lead to additional insights. Arguably, one service could likely change a word or two in the developmental focus areas and values from another service, and these focus areas would equally apply. The true challenge for the services is translating these focus areas from word to deed: taking theory and building deliberate training, education, and experiential opportunities that fulfill it. As the following chronological comparative analysis section will highlight, the USA and USMC demonstrate the value they place in their stated developmental focus areas by emphasizing them in actual training/education curriculum and key developmental experiences. The USAF unfortunately relies much on ad hoc and/or individual leader development to achieve its developmental focus areas vice embedding the competencies in broader training/education and experience.

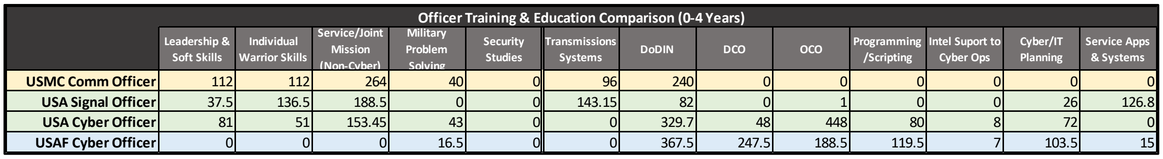
Chronological Analysis

This section will compare the services by analyzing their chronological career periods of training/education and experience, highlighting major takeaways from each developmental period in a career. The section will compare how the services train and educate their cyberspace officers throughout a career to not only build occupationally competent officers, but more importantly, to build effective joint, multi-domain leaders. The takeaways from this section inform overall conclusions regarding the service force development models, largely critical of the USAF force development model.

Years 0-4 (2nd Lieutenant – Captain)

Training and Education (0-4 years). As table 27 illustrates, the three services each approach training differently during the initial four years of an officer's career. While all three services provide initial occupation-specific curriculum to their officers, only the USA and USMC provide institutional training and education during the first 4 years. The Army and Marine Corps both focus institutional training and education on leadership and to understand how their respective service executes its core missions. The Air Force, on the other hand, focuses its initial officer training and education primarily on occupational knowledge, skills, and abilities; largely relying on pre-commissioning training, on-the-job experience, and local mentors to develop leadership skills and understanding of larger Air Force missions and leadership.

Table 27. 0-4 -Year Training & Education Comparison (hours)



Officer Training & Education Comparison (0-4 Years)													
	Leadership & Soft Skills	Individual Warrior Skills	Service/Joint Mission (Non-Cyber)	Military Problem Solving	Security Studies	Transmissions Systems	DoDIN	DCO	OCO	Programming /Scripting	Intel Suport to Cyber Ops	Cyber/IT Planning	Service Apps & Systems
USMC Comm Officer	112	112	264	40	0	96	240	0	0	0	0	0	0
USA Signal Officer	37.5	136.5	188.5	0	0	143.15	82	0	1	0	0	26	126.8
USA Cyber Officer	81	51	153.45	43	0	0	329.7	48	448	80	8	72	0
USAF Cyber Officer	0	0	0	16.5	0	0	367.5	247.5	188.5	119.5	7	103.5	15

Source: Author's Original Work

Upon commissioning, the USA initially sends its signal officers to their 16-week Signal Basic Officer Leadership Course (S-BOLC) and sends cyberspace operations officers to the 40-week Cyber Basic Officer Leadership Course (C-BOLC). These courses incorporate both the occupational competencies required to be an Army signal or cyberspace operations officer, but also provides common foundational army institutional competencies of tactical leadership procedures (which includes leadership and planning), army functions, and even the use of their individual weapon. While this course by no means makes these signal and cyberspace officers ready to lead combat arms forces, it does provide foundational Army-centric mission comprehension so that these officers can better understand their role and how they enable the larger Army mission sets. The signal officers then proceed to relatively common first assignments in the operational army.

The US Marine Corps takes an even more deliberate approach to ensuring their Marine officers understand how the Marines Corps executes its operational missions. By sending all unrestricted officers to complete The Basic School (TBS) immediately after commissioning, these officers undergo a common foundational experience and become provisionally-qualified to lead the most basic of USMC fighting echelons: the Marine Rifle Platoon. With this common foundation, the officers then track to their specific occupational specialties. During the 11-week Marine Basic Communication Officer Course, Marine communications officers build upon their foundational TBS experience with a specific focus on how communications systems enable Marine warfighting in the operational force.

The Air Force takes a significantly different approach to young officer development than the Army and Marine Corps. The USAF no longer provides a common institutional training or education course for its lieutenants, instead focusing entirely on occupational training and education during the first four years of service. The reasons for this fall on the fact that the primary employer of combat effects for the USAF are its rated officers (pilots, navigators, and air battle managers) who require lengthy training pipelines to become qualified and experienced. These training pipelines take up the majority of their first four years of service. Thus, the USAF focuses on resourcing its occupational training and education programs; each of them determines what knowledge, skills, and abilities their given specialty requires. Thus, the USAF cyberspace occupational field trains its new officers through an occupational lens, relying on pre-commissioning education and the first duty assignments to teach the officers about how the USAF executes is core missions, to include cyberspace's role within them.

Setting aside the institutional training differences, all three services provide occupational training to their cyberspace officers. The USMC BCOC and USA S-BOLC focus on the core communications capabilities required for their primary operational forces to execute their missions. Generally, these systems rely on RF transmission systems, DoDIN capabilities, and certain service-specific applications and systems and their curriculum reflects this in its emphasis. On the contrary, the USA cyberspace operations officer training curriculum does not focus at all on core Army transmission systems and mission applications. It instead focuses on the knowledge, skills, and abilities to execute offensive and defensive cyberspace operations, requiring foundational curriculum in DoDIN operations. The Army derives many of these training standards from the USCYBERCOM Joint Cyberspace Training and Certification Standards (JCT&CS) that govern all members assigned to cyber mission force teams.

USAF Undergraduate Cyberspace Training (UCT) is a 6-month course that heavily focuses on the foundational technical and occupational side of being a cyberspace officer. The UCT curriculum does not deliberately emphasize the majority of USAF institutional competencies such as leadership or understanding of the USAF's core missions. Instead, it focuses on occupational competencies with a balance between DoDIN operations, DCO, OCO, and some focus on service-valued systems. Interestingly, the course does not spend any measurable time on RF transmission systems, yet the majority of the USAF's operational missions rely on RF transmission systems.

Upon completion of UCT, USAF cyberspace operations officers receive assignments. Depending upon the assignment, many of the officers will continue on to more advanced and/or specialized training such as the Cyberspace Warfare Operations (CWO) course analyzed in this paper. Thus, though UCT is shorter in duration than the Army's C-BOLC, USAF officers heading to DCO and OCO units receive additional training that begins to satisfy USCYBERCOM JCT&CS standards prior to arriving at their operational unit.

Finally, the USA and USAF initial cyberspace-related occupational training curriculum provides information assurance certifications for its officers to satisfy DoDD 8140/8570 requirements. The USMC does not deliberately provide these certifications as part of its formal curriculum but does afford officers other opportunities to take the certification tests outside of their formal courses. The primary USMC exception are USMC officers who later (as Captains) laterally transfer to the 1700-series cyberspace occupational field. These USMC officers earn DoDD 8140/8570 certification through the USA's Cyberspace Operations Officer Course (COOC).

Key Duties/Experience (0-4 years). Upon successful completion of their requisite cyberspace occupational training, officers from the three services move to their first duty assignments. While some officers continue qualification training in their first duty assignments, this research focuses on the key developmental experiences during these first four years. The preponderance of Marine Communications officers depart BCOC and join Marine Expeditionary Force units, serving as Assistant S6s in maneuver battalions or Assistant Communication Platoon Leaders, eventually leading to key developmental duty as a Platoon Leader. Thus, these Marine officers embed in the primary warfighting organizations of the USMC, focusing their efforts and experience on enabling combat effects during garrison training and on deployments. Only after four years of proven experience in the warfighting arm of the USMC and after selection for retention through he Career Designation Board are Marine Communications Officers afforded the ability to continue as Communications Officers or apply to crossflow into the USMC Cyberspace Operations branch. Thus, USMC communications and cyberspace officers both have a common and foundational experience and understanding of Marine warfighting prior to moving into other echelons, organizations, and mission sets.

Like their USMC communications brethren, USA signal officers primarily join operational Army units with key developmental duty as a platoon leader at some point during their first four years. USA cyberspace operations officers follow a slightly different track. These officers build core technical (occupational) skills within their units, especially if assigned to a cyber mission force (CMF) team. Army cyberspace officers may have the opportunity to serve as a platoon commander, but the primary development positions in the first 0-4 years focus on become occupational experts vice honing larger leadership experiences. While some Army cyberspace operations officers may not support operational Army missions for their first few years of service, they still have a foundational understanding through their Basic Officer Leadership Course of what it means to be an Army officer and warfighting concepts beyond the cyber domain.

The Air Force defines no specific key developmental duty for cyberspace officers, thus experiences for these officers during the first four years of service vary. USAF cyberspace officers assigned to CMF teams may focus on technical and tactical skillsets similar to Army cyberspace operations officers. USAF cyberspace officers assigned to a base communications squadron, combat communications squadron, or air and space communications squadron will focus more on developing leadership experience like a platoon leader.

Due to the disparity in initial experiences, the USAF cyberspace operations officer force development model either deliberately or accidently relies on several means to develop leadership and understanding of core USAF missions. An officer may gain direct leadership experience and understanding of a supported USAF core mission at their first unit. Aside from this dedicated experience, developing leadership competencies and Air Force core missions understanding depends upon the investment of their local leadership and mentors, or self-driven self-development. Thus, the USAF cyberspace operations officer force development model does not build a common experience nor mutual understanding of USAF core missions.

Years 4-10 (Captain – Major)

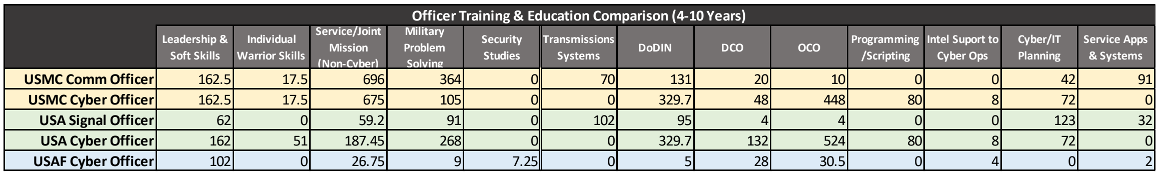
Training and Education (4-10 years). The three services all provide formal institutional professional military education (PME) and occupational training during the 4-10 year portions of a career. The USMC and USAF both bring all line/unrestricted officers together for PME, whereas the USA provides this level of PME within occupational-affiliated courses. The major differences are that the USAF's resident captain-level institutional PME lasts 6.5 weeks versus the Army's captains career courses that includes 13 weeks of common core institutional education, and the USMC's expeditionary warfare school that lasts 37 weeks. Occupationally, the USAF provides common cyberspace education for 3 weeks (Cyber 200), the Army 7-9 weeks (within respective captains' career courses), and the USMC provides 16 weeks (4 weeks in EWS and 12 weeks during MCPC).

Cumulatively, the USMC invests 57 weeks, the USA invests 20 to 25 weeks, and the USAF invests 9.5 weeks of formal institutional and occupational education into their cyberspace occupational fields during this time. Granted the USAF provides many more training opportunities specific to a given cyberspace mission set or additional planning courses, but these courses remain "just in time" training for segments of the cyberspace officer population vice a deliberate part in the development of all cyberspace officers. Therefore, the USAF falls behind its sister services in formal institutional and occupational education across the force during the 4-10-year period.

Beyond the overall total time investment in its cyberspace-affiliated officers during the 4-10-year career time periods, the thematic occupational topics these curriculum hours focus on remain illustrative of what each service values. Table 28 outlines the hours of curriculum for service courses during the 4-10-year window. Occupationally, the USMC communications officer and Army signal officer curriculum continue to emphasize RF transmissions systems and DoDIN operations, but both offer familiarization with offensive and defensive cyberspace operations. Their cyberspace officer course curriculums more heavily focus on offensive and defensive cyberspace operations. The Air Force only provides 3 weeks of occupational education to all its cyberspace operations officers during Cyber 200. With the limited time, the curriculum provides knowledge baselining across DoDIN operations, DCO, and OCO. Despite the

USAF spending significantly less time on community-wide education and training as compared to sister services, the USAF cyberspace occupational joins only intelligence and space operations occupational fields within the USAF that provide standardized occupational education opportunities to their entire officer occupational field.

Table 28. 4-10 -Year Training & Education Comparison (hours)



	Officer Training & Education Comparison (4-10 Years)												
	Leadership & Soft Skills	Individual Warrior Skills	Service/Joint Mission (Non-Cyber)	Military Problem Solving	Security Studies	Transmissions Systems	DoDIN	DCO	OCO	Programming /Scripting	Intel Suport to Cyber Ops	Cyber/IT Planning	Service Apps & Systems
USMC Comm Officer	162.5	17.5	696	364	0	70	131	20	10	0	0	42	91
USMC Cyber Officer	162.5	17.5	675	105	0	0	329.7	48	448	80	8	72	0
USA Signal Officer	62	0	59.2	91	0	102	95	4	4	0	0	123	32
USA Cyber Officer	162	51	187.45	268	0	0	329.7	132	524	80	8	72	0
USAF Cyber Officer	102	0	26.75	9	7.25	0	5	28	30.5	0	4	0	2

Source: Author's Original Work

Institutionally, the curriculum weights of effort during the 4-10-year career period closely mirror the weight of effort during the 0-4-year period. As illustrated in table 28, the USMC and USA invest significant curriculum and time focusing on leadership, service/joint mission, and military problem solving than the USAF. Squadron Officer School is the first institutional education the USAF provides its officers. Relative to its shorter duration (6.5 weeks), the course dedicates significant time to leadership and team-building. However, the remainder of the course serves more as method of normalizing general USAF knowledge across the various occupational fields. The lack of emphasis on military problem solving demonstrates the USAF does not value educating all Air Force captains in these fields. An examination of the USAF organizational construct and key developmental duties these captains will experience during the 4-10-year point in their careers leads one to understand why the USAF currently does not more strongly emphasize formal operations and planning processes during SOS. The service does not require most of its officers to utilize JOPP or similar methodologies until later in their careers, thus familiarization with the processes suffices.

Key Duties/Experience (4-10 years). Experientially during the 4-10-year career periods, all three services emphasize O-3 level leadership as key developmental position for their officers, including the cyberspace/signal/communications occupational fields. The USMC and Army both emphasize company command that includes G-Series as

Company Commander. USAF officers also complete O-3 leadership as flight commander or equivalent, however the Air Force does not grant these officers G-series orders. Therefore, many Marine and Army cyberspace-affiliated officers receive more direct experience in exercising UCMJ authorities 5-10 years sooner than their USAF counterparts. The G-series experience provides the Corps and Army officers more repetitions at making tough commander-level decisions such as UCMJ corrective actions, better preparing them to do the same as future battalion commanders. Their Air Force counterparts typically gain exposure to G-series authorities at the 12-16-year points in their career as squadron commanders.

Years 10-15 (Major – Lieutenant Colonel)

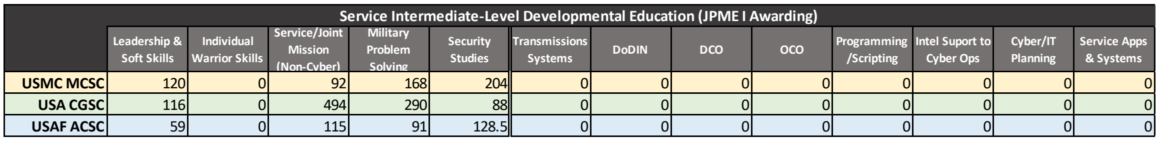
Training and Education (10-15 years). The three services all provide formal institutional professional military education (PME) during the 10-15-year portions of a career in the form of their intermediate level command and staff colleges. Each school shares similarities across curriculum, but also retain significant differences.   All three intermediate-level PME programs bring together members from all occupational fields, thus are their core curriculum does not specialize occupationally.   Each program satisfies JPME I requirements for its students and spends some amount of time on leadership and security studies which, as defined in this essay, includes strategy, theory, international relations, and military history. All three services dedicate similar weight of effort to leadership and other soft skill education.

At table 29 illustrates, the Marines and especially Army diverge from the Air Force program in that Marine and Army curriculum focuses on the interrelated topics of military problem solving. The USA collectively dedicates 290 hours to these topics, the USMC dedicate 168 hours, and the USAF only 94 hours. Looking more deeply into the curriculum, the major differences are in the number of practical exercises the students spend using the military decision and planning methodologies. The USA executes five practical exercises, the USMC four, and the USAF a single exercise.[2] The intent of the

[2] "U.S. Army Command and General Staff College Curriculum Class 2015"; "USMC CSC AY17-18 First Semester Calendar"; "USMC CSC AY17-18 Second Semester Calendar"; Lawnicsak, "Joint Warfighting: 'How We Fight' Syllabus AY 18."

exercises is to provide repetitions and continually improve abilities to lead and participate in these processes. More repetitions result in more experience and understanding.

Table 29. Service Intermediate-Level Developmental Education (hours)



Service Intermediate-Level Developmental Education (JPME I Awarding)													
	Leadership & Soft Skills	Individual Warrior Skills	Service/Joint Mission (Non-Cyber)	Military Problem Solving	Security Studies	Transmissions Systems	DoDIN	DCO	OCO	Programming /Scripting	Intel Suport to Cyber Ops	Cyber/IT Planning	Service Apps & Systems
USMC MCSC	120	0	92	168	204	0	0	0	0	0	0	0	0
USA CGSC	116	0	494	290	88	0	0	0	0	0	0	0	0
USAF ACSC	59	0	115	91	128.5	0	0	0	0	0	0	0	0

Source: Author's Original Work

Beyond the institutional PME schools, the USAF remains the only service with a dedicated, career-field wide cyberspace education course during the 10-15-year point of the officer's career. Cyber 300 is only a 2-week program, yet the advantage it provides is a mechanism for officers (and senior enlisted and civilians) from different USAF cyberspace organizations and experiences to come together for a common educational experience.

Key Duties/Experience (10-15 years). Experientially during the 5-10-year career periods, the services emphasize similar key developmental positions. The Army and USMC emphasize battalion executive officer or operations officer (S3) for officers during this period. Within the USAF, the key positions differ between career fields. For many occupational fields, director of operations (DO) is a key developmental duty similar to XO or S3. For Air Force cyberspace operations officers, officers may fill DO positions or one of 47 O-4 level squadron commands. Furthermore, and like its sister services, O-4s may serve in leadership positions on cyber mission force teams.

Though the key developmental positions across the services may be similar, the actual experiences may differ. The USMC and USA officers in XO or S3 positions lead the planning and manage the execution of military operations within their organizations, using standard military problem-solving methodologies. Furthermore, they must interface and integrate with other warfighting functions (and associated occupational fields) within their battalions or brigades. For Air Force officers serving as DOs or O-4 squadron commanders, the USAF uses service-centric or occupational field-centric processes to plan and execute operations. In practical terms, this means the USMC and

USA officers continue to build upon over 10 years of training/education and experience with operational and planning processes closely aligned to their equivalent joint processes. USAF officers, with some exceptions such as those aligned to sister-service organizations, do not reinforce the joint planning methodologies learned in their intermediate-level PME.

Years 15-20 (Lieutenant Colonel – Colonel)

Training and Education (15-20 years). Like the 10-15-year career period, the three services each have senior-level professional military education programs (residence and correspondence), but only the USAF has an occupational cyberspace course. As stated in chapters 3-5, this paper does not analyze the specific curriculum within these courses as they relatively align in emphasis and scope. Combine this similarity with the fact that only a limited percentage of each services' officers can attend in-residence means that this analysis does not substantially contribute to a comparative examination of how the services develop their cyberspace-affiliated officers.

Beyond the institutional PME schools, the USAF remains the only service with a dedicated, career-field wide cyberspace education course during the 15-20-year point of the officer's career. Cyber 400 is short course, yet the advantage it provides is a mechanism for officers (and senior enlisted and civilians) from different USAF cyberspace organizations and experiences to come together for a common educational experience. Furthermore, it provides a strategic level education on Chief Information Officer roles and responsibilities through a distance education National Defense University course. While Cyber 400 currently remains a USAF-only course, the other military services have voiced interest in the course in the spring of 2018. Thus, the USAF is working with the National Defense University and the services to transform Cyber 400 into a joint course by 2020.[3]

Key Duties/Experience (15-20 years). Experientially during the 15-20-year career period, the services all emphasize O-5 command and joint experience positions. Though the key developmental positions across the services may be similar, the actual command experiences differ. The USMC and USA officers in battalion commanders have subordinate S-staffs spanning the (joint) warfighting functions. The battalion

[3] Lt Col Joseph Wingo, chief, Cyber Force Development, to the author, e-mail, 22 April 2018.

commanders lead their battalions using standard operations and planning methodologies similar to their joint counterpart. Furthermore, the battalion commanders may be responsible not only for its operational arm, but also maintenance, logistics, protection, and communications. USMC and USA communications, signal, and cyberspace battalions may not have the complete span of different subordinate occupational units/missions within their battalions/squadrons compared to a combat arms battalion. However, the cyberspace-related battalions still must address many of the warfighting functions.

With a few exceptions, USAF squadron commanders do not have the same diverse scope as their USMC and USA peers.   While USAF squadron commanders share similar experiences wielding G-series UCMJ authority, their unit functions and processes differ not only in comparison to other services, but between different types of USAF squadrons. Procedurally, USAF doctrine and reality do not result in units using joint planning methodologies. Functionally, a flying squadron commander is not responsible for aircraft maintenance, logistics, or security. Other squadrons provide these functions due the USAF organizational construct. Similarly, a USAF cyberspace operations squadron commander does not have authority over the security forces personnel defending unit facilities nor the electrical power production capabilities and personnel critical to their cyber weapon systems. The tangible result is that USMC and USA O-5 battalion commanders gain tangible experience and perspective outside their occupational field while USAF officers do not command multiple functions until O-6 level command several years later.

Overall Conclusions

Each of these military services aims to incorporate by-law joint officer requirements, United States Cyber Command (where applicable), and service-specific knowledge, skills, and abilities to their cyberspace officer force development models. Each service uses a framework to accomplish the desired officer development with varying degrees of success.

The Army and Marine Corps deliberately train and educate their force at a younger age and couple this training with reinforcing training and experiences throughout a career to build occupationally competent officers, but more importantly, to build effective joint, multi-domain leaders. The Air Force, due to its myriad of specialties and expectations of officers during their career, appears less deliberate when one examines their force development models. The USAF cyberspace community is internally experiencing these challenges as it attempts to operationalize like rated aircrew (e.g. trigger-pullers on keyboard for first 6 years vice leaders of large teams) while much of the community focuses more heavily on leadership at a younger career point.

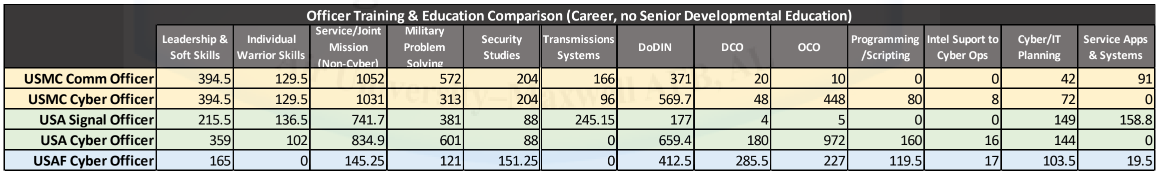
All three services have a force development model that produces pools senior leaders and joint-qualified officers. However, satisfying requirements for being joint, multi-domain leaders does not equate to effective joint, multi-domain leaders. The Army and USMC deliberately train and educate their force on institutional competencies earlier in their careers (within first year) and couple this training/education with reinforcing experience to build what results in joint, multi-domain leaders. The Air Force, due to its myriad of specialties and expectations of officers during their career, is less deliberate. While the USAF retains standard key developmental duties (flight command, squadron commander), each occupational field has distinct force development models for training, education, and non-command experiences.

Training and Education. The most significant finding in this paper is not that the services occupational train their cyberspace officers significantly differently. While there are differences in where each occupational field focuses their cyberspace training, the reasons tie directly to what each service expects their given occupational field to do. What is most compelling is the disparity between the USMC and USA and the USAF with regards the number of hours the spend training and educating their cyberspace, communication, and signal officers in the institutional competencies of leadership, service/joint missions, and military problem solving. Table 30 illustrates the cumulative hours of training and education by thematic variable for the first 20 years of a given officer’s career, assuming a similar officer from each service completes all their own service in-residence PME through the intermediate level.

The disparities immediately stand out. The closest comparison to the Air Force cyberspace officers in *leadership* are Army signal officers (165 hours versus 215.5 hours). The closest comparison to the USAF cyberspace officer in *service/joint mission* focus are Army cyberspace officers (145.25 hours versus 681.45 hours). The closest comparison to USAF cyberspace officers in *military problem solving* are the USMC cyberspace officers (121 hours versus 313 hours). To put everything in perspective, a Marine communications officer who completes all of his or her service PME (through intermediate-level) will have 394.5 hours *leadership* (58.2% more than USAF), 1,052 hours *service/joint mission* focus (86.2% more than USAF), and 572 hours of *military problem solving* (78.8% greater than USAF).

For cyberspace occupational field officers serving a 20-year career and attending their service PME through the intermediate level, a USMC officer spends upwards of two-thirds of their formal training/education focused on institutional competencies. The equivalent USA officer will spend half to two-thirds time on institutional competencies. The USAF officer only spends one-third. Remove intermediate-level PME, and the USAF officer exposure to institutional competencies drops from 33% to 13% of total formal training and education. Their peer USMC and USA officers retain a 32-72% weight of effort focus towards the institutional competencies.

Table 30. Career Officer Training & Education Comparison, no SDE (hours)



	Officer Training & Education Comparison (Career, no Senior Developmental Education)											
	Leadership & Soft Skills	Individual Warrior Skills	Service/Joint Mission (Non-Cyber)	Military Problem Solving	Security Studies	Transmissions Systems	DoDIN	DCO	OCO	Programming /Scripting	Intel Suport to Cyber Ops	Cyber/IT Planning	Service Apps & Systems
USMC Comm Officer	394.5	129.5	1052	572	204	166	371	20	10	0	0	42	91
USMC Cyber Officer	394.5	129.5	1031	313	204	96	569.7	48	448	80	8	72	0
USA Signal Officer	215.5	136.5	741.7	381	88	245.15	177	4	5	0	0	149	158.8
USA Cyber Officer	359	102	834.9	601	88	0	659.4	180	972	160	16	144	0
USAF Cyber Officer	165	0	145.25	121	151.25	0	412.5	285.5	227	119.5	17	103.5	19.5

Source: Author's Original Work

Key Duties/Experience. The key developmental duties defined by the services highlight several things. First, despite the command-related key developmental positions, command in the different services results in different experiential gains. At the O-3 level, Army and USMC company commanders have G-series orders and must focus on different occupational/functional areas as they apply to executing their primary mission. Likewise, USA and USMC battalion commanders. They additionally have S-staffs within their battalions that execute operations and planning processes that mirror higher echelon and joint processes. Thus, the commanders and their staffs inherently learn how to operate the proverbial big rocks of joint processes to include understanding of joint warfighting functions.

As stated during the earlier chronological block comparative analysis, USAF command experiences differ from the Army and USMC. The O-3 level flight command for a cyberspace operations officers may include ADCON/OPCON/TACON of their force to execute their mission, but do not have G-series UCMJ authority. A flight commander in a CMF cyber operations squadron may only have ADCON of their flight as their personnel fill CMF teams who fall under USCYBERCOM or other COCOM authority. This latter model aligns more closely to the USAF flying squadron model. Flying squadron flight commanders have ADCON of their forces, but their subordinates belong to the Director of Operations or another C2 chain during mission execution.

Additionally, at the squadron command level, Air Force squadrons (nor groups or wings) do not organize with an A/J-staffs underneath them. Therefore, the USAF-centric or occupational-type squadron-centric organization structure does not inherently map to a joint structure and the operational and planning processes differ. Nor do commanders at this level have direct authority or responsibility for the supporting warfighting functions that enable their mission.

The Army and USMC view staff experience differently than the USAF. The Army and Marine Corps hold battalion and higher-level staff experience in the operational forces as key developmental experiences. Staff for the USA and USMC teaches and reinforces understanding of how each service executes its operational missions while building depth of experience in standard military problem-solving methodologies. The USAF views staff experience differently.

USAF prioritization of key developmental staff duty completely opposite of its sister services. The service does not identify any staff duty as a key developmental position except to complete joint qualification experience at some point in the later field grade years. Furthermore, the USAF prioritizes staff duty in organize, train, and equip organizations such as Joint Chiefs of Staff, Headquarters Air Force, and its Major Commands over actually warfighting staffs like numbered air forces. Staff duty at the wing level or lower does not count as key developmental duty, except in certain circumstances (Wing Chief of Safety or Wing Weapons and Tactics officer).

The combination of training and education with immediate practical application in operational forces ensures the USA and USMC best posture their cyberspace-affiliated officers to develop not only the knowledge, skills, and abilities their respective service values, but prepares them for future leadership as joint, multi-domain leaders. The USAF's overarching officer force development model and specifically the cyberspace operations officer force development model do not deliberately develop officers into joint, multi-domain leaders. The USAF exquisite individual career management of a select few and/or the self-determination of an individual officer. If the CSAF truly intends to build joint, multi-domain leaders across the USAF, then we cannot leave the products up to chance. The USA and USMC officer force development models seem to better align with the CSAF's vision of building better joint leaders and teams.

Chapter Summary

The comparative analysis of USAF, Army, and USMC cyberspace occupational field force development models illustrated the major shortfalls in USAF cyberspace officer force development. The use of an example case will best summarize the findings in this paper and prepare for a discussion of implications and recommendations in the conclusion. The example compares a USMC communications officer, an Army signal officer, and an Air Force cyberspace officer at the 12-year points of their career and who have yet to (or will not) attend an intermediate-level developmental education program. This example captures the majority of the officers in the services as the majority of cyberspace officers in the USAF and USMC do not attend an in-resident intermediate-level PME program. We also use this example as the officer at this career point represents the transition between the CGO to FGO ranks. The subsequent few years may well determine the member's effectiveness in command, on staff, or in a joint organization executing real-world operations. Therefore, we will compare the preparation between the average 12-year Marine communication officer, Army signal officer, and USAF cyberspace operations officer in the institutional competencies of leadership, service/joint operations, and military problem solving.

The USMC force development model provided the Marine communications officers 274.5 hours leadership, 960 hours of service/joint mission focus, and 404 hours military problem-solving training hours coupled with at least three years direct leadership (2 years on G-series orders) and several years of battalion/squadron or higher operating force staff experience. The Army signal officer experienced 99.5 hours leadership, 247.7 hours of service/joint operations, and 91 planning training hours coupled with similar key developmental experience as the Marine.

Couple these training and education hours with very deliberate key developmental experience as both G-series commanders as a captain and deliberate tactical operating force staff duty (battalion or higher). The results of these deliberate developmental models are officers who, on-average, could build aptitude in operations and planning processes as a part of larger service and joint missions that carry them through their field grade years.

Counter the USMC and Army officers to the 12-year point in an Air Force cyberspace operations officer's career. The USAF cyberspace operations model over the same timeframe generates at most 102 hours leadership, 26.75 hours service/joint mission focus, and 25.5 hours military problem-solving methodologies. Of note is that the majority (17.5 hours of 26.75) of military problem-solving training come in occupational training opportunities vice Air Force-wide institutional courses. Compared to the Army officer, the leadership emphasis is equivalent in the USAF (99.5 to 103 hours respectively), but the USAF only spends 10.8% time on service/joint mission instruction and 28% of the hours to military problem solving relative to the Army. Compared to the Marine Corps communications officer, the disparity is even greater as the USAF provides 37.2% training hours on leadership (102 versus 274.5), 2.9% time spent on understanding the service/joint mission (26.75 versus 1,052), and 17.6% of the hours learning military problem solving (25.5 versus 572).

Meanwhile, the Air Force cyberspace operations officer's personal experience is varied and may or may not reinforce the limited training and education received in these three areas. The officer will likely have completed O-3 level leadership (flight command), but they do not receive G-series orders nor the responsibility and experience that brings. Additionally, the O-3 leadership experience varies as the position could be in anything from a warfighting-centered combat communications unit, to an installation support unit enabling the garrison operational mission, to a cyber mission force team supporting a sister service or combatant command. The staff experiences of its cyberspace operations officers' staff may be just as varied. Due to the USAF's organizational construct and institutional priorities, officers who have served on a staff at this point tend to lean more towards organizing, training, and equipping organizations such as air staff or major command staff.   Each experience brings its own development advantages and disadvantages, however institutionally the challenge is that all receive different development in understanding the service or joint mission (if emphasized at all). The USA and USMC officers in this example have years of dedicated training, education, and experience in understanding missions, warfighting functions, and operational and planning processes that virtually mirror higher echelons within their services and joint organizations. The average USAF cyberspace operations officer is a rank amateur in the same competencies, and yet may serve on a joint or service component warfighting staff within a few years.

The example of a 12-year officers exposes the disparity between developmental models of Army, USMC, and USAF cyberspace officers. Compared to the USA and especially USMC models, the current USAF cyberspace operations officer force development model does not deliberately produce officers with the comparable knowledge, skills, and abilities to effectively lead and operate within joint, multi-domain constructs.   Due to this disparity, is it any wonder that Marine and Army communications, signal, and cyberspace officers writ large are more versed than their Air Force counterparts in larger warfighting and multi-domain constructs and standard military problem solving methodologies as they step into joint staff positions or leadership positions within the 10-20 year points of their careers? It is through this lens that this paper concludes with implications and recommendations for how the USAF cyberspace occupational field can resolve these exposed gaps and challenges.

Conclusion

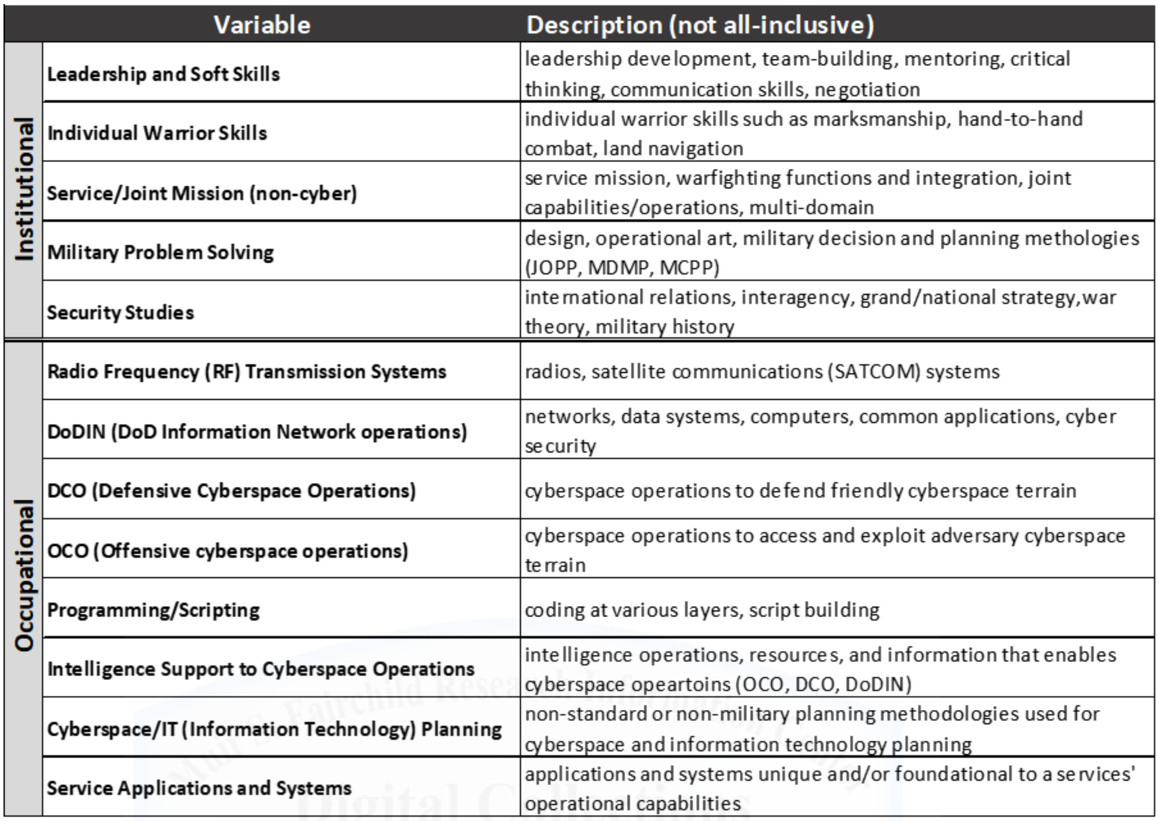
> *It's no longer enough for an Airmen to be good only at Airmanship. We must have a working knowledge of ground maneuver and maritime operations if we are to truly integrate air, space, and cyber operations in a seamless joint campaign.*
>
> David Goldfein[1]

This paper provided a comparative analysis of the current US Air Force, US Army, and US Marine Corps cyberspace-related officer force development models, seeking to identify how and why each service develops its officers to meet joint officer requirements; to be occupationally-proficient; and to be joint, leaders. The research examined the force development models of active duty, line/unrestricted officers within the three services, focusing on USAF cyberspace operations officers, US Army signal and cyberspace operations officers, and USMC communications and cyberspace officers.

The paper's analytical framework began with a review of the extra-service requirements that Federal Law, the Department of Defense, and US Cyberspace Command place upon officers in cyberspace occupational fields. The subsequent three chapters examined the three services individually, first providing a contextual understanding of internal service organizational constructs, their cyberspace occupational fields, and service-defined developmental focus areas. The three chapters then presented an analysis of each cyberspace occupational field; examining the training, education, and experiential components of the respective military service's cyberspace-affiliated officer force development models. As the different services use different formal institutional and occupational training/education course models, this paper leveraged thirteen variables (see Table 31) to delineate and codify similarly themed curriculum into hours of instruction.

[1] David Goldfein, "Air Force Association Air Warfare Symposium Keynote Speaker General David Goldfein" (address, Air Force Associate Symposium, Orlando, FL, February 23, 2018), 10, http://www.af.mil/Portals/1/documents/csaf/CSAF_AFA_Orlando-23Feb18.PDF.

Table 31. Training/education curriculum variables (unit = hours)



	Variable	Description (not all-inclusive)
Institutional	**Leadership and Soft Skills**	leadership development, team-building, mentoring, critical thinking, communication skills, negotiation
	Individual Warrior Skills	individual warrior skills such as marksmanship, hand-to-hand combat, land navigation
	Service/Joint Mission (non-cyber)	service mission, warfighting functions and integration, joint capabilities/operations, multi-domain
	Military Problem Solving	design, operational art, military decision and planning methologies (JOPP, MDMP, MCPP)
	Security Studies	international relations, interagency, grand/national strategy,war theory, military history
Occupational	**Radio Frequency (RF) Transmission Systems**	radios, satellite communications (SATCOM) systems
	DoDIN (DoD Information Network operations)	networks, data systems, computers, common applications, cyber security
	DCO (Defensive Cyberspace Operations)	cyberspace operations to defend friendly cyberspace terrain
	OCO (Offensive cyberspace operations)	cyberspace operations to access and exploit adversary cyberspace terrain
	Programming/Scripting	coding at various layers, script building
	Intelligence Support to Cyberspace Operations	intelligence operations, resources, and information that enables cyberspace opeartoins (OCO, DCO, DoDIN)
	Cyberspace/IT (Information Technology) Planning	non-standard or non-military planning methodologies used for cyberspace and information technology planning
	Service Applications and Systems	applications and systems unique and/or foundational to a services' operational capabilities

Source: Author's Original Work

After the individual service chapters, chapter six presented a comparative analysis across the three services, illuminating similarities and primarily differences between cyberspace officer force development models. The results of this comparative analysis result in the following conclusions and recommendations for USAF cyberspace leaders to consider as they evolve their force development models to include proposed evolutions of training, education, and experience.

Eleven Major Conclusions

The research generates eleven conclusions relevant to USAF cyberspace operations officer development. These conclusions are not only indicative of shortfalls in the USAF cyberspace officer force development model, but many reflect challenges and shortfalls in the overall USAF officer development model as evinced by the USAF's relative lack of emphasis on formal institutional competency development. Personnel involved in larger USAF force development may take lessons learned and derive their own implications from this research.

However, the focus of this paper is on the USAF cyberspace officer community. Thus, the following eleven conclusions start at the macro level and then narrow in on specific conclusions relevant to the USAF cyberspace operations officer community. Keep in mind that a core assumption of this paper is that the USMC and USA produce more qualified joint leaders than the USAF, and subsequently that their officer force development models play a key role in this joint officer production.

Overarching Conclusions:

Conclusion #1: The research shows that all service cyberspace officer force development models satisfy the extra-service requirements leveraged upon them by federal law, the DoD, and USCYBERCOM.

Conclusion #2: All three services' stated officer developmental focus areas address institutional and occupational competencies. Aside from a few service-specific areas of emphasis, the developmental focus areas are very similar across services.

Conclusion #3: A foundational part of the USMC and USA cyberspace operations officer development models is the linkage between training/education with deliberate follow-on duty experiences. The follow-on experiences reinforce learned institutional and occupational competencies to create expertise.

Conclusion #4: Across the service cyberspace officer military occupational specialties, the primary difference between each service's formal training/education is the weight of effort towards institutional competencies. The USMC most heavily weights its formal training/education toward institutional competencies, with the Army a close second, and the USAF a distant third.

Conclusion #5: Cyberspace officer occupational field structures create advantages and challenges for force development. The two cyberspace occupational fields within the USA and USMC allow each to focus their force development models on desired occupational competencies. Cyberspace and cyberspace operations officer models occupationally focus on offensive and defensive cyberspace operations. USA signal officers and USMC communications officers spend more time on their traditional roles and occupational competencies such as RF transmission systems and operational force applications and systems.

The USAF's current force development model for its single cyberspace occupational field creates disconnects between occupational training/education and experience for most of the force. Current occupational training focusing heavily on cyberspace operations (offensive, defensive, and DoDIN), yet most of organizations and positions within the USAF do not currently execute offensive and/or defensive cyberspace operations. However, evolving USAF concepts of cyberspace operations will shift most cyberspace units to providing more defensive cyberspace capabilities, which will better-align occupational training and experiences.

Training and Education Conclusions:

Conclusion #6: Despite the USA and USMC splitting their cyberspace-related occupational fields into two each, the curriculum data illustrates that both services still place weighted efforts towards the institutional competencies of leadership, service/joint missions, and military problem-solving methodologies.

Conclusion #7: The data reflects that the USMC and USA cyberspace officer force development models value institutional competency development through training/education during the first four years of service, whereas the USAF model does not. The USMC most emphasizes institutional competency development during the first four years of service, spending 61% formal training and education hours on institutional competencies. The USA is a close second, spending 25-49% of their training weight of effort towards institutional competencies. The USAF cyberspace operations developmental model only spends 2% curriculum hours on institutional competencies and this 2% occurs during occupational training courses.

Conclusion #8: Among the institutional competencies, the data reflects all three services value leadership and soft skill development over a career. However, the primary differences in weight of effort are that the USMC and USA dedicate significantly more time to understanding service/joint missions and military problem-solving than the USAF.

Conclusion #9: The USAF cyberspace operations occupational training/education curriculum does not sufficiently address radio frequency transmissions systems considering the USAF's reliance on these systems to accomplish its five core missions.

Key Duty and Experience Conclusions:

Conclusion #10: The USMC and USA cyberspace officer force development models demonstrate the value they place in practical experience. They expect their officers to leverage learned institutional and occupational competencies during duty assignments as a necessary part of solidifying expertise in the skillsets. The USAF emphasizes duty types (flight commander, etc.), but actual organizations and experiences vary widely thus do not consistently reinforce the learned competencies in formal training and education.

Conclusion #11: The USCM and USA have better developmental programs to grow joint cyberspace leaders. Both emphasize operating force experience and leadership during the first four years of service to grow future (joint) cyberspace leaders. The USMC's key developmental duty and experience for communications lieutenants in the 0-4-year period best provides the foundational experience needed to grow its officers. The USMC's emphasis on platoon leadership within the operating forces for its communications (and eventual cyberspace) officers provides a foundational understanding of MAGTF operations/missions, leadership, and problem-solving methodologies while also enabling them to directly apply occupational knowledge. The USA model echoes the USMC model for signal officers (25A) but deviates for its cyberspace operations officers (17A) due to Cyber Mission Force team requirements. USAF cyberspace operations force development model currently lacks a similar key development for officers in the 0-4-year range due to the breadth of occupational duty positions and units across the service.

Fifteen Recommendations

The eleven presented conclusions lead to fifteen specific recommendations for the USAF cyberspace operations community (senior leaders, career field manager, etc.). This paper does not attempt to tell the community *how* to execute following recommendations as there are many different methods to institute change. Instead, the following fifteen recommendations aim to provide a list of necessary actions and objectives. This list follows the same themes used in the conclusions section reprising the categories of overall themes, training and education, and experience.

Overarching Recommendations:

Recommendation #1: Do Not Wait for USAF to Solve Institutional Problems. The USAF cyberspace operations officer community must take the initiative to reduce the institutional developmental shortfalls in cyberspace officer force development. The institutional USAF has yet to publish a deliberate plan to build joint leaders in alignment with the CSAF's focus area. Therefore, if the USAF cyberspace community desires to build effective joint leaders more in alignment with its sister services, it must begin addressing the challenge itself.

Recommendation #2: Evaluate and Balance Institutional and Occupational Competency Development. To internally resolve institutional force development shortfalls, the USAF cyberspace officer community will need to decide how to best balance institutional competency requirements, existing and evolving occupational competencies, and associated resource requirement deltas.

Recommendation #3: Define Desired Officer Force Development Model. The USAF cyberspace officer occupational field must determine a deliberate officer force development model and prioritize desired competencies that addresses the challenges and disparities illuminated by this research. Due to the institutional nature of the identified shortfalls, the following twelve subordinate recommendations are agnostic to future USAF cyberspace operations officer force structure discussions (e.g. splitting the career field like the US Army or USMC).

Recommendation #4: Shift Lexicon and Processes. The USAF cyberspace community must embrace and prioritize use of joint lexicon and processes when developing its cyberspace force and within all cyberspace organizations. The major challenge to the USAF cyberspace community is that it still must understand and translate existing lexicon, methods, and processes specific to the USAF, USCYBERCOM, and to the commercial information technology industry.

Recommendation #5: Emphasize USAF Missions and Capabilities. The USAF cyberspace officer force development model must emphasize understanding of USAF missions/capabilities and joint warfighting functions. This includes understanding how the AF executes its missions (capabilities, functions, and processes), the supporting cyberspace capabilities to these missions, and how they can protect/defend those capabilities from cyberspace threats. This goes beyond just the systems used during a mission, but also the logistics, maintenance, and medical cyberspace-enabled capabilities that that enable said mission.

Recommendation #6: Integrate Military Problem-Solving Methodologies. The USAF cyberspace operations officer community must integrate military problem-solving methodologies such as design and JOPP into the cyberspace operations officer force development model. Joint doctrine addresses, and the services deliberately leverage, design and JOPP-like military planning process into their operations; thus, it behooves USAF cyberspace operations officers to build knowledge and experience with these common methodologies. Course directors of Cyber 200 and Cyber 300 have already integrated introduction to design into their latest curriculum. These grassroots efforts are first step in the right direction, but the community must deliberately and systematically incorporate standard military problem-solving methodologies across the force development model.

Training and Education Recommendations:

Recommendation #7: Avoid Single-Serving Training and Education. The USAF cyberspace operations officer community must integrate institutional competencies such as military problem-solving and USAF/joint missions across the full spectrum of occupational training and education courses.

Recommendation #8: Leverage Existing Opportunities. The USAF cyberspace operations community must continue to maximize and encourage use of existing training and education courses to address the institutional competency gaps. Formal programs include the USMC Expeditionary Warfare School and sister-service intermediate developmental education programs. The community should also deliberately encourage its officers to apply for the Multi-Domain Operational Strategist (MDOS) concentration during ACSC which focuses specifically on problem solving across multiple domains. [MDOS source] Finally, the community must target communications towards promising officers for apply for advanced studies group programs. These existing opportunities do not address most of the USAF cyberspace operations officer population but will ensure a subset receive and can propagate these institutional competencies.

Recommendation #9: Integrate Stop-Gap Courses into Formal Development. The USAF cyberspace operations community should evaluate existing stop-gap or just-in-time training courses that already address identified competency shortfalls. Once identified, deliberately integrate curriculum or courses into the formal developmental training and education model for all cyberspace officers. One primary example to evaluate is the USAF Cyber College's Functional Mission Analysis – Cyber (FMA-C) course. The 5-day FMA-C course includes an introduction to military problem solving (design and systems thinking) coupled with a review of USAF core missions. The course then presents a framework for analyzing USAF mission capabilities, processes, and information flow. It presents a framework for USAF cyberspace officers to deliberately analyze (problem solve) and build understanding of capabilities and processes of how the USAF executes its five core missions. [source: FMA-C slides] This course alone addresses two of the major identified institutional competency shortfalls.

Recommendation #10: Add Institutional Competencies to Occupational Courses. The USAF cyberspace operations officer community must determine how and where it wants to add identified institutional competencies into existing curriculum and courses. Solutions may be integration into existing lessons or adding entirely new lessons. One example of the former is to use examples of actual USAF capabilities, processes, or problem sets when instructing foundational cyberspace knowledge, skills, and abilities. Another example may include the adding of military problem-solving lessons followed by threading the use of design and military planning methodologies into existing practical exercises and evaluations.

Recommendation #11: Add RF Transmission to Occupational Courses. The only occupational training recommendation is for the USAF to add fundamentals of radio frequency (RF) transmission systems back into occupational cyberspace courses. As highlighted in chapter three, the majority of USAF weapon systems rely on RF transmissions systems for communications, navigations, and employment. USAF cyberspace officers may supervise enlisted transmissions personnel, lead projects involving radios, provide cyberspace protection and defense to weapon systems leveraging RF technologies, or use RF transmission capabilities to coordinate/integrate cyberspace effects with maneuver platforms.

Thus, training and education on foundational RF theories and capabilities are important throughout the force development model.

Key Duty and Experience Recommendations:

Recommendation #12: Reinforce Military Problem-Solving Thru Repetition. The USAF cyberspace operations community must emphasize the use of institutional competencies during duty assignments. The use of institutional knowledge, skills, and abilities during duty assignments reinforces the concepts for the individual while increasing proficiency. The first major recommendation for the community to encourage (and reward) officers to utilize military problem solving (design and JOPP) in their duty units, no matter the echelon. For example, a lieutenant charged to lead a project should leverage design and a military planning methodology. While a project is different from a military combat operation, both scenarios must solve the problem of how to achieve a desired future state from their current state. The primary challenge to this recommendation will be the general lack of knowledge, skills, and abilities of military problem solving by the average, older USAF cyberspace officers. Refer to recommendations seven through ten for part of the solution.

Recommendation #13: Foster USAF and Joint Mission Understanding. The USAF cyberspace operations community must emphasize and reinforce development of USAF and joint mission knowledge within all our cyberspace organizations, be it base communications squadrons, cyber operations squadrons, or organize/train/equip staffs. Utilization of methodologies like Functional Mission Analysis-Cyber in line units represents one deliberate method to foster experience in this realm.

Recommendation #14: Build Common Experience. The USAF cyberspace operations community should investigate establishing a common experience for most cyberspace operations officers in the first four years of their career. The aim is to reinforce desired institutional competencies such as USAF mission understanding and military problem solving. An example in the USMC and US Army are the services ensuring communications/signal lieutenants to lead platoons within the Marine Expeditionary Forces.

A challenge for all services is creating a common experience for officers going to Cyber Mission Force or like units. Depending upon the unit, the officers will face different mission sets and developmental opportunities (defensive versus offensive, service-retained versus COCOM support). This challenge is the greatest for the USAF with its single cyberspace officer occupational field. One USAF cyberspace lieutenant in their first four years of service may lead airmen in executing DoDIN operations in a base communication whereas a peer will spend upwards of two additional years training to execute offensive cyberspace operations.

Recommendation #15: Pursue Earlier Joint Duty Experience. Aside from evolving internal USAF cyberspace officer experiences, the USAF cyberspace officer community must deliberately seek and value external service experiences for its officers earlier in their careers. This experience may take the for of formal duty assignments to joint organizations (i.e. combatant command staffs), participation in joint exercises, or individual deployments to combined/joint operations. The experience earlier in a career will educate and reinforce joint mission understanding and military problem-solving methodologies. Furthermore, these officers can then bring back and integrate the gained knowledge/experience into USAF organizations, further augmenting the desired force development of other cyberspace officers.

Closing Thoughts

This concluding chapter presented eleven conclusions and fifteen recommendations arguing that in order to build joint leaders, the USAF cyberspace operations officer community should re-balance its force development model to align better with USMC and USA weights of effort. However, this paper did not fully explore why the USMC and USA uses the weight of effort and focus in their development of future leaders within the officer corps. Further research on the history, logic, and decisions that led to the current USMC and USA force development models may illustrate additional considerations for integrating aspects USMC and USA force development into USAF cyberspace officer development.

Nevertheless, the recommendations supplied in this conclusion reflect tangible steps the USAF cyberspace operations community can take to start deliberately producing more effective joint leaders. These recommendations require deliberate and sustained action within the context of currently undefined resource requirements. To allay concern that this study and its conclusions and recommendation is a finger-pointing exercise, then please know that the author's next assignment places him in the middle of the formal training and education process for newly commissioned officers entering the cyberspace career field.

The reader may also be skeptical that the USAF cyberspace community can internally resolve USAF institution-spanning challenges; however, the USAF cyber operations community does have the flexibility and institutional "top cover" to accomplish the recommendations. First, the CSAF specifically highlighted his large priorities which include building joint leaders and teams. The overarching aim of the recommendations provided in this chapter align with the CSAF's focus area. Second, the Secretary of the Air Force and the CSAF frequently emphasize innovation at all echelons within the USAF. Therefore, the highest levels of USAF leadership are empowering members of the USAF, including USAF occupational communities, to take the initiative solve problems through new and novel approaches that align with overall USAF priorities and vision. Finally, having two parent organizations (USAF and USCYBERCOM) presents challenges, but also presents opportunities. If resourcing or policy challenges interfere with completing the recommended actions, the USAF cyberspace community may attempt to leverage either parent organization to break the proverbial logjam.

The USAF cyberspace community can quickly achieve some of the fifteen presented recommendations, while others will take longer and may require overcoming policy and resourcing challenges. As Morgan Freeman's character Red in the Shawshank Redemption states, "…all it takes really... pressure... and time."[2] Likewise, the USAF cyberspace operations community can more effectively build joint leaders if it stays committed to solving the identified institution shortfalls in current USAF cyberspace operations officer force development.

[2] Frank Darabont, *The Shawshank Redemption* (Burbank, California: Warner Bros. Pictures, 2004).

Bibliography

10 USC Chapter 38: Joint Officer Management, 10 USC Ch. 38 §661. http://uscode.house.gov/view.xhtml?path=/prelim@title10/subtitleA/part2/chapter38&edition=prelim.

10 USC Chapter 38: Joint Officer Management, 10 USC Ch. 38 §662. http://uscode.house.gov/view.xhtml?path=/prelim@title10/subtitleA/part2/chapter38&edition=prelim.

10 USC Chapter 38: Joint Officer Management, 10 USC Ch. 38 §664. http://uscode.house.gov/view.xhtml?path=/prelim@title10/subtitleA/part2/chapter38&edition=prelim.

10 USC Chapter 38: Joint Officer Management, 10 USC Ch. 38 §668. http://uscode.house.gov/view.xhtml?path=/prelim@title10/subtitleA/part2/chapter38&edition=prelim.

10 USC Chapter 107: Professional Military Education, 10 USC §2151, §2155. http://uscode.house.gov/view.xhtml?path=/prelim@title10/subtitleA/part3/chapter107&edition=prelim.

“24th Air Force.” Air Forces Cyber, 6 February 2017. http://www.afcyber.af.mil/About-Us/Fact-Sheets/Display/Article/458567/24th-air-force-afcyber/.

“780th Military Intelligence Brigade.” 780th Military Intelligence Brigade. Accessed 17 April 2018. https://www.inscom.army.mil/msc/780mib/.

“2019 Advanced Academic Degree (AAD) and Special Experience Exchange Duties Selection Process Guide.” Air Force Personnel Center, 4 April 2018.

“AFSC 17X Cyberspace Operations Officer Career Field Education and Training Plan.” Department of the Air Force, 15 August 2014.

“Air Command and Staff College Resident Curriculum.” Air University, 5 October 2017. http://www.airuniversity.af.mil/ACSC/Display/Article/922353/resident-curriculum/.

Air Force Instruction (AFI) 10-403. *Deployment Planning and Execution*, 6 October 2016.

Air Force Instruction (AFI) 36-2640. *Executing Total Force Development*, 29 December 2011.

Air Force Instruction (AFI) 38-101. *Air Force Organization*, 31 January 2017.

Air Force Manual (AFMAN) 36-2647. *Institutional Competency Development and Management*, 15 September 2016. http://static.e-publishing.af.mil/production/1/af_a1/publication/afman36-2647/afman36-2647.pdf.

“Air Force Officer Classification Directory (AFOCD).” Air Force Personnel Center, 31 October 31 2017.

Albertson, Trevor D. “Airpower I: Capabilities and Limitations in American Airpower Syllabus AY 18.” United States Air Force Air Command and Staff College, 2018.

Arenas, Fil. “Leadership Syllabus AY 18.” United States Air Force Air Command and Staff College, 2018.

Army Regulation (AR)10-87. *Army Commands, Army Service Components, and Direct Reporting Units*. 11 December 2017. https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/ARN2541_AR10-87_WEB_Final.pdf.

Ashdown, Vic L. “Cyber 400 Schedule - 18002.” 333d Training Squadron, 20 April 20 2018.

“AY2014-02 and CGSOC Class 2015 Combined Strawman.” U.S. Army Command and General Staff College, 21 November 2014.

Beck, James. “FY15 Approved BOLC Common Core Task List.” US Army Combined Arms Center, 29 January 2016.

Blankenship, Lt Col Jeffrey, former duty with Air Force Senior Leader Matters Office. Interview by the author, 29 September 2017.

Canady, Lt Col David, (former SAF CIO/A6 staff officer). Interview by the author, September 29, 2015.

“CGSC Circular 350-1: U.S. Army Command and General Staff College Catalog.” U.S. Army Command and General Staff College, January 2016.

Chang, Capt Joshua D, course director, Basic Communications Officer Course, Communications Training Battalion. To the author. E-mail, 12 April 2018.

“Communications Training Battalion (CTB): CTB Courses 2017.” http://www.trngcmd.marines.mil/Portals/207/Docs/MCCES/CTB/CTB%20COURSES%202017-%20Enclosure%20(2).docx?ver=2017-11-22-171439-797.

Curtis E. Lemay Center for Doctrine Development and Education. “Annex 1-1 Force Development Appendix: Institutional Competency List,” 17 April 2017. http://www.doctrine.af.mil/Portals/61/documents/Annex_1-1/1-1-D06-Appendix-1-Competency.pdf.

“Cyber Technical College.” Cyber School, U.S. Army Cyber Center, 15 September 2016.

“Cyber Warfare Operations (CWO) Training.” 39th Information Operations Squadron, January 2017.

Darabont, Frank. *The Shawshank Redemption*. Burbank, California: Warner Bros. Pictures, 2004.

Day, Maj Andrew. “Cyberspace 300 Course Syllabus (FY18).” Air Force Institute of Technology, 12 February 2018.

Defense Information Systems Agency. “DoD Approved 8570 Baseline Certifications.” IASE: Information Assurance Support Environment. Accessed 20 January 2018. https://iase.disa.mil/iawip/Pages/iabaseline.aspx.

Department of the Army Pamphlet 600-3. *Commissioned Officer Professional Development and Career Management, Cyber Branch*, 17 January 2018.

Department of the Army Pamphlet 600-3. *Commissioned Officer Professional Development and Career Management*, *Signal Corps Branch,* 1 June 2017.

Department of the Army Pamphlet 600-3. *Officer Professional Development and Career Management*, 26 June 2017.

“Expeditionary Warfare School.” Marine Corps University. Accessed 22 March 2018. https://www.usmcu.edu/ews.

Field Manual (FM) 3-90.6. *Brigade Combat Team*, 14 September 2010. https://usacac.army.mil/sites/default/files/misc/doctrine/CDG/cdg_resources/manuals/fm/fm3_90x6.pdf.

Goldfein, Gen David L. “Air Force Association Air Warfare Symposium Kenote Speaker General David Goldfein.” Orlando, FL, 23 February 2018. http://www.af.mil/Portals/1/documents/csaf/CSAF_AFA_Orlando-23Feb18.PDF.

Goldfein, Gen David L. "CSAF Focus Area: Enhancing Multi-Domain Command and Control...Tying It All Together," March 2017. http://www.af.mil/Portals/1/documents/csaf/letter3/CSAF_Focus_Area_CoverPage.pdf.

Goldfein, Gen David L. "CSAF Focus Area: Strengthening Joint Leaders and Teams," October 2016. http://www.af.mil/Portals/1/documents/csaf/letters/16%2010%2013%20Focus%20Area%20II.pdf?ver=2016-10-13-105649-460&timestamp=1476371621707.

Goldwater-Nichols Department of Defense Reorganization Act of 1986, Pub. L. No. 99–433 (1986). http://history.defense.gov/Portals/70/Documents/dod_reforms/Goldwater-NicholsDoDReordAct1986.pdf.

Grieco, Kelly A. "War Theory: The Evolution of War and Military Thought Syllabus AY 18." United States Air Force Air Command and Staff College, 2018.

Higby, Maj Gen Patrick C. "USAF Cyberspace Operations Officers Mentoring and Development." USAF Cyberspace Force Development Team, March 20, 2017.

Hochrine, Capt William A. "MAGTF Communications Planners Course Syllabus." U.S. Marine Corps Communications Electronics School, 2018.

Hochrine, Capt William A., course director, MAGTF Communications Planners Course. To the author. E-mail, 10 April 2018.

Hochrine, Capt William A., course director, MAGTF Communications Planners Course. To the author. E-mail, 16 April 2018.

Hutto, J. Wesley. "International Security I: The Context of International Security Syllabus AY 18." United States Air Force Air Command and Staff College, 2018.

Joint Chiefs of Staff. *DOD Dictionary of Military and Associated Terms*, April 2018. http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf?ver=2018-03-27-153248-110.

"Joint Cyberspace Training and Certification Standards." US Cyber Command, 14 October 2016.

Jones, Pete. "Master Training Schedule: Signal Captains Career Course." 442nd Signal Battalion, U.S. Army Signal Center, February 5, 2018.

Kevin E. Blanchard. "Air and Space Basic Course: A Cost Effective Contribution to Air Force Officer Professional Development?" Air University, February 16, 2011.

Knopp, Maj Matthew A., operations officer, Communications Training Battalion. To the author. E-mail, 9 April 2018.

Lawnicsak, Brent A. "Joint Warfighting: 'How We Fight' Syllabus AY 18." United States Air Force Air Command and Staff College, 2018.

Lee, Caitlin, Bart E. Bennett, Lisa M. Harrington, and Darrell D. Jones. "Air Force Senior Leader Representation in the Joint Community." RAND Corporation, 2017. https://www.rand.org/pubs/research_briefs/RB9970.html.

"United States Air Force Weapons School." Nellis Air Force Base, 10 May 2016. http://www.nellis.af.mil/About/Fact-Sheets/Display/Article/284156/united-states-air-force-weapons-school/.

Lustig, Ken. "Weapons School Integrates Cyber Warfare." Nellis Air Force Base, 30 May 2012. http://www.nellis.af.mil/News/Article/284777/weapons-school-integrates-cyber-warfare.

Magruder, Lt Col Daniel L. “Developing Air Force Field Grade Officers for Joint Leadership.” Air & Space Power Journal 32, no. 1 (Spring 2018): 52–64.

Marine Corps Order (MCO) 1500.61. *Marine Leader Development*, 28 July 2017

Marine Corps Order (MCO) 1533.4B. *Professional Military Education*, 25 January 2008.

Marine Corps Order (MCO) P1400.31C. *Marine Corps Promotion Manual, Volume 1, Officer Promotions*, 9 August 2006.

McHugh, John M. “General Order No. 2014-63: Establishment of the United States Army Cyber Branch.” Headquarters, Department of the Army, 21 August 2014.

Mezzell, Ann. “International Security II: The Conduct of National Security Syllabus AY 18.” United States Air Force Air Command and Staff College, 2018.

“National Security Agency Development Programs.” Intelligence Careers. Accessed 20 January 2018. https://www.intelligencecareers.gov/nsa/nsadevprograms.html.

“Naval Postgraduate School Academics.” Naval Postgraduate School, 2018. http://www.nps.edu/web/guest/academics.

Navy Marine Corps (NAVMC) 1200.1D. *Military Occupational Specialties Manual (DRAFT)*, 2018.

Navy Marine Corps (NAVMC) 3500.56C. *Communications Training and Readiness Manual*, 2 November 2016.

“NETCOM: U.S. Army Network Enterprise Technology Command.” U.S. Army. Accessed 17 April 2018. http://www.netcom.army.mil.

Nettis, Maj Kimber. “Cyberspace 200 Course Guide (FY18).” Air Force Institute of Technology, 15 March 2018.

Patt, Robert D. “Undergraduate Cyberspace Training (Phase 1) Course Chart.” 333d Training Squadron, 28 September 2016.

Patt, Robert D. “Undergraduate Cyberspace Training (Phase 2) Course Chart.” 333d Training Squadron, 22 September 2016.

Perez, Maj Gilberto, former EWS student. Interview by the author, 18 April 2018.

Pomerleau, Mark. “Here’s How the Army Wants to Integrate Cyber, EW into Operational Formations.” Fifth Domain, 2 October 2017. https://www.fifthdomain.com/dod/army/2017/10/02/heres-how-the-army-wants-to-integrate-cyber-ew-into-operational-formations/.

Pyburn, Col Bradley L., commander, 67th Cyber Wing. Interview by the author. 7 March 2018.

Schlegel, Maj Karl W., communications officer, USMC. Interview by the author, 13 November 2017.

“Signal Basic Officer Leaders Course (SBOLC).” The Official Homepage of the U.S. Army Signal School, 30 March 2016. https://signal.army.mil/index.php/organizations/15th-regimental-signal-brigade/442nd-signal-battalion/25-courses/93-sbolc.

Skehan, Capt Patrick. “0602 Career Path Road Map,” 5 March 2018.

Skehan, Capt Patrick, 600 and 1700 captain monitor, USMC. Interview by the author, 28 February 2018.

Smith, Derrick J. “Cyber CCC Course Map.” U.S. Army Cyber School, Cyber Center of Excellence, 26 January 2018.

Speigle II, W.R. "The Basic School: Continuing to Successfully Prepare Second Lieutenants to Be Officers." United States Marine Corps Command and Staff College, 17 April 2008. http://www.dtic.mil/dtic/tr/fulltext/u2/a491616.pdf.

"Squadron Officer School (SOS) In-Resident Course Catalog." Air University Squadron Officer College, 24 August 2017.

"The Basic School Training Command: Phase 0-IV Student Materials." http://www.trngcmd.marines.mil/Units/Northeast/The-Basic-School/Academics/FY16-PHASE-0/.

"Types of MAGTFs." U.S. Marine Corps Concepts & Programs, 23 January 2015. https://marinecorpsconceptsandprograms.com/organizations/marine-air-ground-task-force/types-magtfs.

"Undergraduate Cyberspace Training (Phase 1) Plan of Instruction." 333d Training Squadron, 28 September 2016.

"Undergraduate Cyberspace Training (Phase 2) Plan of Instruction." 333d Training Squadron, 22 September 2016.

"United States Marine Corps: America's Expeditionary Force in Readiness." Headquarters United States Marine Corps, 21 April 2015. http://www.hqmc.marines.mil/Portals/61/Docs/20150420_SIG_USMC%20101Brief_FINAL.pdf.

"United States Marine Corps Command and Staff College Curriculum." United States Marine Corps Command and Staff College, 2017.

"U.S. Air Force." U.S. Air Force. Accessed 10 March 2018. https://www.airforce.com/mission.

"U.S. Army Command and General Staff College Curriculum Class 2015," August 2014.

"US Army Cyber Basic Officer Leadership Course B Weekly Training Schedule," 15 July 2016.

"U.S. Army Cyber Command." U.S. Army Cyber Command. Accessed 12 April 2018. http://www.arcyber.army.mil/.

"U.S. Army Organization: Who We Are." U.S. Army. Accessed 17 April 2018. https://www.army.mil/info/organization.

"U.S. Marine Corps Forces, Cyberspace Command (MARFORCYBER)." U.S. Marine Corps Concepts & Programs, 12 February 2018. https://marinecorpsconceptsandprograms.com/organizations/operating-forces/us-marine-corps-forces-cyberspace-command-marforcyber.

"USMC CSC AY17-18 First Semester Calendar." United States Marine Corps Command and Staff College, 3 August 2017.

"USMC CSC AY17-18 Second Semester Calendar." United States Marine Corps Command and Staff College, 3 August 2017.

"USMC Expeditionary Warfare School AY18 Curriculum Timeline." Marine Corps University Expeditionary Warfare School, 2017.

Van Ovost, Jacqueline D. "CJCSI 1800.01E Officer Professional Military Education Policy." Chairman of the Joint Chiefs of Staff, 29 May 2015. http://www.jcs.mil/Portals/36/Documents/Doctrine/education/cjcsi1800_01e.pdf?ver=2017-12-29-142206-877.

Venable, Heather P. “Airpower II: Integrating Air, Cyber, and Space into Multi-Domain Operations Syllabus AY 18.” United States Air Force Air Command and Staff College, 2018.

“Welcome to Squadron Officer School.” Air University, 5 April 2018, http://www.airuniversity.af.mil/SOS/.

“Who We Are: Our Purpose.” Marines, 2018. https://www.marines.com/who-we-are/our-purpose.html.

Wieland, Steven T. “Cyber Squadron Enabling Concept.” SAF CIO/A6, 15 March 2018.

Williams, John. “Master Training Schedule: Signal Basic Officer Leader - Branch.” Signal School, U.S. Army Cyber Center of Excellence, 15 February 2018.

Wingo, Lt Col Joseph, chief, Cyber Force Development. To the author. E-mail, 22 April 2018.