DEPARTMENT OF THE NAVY CYBER WORKFORCE

LEADERSHIP DEVELOPMENT CAPSTONE STUDY

Daniel R. Parilla and Stephanie L. Wills
In partial fulfillment of the requirements for the degree of
Doctor of Education in Leadership and Learning in Organizations
Peabody College of Education and Human Development,
Vanderbilt University

April 2021
Nashville, TN

Acknowledgments

To the Department of Navy employees, current and retired, civilian, and military, it was a privilege to hear your insights and experiences on the cyber domain.

To our client, Mr. Joshua Reiter, we express our sincere appreciation for allowing us to look at an organizational problem in both leadership and learning that was both unique and timely. We hope our project effort and findings from our qualitative interviews and survey will be of use for you and the Navy's cyber leaders for years to come.

To the Vanderbilt community and especially Cohort 3 for supporting us through this program. We could not have fathomed the community of friends and colleagues that could be formed from choosing this path and this program. We have been very blessed.

To our advisers, Dr. Marisa Cannata and Dr. Cynthia (Cindy) Nebel, for your guidance and support, particularly for partnering with us in delivering this work and pushing us to deliver the best product we could.

To our family, friends, and co-workers who have supported and sustained us over the last three years. Special thanks to Dr. Walterzene Dabney for her candid guidance, mentorship, and support.

To our children, you have been amazing throughout the past three years! You have selflessly given up time to allow us to read, research, and write papers. We hope that we have inspired you to realize that anything you put your mind to is within your reach. Live your lives as if they are great stories.

To our spouses, Lesley Parilla, and Michael Wills, we each would have never pursued doctoral degrees, much less have accomplished this goal without your support, encouragement, and love. You knew before we did that, we could do this.

Table of Contents

Table of Figures

List of Tables

Executive Summary

The development of cyber as a warfighting domain and a means to deliver effects while providing a defense method from threats has created a dynamic community in the United States Navy and the Department of the Navy. To better understand the lifecycle of cyber professionals and to facilitate their placement, training, and career progression, the Department of the Navy Chief Information Officer (DoN CIO) requested a study to analyze the balance between skills, including Knowledge, Skills, and Abilities (KSAs), that leadership demands and the skills that are held by the members of the Navy's cyber workforce, specifically for leadership and learning for the future cyber workforce. Previous studies conducted by the United States Air Force (USAF) and the Department of Defense (DoD) have provided a wealth of data that can be analyzed to determine sourcing, entry skill set, initial job placement, and longevity/career success of defense cyber professionals. These studies have not provided insight into the matching or mismatching of technical skills and the interpersonal skills needed for a cyber professional to succeed as a leader in the Department of Navy (DoN). This study sets about to provide insight into how effective training, experience, and career progression of cyber leaders will impact those with a highly technical skillset and how reinforcement of desired cyber leadership skills can be better accomplished. A detailed series of interviews with professionals at various levels in the Department of Navy provide these initial insights.

The purpose of this capstone is to identify and progress gaps in leadership, training, and development of the Department of the Navy Cyber Workforce for broader consideration. By creating an understanding of shortcomings in the alignment of training to the requisite skills and roles that are necessary for Navy cyber leaders, we hope to broaden the body of knowledge on cyber leadership skills and sustainment to facilitate the development of a more robust cyber warfighter community that will enhance the Navy's ability to operate in the cyber domain. This study was focused on 3 Research Questions:

RQ1. What kinds of skills and capabilities will Department of Navy cyber supervisors need to effectively lead the cyber workforce?

RQ2. How can the Department of Navy develop the appropriate supervisory and leadership personnel responsible for leading, managing, and developing the rest of the cyber warfighting force?

RQ3. What intellectual infrastructure is needed to support viable, sustainable cyber management/leadership?

Utilizing over 20 hours of interviews, combined with results from a survey of over 150 graduating seniors from Fairfax County Public Schools (FCPS) in Virginia, data was analyzed using lexical coding to understand common expectations for training and development for the U.S. Navy's (USN) Cyber warfare communities. This study determined that while desired skills demanded of DoN cyber leaders by seasoned senior leaders match the expectations of the incoming entry-level workforce, there remains little consistency in training availability for supplying and sustaining the Department's cyber supervisors, managers, and leaders. Furthermore, a lack of mid-grade professionals (both officer and enlisted) has led to an erosion of sustainable career pathways within the uniformed-Navy cyber field.

Our research revealed no identifiable career path or training path for the DoN cyber force (military or civilian component). Consequently, DoN cyber personnel and commands create their own training and leadership paths that address their individual missions and personnel needs. Four-year degrees are not critical for most cyber professionals, as current academic curricula are not delivering necessary cyber technical knowledge coupled with essential leadership skills. However, broad intellectual and professional experience is necessary to levy varied, multi-layered lenses and perspectives for leading and managing any team. Sufficient technical understanding, not specific technical expertise, is necessary for understanding and translating the cyber “system.” While no particular professional or IT certifications were identified as necessary across cyber leaders, job-dependent certifications like CISO, CISSP or MCC level, Project Management Professional (PMP), or DAWIA (defense acquisition-related) certifications for cyber personnel focused on acquisitions are useful as training investments.

RQ1 – learning: We discovered that the following leadership and managerial traits should be focused on by DoN cyber as necessary for cyber leaders: communication/translation, collaboration/teamwork/relational skills, intellectual curiosity, self-motivation, integrity/honesty, and confidence. While some of these traits can be trained in educational settings (for example: writing, communication), others (like teamwork, honesty, integrity) must be performed to truly develop them. Soft skills proficiency is essential for cyber leaders. This proficiency must be accomplished through experience, problem-solving and critical thinking opportunities, and life-long learning built on a foundation of basic people skills and a desire for individual advancement.

RQ2 - organizational structure: Our research indicates that the appropriate leadership and supervisory development path needs to include On The Job Training (OJT), mentorship, experiential learning, and systems thinking that exposes cyber professionals to executive focus areas like budgeting, strategy, policy, resource requirements, etcetera. Additionally, the path needs to include learning scaffolding and reinforcement opportunities for perishable cyber-related leadership and managerial skills.

Lastly, RQ3 – the strategy to develop the intellectual infrastructure necessary for sustaining cyber should include "industry-izing," governance structure with a learning, mentoring, developmental strategy, and a Cyber Leadership Development Board (CLDB). Through the application of a Cyber Operational Leadership Training and Selection (CYBOLTS) process, the DoN Cyber community is positioned to meet the framework defined by both Congressional Cyberspace Solarium Commission (CSC) (Bate, 2020) and a 2020 Naval Administration Message (NAVADMIN), which is an official correspondence focused on reestablishing Navy leader development frameworks (Department of the Navy, 2020).

Introduction

The cyber domain encompasses everything pertaining to moving, protecting, defending, and even attacking assets on networks. Cyber affects all people somehow tied to networks—meaning almost everyone, almost every day. When we consider cyber, and specifically security, it regards protecting the data and integrity of computing assets belonging to or connecting to our personal, organizational, and national networks. Our individual, professional, and national arena's most sensitive data are held in the cyber domain. Everything from the basic conduct of banking, research, effective business and communications, identity theft, data breaches, and cybercrime occurs in this arena. Cyber security or defense is all about the security and protection of this domain.

The Department of the Navy is faced with the continual challenge of manning, training, and equipping its force with the technology, skills, and equipment necessary to meet not only today's cyber challenges but also to create a framework for developing the hard and soft skills essential to lead and manage a future cyber workforce. To date, most of the efforts have been put to recruiting and training the cyber worker and not toward the leadership responsible for employing that workforce (Baker, 2016). Thus far, technological awareness capability has defined the knowledge that technicians will need and how they can be adapted to cyber field challenges; however, individual skill capacity and development across leadership and management skills have been lacking. This has led to a gap in what leadership sees as the desirable traits and ability to implement them (Dawson & Thompson, 2018).

Over the past decade, the cyber operations and security market have rapidly grown in the commercial, civil, defense, and federal sectors (Baker, 2016). Cell phones, computers, banking and security apps, Fitbits, Bluetooth enabled and smart devices, medical equipment, etcetera all operate in, or are impacted or vulnerable in, the cyber realm. This arena affects every individual's daily life, and consequently, is viewed as a critical civilian, commercial, and warfighting domain, which is an increasingly contested terrain (Leigher, 2011). Accordingly, there has been a significant upswing in demand for leadership, management, cyber enablers, education, training, and a myriad of other associated services, for executing effectively across the cyberspace arena. Due to its sheer magnitude and ubiquitous impact, this problem has an estimated global personnel shortage of three million workers. It will require a major effort to recruit and retain cyber workers and build cyber leaders (Crumpler & Lewis, 2019). For our research's discrete focus across this problem set, many challenges face cyber portfolio supervisors, managers, and leaders in the years ahead. They have to learn to lead and manage an immense, unfamiliar transformation. They must define the skills needed to discover, adapt and train 21st-century cyber leadership while creating the related education and training needed to build sustainable workforce development structures (Dawson & Thompson, 2018).

This capstone aims to identify gaps in leadership skills and the leadership training of the Department of the Navy cyber workforce. By creating an understanding of shortcomings in the alignment of training to the requisite skills and roles necessary for leaders, we hope to facilitate the development of a more robust cyber warfighter community that will enhance the Navy's ability to operate in the cyber domain**.** These gaps fell into the focal areas of Learning, Organizational Structure, and Strategy throughout this study.

DoN Cyber Organizational Structure

Our client, Mr. Joshua (Josh) Reiter, was the Director for Cyber Workforce Policy and Planning in the Cyber Security Division (OPNAV N2N6G) in January 2020 when our capstone began. However, he is now the Director of Information Warfare (IW) Manpower & Training Integration (OPNAV N2N6IM) after a reorganization. He remains responsible for cyber workforce policy and planning. Mr. Reiter is a Department of Navy Senior Executive and direct advisor to the Secretary of the Navy's (SECNAV) Chief Information Officer (CIO). DoN CIO has been tasked with conducting research and framework to identify the specific hard and soft skills required to lead and manage the future cyber workforce. This effort must look at how these findings will potentially influence and impact the U.S. Department of the Navy's efforts regarding leadership and management of the current and future cyber workforce. DoN CIO contends that the cyber sector has a good sense of focus on what an effective cyber worker needs to look like. The same cannot be said to understand what an effective cyber leader or cyber enabler is, which is the most critical component of our research and the gap he would like us to inform. Specifically, research is needed to understand what future leaders will require through hard and soft skills, education and training, and certifications to lead the future cyber workforce effectively. As the workforce evolves, this assessment will guide how leaders and managers develop a time and experience continuum to build and maintain cyber leadership acumen.

The U.S. Navy's cyber operating force (COF) is composed of officers, chief petty officers, and enlisted sailors in 28 active commands, 40 cyber mission force units, and 27 reserve commands located internationally as well as stateside. The total USN cyber workforce is over 44,000 sailors and civilian, with half being active duty (DoN CIO, 2021). Within this domain, the Navy has established a Cyber Warfare Engineer (CWE) program for naval officers to provide a career path for technical experts in the cyber field. Still, numbers are currently limited to only 100 officers in this designator. The CWE program is expected to double to 200 cyber-only focused officers in the next decade. The remainder of the cyber officer cadre supporting cyber come from cryptologic warfare or intelligence communities and are part of the Information Warfare Corps (IWC) (United State Navy IDC, 2010).

Additionally, numerous civilian jobs support the DoN cyber community. This study considered the career of active-duty servicemembers and DoN cyber civilians and their potential leadership development. Additional leadership/management-focused needs and opportunities to develop the DoN civilian cyber leaders in the workforce, who represent DoN’s primary mid-level continuity.

Relevant Literature/Conceptual Framework

DoN CIO's questions required us to understand what future cyber leaders will require from leadership, skills, education, and certification perspectives. Relevant literature was reviewed to identify existing cyber workforce development, education, and expertise, and gaps to get a sense of the scope of related issues. Dawson and Thomson (2018) indicate that defining the knowledge, skills, attributes, and other effective cybersecurity workforce characteristics is complicated due to unique cyber field challenges. The authors adopt six factors for the future of cybersecurity workforce development: systemic thinkers, team players, passion for continuous learning, strong communication skills, a civic duty sense, and an appropriate mix of technical and social skills. Several sources spoke to the significance of social intelligence skills for success. Baker (2016) defines the present challenge as one that prevents a thorough understanding of what a cyber leader should look like. While training standards and competency assessments for existing cyber worker positions are still being defined and developed, they have not yet developed to the point of providing measurable criteria required for validating skill proficiency across roles and responsibilities vertically through cyber hierarchies. However, she reiterates what other researchers have articulated: there is a lack of soft skills--the non-technical attributes like communications and human behavior modeling and learning--essential for setting the right culture in the cyber workforce. Crumpler and Lewis (2019) also explain that cybersecurity professionals lack critical, soft skills (often more important than hard skills) like teamwork, problem-solving, and communication/writing skills. This dearth of skills applies to cyber leaders as well. Emphasis should thus be placed on "softer" skills, fostering innovation, problem-solving, and self-directed inquiry (Caulkins, Badillo-Urquiola, & Leis, 2017).

The IEEE (Institute of Electrical and Electronic Engineers) conference report (2016) proposes practical education strategies and identifies emerging cyber-education opportunities that may strengthen cyber leader development and sustainment. They highlight the human-centric cyber-educational curriculum and the human side of cybersecurity. It is proposed that current cybersecurity education ignores the importance of human-centered training areas despite every aspect related to cybersecurity being inseparably tied to human elements and behaviors (Caulkins, Badillo-Urquiola, & Leis, 2017). The current cybersecurity education ecosystem, according to Crumpler and Lewis, lacks common metrics or rankings for fundamental knowledge for employee-related programs, certifications, and degrees that would be most effective for a common baseline set of skills for employers and organization needs to build the role-specific knowledge necessary to strengthen the cybersecurity talent pipeline. The International Information System Consortium identified in 2018, in their annual Cybersecurity Workforce Study (ISC)2, that one of the key hindrances for cyber professionals is the lack of standardization around the cybersecurity profession as a whole, across team structure, titling and responsibilities, and terminologies (ISC2, 2018).

Leading the Cyber Workforce

During the standup of DoD Cyber efforts in 2010, RAND Corporation, an American nonprofit global policy think tank that provides research and analysis to the U.S. Armed Forces and helps to improve defense-related policy and decision-making, was asked by the United States Air Force to identify and analyze the human capital management issues associated with the establishment of a formal cyberspace organization. RAND's study addressed three research questions that remain relevant today to creating a sustainable cyber force, which can align against the human capital requirements and organizational outcomes. RAND's 2010 three main foci were:

1. Specific types of training, education, and experience necessary to produce a competitive skill set to be used in subsequent tours (i.e., periods of employment). (RQ1&2)
    a. How do these organizations' positions require cyber-hybrid skills— combinations of the mainstream specialty's skills and specific cyber skills gained through OJT?
2. The effective utilization of comprehensive cyber and leadership skill sets as necessary during specific assignments. (RQ1&3)
    a. What training needs are common across cyber-hybrid positions?
    b. Can the hybrid skills be used in other tours (follow-on cyber employment)?
3. These experienced cyber warriors must be effectively used after the end of their tour. (RQ1&3)
    a. How are subsequent assignments programmed for continued effective reinforcement of skills attained during a tour?

These questions identified a lack of in-depth cyber experience at higher levels, particularly in policy, planning, doctrine, and programming. These particular leadership positions require knowledge and skills gained through multiple cyber-related assignments to effectively lead and manage the cyber force (Scott, Conley, Mesic, O'Connell, & Medlin, 2010). While this study was focused on the U.S. Air Force during the establishment of the initial unified cyber warfighting structure, many of their questions, methodologies, and findings continue to be relevant to the U.S. Navy and the entire Department of Defense's cyber workforce leadership challenges and opportunities.

Despite ten years of development in the U.S. industrial-related and DoD cyber domains, since the initial RAND study was published in 2010, many of the challenges presented a decade ago continue to remain inadequately addressed for progressing and sustaining the needs of leaders in the U.S.'s defense cyber force. In 2019, a follow-on RAND study on recruiting and retaining cyber professionals was undertaken for the U.S. Air Force and demonstrated persistent issues. This study's findings showed that technical expertise, leadership, communication, and critical thinking skills remain essential skills needed for officers in the USAF cyber workforce, and opinions of necessary education and cyber development varied across those interviewed.

The literature demonstrates a lack of critical human factor development in the cyber workforce, specifically leadership and managerial hard and soft skills necessary to lead the future cyber force. Consequently, this Capstone research investigated the challenges the cyber workforce, specifically at the leadership and management level, will likely face in the years to come and generally proposes a framework of interventions shaped by industry best practices in 21st-century workforce development, leadership development, and in the “future force” cyber realm as potential solutions. Throughout the capstone research, we endeavored to discern broader workforce leadership aspects, in both literature and as discovered in practice, that are successful, acknowledge how and when they appear useful, and recommend ways to replicate these aspects for leadership cyber workforce.

Dawson and Thomson (2018) said that knowledge, skills, attributes, and other effective characteristics for the cybersecurity workforce should focus on six factors for the future of cybersecurity workforce development, those of systemic thinkers, team players [teamwork], passion for continuous learning, strong communication skills, a civic duty sense, and an appropriate mix of technical and social skills. Several other sources reviewed spoke to the significance of social intelligence skills for success, just as Baker (2016) and Crumpler and Lewis (2019) suggested a noted lack of soft skills across the cyber domain that required focus--attributes like communications and human behavior modeling and learning, to be specific, were essential across cyber leaders for setting the right expectations and culture in the cyber workforce. A 2020 investigative report, across 48 cyber professionals interviewed for the National Science Foundation, found that cyber defense professionals rated "communication and other non-technical skills as being very important for all cyber defense jobs" (Computer News Weekly, 2021). The Texas Tech University (Armstrong, Jones, Namin, & Newton, 2020) study stated that the following five curricula characteristics must be cultivated in future curricula development for necessary cyber professional's cyber proficiency across knowledge, skills, and abilities:

1. A computing-based foundation,
2. Crosscutting concepts that are broadly applicable across the range of cybersecurity specializations,
3. A body of knowledge containing essential cybersecurity knowledge and skills,
4. A direct relationship to the range of specializations meeting the in-demand workforce domains, and

5. A strong emphasis on the ethical conduct and professional responsibilities associated with the field.

Ten of the 19 significant Knowledge Skills and Abilities (KSA) identified in this subjective study (Armstrong, Jones, Namin, & Newton, 2020) were also subjectively identified as significant across our qualitative interviews as well. Curiosity, collaboration skills, ability to self-motivate, communication skills (across and up), and adaptability noted in the top ten KSAs of the study were also each noted in the majority of our interview responses:

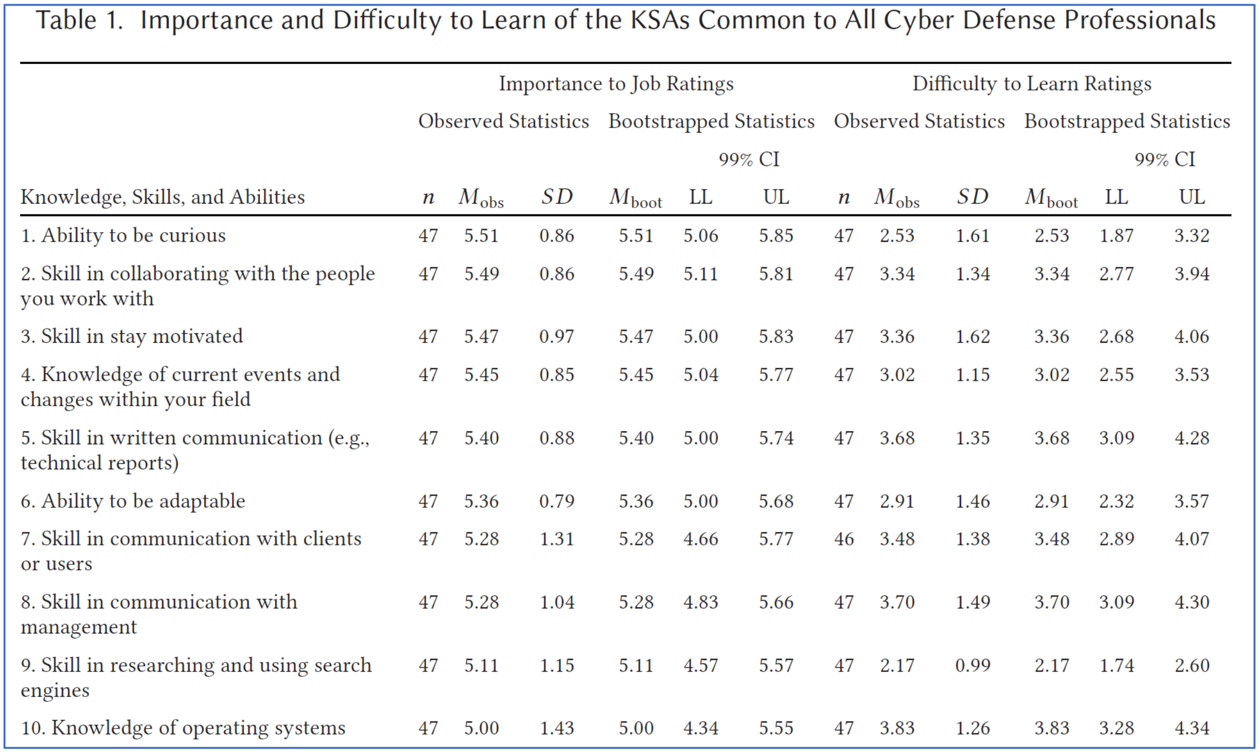


Table 1. Importance and Difficulty to Learn of the KSAs Common to All Cyber Defense Professionals

	Importance to Job Ratings						Difficulty to Learn Ratings					
	Observed Statistics			Bootstrapped Statistics			Observed Statistics			Bootstrapped Statistics		
					99% CI						99% CI	
Knowledge, Skills, and Abilities	n	M_{obs}	SD	M_{boot}	LL	UL	n	M_{obs}	SD	M_{boot}	LL	UL
1. Ability to be curious	47	5.51	0.86	5.51	5.06	5.85	47	2.53	1.61	2.53	1.87	3.32
2. Skill in collaborating with the people you work with	47	5.49	0.86	5.49	5.11	5.81	47	3.34	1.34	3.34	2.77	3.94
3. Skill in stay motivated	47	5.47	0.97	5.47	5.00	5.83	47	3.36	1.62	3.36	2.68	4.06
4. Knowledge of current events and changes within your field	47	5.45	0.85	5.45	5.04	5.77	47	3.02	1.15	3.02	2.55	3.53
5. Skill in written communication (e.g., technical reports)	47	5.40	0.88	5.40	5.00	5.74	47	3.68	1.35	3.68	3.09	4.28
6. Ability to be adaptable	47	5.36	0.79	5.36	5.00	5.68	47	2.91	1.46	2.91	2.32	3.57
7. Skill in communication with clients or users	47	5.28	1.31	5.28	4.66	5.77	46	3.48	1.38	3.48	2.89	4.07
8. Skill in communication with management	47	5.28	1.04	5.28	4.83	5.66	47	3.70	1.49	3.70	3.09	4.30
9. Skill in researching and using search engines	47	5.11	1.15	5.11	4.57	5.57	47	2.17	0.99	2.17	1.74	2.60
10. Knowledge of operating systems	47	5.00	1.43	5.00	4.34	5.55	47	3.83	1.26	3.83	3.28	4.34

Figure 1 2020 KSA Study (Armstrong, Jones, Namin, & Newton, 2020)

This 2020 study on KSAs was a follow-up to a previous 2018 study (Jones, Namin, & Armstrong, 2018) from interviews with cybersecurity professionals. The persistent study of cyber professional skills and education provides little definitive guidance based on industry demand for what cyber leaders must have in skills and capabilities. Keith et al. (2018) said, “there is little academic study as to whether KSAs being taught in existing cybersecurity programs match those demanded by the cybersecurity workforce.” The results of the 2018 study identified the following KSAs as most important for cybersecurity professionals, mirroring many of the requisite leadership and management skill attributes identified in our capstone research:

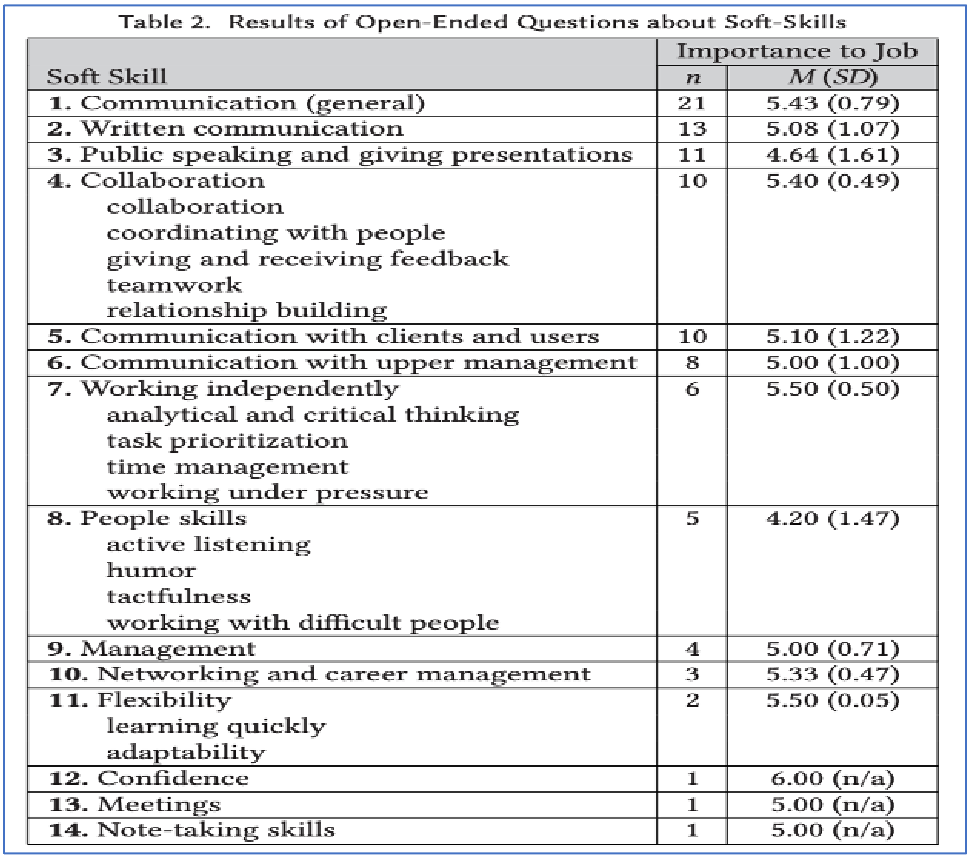


Table 2. Results of Open-Ended Questions about Soft-Skills

	Importance to Job	
Soft Skill	*n*	*M* (*SD*)
1. Communication (general)	21	5.43 (0.79)
2. Written communication	13	5.08 (1.07)
3. Public speaking and giving presentations	11	4.64 (1.61)
4. Collaboration collaboration coordinating with people giving and receiving feedback teamwork relationship building	10	5.40 (0.49)
5. Communication with clients and users	10	5.10 (1.22)
6. Communication with upper management	8	5.00 (1.00)
7. Working independently analytical and critical thinking task prioritization time management working under pressure	6	5.50 (0.50)
8. People skills active listening humor tactfulness working with difficult people	5	4.20 (1.47)
9. Management	4	5.00 (0.71)
10. Networking and career management	3	5.33 (0.47)
11. Flexibility learning quickly adaptability	2	5.50 (0.05)
12. Confidence	1	6.00 (n/a)
13. Meetings	1	5.00 (n/a)
14. Note-taking skills	1	5.00 (n/a)

Figure 2 2018 KSA Study (Jones, Namin, & Armstrong, 2018)

Over more than just the past decade, education systems have created a separation between the training that cyber technicians receive and the training of the leader who will be responsible for implementing those technicians (Virginia Dept. of Education, 2017). From high school courses through to college and technical schools, as confirmed across other relevant literature, courses of study predominantly focus on cyber workers' technical skills but not on leadership skills. As an example of this, the National Initiative on Cyber Security Education (NICE) Workforce Framework 2.0 defines the cyber workforce's standard roles and has attempted to redefine many of the related Knowledge, Skills, and Abilities. However, looking into the NICE KSAs of Executive Cyber Leadership (OV-EXL-001), the primary knowledge and ability requirements listed are technical focused, and associated skills do not even include requisite leadership fundamentals. These same professionals are directed to lead budget, staffing, and contracting but are not given a skill description on how they are to accomplish these leadership tasks (NIST, 2019). The education requirement for this same Executive Cyber Leadership position recommends a bachelor’s or an associate’s degree but again focuses on the technical side and not the leadership side for a manager or supervisory role.

A 2020 Congressional Cyberspace Solarium Commission, established in FY2019, was tasked to identify a strategic approach to protect the U.S. against attacks of significant consequence in cyberspace, found that when looking at the cyber technician aspect, requirements to have at least a bachelor's degree across the cyber force, shut out "a wealth of talent represented by self-taught employees, employees with an associate's degree and industry certifications, and those with many other unconventional educational backgrounds. Employees below the bachelor's level who possess solid cyber skills have shown both an ability to make immediate and valuable contributions to critical cyber tasks and a propensity to embrace continuing professional development" (Bate, 2020).

Finally, after reading Scott et al.'s address of "How Should Cyber's Strategic Human Capital Be Developed?" (Scott, Conley, Mesic, O'Connell, & Medlin, 2010), we resolved what was required for our project's research questions.

Research Questions:

RQ1. What kinds of skills and capabilities will the Department of the Navy cyber supervisors need to effectively lead the cyber workforce?

RQ2. How can the Department of the Navy develop the appropriate supervisory and leadership personnel responsible for leading, managing, and developing the rest of the cyber warfighting force?

RQ3. What intellectual infrastructure is needed to support viable, sustainable cyber management/leadership?

Project Design

Qualitative Interview Data Acquisition

This project utilized a mixed-methods approach principally focused on qualitative data from semi-structured interviews. At the client's request, we also pursued varied quantitative data points to analyze potential surveys available from relevant literature and (ISC)2’s annual Cybersecurity Workforce study, and other accessible cyber climate survey-related data for possible incorporation. We sought to define the current cyber understanding of leaders and warfighters and the desired skill versus actually delivered skill within the DoN and across the cyber workforce.

Our initial project design goal for data collection targeted thirty interviews, ten across each cycle/employee level (entry-, mid-, and senior-level interviews). However, during project execution, due to achieving saturation of themes and difficulty in obtaining mid- and entry-level interviews during the COVID-19 pandemic, we modified the plan. Instead, we conducted nineteen qualitative interviews, including senior (14) and mid-level (5) cyber professionals. To understand what skills entering cyber professionals see as necessary skills to succeed in the cyber field, we obtained 158 anonymous entry-level quality survey responses from a Fairfax County Public Schools (Fairfax, Virginia) sponsored survey of graduating seniors enrolled in cyber programs. Graduating high school seniors represent the focus of primary recruiting efforts across the Navy for entry-level USN positions. Finally, we conducted a generous review of applicable literature pre-project and post-interviews to capture cyber workforce gaps, needs, and challenges for further understanding the cyber workforce and additional clarity on new aspects and insights discovered in interviews and surveys.

Throughout qualitative data gathering, leadership-level personnel were interviewed to gauge their current understanding of leading and managing the emerging cyber workforce. We then looked at how entry-level perceived skills, collected in the FCPS survey, align with senior leadership's conveyed expectations. The second set of interviews focused on mid-career (roughly 5-12 years in the field) cyber professionals. They were conducted to determine how their skillsets and perceptions on leadership have changed or developed in response to the changing demands of the cyber sphere-of-operations over time after working in it at a mid-level. The third set of data collection focused on incoming, junior (entry), technical level personnel to determine what skills and abilities they believe they are bringing to the force that will need to be managed by cyber leaders.

Entry-Level Survey Data Acquisition

This data collection capture was facilitated by a curriculum survey conducted in Fairfax County Public Schools for graduating high school seniors enrolled in various cyber fundamentals programs. 158 students across FCPS courses presently offered in A+, CompTIA, Cyber Fundamentals, Cyber Security Fundamentals Networking, Oracle and Cisco standard courses, and programming and data management curricula participated in the survey. During all class years during the 2020-21 school year, the total enrollment in these courses is 1,151 students. The anonymous, open-ended, entry-level quality survey responses assembled a richer data source than the original project design expectation of ten entry-level interviews from existing Department of Navy employees. These respondents are Gen Z (born 1996-on), which will principally be led and managed by Millennials or Gen Y (born 1977-1995), as well as Generation X (born 1965-1976). The FCPS survey captured data regarding what future entry-level members of the cyber workforce consider is important across leadership skills and capacities of their future supervisors, leaders, and managers. It captured beliefs on cyber skills, capabilities, and leadership. This data helped us compare leadership level understanding of leading and managing the emerging cyber workforce against future cyber worker’s perceptions to determine similarity and difference gaps in skills appreciation.

Methods of Interviews

We conducted interviews of professionals at the mid-level (federal civilians at the GG-13/14 level, military officers at the O4 level, and industry) and senior-level ((Navy Admirals, Captains, and Commanders (O5-O8 level on an O1-O10 military rank spectrum)), equivalent senior federal executives (C-suite level) and industry representatives) around the Department of Navy. Interviews were structured across roughly fourteen primary interview questions pertinent to understanding mid-level and senior-level insights. We initially anticipated conducting roundtable (focus group) interview formats, as well. However, only one of the eighteen interviews had two participants; the remainder were individual interviews. All eighteen interviews of nineteen people conducted were represented and treated as identity confidential.

Thirty-three interview requests were solicited, and nineteen were conducted. Interviews were conducted virtually. Due to the current pandemic (COVID-19), all interviews maintained the Centers for Disease Control (CDC) approved social distancing guidance by utilizing Zoom, Teams, and WebEx virtual meeting and teleconference systems. We emailed our research questions and interview questions, depending on the interviewee's seniority-level, before interviews for their preparation and consideration. Each interview lasted about one hour, yielding over twenty hours of recorded qualitative interview data for analysis. We generally allowed the interviewee to respond and inform us on the key points that they desired to convey in a free-flowing way, asking clarifying and prompting questions as we went. This semi-structured format execution allowed us, we believed, to hear what the interviewee desired to convey most as insights. However, not strictly subsequently proceeding through questions for each interviewee consistently created some unanticipated inconsistency in interviewee responses sequencing and potentially impacted keyword/theme coding. Consequently, this also impacted and potentially skewed our perceptions of themes and data significance.

Interviewees were selected by request to various commands in the cyber domain of the Navy, specifically, U.S. Fleet Forces Command (FFC), Fleet Cyber Command, and cyber-related personnel and policy elements subordinate to the Secretary of the Navy's and the Chief of Naval Operations' (CNO) offices (OPNAV). Several interviewees came from OPNAV N2/N6, the Navy's primary office focused on national security and operations, to include resourcing cyber-related capabilities. The capability centers interviewed came from the Navy Cyber Defense Operations Command (NCDOC), Navy Cyber Warfare Development Group (NCWDG), Office of Naval Intelligence (ONI) personnel, and the U.S. Naval Academy's (USNA) Center for Cyber Security Studies. Our project planning anticipated interviews with the Information Warfighting Development Centers (IWDCs); however, we could not directly interview the "schoolhouses." We were able, though, to achieve a wealth of data from "snowballing" our interview contacts and professional networks to garner interviews with some now-retired-from-the-Navy senior-officers currently in private cyber industry work (Raytheon, Cisco, SAIC, and EXCEL Technologies) that provided fuller pictures of their perception of the cyber domain and leadership in it. Participation was voluntary, and to ensure confidentiality, only a thematic synopsis of responses, without name attribution, will be given to our capstone client for further use.

Data Analysis and Interpretation

Fairfax County Public School's survey data was collected from unstructured responses to questions regarding skill sets necessary for success in the cyber field. From this open-ended survey, the top leadership and managerial characteristics identified across the survey responses were: communication, experience, integrity, confidence, knowledge, commitment, courage, and honesty (Appendix

4) (FCPS CTE, 2020). This survey was produced from 320 respondents to open-ended questions presented to students in various cyber programs across the county. When only the high school seniors' responses were selected, this yielded 158 respondents. 78 of the 158 respondents answered the three cyber-specific questions (one on leader/manager skills, one on technical, and one on non-technical skills already trained to).

Once the more than twenty hours of recorded and transcribed Zoom, Teams, and WebEx virtual notes from the nineteen interviewees were completed, survey data from the Fairfax County Public Schools survey was compiled with the 78 refined responses; both sets were imported into MaxQDA for coding and analysis. Interviewer comments were removed from the search, and initial coding (lexical search) was based upon the capstone's three research questions and were implemented in the following manner:

- RQ1 was coded as Skills and Capabilities and generated 528 references across the interviews.
- RQ 2 was coded as Leading Managing Developing and generated 679 direct references in the interviews.

- Finally, RQ3 was coded as Intellectual Infrastructure Sustained Training. It generated 781 coded segments across the interviews, which also encompasses RQ1 and RQ2 items into consideration and is represented by the cloud (Figure 3) and table (Table 1) below:

Initial coding allowed us to create a word cloud of terms related to each of the interviews' traits (Figure 3 and Table 1).

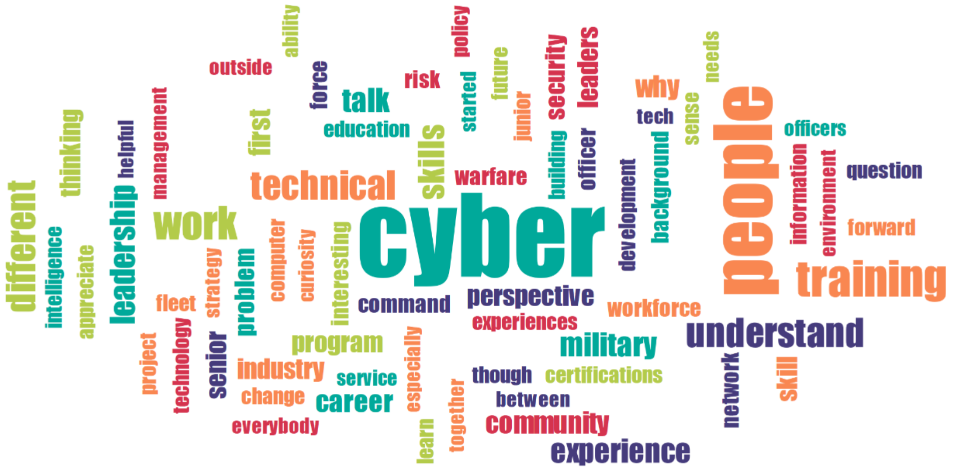


Figure 3 Interview Word Cloud

Word	Frequency	Rank	Documents %
cyber	754	1	100.00
people	504	2	100.00
training	264	3	100.00
technical	195	4	100.00
understand	186	5	100.00
different	185	6	100.00
skills	166	7	93.75
leadership	149	8	93.75
experience	137	9	100.00
military	130	10	100.00

Table 1 Interview Word Frequencies

This provided our first look at the relative importance of the traits necessary that our client needs to consider for leadership and managerial skill and capacity development in the current and future cyber leaders. With this visual, we refined our coding to incorporate the top characteristics also identified from the FCPS survey (Figure 4, Table 2).

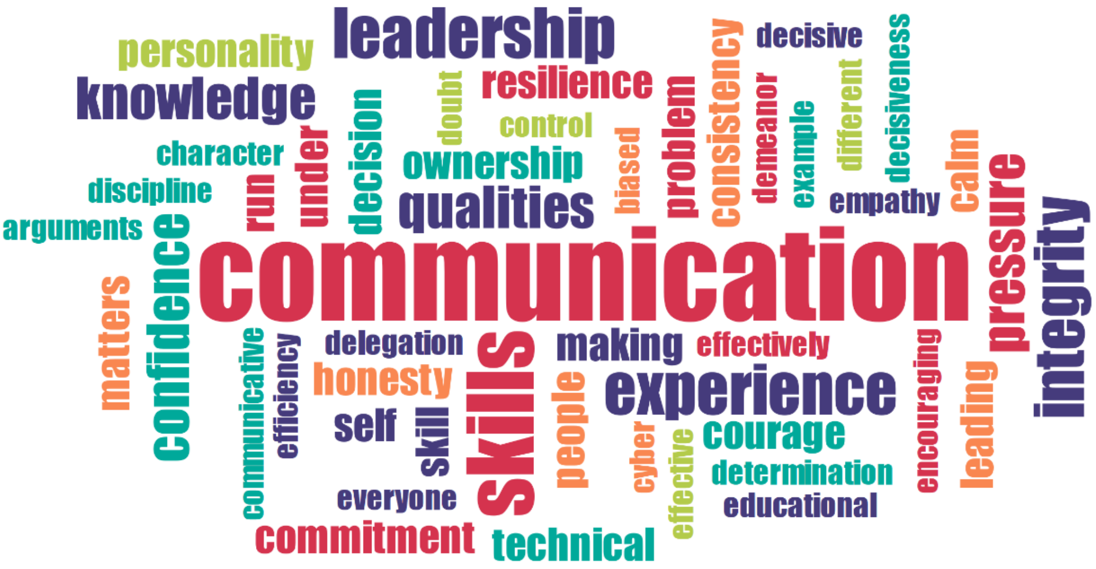


Figure 4 Refined Combined Word Cloud

Word	Frequency	Rank	Answers containing (%)
communication	9	1	11.69
skills	6	2	7.79
experience	4	3	5.19
integrity	4	4	5.19
leadership	4	5	3.90
confidence	3	6	3.90
knowledge	3	7	3.90
pressure	3	8	3.90
commitment	2	9	2.60

Table 2 FCPS Word Frequencies

These additional lexical codes highlighted the most critical coding sets and their component traits. They identified commonalities and distinctions between the skills that senior leadership demands and entry-level workforce perceptions. These traits were then re-coded into Communication, Integrity, Leadership, People Skills, Technical Skills.

Leadership, People and Development

The commonality of desired skills refutes the perception that cyber leadership-level and technical-level employees are not focused on the same skills. Specifically, Leadership, People, and Development are at the forefront of both groups, with over 700 related segments identified in the interviews. When combined, these skills were also the highest responses for skills that entry-level personnel expect to need and are necessary to succeed in the cyber field.

Furthermore, there was a distinction between technical skills and being seen as a technical expert. Only six specific responses from interviewees characterized "technical expert" as a necessary trait for leadership in the cyber community. When contrasted with a baseline technical skill set that generated 288 responses, the interviews established that while technical understanding is essential, a leader does not necessarily need to be the subject matter expert; instead, they need to rely on and manage the technical skills that their workforce possesses.

We were surprised in our project design execution by the difference between what we believed we heard in the moment as interviewers capturing themes in real-time versus what the MaxQDA qualitative interview coding application picked up in over 65,000+ words spoken.   However, not strictly proceeding through questions sequentially for each interviewee created some unanticipated inconsistency in interviewee responses and potentially impacted keyword/theme coding. To resolve the issue, we manually reviewed each transcript while also listening to the recordings to ensure data integrity further. We then undertook a laborious process of combing through each transcript, sifting and compiling original quotes at four distinct leadership binned levels: mid-level civilians (now DoN GG-13/14s and industry), senior-level active-duty

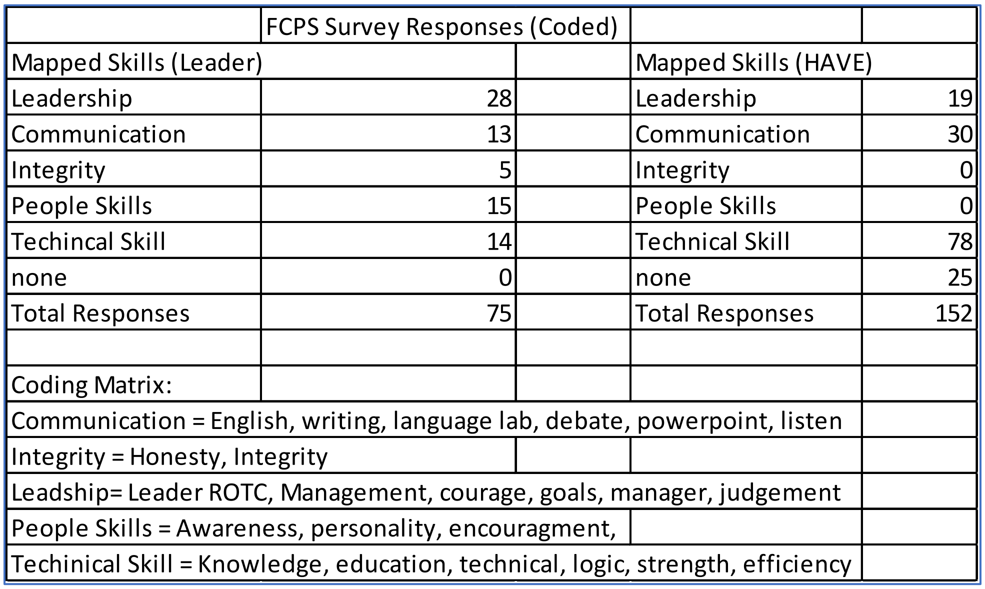
Captains (O6), senior-level retired military Captains (O6) now senior federal executives, and finally, senior-level retired Admiral (O8), Captain (O6) and Commanders (O5) now industry executives. Sifting for original quotes to represent our qualitative data allowed additional capacity for binning of themes for findings.

Despite this difference in what we heard and what was captured in transcription, we had to consider what was essential for developing the skills to lead and manage the cyber workforce. Our data analysis uncovered that several critical components support the continual challenge of staffing, training, and equipping the DoN cyber force with the technology, skills, and equipment necessary to meet current and future cyber challenges. These leadership, people, and development components aligned to three primary loci that needed to be reviewed: learning, organizational structure, and strategy.

Findings

Survey Responses

The FCPS survey provided two very distinct data points regarding cyber leadership and managerial capacities. First, what leadership and management skills have students received that will enable them to be a cyber leader. Next, what leadership and management skills students enrolled in a cyber program expect their future bosses (leaders) will have. For skills that they have already been trained in, as expected, technical foundational skills such as programming, security, network operations were the top reported skills, with 78 responses indicating training in one or more of these areas. Contrast this to students' expectation that their leaders will have leadership skills (including management, courage, goals, judgment) as indicated by 28 responses. A total of 61 responses included leadership, communication, and people skills, while only 14 survey responses called out a need for technical skills.



	FCPS Survey Responses (Coded)			
Mapped Skills (Leader)			Mapped Skills (HAVE)	
Leadership	28		Leadership	19
Communication	13		Communication	30
Integrity	5		Integrity	0
People Skills	15		People Skills	0
Techincal Skill	14		Technical Skill	78
none	0		none	25
Total Responses	75		Total Responses	152
Coding Matrix:				
Communication = English, writing, language lab, debate, powerpoint, listen				
Integrity = Honesty, Integrity				
Leadship= Leader ROTC, Management, courage, goals, manager, judgement				
People Skills = Awareness, personality, encouragment,				
Techinical Skill = Knowledge, education, technical, logic, strength, efficiency				

Table 3 FCPS Survey Coded Responses

Once these skills were encoded as described in table 3 above, we combined integrity into the leadership skills category, applied the same coding to the interview structure, and arrived at (Figure 5) to depict the leadership and managerial skills required of leaders within the cyber community.

Specifically, this led to the top 25 traits list, as shown in table 4 and Figure 5, representing holistic findings.

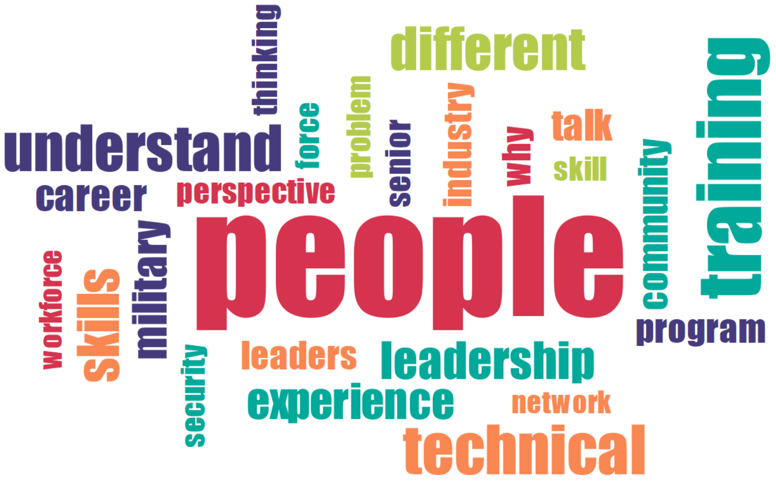


Figure 5 FCPS Survey Word Cloud

Word	Word length	Frequency	%	Rank	Documents	Documents %
people	6	546	1.51	1	17	100.00
training	8	274	0.76	2	17	100.00
technical	9	205	0.57	3	17	100.00
understand	10	190	0.53	4	17	100.00
different	9	188	0.52	5	17	100.00
skills	6	173	0.48	6	17	100.00
user	4	166	0.46	7	5	29.41
leadership	10	162	0.45	8	17	100.00
military	8	147	0.41	9	17	100.00
experience	10	144	0.40	10	17	100.00
talk	4	132	0.37	11	17	100.00
career	6	131	0.36	12	17	100.00
community	9	125	0.35	13	17	100.00
industry	8	124	0.34	14	16	94.12
program	7	116	0.32	15	15	88.24
why	3	116	0.32	16	17	100.00
leaders	7	112	0.31	17	17	100.00
senior	6	108	0.30	18	15	88.24
thinking	8	106	0.29	19	17	100.00
perspective	11	104	0.29	20	16	94.12
workforce	9	104	0.29	21	15	88.24
skill	5	99	0.27	22	15	88.24
problem	7	97	0.27	23	17	100.00
security	8	96	0.27	24	15	88.24
force	5	91	0.25	25	17	100.00

Table 4 FCPS Top 25 Traits

Summary of Interviews

Interviewee Backgrounds

Eighteen of our interviewees are presently cyber leaders and officers in the Navy (4), retired after full 20–30-year careers in the Navy (11) or Army (1) with some Navy cyber jobs, or have prior military service (2) from which they then joined the DoN cyber effort in the federal government. This is an important factor when considering the leadership and management development lenses that these interviewees apply to their qualitative perceptions. These cyber leaders were "built" and developed inside a structure that has factored in deliberate opportunities and training milestones to build and use their leadership and management skills over time. They each had significant opportunities to develop foundational leadership skills such as effective communication, problem-solving, decision-making, teamwork, collaboration, risk management, people skills, business skills, and project management capabilities. Our interviewees each have had the opportunity, as Navy cyber is just over eleven years old, to build, develop, and now strategize for the Navy cyber system that currently exists. Because of their military backgrounds, these interviewed leaders know public service as well as their demonstrated commitment to it.

Our interviewees presented diverse backgrounds in education, career paths, and cyber employment. Many developed their leadership skills in their early career over progressive leadership opportunities in communities other than cyber. Consequently, we have to be careful in prescribing any one-size-fits-all development plans, paths, or right or wrong deemed capabilities and instead capitalize on the training available to more established warfare communities. This notion is bolstered in an interview with a comment of, "…people are looking for the one-size-fits all approach page, and that does not work" (Int-4, 2020). A DoN cyber leader previewed their prescription of the necessary cyber leader development path stating, "A little bit of OJT a little bit of these hands-on certifications. Guild on the job training is how we end up building people; it's ad hoc" (Int-2, 2020).

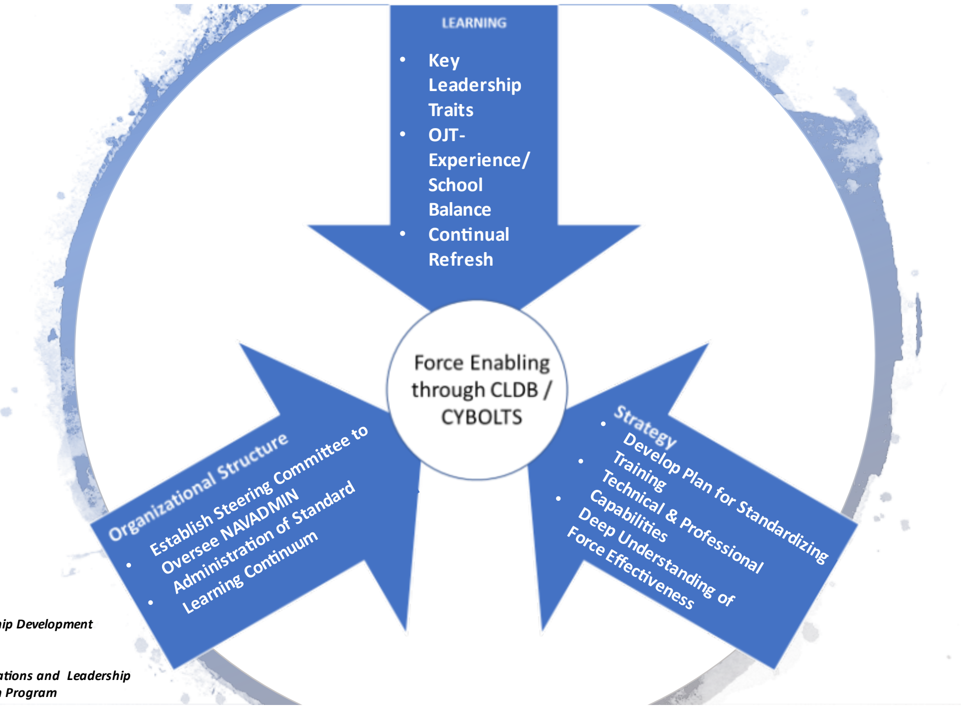
Many interviewees indicated a need and desire for broad learning opportunities that allowed them to learn and grow from the environments and experiences they encountered flexibly and creatively. Though, we noted, this is not a one-size-fits-all, standardized path. Curiosity, passion, life-long learning, and self-development that iteratively builds an effective cyber leader and manager up, we found to be very individual-based and personal, requiring a significant amount of personal initiative and determination. This notion indicates a significant shift in what cyber leader development and investment need to be into the future. The significance of these noted attributes and skills across our findings increases the broader body of knowledge on both leadership and learning for organizations.

Additionally, our interviewees each spoke about their cyber careers as ones of happenstance and “dumb luck” (Int-12, 2020) employment that they came to love. They did not have the opportunity to intentionally affiliate with the cyber community; they were detailed into the job and then found ways to stay around it and make it part of their careers. They predominantly started their careers as aviation, surface warfare officers, submariners, cryptologists, strategic intelligence officers, information technologists, or naval architects. In the past ten plus years, they were afforded opportunities to establish and command TENTH Fleet, NCWDG, and Naval Information Operations Command or do acquisitions, manning, and data and statistical analysis jobs. These unique career paths or trajectories shaped their cyber, leadership, and management experiences and views. Almost all of our interviewees perceived nothing “traditional” in their experiences from which to standardize from. One aspect that we did hear as standard in this area was their belief that they were each forged by on-the-job training, critical watch floor experiences, and trial by fire that honed their out-of-the-box thinking, flexibility, communication skills, and human skills ((Int-13, 2021) (Int-7, 2020) (Int-4, 2020) (Int-16, 2021)).

Many commented that they wish they had more opportunities to experience the industry side of cyber, giving them a better, clearer understanding of the field, not just defense-focused defensive and offensive cyber aspects. One mid-level interviewee stated, "[It] was an invaluable experience to learn how industry is doing it" (Int-15, 2020). Another senior, now in industry, alluded to the potential that industry is grappling with technical and non-technical career paths for leaders and managers versus technical subject matter experts. They said, "industry is moving towards a model where there's two distinct career paths. There's a management leadership career path out here, and there's a technical career path where when you get to a certain level, you do manage and supervise, but it is in technical verticals. In both places, though, fundamental proof of technical expertise somewhere in your background is expected" (Int-13, 2021). Another retired senior, now industry senior, stated that, "…when you really look at what commercial industry does...cyber is not something that supports business--it is part of business. They are willing to invest in it, and they are willing to have the right people work on it. I mean, it's stunning to see what is actually in the art of the possible" (Int-1, 2020).

Development of Learning, Organizational Structure, and Strategy

Many key prevalent findings are presented across our qualitative interviews that are significant when considering our specific cyber leadership and management findings and recommendations. As the interviews were completed, it became clear that each of these pervasive findings fell into three distinct areas: Learning, Organizational Structure, and Strategy. RQ 1 is most closely mapped with learning, RQ2 is aligned primarily with organizational structure, and RQ3 aligns with the overarching theme of an intellectual infrastructure strategy. These three themes define the stated skills and efforts needed for creating development and intellectual sustainment considerations for Department of the Navy aspiring leaders and current leaders and developing a cyber leader development plan for civilian and military leaders. This mapping is demonstrated in Figure 6.


LEARNING
• Key Leadership Traits
• OJT- Experience/ School Balance
• Continual Refresh
Force Enabling through CLDB / CYBOLTS
Organizational Structure
• Establish Steering Committee to Oversee NAVADMIN
• Administration of Standard Learning Continuum
Strategy
• Develop Plan for Standardizing Training
• Technical & Professional Capabilities
• Deep Understanding of Force Effectiveness

CLDB= Cyber Leadership Development Board

CYBOLTS= Cyber Operations and Leadership Training and Selection Program

Figure 6 3 Means to Cyber Leader Development

Learning – RQ1

What kinds of skills and capabilities will DoN cyber supervisors need to effectively lead the cyber workforce?

Learning is considered the ultimate strategic advantage and is essential in the organizer's arsenal toward addressing this RQ. Put simply by one respondent, "[learning] let's one understand the limitations of the art of the warfare and the advantages" (Int-3, 2020). As conveyed in our initial project introduction, to defend against cyber threats, now and into the future, a significant demand for a skilled cybersecurity workforce is necessary—in the realm of hundreds of thousands of skilled employees required in the U.S., with cyber leaders applying honed leadership and management acumen in place to lead them. Previous studies conducted by the USAF and the DoD have not provided insight into the critical leadership and interpersonal skills needed for a cyber leader to succeed in the Department of Navy when leading highly technical cyber experts. However, non-military literature over the past decade and recent congressional findings up to 2020 convey that attention on the correct cyber skills, capabilities, leadership qualities, and sustainment training have been near-constant topics of focus without clear, definitive findings to inform a development pathway.

The ultimate goal of RQ1 was to discover, discern and define the key skills and capabilities necessary for effectively leading cyber warriors to develop a strategy that will underwrite a learning plan. We find it crucial to balance human skills and technical understanding as a cyber leader and manager from qualitative data. There is a significant overlap in the cyber domain across leadership and relational skills, problem-solving, and critical thinking skills while also needing progressive experience, varied qualifications, and sufficient technical expertise. So, a balanced mix of human skills, capabilities, and also technical skills is necessary. Our findings agree with the need for upskilling a leader's skills and capabilities across a myriad of identified hard and soft skills previously noted in our lexical coded outputs (Figure 5, table 4).

People: Leading DoN's Most Important Cyber Asset

Every interview that we conducted pointed out that "people" (546 responses from all interviewees) were ultimately at the core of any cyber leadership and management program. Thus, developing these skills is essential to maintaining an effective cyber force. A retired senior, now federal executive, said, "I think that the skills and capabilities that you are talking about are people skills. You have got to have the people skills... that is still the foundation of leading any workforce…. Secondarily, then, is [you take care of] the technical acumen because no amount of the technological expertise is going to overtake those basic tenets of leadership" (Int-10, 2021).

Becoming a good cyber leader requires practice in focusing on people as the most important aspect of leadership. The surest way to lead the cyber workforce is based on diligent preparation for working with people from day one in the cyber community. Developing a cyber leader requires a sound approach, knowledge of the enterprise and its activities, and the key people to undertake the following leadership actions: 1. making the decision, and 2. motivating their workforce behind that decision. This second responsibility (motivation) requires engaging, empowering, and inspiring their cyber team. One interviewee suggested, "I think as a leader right now, leaders develop talent, managers use talent, and I think you need both [of these skills]. I think leaders provide a new vision, direction, prioritization..." (Int-2, 2020). Stated differently by another senior interviewee, "we lead people that take care of machines, so we need to take care of people and manage the things [the machines] … [We need to] continue to emphasize [our focus on] the people who are doing the work…" (Int-4, 2020).

Cyber leaders must build themselves and the team around them up with the right mix of skills and experience to handle all aspects of varied cyber situations. To be successful leaders, any leader must rely on a sound foundation built from broad exposure and diverse experiences to solve problems flexibly and creatively. “[Leaders] bring more of those soft skills with them, like team-building, problem-solving, [and hard skills of] critical thinking and are able to think at a higher level... [Leaders] in their careers get opportunities to use communication skills, critical thinking, and executive briefing opportunities. They are learning a lot of the collaborative skills through the nature of the work that they are doing, and then they are transitioning back as that senior leader, having both packets of skills [soft and hard skills]…” (Int-5, 2020). A mid-level leader also stated, “leadership is where you get out and about and are able to understand your people. That leader does not need to know how to work a keyboard. But, they do need to understand what they want their people to accomplish, or to be able to accomplish and what is realistic” (Int-12, 2020).

Developing a balanced mix of human skills, and capabilities, and technical skills is necessary. This skills mix (coded as Leadership in our lexical coding) incorporates communication, experience, understanding, and perspective that our senior interviewees identified, as did 75 responses from the FCPS survey. “Perhaps more than any other warfighting community, cyber is subject to continual evolutionary and revolutionary developments” (Int-16, 2021); consequently, leaders need to be equipped with sufficient skills.

Understanding and developing these skills comes from a strong foundation of past technical skills and expertise and exposure to a wide variety of cyber problem sets that change quickly and frequently over time. This technical skills foundation combined with daily practice builds cyber leaders' confidence in their ability to perform greater and greater leadership efforts. While cyber leaders must understand the technical aspects, they do not need to be technical experts. Interviewee 15 pointed out that leaders need “a working understanding, not necessarily in-depth, current technology, and the basic cyber theories. They don't need to get very specific… they have got to have that basic understanding. So, they can actually talk the lingo” (Int-15, 2020). As put by one interviewee, “... everyone needs to at least have a basic understanding of cyber. It doesn't have to be in-depth. That's why you have your more technical people who have got the experience. But a supervisor needs to be able to understand it enough. Especially … to understand what is being discussed and if it makes sense…” (Int-17, 2020). A few mid-level leaders in the community also acknowledged that while cyber technical skills will atrophy over time, leaders' ability to understand and interpret their personnel's efforts is essential. Other comments on the technical understanding balanced with leadership included:

"… I am not technically savvy. I do not go in and hit the keyboard and code magically comes out. I am not connecting cords. But what I was good at was asking the question of the techie people and interpreting it in a way so that leaders could understand it…" (Int-14, 2020).

"…you have the people in the middle, the people that have to interpret one to the other. When the leader says, find me the rock, your job in the middle is to turn that into tech speak so that the tech guys can understand that requirement of what rock that really means. And when the techie finds the rock, the person in the middle goes back to the leadership and turns that rock back into information they understand" (Int-14, 2020).

People skills, and the ability to interpret the technical skill set is developed at the mid-level leadership cadre. This is the level where sailors and civilians are senior enough to understand the role of cyber and its integration into the larger battlespace. While they may have been taught or at least had the chance to observe these skills, it is not until a growing cyber leader is in a mid-level position that they have the opportunity to apply these skills (and that they truly understand their importance.) They must know their networks: the technical (internet etc.) and the intellectual (people). They have to know what they need their team to do, what information they need from their team, and who they need to report up to.

As a DoD element, the people we interviewed work in a hierarchical military environment and have excellent leadership skills and great discipline. They typically have the strong communication skills needed for the clarity and effect required in their day-to-day employment. Over a career, they received training and experiences for proficiency in the jobs they were asked to carry out. One respondent noted that “[Communication] needs to be able to be clear to the leadership side, but you also have to be able to ask the right question” (Int-14, 2020). Technical experts are often placed in nascent leadership roles and do not have the organizational understanding to interpret, direct, and communicate their personnel's efforts. Unfortunately, two interviewees stated that, “people don't understand the org charts and the lines of authority and who is responsible for what from the outside looking in…. What are the authorities? What are the rules?

What are the policies…?" (Int-2, 2020). Early training in these fundamental competencies will lead to success for leaders and executives. These skills that must be taught ((also defined as Office of Personnel Management (OPM) competencies (DCPAS, 2013)) include interpersonal skills, oral communication, integrity/honesty, written communication, continual learning, and public service motivations.

We have frequently heard that leadership skills are innate behaviors, and there are numerous references to "born leaders" that our interviewees noted (Int-2, 2020). This acceptance of ability has undermined the fact that many of these skills can be taught, refined, and developed by a training and education pipeline that develops more than the technical skills. Even high school seniors (from the FCPS survey) called out that they knew they needed to develop effective communication, people, and leadership skills. Still, many have not received training in these skills (only 49 responses identified having received training in these areas). While all 78 respondents acknowledged a baseline level of technical training, 25 respondents specifically stated that they had received no prior education or training in any of the coded areas of communication, leadership, people skills, and integrity. Those entering the Navy are not necessarily bringing these skills with them and will need to be trained and given the opportunity to develop a leadership skill set to transition into mid-level leadership roles.

Additional skills such as budget, authorities, project management, and problem-solving can also be taught and then exercised by personnel under the guidance of mid and senior-level personnel until proficiency is proven. Several interview responses specifically noted functional leadership skills of problem-solving and conflict resolution as skills that can also be trained throughout one's career to be ready for increasingly complex leadership roles. An interviewee noted, "What we need to do is train folks to lead! Conflict resolution is probably the biggest one for me and I've seen that with a lot of techies. That is probably the hardest thing for techies to do is when two people disagree to kind of come to a resolution" (Int-15, 2020). One interviewee stated that character integrity, knowledge, education, and courage are necessary, and interviewee number 10 states, "… it's communicating; it's motivating, it's all underpinned by character integrity…" (Int-10, 2021). Integrity is a trait, though, that cannot be classroom taught, as interviewee 3 noted, "Character can't be grown overnight. That's something that's learned over the long term" (Int-3, 2020).

Our findings for RQ1 regarding labeled skills and capabilities are consistent with findings conveyed in previous research and literature on what cyber leaders require now and in the future. Knowing how to communicate and translate effectively, and listening to others, are critical skills conveyed by our responders. While all the cyber leaders were comfortable with the technology they are working with, they also needed to guide others about specific technical skills pertinent to each job and employment. As leaders, they had to balance the right mix of managing efforts and leading people. Simply put, by interviewee 10, "…I don't care what you put down as the descriptor of the objective, if you are going to be a leader, you have got to have the people skills" (Int-10, 2021).

Entry Level Views on Leadership and Management Skills

Even in the early stages of student's training and education, those potentially entering the cyber workforce have seen a mismatch between their skills and what they believe will ultimately either be desired or required by the cyber community. They recognize the distinction between their learning of technical skills, as well as developing their leadership and management skills. As one respondent noted, "The qualities for a successful organization are good communication and good skills and experience" (FCPS CTE, 2020). They also acknowledged traits such as “motivation,” “character,” and “the ability to work under pressure…” (FCPS CTE, 2020), as essential leadership skills. Additional survey responses (also noted in Appendix 4) included: “Good judgment,” strength in their field,” “efficiency,” “communication skills,” “honesty,” “integrity,” “hardworking,” “decisiveness,” “educational experience,” “character,” “prior knowledge,” “strict,” “self-awareness,” “courage,” “non-biased,” “morale-building,” and “consistency” (FCPS CTE, 2020). Yet, they identify that they have had few opportunities to practice these skills from the prescribed training and education they have thus far received for their desired cyber career path.

Diverse Learning is Necessary

Our interviewees’ educations ranged from bachelor’s in mathematics and computer science to English, economics, and history degrees. Many had master’s degrees in operations research, organizational strategy, or systems engineering. Several had PhDs in STEM-related topics. Some had relevant industry cyber certifications like CISSP and CISO, and others had project management or defense acquisition certifications. Liberal arts skills were highly valued when they were coupled with basic cyber fundamentals understanding. Our interviewees also indicated that strict cyber certifications are no longer applicable or necessary though, with one stating, “certifications, are great, especially if you want to learn more toward the techie heavy side, but [they are not] necessarily a requirement to be a good leader in the cyber world“ (Int-14, 2020).

Both current and retired DoN leaders opined that they do not believe that four-year engineering or STEM-focused degrees are required to lead the cyber workforce of the future, be it for civilian leaders or USN sailors. Over half of our interviewees said that they had liberal arts backgrounds in undergraduate and graduate degrees that seemed consequential for developing their strategic thinking competency, critical thinking, problem-solving, and better affect their acquisition and resourcing capacities. With responses such as, “I would say that our best Admirals are those who have liberal arts backgrounds because they understood the person [understood people better] and why we were applying this technology…” (Int-15, 2020). It became clear across our project that liberal arts degree holders learn to formulate compelling arguments, communicate well when speaking and in writing, and know how to solve problems--all key leadership and management traits noted throughout our literature review and data. A senior, now federal executive, interviewee said that they find liberal arts backgrounds were centered around “more softer skills” proficiency (Int-10, 2021).

One of our mid-level interviewees stated, “You need people from varied backgrounds to provide a holistic perspective because you don't want to get pigeonholed into one thing, and then you miss something important. Maybe something that someone else who has an economics background, or accounting, or history background might think of that I as an IT background person might completely overlook” They went on to say, “It is critical really, having very broad experience. [Cyber professionals need] leadership experience over different portfolios, whether as a team lead or as a supervisor doing strategy and planning and understanding requirements. [We need] very broad experience... You need these different viewpoints to see these different trends that we don't normally see as a tech person” (Int-17, 2020)

Even one of our more technical interviewees (an engineer) stated, “There has to be an aspect of liberal arts education that is important to understanding the bigger picture” (Int-2, 2020). Another suggested, it’s “a good thing... [that DoN cyber professionals have] liberal arts educations that are technically comfortable and can survive in both [technical and non-technical] environments where senior officers [and civilian leaders] expect them to be able to think on their feet and provide good advice, but certainly [to] also understand the limitations and advantages of the art of warfare" (Int-16, 2021). They suggested that this type of training, education, and development is critical for understanding bigger picture situations and thinking and better capacities in problem-solving and not pigeon-holed thinking. Our interviewees who experienced liberal arts foundational education felt that this benefitted their abilities in communication.

Lifelong Learning

Interviewees were very clear that consistent development and technical refresh are critical toward maintaining cyber currency and capacity in any cyber position. Recurring statements such as, "Because things do change some, I don't have to understand all the changes. But I do need to understand if there are additional things out there. So, I think that's one other thing you need to do look at how often anything needs to be refreshed" (Int-12, 2020) Another suggested, "Lifelong learner mindset and ability to adapt to change, I think those skills are more important now than they have been in the past…" (Int-2, 2020). None of our interviewees believe that specific degree paths or certifications are critical when looking at how to mold a cyber leader and manager.

Throughout our data collection, many topics presented that we believed we heard as immensely significant to cyber workforce development, the notions of curiosity, passion, and the importance of lifelong learning. Our interviewees discussed inherent curiosity as if it were an essential part of their personalities. It is a requirement associated with cyber development paths, as well as with personal growth effectiveness. A mid-level interviewee said, "…if you're passionate about something if you're curious about it, you're going to find new things, you're going to be successful at it. Only good things can come from that.... People who don't have that mindset will remain stagnant, and they just don't offer the best product" (Int-9, 2020). This curiosity and a passion for problem-solving, big-picture thinking, for being able to ask the right questions and to develop successful outcomes is borne out of a passion for lifelong learning and consistent, persistent self-development. Whereas cyber professionals may have been excluded from jobs in the past because they did not have a specific degree or a specific amount of experience for a role, there now seems to be more focus on lifelong learning, curiosity, and refresh skills instead of certain types of degrees, certifications, or specified experiences.

Cyber leader skills and capabilities need to be practiced daily; they need to be war-gamed by practitioners consistently. This will allow for a cycle of learning, rehearsal, application, reflection, and consistent revision to prepare cyber leaders for the future. "So, I think that that really becomes a question of lifelong learning, it becomes a question of constant revisit [and] reflection. And then are you able to pull all of the pieces, that make up the whole together, rather, so that it's greater than the sum of the sum of its parts" (Int-10, 2021).

Organizational Structure (Force Enablers) – RQ2

How can the DoN develop the appropriate supervisory and leadership personnel responsible for leading, managing, and developing the rest of the cyber warfighting force?

Insights into the skills identified by Research Question 1 have led us to understand that there is a lack of a coherent or robust leadership and management development training pipeline. This gap has severely reduced the ability of the DoN not only to retain sailors and officers who desire to progress to a high level of leadership on the military side, but it also impacts the retention possibilities of civilian federal employees who make up the leadership and managerial continuity across the DoN cyber workforce. A senior leader stated: “There's no Navy school I can send them to and say, hey, go take this training in Pensacola, because it's really good and it will be broadening for you, or you'll learn a new skill set, or you need this for the next job. Those courses don't exist, especially for the mid-career...” (Int-2, 2020).

No Standardized DoN Cyber Leader Path

There is no single standardized path of skills, capacities, appropriate leadership or management development sequencing or singularly focused training, experience, or a la carte soft and hard skills infrastructure that we see as viable for developing all DoN cyber leaders and managers. Mid and senior cyber leaders indicate a high level of concern about the future leader potential combined with the rapid pace of changes within the cyber field. In our initial meeting with Mr. Reiter, it became clear that there was a distinct lack of understanding across the DoN about the fundamental differences between a cyber technical professional's skills and those of a cyber leader. Too often, knowledge becomes equated with mastery.   Whether it was purely technical, “You are telling me that you're doing [technical skills] proficiency testing and you're not. You're testing knowledge, not proficiency…” (Reiter, 2020). Or, if it was focused on leadership skills such as refining, as one leader stated, “…someone who's experienced enough to be at least aware of what the other parts are, that tie in together” (Int-16, 2021).

The cyber community differs in many ways from the traditional Naval Line Warfare communities (Surface, Aviation, Subsurface). A respondent stated that:

“You're stepping off our, sort of, perfect path [when you jump into a cyber tour], and that's okay. Matter of fact, it's built into the aviation community to do those kinds of things. It's not built-in yet though to the Information Warfare Community and the CWE because it's still on every path [that] leads to admiral” (Int-15, 2020).

Despite efforts to define the cyber domain to place it on equal footing with the rest of the warfare communities, it remains a very distinct community whose political identity was described as a force multiplier and not a force application unto itself [like the other warfare communities present]. This divergent view of the role of cyber within warfare has led to sporadic and often underfunded or misguided funding efforts to build the community's skill set; as a senior interviewee noted, “a lot of times you have people who don't know what they don't know” (Int-14, 2020).

While there have been developments in technical training opportunities for USN sailors and DoN civilians, these continue to lag industry opportunities. 16 of our interviewees stated that the Navy is unable to take advantage of the training opportunities that industry has developed or to capitalize on the leadership and management skills gained in a particular school until later in the career path since traditionally the military has designed their own training programs, there is a reluctance to use industry or civilian equivalents. Several senior interviewees noted, when asked specifically about program management pipelines, that, “I don't know of any training pipeline to do that right now, it'd be useful...” (Int-15, 2020). While military-specific schooling “…works and is essential with submarines and weapon systems…" (Int-1, 2020), there are advantages to cyber in utilizing industrial programs. Due to the perishable nature of cyber technical skills, the cyber community is significantly impacted by training or skill sustainment opportunities. While many interviewees indicated that they had taken advantage of Kahn Academy and Google schooling (Int-7, 2020), these opportunities are noted as ad hoc. They cannot be scripted as formal solutions into a robust career progression or development path. The DoD, consequently, as discovered across major commands we interviewed, has had to seize the opportunity to develop and utilize in-house training opportunities, including a Navy Community College and standardized cyber familiarity courses. These courses only provide a cyber basics foundation and not the depth level of expertise that industry and academic communities can provide.

Training has often been relegated to an ad-hoc or as-available occurrence for military and civilian leaders alike. Yet, several of our interviewees noted its importance and consistently stated, "What are you going to invest in? What do you value now? And, in order for you to be able to actually come up with an outcome of value, you have to invest in the development of the force… allowing folks to be able to put training into context, and then be able to reinforce it. And,

and I think the reinforcement of what you learn in an experience, bringing that experiential aspect to it, is incredibly important, to be able to have something that sustains [learning]" (Int-10, 2021). Despite these efforts, one interview respondent stated, "… we tend to take risks on things like training and development because we are so focused on developing the here and now…[consequently] we are not finding anywhere near the success we wanted…" (Int-10, 2021). Across government, including in DoD and cyber, when budget concerns call for cutting costs, the first effect is to seek budgetary efficiencies and cut training and learning opportunities. While these opportunities are frequently minimal expenditures in the multi-billion-dollar budget of the Navy (and its various communities), because of the political framework, they are often seen as easy to do without. As mentioned to us, "[things were] maybe not funded …. I don't feel short-changed, but I probably was in terms of training …" (Int-16, 2021). When training is not planned, intentional or focused, then "These actions carry a high degree of political risk and loss of support for their mission" (Int-10, 2021).

Mentorship

Traditional communities can shoulder this burden of in-house training easier than the cyber community. For example, instructor pilots can take on familiarization training with more flight students. Senior Officers of the Deck (shipboard leaders) can step in and provide on-the-spot structure and mentorship for junior personnel (Parilla, 2020). However, the cyber community has neither the capacity nor capability to provide this level of training and mentorship. Mentorship is essential as an early application of many leadership skills. As simply put by a respondent, "It is a sailor's first opportunity to apply what they have learned in an informal sense" (Int-15, 2020). There is a realization that in spite of the short timeframe and rapid development, leadership and mentorship opportunities exist, and these experiences were expressed as critical across our interviews for growing cyber professionals and for testing out leadership and management skills. Put simply, "if you want to bring everybody up, you probably need somebody [like a mentor] helping with the intellectual curiosity…" (Int-1, 2020).

Experience: OJT and "Doing"

A mid-level interviewee stated, "You have to have on-the-job experience...you need repetition to build upon that, and if you don't have someone above you, [like a team lead, supervisor or mentor] who can lead you through that process, it is really hard to get it, and you're going to run into problems" (Int-17, 2020). Developing leaders need a chance to practice and develop these skills before they are placed in a position where they have to use them. "I was OJT from day one, and without [my mentor], I would have been absolutely lost" (Int-16, 2021), stated one interviewee. Another mid-level leader said, "I think the real-world experience beats classroom experience every day" (Int-9, 2020). Ultimately, another mid-level interviewee conveyed that what mattered was that "…it was all about those experiences at the right time at the right place..." (Int-8, 2021). One of our senior leaders, now a federal executive, said, "It is really important to shift people around a bit to show them that they can learn new things and to allow them to internalize that growth. Every once in a while, being thrown in an uncomfortable position is actually good—especially if you survive. Gaining experience is very valuable in a very direct way! Spending time at sea, ashore, in different mission sets, you get a much better feel for how "the corporation operates [through experiences and doing]" (Int-4, 2020).

The necessity of informal training around a coffee, or water cooler discussion, cannot be discounted and needs to be understood as critical to the growth and development of cyber professionals and leaders and managers, writ large. A respondent stated, "So, at every level, it might be an unofficial senior guy on the floor. They might say, hey, new guy, have you had your coffee today? Let's go have coffee. Just that small step can mean the difference between whether or not that person opens up [broadening training opportunities of an informal nature that have significant impact]…" (Int-14, 2020). And, another noted that, "There's no expectation that an ensign on day one is going to be capable, you're going to put him through school, you're going to put that person in a Division Officer job where he's got a [experienced] chief over him. But, the Navy hasn't invested in that kind of cyber pipeline for our officers" (Int-2, 2020). As another interviewee stated, "…I also realize there's a lot of continuous training that has to happen on the job in the fleet…" (Int-4, 2020).

Another interviewee exemplified it as, "… it's almost a hybrid of mentorship and training. Because that's how you're going to get after a rapidly changing field like [cyber] where you need to stay up to speed" (Int-2, 2020). These informal and sometimes lateral learning opportunities provide a fundamental understanding of the transition from technical to leadership roles within the community. While many established communities may have opportunities in their development, the cyber community's nascency prevents their codification. "The education and mentoring piece is really in the early stages. And on the cyber side, on the operator side and the developer side, we're going to almost a guild model of journeyman, apprentice, master, where you've got apprentices training journeyman and masters training apprentices because what you need is essentially mentorship" (Int-2, 2020).

Understanding the balance between formalized and informal transition from technician to leader underscores the necessity for operational reinforcement for training at the more senior apprentice level to begin to understand their integration into the overall structure of the force. This model needs to be flexible to take advantage of the development opportunities that may happen ad-hoc is essential not just to incorporate what training a person may have obtained. Still, it ensures that the training is captured and utilized to benefit the individual and the organization. Interviewee 10 said, "…it would be more beneficial to be able to go out and get two weeks in a very focused instruction, dealing with a particular aspect of it, then to go apply it, and then come back and do six weeks, and then go back and apply that particular piece, and then constantly refresh and go back and pull it all together, so that now all factors in together in a cumulative effect" (Int-10, 2021). This time-critical training was reinforced by interviewee 9's statement of, "in the cyber world, it's so dynamic, and it's always changing. I feel like if I don't take a class every other month, I'm already behind" (Int-9, 2020).

Our interviews and research indicated the absolute necessity for immersive training programs coupled with mentorship as a best-practice development and leadership model as one stated that to create a program that could provide a realistic scenario-based training plan, "we modeled that often from… a lot of stuff that we knew was available…" (Int-1, 2020). This focus on education, mentorship, and training, pursued by those with passion and curiosity to dig deeper into the how and why of cyber, will create a culture of learning that supports the skills recommended in RQ1 and create a deeper understanding of the cyber force and its effectiveness in being reactive to change while developing a proactive approach to emerging challenges.

Lack of Mid-Career Structure

Many formative leadership experiences happen at the mid-level of one's career. It is this timeframe that allows the technical expert to transition to leadership and management positions. Within the aviation community, for example, pilots complete all of the requisite training for flying. Still, it is not until they finally sign for the aircraft and have to make the decision for themselves that they truly understand the implication of leadership and the importance of the people, communication, managerial skills that a leader must incorporate (Parilla, 2020).

In the traditional warfare communities, these mid-level officers, enlisted and federal civilians comprise a mentoring cadre that guides junior personnel along their career path and provides them a template for a sustainable career. It is essential to know that many entering the cyber community already have civilian work experience and will work alongside those with a very different personality and mindset (Google versus military approaches). Mid-level leaders bring unique skills with them, as pointed out by an interviewee, “I think once you have mastered the ability to just deal with people… cooperate… be productive with [others, it has effect]…” (Int-9, 2020). This requires a strong mid-level professional to bridge the gap between the technician and senior leader. Understanding the experiences, they have had and providing them with the opportunity to go beyond technical into leadership roles will help select sailors look for a broader experience.

Without a commonly understood career path, it is difficult for mid-level leaders to mentor, develop, and deliver training to junior personnel so that they are ready to capitalize on their mid-career options and ready themselves for future leadership and management requirements. This gap in career progression was highlighted by several interviewees who noted that the lack of those who came up through the ranks in cyber led to a break down in mentorship and guidance right at the point in one's career where they would be making the connection from technician to leader. As one respondent stated, “they stagnated in part because they didn't have that O5/O6 mid-career leadership that had done the job that understood what they were going through…” (Int-2, 2020).

A respondent noted that “So you need kind of those mid-career guys like me who have been doing it for a long time to teach and explain and give that “why” to the new folks coming in. There's just not many folks like me who have gotten the opportunity to stay in a cyber job for multiple tours” (Int-2, 2020). As another senior member said, “I'm thinking more of mid-term leadership. It's where it's very lacking…” (Int-15, 2020). These transitory placements in the mid-level officer ranks cannot provide the depth of detail necessary to develop junior personnel or even provide them with a career path to emulate. Every senior interview that we conducted recognized that most cyber leaders continue to be transitions from other communities. Whether the transition was from the

Intelligence, Cryptologic, or Line communities, these personnel are insufficient to mentor junior cyber personnel. This becomes more significant with deleterious effect, as the entry tour for junior personnel remains six years or less if they are not inspired with a path forward. The Naval Personnel Command shows a 76 percent overall retention rate between the first and third enlistment. Contrast this with the cyber retention rate of 53 percent (Werner, 2020).

Without a system of career progression integrated into the cyber community, a technical cyber person must choose during his first tour between allowing his skill set to atrophy and promoting along a prescribed hierarchical path, or they make the transition out of the Navy to seek continued technical opportunities (at a higher wage level) within the civilian community (Int-6, 2020). They simply do not retain long enough to take advantage of what little leadership opportunities are available. If they choose to remain in the service, as an interviewee stated, "You know when you get to that mid-level officer level within the military, or looking at O3 to O4 transition, and at your GS 12 moving up into that more senior leadership. That is where they're ditching those technical skills for a greater application, greater applicability within the military [and DoN]" (Int-5, 2020).

Efforts in Progress

The Navy is creating academic offerings that might begin to meet the infrastructure gaps in the cyber leadership development efforts. The DoN recently (2020) stood up the Navy Community College for more enlisted sailors to study cyber topics in Quantico, Virginia (Reiter, 2020). As well, the U.S. Naval Academy has had a cyber-focused degree for midshipmen since 2016, and it is presently re-baselining its courses aligned to shifting cyber needs and realities (Int-11, 2021). The Naval Post-Graduate School in Newport, RI, is also modifying its curriculum with cyber-focused academia and is developing a cyber warfare-specific master's degree (Int-2, 2020). One particular interviewee noted that “We're basically forming the hybrid degree [and] the goal is through education to demystify some of these cyber things… I think that master's level is part demystification of some of these other topics…” (Int-2, 2020).

Meanwhile, the Navy is also executing a program known as the Cyber Warfare Engineer Officer, in place since 2017, to develop a distinct cadre of cyber professionals to provide defense against attacks, deliver tactical advantages, develop tools and techniques, and aid the Information Warfare Community in gaining a deeper understanding of the adversary in cyberspace operations. The

CWE initiative is nearing 100 personnel, ensuring a dedicated career path and career expectations, and reducing mid-level cyber professionals' gap. The goal is to create a distinct group of cyber professionals over the next decade and beyond. These professionals are destined to work to fill some of the leadership needs that have been identified across RQ2. These efforts must define OJT, mentorship, standardized career structure, and ultimately leadership roles in the cyber community to create the current and next-generation cyber leader.

Strategy - RQ3

Developing the infrastructure that is needed to support viable, sustainable cyber management/leadership?

In order to create a robust cyber leadership and management learning structure, our findings, aligned with the CSC 3 (2020) recommendations, and require the development of training and mentorship programs that can provide emerging cyber leaders with guidance, real-time education, and the chance to apply their skills as acquired to support the force better (Reith & et. al, 2019) (Int-10, 2021). This will ensure that they can maintain a high level of technical acumen while also developing leadership and management skills applicable to wide-ranging circumstances and creating the foundation for leadership at higher levels. As a senior respondent said, "…you take one and train one and then mentor them to ensure that when you leave that somebody else is going to benefit from what you learned going forward" (Int-10, 2021).

The military has adopted the training of their cybersecurity talent independently and not in a unified manner. Traditional strategies and methods for developing the DoN cyber workforce have proven insufficient in meeting the cyber force's learning needs over this time. The DoN needs to, as one interviewee stated, "move away from the Industrial Age training model toward a learning, adaptive and responsive training pipeline [across traditional learning as well as leadership development] that produces highly educated and specialized cyber leaders armed with current tactics, techniques, and procedures" (Int-7, 2020).

Industry Training Model

An industry representative stated, "I have to put deliberate effort into my own training, to keep up on the state of industry, where technology is going…" (Int-1, 2020) Industry has invested in significant learning and development opportunities. They have predominantly aligned their organizational structures to business investment managers and technical support. They have robust strategies in place for effective business and leadership of their workforce. They have also made progress in addressing and facing many of the latest complex technical developments in cybersecurity, as these challenges affect their fiscal bottom-line (Int-1, 2020).

Traditional cyber training and education methods, which military and non-commercial entities utilize to improve technical capacity, are inefficient, riddled with complex challenges, and use inadequate cyber training and curriculum development in an attempt to remain current, but are not necessarily aligned with real-world actions that industry uses for their constant refresh of skills (Int-

12, 2020). Our findings in RQ2 stated that "cyber is not something that supports business, it is part of business… I mean, it's stunning to see what is actually in the art of the possible" (Int-1, 2020). This understanding is all the more important when developing a strategy to develop and sustain cyber leadership.

The cyber curriculum content requires more frequent updates more often than traditional disciplines. And a cyber curriculum can be challenging to pull off the shelf and teach because information and operational technology are inherently disruptive. Hence, it is all the more important to integrate this understanding across all warfighting areas. As an interviewee stated, "high-level policies, strategies… the big picture stuff, and then a very targeted approach" (Int-10, 2021) this requires both a localized cyber knowledge as well as a generalized understanding of cyber effects.

This critical requirement of continual refresh means that any shortfall of cyber professional experiences in training, education, or application opportunities will reduce the Navy's (and the DOD and civilian counterparts) abilities to maintain agile and effective countermeasures and proactive defense postures in the cyber domain. "I think that it has got to be continuous… I keep learning… I still have to put deliberate effort into my own training to keep up on the state of industry" (Int-1, 2020).

As noted by one interviewee, "…the average cyber incursion costs the affected party over $4.8M, and yet, the average command training budget is under $5M per year…" (Int-8, 2021). As stated in RQ2 as a political risk, If the reason for the reduction in training is budgetary constraints, this neither enables a strategic force structure nor provides for a viable or sustainable leadership infrastructure. Despite low opportunity costs and high benefits, many efforts fall victim to shrinking budgets and fiscal requirements. If current leaders do not understand the fiscal environment and cannot weigh constraints against force enabling training, the force's overall readiness continue to decline "while the knowledge is fresh, yeah, I think it can't be undersold…" (Int-10, 2021). It is clear, as stated in findings for RQ2 that there is presently no existing infrastructure being used to create a sustainable cyber management or leadership program, nor is there a consolidated, programmed, or robust education and training program for aspiring cyber technicians to transition from technical capacities toward greater leadership roles.

There remains a lack of a robust structure to develop leaders and warfighters with the judgment, creativity, problem-solving skills, technical capabilities, and a deep understanding of how cyber creates an effective force. These skills were identified across all three of our research questions, as they underpin the development of the training and infrastructure necessary to support a cyber force. Once a strategy is defined, a learning plan can be developed to support this goal. As one interviewee noted, DoN cannot continue to be "rushed to build some capability… but I don't necessarily think there's a strategy to move us forward" (Int-17, 2020).

Throughout our interviews conducted in 2020, we found the same gaps and demands as the updated RAND study (2019) found. In particular, RAND noted that "A perceived lack of clarity in the vision for the cyber workforce is hindering the mission and morale." Our Interviewee 2 stated, "…but you can't have a vision about where the Navy should go… if you're just relying on your workforce to be the experts…" (Int-2, 2020). RAND's assessment was that, "Little connection is made between strategic vision and the tactical task on which the workforce focuses daily." This was reinforced by one of our interviewees noting, "strategic dialogue seems to be along the lines of people versus machines, I think just because the way that we ‘value human resources’ we keep looking at them as being on the expense side [and not the asset] of the ledger…. We cannot replace labor” (Int-4, 2020), (Hardison, et al., 2019).

Furthermore the 2019 RAND study found that, “There is a perceived mismatch between the training provided and the skill levels of people completing it” (Hardison, et al., 2019). Our interviewee said, “…what I saw in the Navy was all over the place…. Senior people in charge of tiny things junior people in charge of massive things. And definitely not the sense that the people had shown success with a smaller scope and span of control before they moved on” (Int-13, 2021). Finally, from the 2019 RAND study, “Critical technical acumen may be atrophying due to not allowing cyberspace professionals adequate continuation training during their careers” (Hardison, et al., 2019). A DoN interviewee commented, “It can't be, I'm going to do this for three or four years and then go do something else and then come back. The technology changes too fast. The organization changes too fast. And that may just be a function of it's all relatively new and in the new growth phase. Things are changing really quickly. “ (Int-2, 2020). A second respondent noted that “they don't have to be an expert in it, but they do have to have at least a basic understanding” (Int-14, 2020). And another respondent stated, “Our focus areas are so broad and so varied, that it is kind of hard to have a one-stop kind of training thing” (Int-14, 2020).

The fact that these concerns are still un-addressed over the last ten or more years underscores that without a common strategy upon which to pin the training, mentoring, and career pathway of cyber leaders and managers, there will be a continuation of the shortfalls in individuals trained, able and willing to assume leadership positions beyond their technical skillset as the force continues to develop.

Recommendations

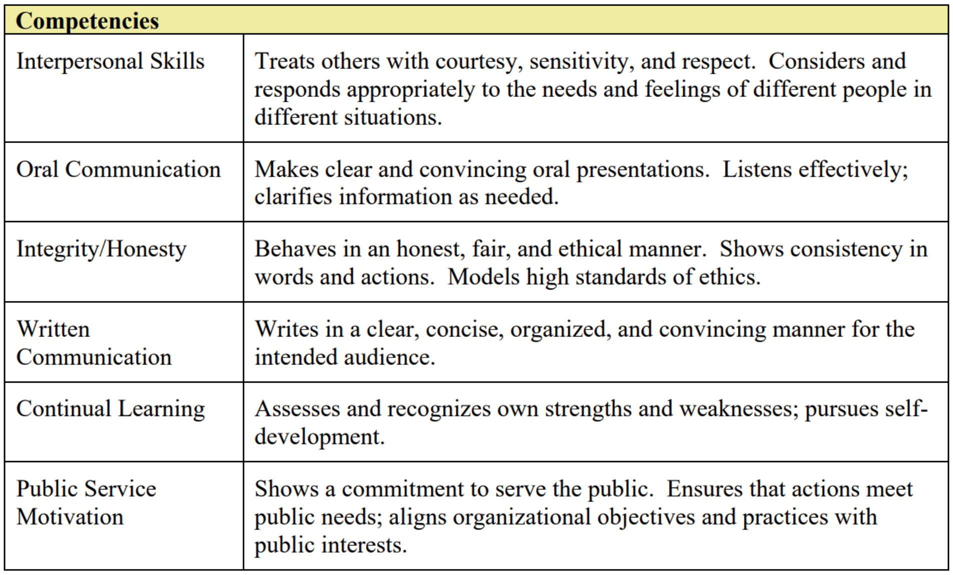
The three pillars identified in this study: Learning, Organizational Structure, and Strategy, allow us to make specific recommendations toward each of the research questions and apply them to these pillars to achieve the ultimate goal of a Navy Cyber Leader Development Plan. The following cyber leader and manager development recommendations provided in this capstone are not new ideas. Many of these ideas have previously circulated in the federal government and Navy’s cyber domain but remain unimplemented or underutilized, often due to alignment hurdles. Consequently, across our interviews, we found that Navy organizations have each set up their own assortment of cyber development programs, perpetuating disjointed and inefficient efforts across divided resources that should now be integrated across DoN cyber stakeholders. This notion is not DoN cyber centric; the broader cyber system in the U.S. “for federal (and national) cyber workforce development is complicated, uneven in its focus, and lacking foundational principles and access to common resources—thereby encouraging the current practice of reinventing competing workforce development strategies in various stovepipes” (Bate, 2020, p. 3).

Learning (RQ1):

Expand access to real-time, classroom, and virtual training for leadership essentials.

We discovered that the following leadership and managerial traits should specifically be focused on by DoN cyber as crucial for cyber leaders and managers: communication/translation, collaboration/teamwork, relational skills, intellectual curiosity, self-motivation, integrity/honesty, and confidence. A healthy mix of both soft and hard skill proficiency is essential for building cyber leaders. While some of these traits can be trained to or skills refreshed in educational settings or on virtual and just-in-time platforms (for example: writing, communication), others (like teamwork, integrity, and intellectual curiosity) must be performed to truly mature and sustain them. Their proficiency is accomplished through experience, problem-solving and critical thinking opportunities, and life-long learning built on a foundation of fundamental people skills and a desire for individual advancement.

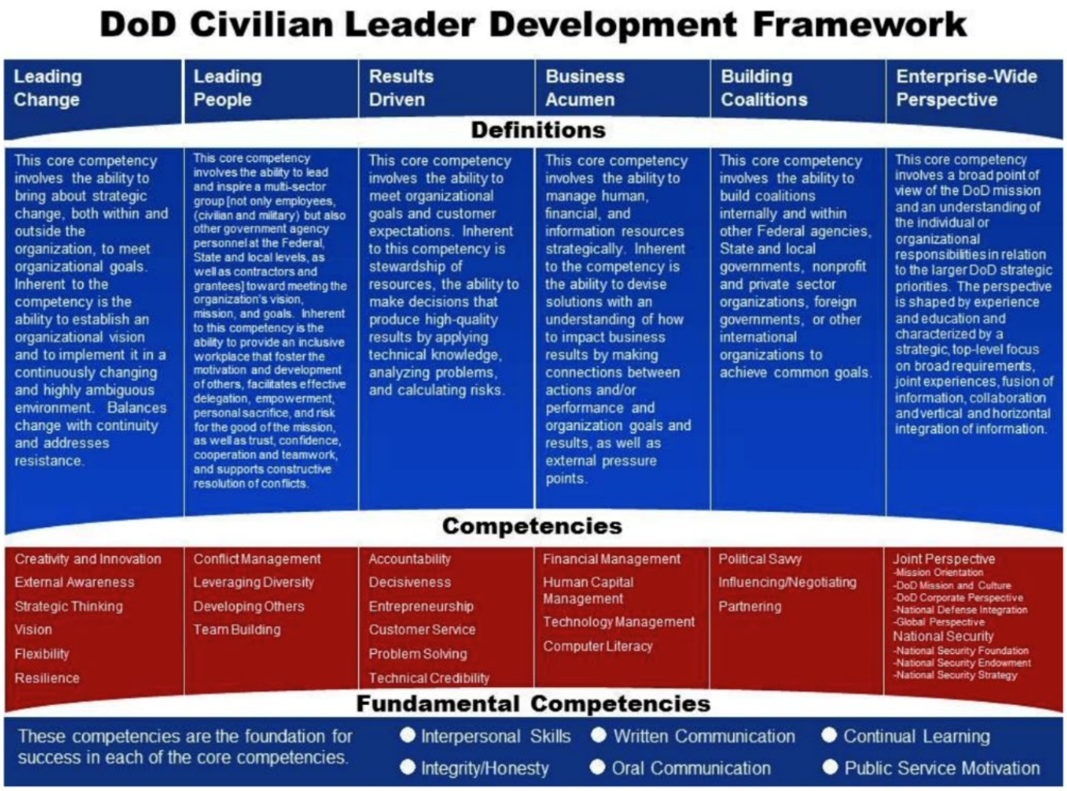
For the federal workforce writ large, the Office of Personnel Management provides that the personal and professional attributes of interpersonal skills, oral communication, integrity/honesty, written communication, continual learning, and public service motivation are critical as foundational executive qualifications for leadership and managerial performance (OPM, 2020). These same attributes directly align to RQ1 identified cyber leader and manager skill requirements from our project.



Competencies	
Interpersonal Skills	Treats others with courtesy, sensitivity, and respect. Considers and responds appropriately to the needs and feelings of different people in different situations.
Oral Communication	Makes clear and convincing oral presentations. Listens effectively; clarifies information as needed.
Integrity/Honesty	Behaves in an honest, fair, and ethical manner. Shows consistency in words and actions. Models high standards of ethics.
Written Communication	Writes in a clear, concise, organized, and convincing manner for the intended audience.
Continual Learning	Assesses and recognizes own strengths and weaknesses; pursues self-development.
Public Service Motivation	Shows a commitment to serve the public. Ensures that actions meet public needs; aligns organizational objectives and practices with public interests.

Figure 7 (OPM, 2020)

These competencies have been identified and integrated across most established federal and defense learning continuums, including DoD’s Civilian Leader Continuum Development Framework and DoN’s Civilian Workforce Development Framework (2016). See Figures 8 and 9 as depictions of these frameworks, which align to and already go far toward resolving RQ2 and RQ3 of this project (DCPAS, 2013), (DoN, 2016). Accordingly, many federal and academic courses are already available to impact fundamental capacities and proficiencies for the successful performance of the government’s business. These skills and competencies can be presented in varied educational environments to accommodate and capitalize on the workforce's diverse backgrounds, followed by real-time on-the-job training reinforcement. DoN cyber focus areas revealed in RQ1 tie to listed DoD leadership competencies that primarily fall under the Leading People, Business Acumen, and Building Coalitions categories below, and specifically its Fundamental Competencies:



DoD Civilian Leader Development Framework

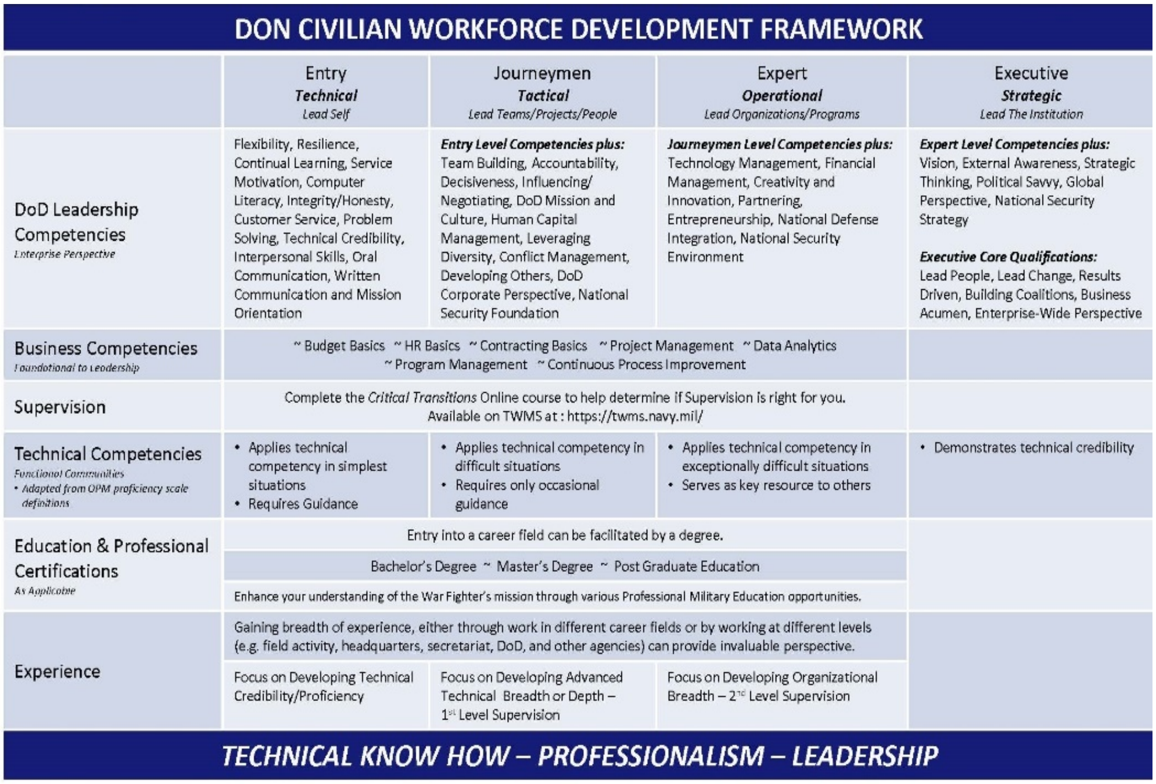
	Leading Change	Leading People	Results Driven	Business Acumen	Building Coalitions	Enterprise-Wide Perspective
Definitions	This core competency involves the ability to bring about strategic change, both within and outside the organization, to meet organizational goals. Inherent to the competency is the ability to establish an organizational vision and to implement it in a continuously changing and highly ambiguous environment. Balances change with continuity and addresses resistance.	This core competency involves the ability to lead and inspire a multi-sector group [not only employees, (civilian and military) but also other government agency personnel at the Federal, State and local levels, as well as contractors and grantees] toward meeting the organization's vision, mission, and goals. Inherent to this competency is the ability to provide an inclusive workplace that foster the motivation and development of others, facilitates effective delegation, empowerment, personal sacrifice, and risk for the good of the mission, as well as trust, confidence, cooperation and teamwork, and supports constructive resolution of conflicts.	This core competency involves the ability to meet organizational goals and customer expectations. Inherent to this competency is stewardship of resources, the ability to make decisions that produce high-quality results by applying technical knowledge, analyzing problems, and calculating risks.	This core competency involves the ability to manage human, financial, and information resources strategically. Inherent to the competency is the ability to devise solutions with an understanding of how to impact business results by making connections between actions and/or performance and organization goals and results, as well as external pressure points.	This core competency involves the ability to build coalitions internally and within other Federal agencies, State and local governments, nonprofit and private sector organizations, foreign governments, or other international organizations to achieve common goals.	This core competency involves a broad point of view of the DoD mission and an understanding of the individual or organizational responsibilities in relation to the larger DoD strategic priorities. The perspective is shaped by experience and education and characterized by a strategic, top-level focus on broad requirements, joint experiences, fusion of information, collaboration and vertical and horizontal integration of information.
Competencies	Creativity and Innovation External Awareness Strategic Thinking Vision Flexibility Resilience	Conflict Management Leveraging Diversity Developing Others Team Building	Accountability Decisiveness Entrepreneurship Customer Service Problem Solving Technical Credibility	Financial Management Human Capital Management Technology Management Computer Literacy	Political Sawy Influencing/Negotiating Partnering	Joint Perspective -Mission Orientation -DoD Mission and Culture -DoD Corporate Perspective -National Defense Integration -Global Perspective National Security -National Security Foundation -National Security Endowment -National Security Strategy

Fundamental Competencies

These competencies are the foundation for success in each of the core competencies.

- ● Interpersonal Skills
- ● Integrity/Honesty
- ● Written Communication
- ● Oral Communication
- ● Continual Learning
- ● Public Service Motivation

Figure 8 (DCPAS, 2013)



DON CIVILIAN WORKFORCE DEVELOPMENT FRAMEWORK

	Entry ***Technical*** *Lead Self*	Journeymen ***Tactical*** *Lead Teams/Projects/People*	Expert ***Operational*** *Lead Organizations/Programs*	Executive ***Strategic*** *Lead The Institution*
DoD Leadership Competencies *Enterprise Perspective*	Flexibility, Resilience, Continual Learning, Service Motivation, Computer Literacy, Integrity/Honesty, Customer Service, Problem Solving, Technical Credibility, Interpersonal Skills, Oral Communication, Written Communication and Mission Orientation	***Entry Level Competencies plus:*** Team Building, Accountability, Decisiveness, Influencing/ Negotiating, DoD Mission and Culture, Human Capital Management, Leveraging Diversity, Conflict Management, Developing Others, DoD Corporate Perspective, National Security Foundation	***Journeymen Level Competencies plus:*** Technology Management, Financial Management, Creativity and Innovation, Partnering, Entrepreneurship, National Defense Integration, National Security Environment	***Expert Level Competencies plus:*** Vision, External Awareness, Strategic Thinking, Political Savvy, Global Perspective, National Security Strategy ***Executive Core Qualifications:*** Lead People, Lead Change, Results Driven, Building Coalitions, Business Acumen, Enterprise-Wide Perspective
Business Competencies *Foundational to Leadership*	~ Budget Basics ~ HR Basics ~ Contracting Basics ~ Project Management ~ Data Analytics ~ Program Management ~ Continuous Process Improvement			
Supervision	Complete the *Critical Transitions* Online course to help determine if Supervision is right for you. Available on TWMS at : https://twms.navy.mil/			
Technical Competencies *Functional Communities* *• Adapted from OPM proficiency scale definitions*	• Applies technical competency in simplest situations • Requires Guidance	• Applies technical competency in difficult situations • Requires only occasional guidance	• Applies technical competency in exceptionally difficult situations • Serves as key resource to others	• Demonstrates technical credibility
Education & Professional Certifications *As Applicable*	Entry into a career field can be facilitated by a degree.			
	Bachelor's Degree ~ Master's Degree ~ Post Graduate Education			
	Enhance your understanding of the War Fighter's mission through various Professional Military Education opportunities.			
Experience	Gaining breadth of experience, either through work in different career fields or by working at different levels (e.g. field activity, headquarters, secretariat, DoD, and other agencies) can provide invaluable perspective.			
	Focus on Developing Technical Credibility/Proficiency	Focus on Developing Advanced Technical Breadth or Depth – 1st Level Supervision	Focus on Developing Organizational Breadth – 2nd Level Supervision	

TECHNICAL KNOW HOW – PROFESSIONALISM – LEADERSHIP

Figure 9 (DoN, 2016)

Continuous training and sequential development, as depicted in Figure 9, are essential to instituting robust leader learning. DoN cyber professionals who envision themselves taking on increasing leadership roles in the future can take advantage of available courses while incorporating other DoN cyber leadership development opportunities, both formal and informal, offered by NCWDG, NCDOC, ONI, TENTH Fleet. DoN cyber professionals also have access to diverse training available from industry, such as Cisco Academy and Google Grow Program, that provides broadened intellectual development opportunities (Google Grow, 2021) (Cisco, 2021). Throughout our interviews, Navy cyber leaders indicated that these types of education and training could enable mid- to senior-level cyber practitioners to integrate learning with more holistic leadership training (Int-17, 2020). These combined development opportunities will begin to populate a talent pool from which individuals with the requisite leadership potential can be drawn (Bowles, 2017).

Organizational Structure (RQ2):

Create a DoN Cyber Leadership Development Board (inclusive of all stakeholders) to guide the integration of efforts for developing cyber leadership and management depth.

Aligning training programs delineated in RQ1 recommendations and development initiatives across DoN cyber stakeholder organizations creates enhanced scalable talent development options and opportunities. The creation of a Cyber Leadership Development Board (CLDB) to guide and integrate these efforts will organize the wide array of available leadership and management development programs, training, and sustainment possibilities across industry, federal and military learning and leading options to meet individual development needs across emerging DoN cyber leaders. This board would function similarly to the Navy's Civilian Oversight Board (NCOB) run by N2/N6.

Naval Information Warfare Systems Command (NAVWAR) is developing an Information Warfare training strategy construct with accompanying governance, requirements, and assessments that will go far in addressing many issues noted throughout this study toward delivering proficient and agile mission-ready cyber leaders and managers. CLDB involvement with the NAVWAR effort is essential to maintain a consistent effort for designating and delivering required IW competencies. Using the Cyber Leadership Development Board, DoN Cyber can ensure that current and future best practices are discovered and applied while providing a conduit for change and improvement that can respond to the cyber field's dynamic nature. A CLDB would be positioned to be a proactive approach to align changing technologies and learning opportunities in the development of supervisors, leaders, and managers across the DoN cyber workforce.

Implementation of a Training, Application, and Reflection Continuum.

Sailors and civilians need to develop their ability to communicate, hone their problem-solving and critical thinking abilities, and nurture their desire for continual learning when taking on more challenging positions in increased cyber leadership roles. Our research indicates that the appropriate leadership and supervisory development path need to include schooling, OJT and qualifications in the workspace, self-guided learning, mentorship, and experiential learning that exposes cyber professionals to executive focus areas like budgeting, strategy, policy, resource requirements, etcetera.

The DoD Civilian Leader Development Continuum (DCPAS, 2013) presented in Figure 10 defines an established and still valid progression that builds leaders up from self-management to executive management. This aligns with Figure 9 DoN Civilian development framework. Creating opportunities for cyber leaders to learn and then practice their skills across this type of progression remains essential.

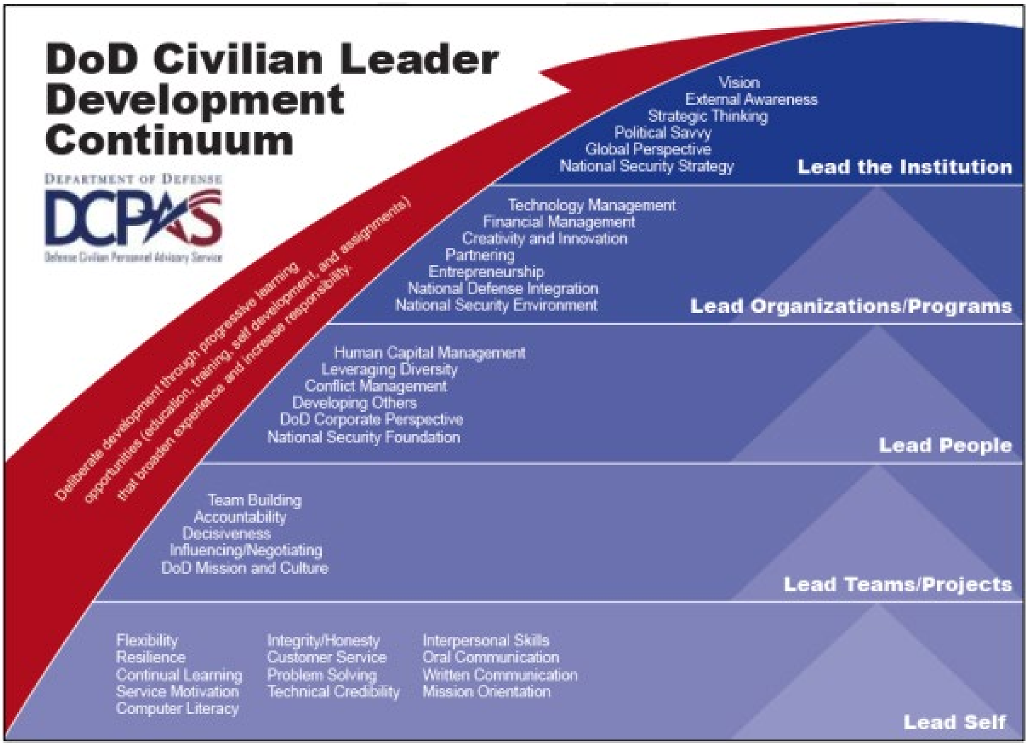


Figure 10 (DCPAS, 2013)

In academia and industry cyber employment, significant focus is placed on hands-on, experiential learning and comprehensive/constant development to meet a constantly evolving industry with a shifting threat landscape—be it for cyber technicians or their leaders (Baker, 2016). This type of learning lends itself toward broad knowledge and concept integration across varied problem sets in the domain. We recommend utilizing “trial-by-fire” watch-floor and rotation opportunities to capitalize on and scaffold for reinforcement perishable cyber-related leadership and managerial skills that emerging leaders have just learned.

Organizing opportunities for cyber professionals to create, draft and present their non-technical skills through written and oral methods will give them a more integrated team leadership and executive experience. DoN cyber exercises (potentially with industry involvement) will present real-world challenges and develop the requisite knowledge, leadership skills, and operational procedures necessary for successful, integrated operations. These opportunities will allow professionals to lead progressively more significant projects and teams, further enhancing (and proving) their leadership potential. Our interviewees indicate that a demonstration of skills, tool use, and techniques is critical as a screening and performance perspective for workplace leaders. To do this, cyber professionals must have gained competence from applying leadership skills in hands-on exercises (Knapp, Maurer, & Plachkinova, 2017).

Neither data nor research suggested that any specific certifications, classes, or programs are the panacea for developing DoN cyber leaders/skills or capabilities (ISC2, 2021). So, partnering with a CLDB designated "education consortium" that includes USNA, Naval Post Graduate School (NPS), Navy

Community College cyber-related efforts, among others, will allow DoN cyber employees (civilian and military) to virtually "audit" courses if they are not enrolled students for continuous self-development. After some time, it would become clear who are the curious, lifelong learners.

As sailors and civilians move along this development continuum, their areas of responsibility and leadership opportunities increase. Figure 8 shows how the fundamental competencies nest with the application of those competencies and drive the individual's overall leadership potential.

Several training plans in the Department of the Navy are in development for various workforces. Of particular note, the Navy Civilian Career Path specifies that while some fields have clear pathways for development, others have progressions that are not well defined. This model relies on a continual learning plan. By focusing on a progression of entry, journeyman, expert senior leader skillsets for development (DoN, 2016), the cyber workforce can develop leadership milestones while maintaining flexibility when those milestones are attained, Figure 9 lays out this path.

CYBOLTS

Cyber Operations and Leadership Training and Selection (CYBOLTS) Program.

DoN Cyber should consider implementing a Navy cyber-only focused leadership development program as a significant step in building DoN cyber leaders and in creating leader and manager sustainment paths for the same. High-potential DoN cyber emerging leaders, civilian and military, could be nominated and selected each year through an application and selection process. Like the Civilian Leadership Program at ONI, or the NAVIGATION program at N2/N6, CYBOLTS is an exemplar multi-year long, nomination-based program that would consist of a series of highly experiential workshops, crucial cohort-building experiences, hands-on rotational developmental assignments, and networking for collaboration. These opportunities address leadership topics and the situational understanding that will allow for sustainment through reflection and growth focused on leadership attributes from across OPM and DoD's fundamental competency areas.

Candidates who also apply and participate in the education programs defined by the CLDB will demonstrate that they are interested in a cyber leadership track. As these professionals continue signing up and showing up to improve their capacities and knowledge from courses in the education consortium, then the CLDB could further invest in these emerging leaders' (CYBOLTS participants) development with more expensive opportunities like DoD CISO, Harvard, and PMP programs.

Strategy (RQ3):

Alignment between NAVADMIN 2020 and CSC to implement DoN Cyber Standards.

Lastly, the strategy to develop the intellectual infrastructure necessary for sustaining cyber should include "industry-izing," governance structure with a learning, mentoring, and developmental strategy, and a Cyber Leadership Development Board. Through the application of a Cyber Operational Leadership Training and Selection (CYBOLTS) process, the DoN Cyber community is positioned to meet the framework defined by both Congressional Cyberspace Solarium Commission (Bate, 2020) and a 2020 NAVADMIN (official correspondence) focused on reestablishing Navy leader development frameworks (Department of the Navy, 2020).

There must be an overall strategy to develop leaders who possess the skills necessary to implement a cyber force properly. These leaders must be consistently trained as systemic thinkers who understand teamwork and possess strong communication skills, including translating and applying the technical data to a larger picture.

One area that we heard our interviewees speak to numerous times was the need for understanding national-level cyber organizational structure, policy alignment, and cyberspace capabilities.   With a better understanding of the strategic approach and, perhaps, a Cyber Foundations primer, DoN cyber organizations would be better equipped to conduct their cybersecurity missions on behalf of the federal government. Comments such as, “strategy would be helpful…. We've rushed to build some capability according to a Navy mandate… but I don't necessarily think there's a strategy to move us forward” (Int-14, 2020). Even the CSC’s Final Report (2019) stated, “any effective strategy for cyberspace will require a coordinated effort across the multiple stakeholders…that are all responsible for securing and defending the United States in this domain. Therefore, the strategy must explicitly align and synchronize stakeholder strategic objectives, identify lines of effort to put the strategy into operation, clarify what priority should be given to various efforts, and articulate common principles of risk” (Morgus, 2019, p. 5).

As the CSC recently suggested to the Hill in 2020, “having the structures in place to create and implement a cyber workforce development strategy is critical. While numerous individual efforts have emerged across the federal government to address various workforce challenges, there is limited coordination. DoN Cyber would be well served in organizing, developing, and stimulating growth in their

DoN cyber leader talent pool. If they begin to lay the groundwork for their own DoN Cyber leadership and managerial development strategies, this will enable substantive and coordinated investment in building and growing cyber leaders.

Our recommendations of a Cyber Leader Development Board, partnership with a Navy-centric cyber education consortium, and the delivery of a CYBOLTS leader development program would create the necessary structures for DoN Cyber to sustain intellectual infrastructure in the development of cyber leaders and managers for years to come. The CLDB could enable a clear plan to distribute resources and designate responsibilities to avoid the pitfalls of slow progress in cyber workforce improvement (Bate, 2020).

Conclusions

Context and Personal Connections

Throughout the time that this capstone was under development, election integrity was considered, Solar Winds data breaches occurred across numerous federal systems, city water networks were attacked in an attempt to poison public water systems, city and state-run organizations were temporarily shut down after network attack, and numerous bank and data breaches have occurred harmfully impacting common people. Cyber, particularly a national cybersecurity strategy, has recently taken on extraordinary focus as Americans are waking up to the significant vulnerabilities in play as individuals, as employees, and as citizens. There is a keen focus now on studying and assessing cybersecurity writ large and on the technologies, processes, and practices designed by industry and the national security apparatus utilized to protect networks, devices, programs, and data from attack, damage, or unauthorized access. For our purposes, from professional connection via our careers, our focus throughout this capstone has been specific to the Department of the Navy and the Navy's efforts in the cyber domain.

As an introduction to this capstone's authors, both of our professional careers have been with the DoN for decades. Both of us retired from either naval service or the Navy's federal employment in the Intelligence Community after more than a decade in Naval uniform. Both of our careers have impacted the nation's security posture from their naval employment, frequently dealing in aspects of the cyber domain throughout our careers. We realize the immense impact that cyber, in national security and naval operations, has on any system tied to networks--as well as how much we now all blindly rely on networks. The cyber domain holds so much potential for positive effect, but also an absolute catastrophe. As researcher practitioners studying the day-to-day leadership and learning inside organizations, the cyber domain offers endless opportunities for studying skills, capabilities, learning and development, career paths, and career sustainment across cyber for cyber leaders.

A large portion of these interviews renewed focus on what author Dan Parilla encountered in his over twenty years in the Navy. A pilot by training and designation saw how the traditional warfighting communities aligned to a standardized political organizational framework and how career paths were shaped by adherence to a common (and transparent) progression. Officers were expected to complete one or two tours in their primary career role, then seek out a disassociated sea duty option that would allow them to interact with members from across the Navy enterprise to have an opportunity to develop richer technical and leadership skills. Following this tour, the officers would then return to their primary community for a mid-level leadership position, such as a department head. After this tour, they would screen for command while serving in another staff role, supporting, and having the mentorship from many senior leaders with vast exposure to a myriad of skills they could add to their toolkit.

Education opportunities were sporadic at best and often required them to be sandwiched in between other tours. Those who were able to build in time (by shortening tours) could attend the Naval War College for a 9-month program in a master's degree that would expose them to crucial leadership capacities like acquisitions, national strategy development, and critical thinking opportunities etcetera. The Navy's focus in these advanced education opportunities was not on attaining the degree, but rather on the officer receiving a joint service qualification (included as part of the degree program) and available through self-study and correspondence classes.) Many officers chose the correspondence option because they could not afford to take time out to deviate from their regular career path focused on their current job to explore the more academic options that might benefit them across the remainder of their careers as leaders.

By pure chance, following an officer-in-charge tour in Afghanistan, he worked with emerging technological reconnaissance systems. Dan was offered a Fleet Cyber Command position (TENTH Fleet), where he was qualified as a Cyber Battle Watch Captain and Cyber Operations Planner. He had the opportunity, while there, to act as a mentor to several junior officers. However, most of them were from the cryptologic community, and his career background did not provide them much guidance in their career pathways. Despite this lack of career overlap, his keen understanding of cyber operations made him a valuable staff member. He was a lead instructor to those seeking to qualify on the watch floor.

As was mentioned in many of our interviews, it is essential to note that Dan's background, like so many others, was decidedly not technical or cyber-related. With an undergraduate degree in Psychology and a master's degree in International Strategic Studies, he would have seemed an unlikely choice for the cyber field. Again, this same story of fate and sheer weird luck was reinforced across most of our interviews. Dan's conveyed experience in the cyber realm now seems more common in executing a non-traditional path to cyber than he ever realized. Finally, since he did not want to transition out of the Aviation community for a continued role in Cyber, he left the cyber field behind and returned to the cockpit at the end of his tour at TENTH Fleet. It was not until this study that his career path, and the similarities in experience and opportunity, became more relevant than he could have previously realized.

Final Thoughts:

Through the application of due diligence regarding the research questions presented and utilizing the three defined concepts of Learning, Organizational Structure as the force enabler, and Strategy, DoN can begin the process of enhancing cyber professionals through a recommended Cyber Operational Leadership Training and Selection process. Ultimately, a renewed focus on education's essential on-the-job training, mentorship, diverse learning, and leadership and managerial development experiences are paramount. Creating a robust learning and career path for cyber professionals and leaders will allow the entire cyberwarfare community to align with the more established and traditional naval warfare domains. Cyber is not a singular domain unto itself, but a domain through which all other domains operate.

The varied research, combined with the opinions expressed across the professional interviews, creates a sense that cyber is more than merely a force multiplier. It is an essential force enabler that can define freedom of operation for the military and the global community. When Fleet Cyber Command was established, they chose to number it as TENTH Fleet. The historical context of TENTH Fleet as the original anti-submarine fleet underscores a domain's ability to have both tactical and strategic importance. In the case of cyber, this importance has implications beyond the strategic, and it can and will influence policy and global objectives. Of key importance to this broad-reaching effect are understanding, learning, and leadership.

A leadership cadre of cyber professionals that can understand, communicate, and direct the development and implementation of the technical foundations of cyber operations is essential not just to the success of the Navy but it is essential to creating a more comprehensive, responsive, and adaptive cyber community that can and must span the DoD, Federal, civilian, and corporate structures. The Department of the Navy will need to develop and implement a strategy that can facilitate this learning and enable forces within cyber and across all of its domains.

References

Armstrong, M. E., Jones, K. S., Namin, A. S., & Newton, D. C. (2020). Knowledge, Skills, and Abilities for Specialized Curricula in Cyber Defense: Results from Interviews with Cyber Professionals. *ACM Trans. Computing Education*, 1-25. doi:https://doi-org.proxy.library.vanderbilt.edu/10.1145/3421254

Baker, M. (2016). *Cyber Workforce Development-21st Century Cyber Education and Training.* Pittsburgh: Software Engineering Institute.

Bate, L. (2020). *Growing a Stronger Federal Cyber Workforce CSC White Paper #3.* Washington D.C.: Cyberspace Solarium Commission.

Bolman, L. (2017). *Reframing Organizations: Artistry, Choice and Leadership.* Hoboken: Jossey-Bass.

Bowles, S. F. (2017). Adaptive Leadership in Military and Government Settings. In B. P. Bowles S. (Ed.), *Handbook of Military Psychology.*

Caulkins, B. D., Badillo-Urquiola, K., & Leis, R. (2017). Cyber workforce development using a behavioral cybersecurity paradigm. 2016 IEEE International Conference on Cyber Conflict. *Institute for Simulation & Training (UCF)*, 1-7. doi:https://doi.org/10.1109/CYCONUS.2016.7836614

Cisco. (2021). *Cisco Academy*. Retrieved from Cisco Academy: https://netacad.com

Computer News Weekly. (2021). Researchers from Texas Technical University Provide Details of New Studies and Findings in the Area of Computing Education (Knowledge, Skills, and Abilities for Specialized Curricula In Cyber Defense: Results From Interviews With Cyber...). *Computer News Weekly*, 853-862.

Crumpler, W., & Lewis, J. (2019, January). The Cybersecurity Workforce Gap. *Center for Strategic and International Studies*, 1-10. Retrieved from http://www.isaca.org/Knowledge-Center/

Dawson, J., & Thompson, R. (2018). The future cybersecurity workforce: Going Beyond technical skills for successful cyber performance. *Frontiers in Psychology*, 1-12. doi:https://doi.org/10.3389/fpsyg.2018.00744

DCPAS. (2013). *DCLP.*

Department of Defense. (n.d.). *DoD Cyber Excepted Service (CES)*. Retrieved from DoD Cyber Exchange Public: https://public.cyber.mil/cw/dod-cyber-excepted-service-ces/

Department of the Navy. (2020). *NAVADMIN 025-20.* DoN.

DoN. (2016). *Navy Civilian Career Path.*

DoN CIO. (2021). Workforce Lunch and Learn. Washington, DC. Retrieved from fcc.navy.mil: https://fcc.navy.mil

FCPS CTE. (2020, 10). Cyber Fundamentals Graduation Survey. Fairfax, VA.

Google Grow. (2021). *Google Training*. Retrieved from Google Certification and Training: https://grow.google.com

Gregory, H., Golding, J., & Casch, D. (2001). Naval Retention and what to do about it?

Hardison, C. M., Payne, L. A., Hamm, J. A., Clague, A., Torres, J., Schulker, D., & Crown, J. S. (2019). *Attracting, Recruiting, and Retaining Successful Cyberspace Operations Officers: Cyber Workforce Interview Findings.* Santa Monica: Rand research.

Int-1. (2020). Cyber Interview. (Parilla, & Wills, Interviewers)

Int-10. (2021). Cyber Interview. (Parilla, & Wills, Interviewers)

Int-11. (2021). Cyber Interview. (Parilla, & Wills, Interviewers)

Int-12. (2020). Cyber Interview. (Parilla, & Wills, Interviewers)

Int-13. (2021). Cyber Interview. (Parilla, & Wills, Interviewers)

Int-14. (2020). Cyber Interview. (Parilla, & Wills, Interviewers)

Int-15. (2020). Cyber Interview. (Parilla, & Wills, Interviewers)

Int-16. (2021). Cyber Interview. (Parilla, & Wills, Interviewers)

Int-17. (2020). Cyber Interview. (Parilla, & Wills, Interviewers)

Int-2. (2020). Cyber Interview. (Parilla, & Wills, Interviewers)

Int-3. (2020). Cyber Interview. (Parilla, & Wills, Interviewers)

Int-4. (2020). Cyber Interview. (Parilla, & Wills, Interviewers)

Int-5. (2020). Cyber Interview. (Parilla, & Wills, Interviewers)

Int-6. (2020). Cyber Interview. (Parilla, & Wills, Interviewers)

Int-7. (2020). Cyber Interview. (Parilla, & Wills, Interviewers)

Int-8. (2021). Cyber Interview. (Parilla, & Wills, Interviewers)

Int-9. (2020). Cyber Interview. (Parilla, & Wills, Interviewers)

Iordanoglou, D. (2018). Future Trends in Leadership Development Practices and the Crucial Leadership Skills. *Journal of Leadership, Accountability and Ethics*. doi:https://doi.org/10.33423/jlae.v15i2.648

ISC2. (2018). *Cybersecurity Workforce Study*. Retrieved from ISC2 Cybersecurity: https://www.isc2.org/-/media/ISC2/Research/2018-ISC2-Cybersecurity-Workforce-Study.ashx?la=en&hash=4E09681D0FB51698D9BA6BF13EEABFA48BD17DB0

ISC2. (2021). *Cybersecurity Workforce Study*. Retrieved from ISC2 Cybersecurity: https://www.isc2.org/-/media/ISC2/Research/2018-ISC2-Cybersecurity-Workforce-Study.ashx?la=en&hash=4E09681D0FB51698D9BA6BF13EEABFA48BD17DB0

ISSC. (2018). *Cybersecurity Professional Focus on Developing New Skills as Workforce Gap Widens*. Retrieved from International Information System Security Certification Consortium: https://www.isc2.org/-/media/ISC2/Research/2018-ISC2-Cybersecurity-Workforce-Study.ashx?la=en&hash=4E09681D0FB51698D9BA6BF13EEABFA48BD17DB0

Jones, K. S., Namin, A. S., & Armstrong, M. E. (2018, August). The Core Cyber-Defense Knowledge, Skills, and Abilities That Cybersecurity Students Should Learn in School: Results from Interviews with Cybersecurity Professionals. *ACM Trans. Comput. Educ*, 1-12. doi:https://doi.org/10.1145/3152893

Knapp, K. J., Maurer, C., & Plachkinova, M. (2017). Maintaining a Cybersecurity Curriculum: Professional Certifications as Valuable Guidance. *Journal of Information Systems Education*, 101+. Retrieved from https://link.gale.com/apps/doc/A521590982/AONE?u=tel_a_vanderbilt&sid=AONE&xid=fb6eb8d3

Leigher, W. (2011, February). Learning to Operate in Cyberspace. *Proceedings*, pp. 32-37.

Mango, E. (2018). Rethinking Leadership Theories. *Open Journal of Leadership*, 57-88. doi:https://doi/org/10.4236/ojl.2018.71005.

Morgus, R. (2019). *CSC White Paper #5: Transition Book for the Incoming Biden Administration.* Washington D.C.: US Cyberspace Solarium Commission.

Navy Times. (2021, Jan 8). Retrieved from https://www.navytimes.com/news/your-navy/2021/01/08/navy-kicks-off-naval-community-college-pilot-program-for-sailors-marines-and-coast-guardsmen/

Nelson, T. &. (2017). Addressing Complex Challenges through Adaptive Leadership: A Promising Approach to Collaborative Problem Solving. *Journal of Leadership*, 111-123. doi:https://doi.org/10.12806/v16/i4/t2

NIST. (2019). *Executive Cyber Leadership*. Retrieved from NICCS (National Initiative for Cyber Security Workforce): https://niccs.us-cert.gov/workforce-development/cyber-security-workforce-framework/executive-cyber-leadership

OPM. (2020). *SES Desk Guide*. Retrieved from OPM.GOV: https://www.opm.gov/policy-data-oversight/senior-executive-service/reference-materials/ses-desk-guide.pdf

Parilla, D. R. (2020, 21). Personal Experience.

Reiter, J. (2020). Kickoff Interview. (D. Parilla, & S. Wills, Interviewers)

Reith, M., & et. al. (2019). *Rethinking USAF Cyber Education and Training.*

Scott, L., Conley, R., Mesic, R., O'Connell, E., & Medlin, D. (2010). *Human Capital Managementfor the USAF Cyber Force. RAND Project Air Force, Santa Monica, CA.* .

SECNAV. (2008, April). OPNAVINST 5300.8C.

Turk, R. (2013). *Preparing a Cyber Security Workforce for the 21st Century.* Leavenworth: USA War College.

United State Navy IDC. (2010). *Information Dominance Corps.* Annapolis: U.S. Naval Academy.

Virginia Dept. of Education. (2017, June). Cybersecurity Pathways for High School. Richmond, VA. Retrieved from https://www.doe.virginia.gov/instruction/career_technical/cybersecurity/cyber-courses-2017.pdf

Werner, B. (2020, January 20). *Navy 2019 Retention Rates*. Retrieved from USNI News: https://news.usni.org/2020/01/20/navy-hits-2019-enlisted-sailor-retention-targets

Appendix 1. Interview Structure

RQ1. What kinds of skills and capabilities will Department of Navy cyber supervisors need to effectively lead the cyber workforce?

RQ2. How can the Department of Navy develop the appropriate supervisory and leadership personnel responsible for leading, managing, and developing the rest of the cyber warfighting force?

RQ3. What intellectual infrastructure is needed to support viable, sustainable cyber management/leadership?

1) Questions presented to senior personnel:
    a. (RQ1) What (experience-based qualities) are the leadership qualities for effective organizations?
    b. (RQ1) What leadership experience have you had?
        i. Was your training appropriate for the skill set and job definition?
    c. (RQ3) How do you see the cyber workforce developing?
    d. (RQ2/3) What gaps in cyber leadership and management training or experiences do you think currently exist?
    e. (RQ2) What depth of cyber experience do you see in your community?
    f. (RQ1) What training in planning, policy, or doctrine have you received?
        i. How well does this match your expectations?
    g. (RQ2) What training in planning, policy, or doctrine was lacking in your training path?
    h. (RQ3) What can you tell me about budgeting in terms of program development and execution? How does this familiarity impact cyber leadership capacity?
    i. (RQ1/3) What standardization in cyber training and leadership development is necessary?
    j. (RQ/2) How do these skills hold up or change as a leader or manager moves through the leadership structure?

        i. Do these skills align with the training of division heads, branch heads, and team leads?

    k. (RQ2) Do your current, or expected certifications meet requirements for follow-on leadership jobs, in or out of the DOD cyber realm?
    l. (RQ1) Do you feel you have a viable career path to senior leadership (or beyond)?
    m. (RQ3) Are there requirements that NISST and DOD define differently for cyber professionals?
        i. Are they incompatible definitions?
    n. (RQ1/2/3) Post COVID-19 forced isolation, what additional gaps/successes have been discovered that will define future effective cyber leadership?

2) Questions presented to mid-level personnel:
    a. (RQ1) What (experience-based) are the leadership qualities for effective organizations?
    b. (RQ1) Discuss the training you have received or been offered (hard and soft?)
    c. (RQ3) How well does training available/advertised align with the skills that you are expected to have?
    d. (RQ1) How many years of cyber experience and leadership do you have?
    e. (RQ1/2) Are you appropriately trained for your next position in terms of:
        i. Technical
        ii. Leadership
        iii. Experiential
    f. (RQ2) What depth of cyber experience do you see in your community?
    g. (RQ1) What training in planning, policy, or doctrine have you received?
        i. How well does this match your expectations?
    h. (RQ2) What do you know about budgeting, program development, and execution?
    i. (RQ1) What skillset did you have upon recruitment?
        i. Are you using it now?

j. (RQ1/3) What can be learned from this transition applicable to cyber leader development?
    i. How have you adapted to this transition?
k. (RQ1/3) Who was the transition (COVID-19) leader?
    i. What skill sets did they possess?
l. (RQ2) Do your current, or expected certifications meet requirements for follow-on leadership jobs in or out of the DOD cyber realm?
m. (RQ1) Do you feel you have a viable career path to senior leadership (or beyond)?

3) Questions presented to entry-level personnel: Should we place the FCPS Survey right behind this?
    a. (RQ1) What (experience-based) are the leadership qualities for effective organizations?
    b. (RQ1) Discuss the training you have received or been offered (hard and soft?)
    c. (RQ1/2) Are you being trained for your next position? How and in what focus areas/priorities?
    d. (RQ1) What skillset did you have upon recruitment?
        i. Are those skills still being utilized or advanced?
    e. (RQ1/3) What skillsets did your direct report/supervisor exhibit during the COVID-19 transition that you found effective?
        i. Were these skills apparent before the crisis response?

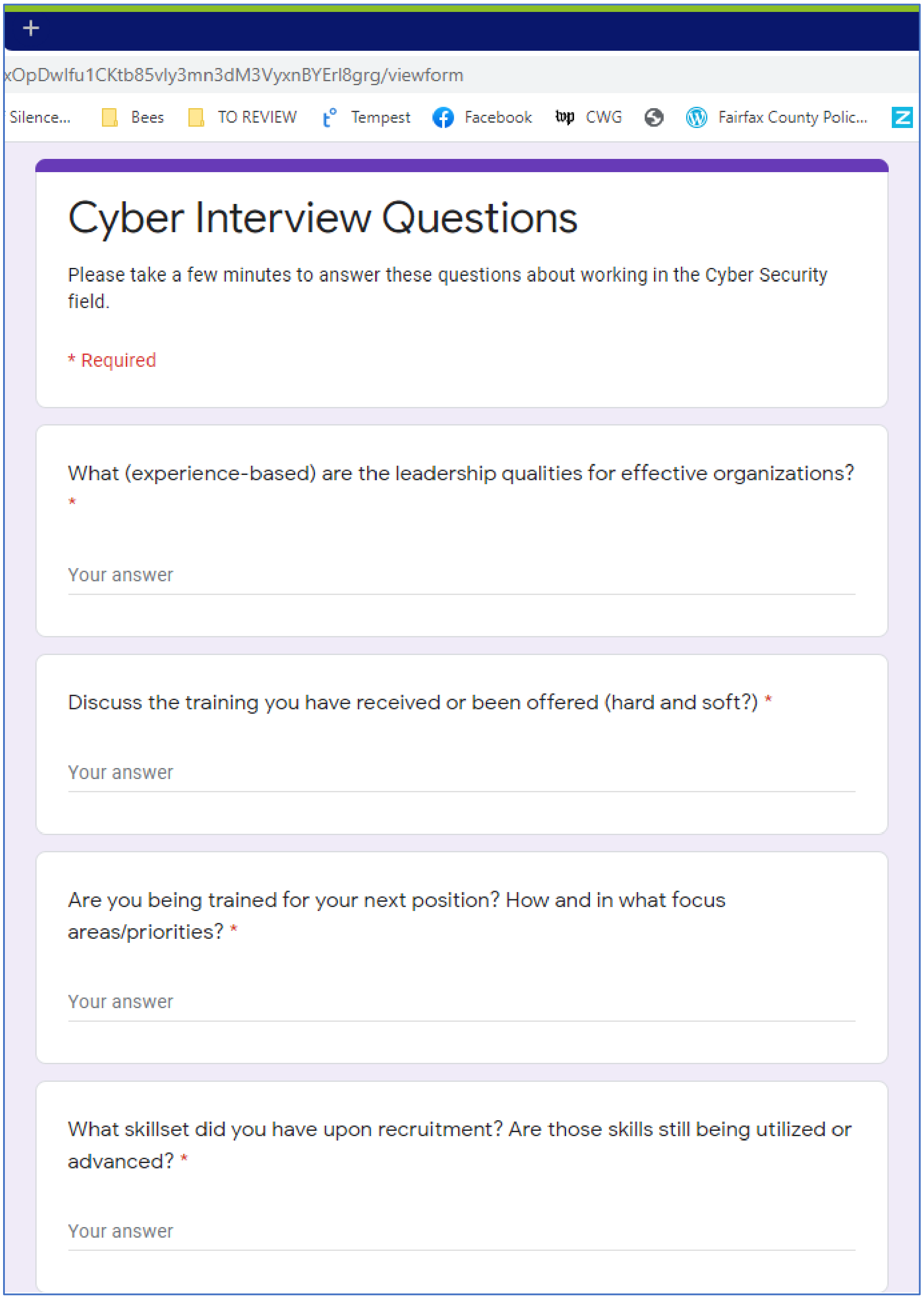
Appendix 2 RQ Coding Output

Code System	Memo	Frequency
Code System		1722
People	2/1/2021 9:58 AM Lexical Search - ANY: People Within: Document	425
Technical Expert	2/1/2021 9:58 AM Lexical Search - ANY: Technical Expert Within: Document	6
Recognition	2/1/2021 9:57 AM Lexical Search - ANY: Achievement Success Recognition Advancement Within: Document	29
Financial Benefit	2/1/2021 9:57 AM Lexical Search - ANY: Money Pay Compensation Reward Within: Document	89
Lifelong Learning	2/1/2021 9:56 AM Lexical Search - ANY: Learning Curiosity Lifelong Challenge Motivation Encouragement Within: Document	185
LEADERSHIP	2/1/2021 9:55 AM Lexical Search - ANY: Leadership Mentor People Communication Challenge Within: Document	700
Technical Skills	Use of Technical Skills / Cyber Fundamentals	288

Code System	Frequency
Code System Totals	3474

RQ1 Skills/Capabilities	194
RQ2: Leading Managing Developing	26
RQ3: Intellectual Infrastructure Sustain Training Ex	787
Sub Category Coding	
development develop growth	287
Passion / Curiosity	57
People - relational	430
Technical Expert	6
Financial Benefit	89
Lifelong Learning	185
LEADERSHIP	700
Technical Skills	288

Appendix 3 – FPCS Survey Sample



+
xOpDwlfu1CKtb85vly3mn3dM3VyxnBYErl8grg/viewform
Silence... Bees TO REVIEW Tempest Facebook CWG Fairfax County Polic...

Cyber Interview Questions

Please take a few minutes to answer these questions about working in the Cyber Security field.

* Required

What (experience-based) are the leadership qualities for effective organizations? *

Your answer

Discuss the training you have received or been offered (hard and soft?) *

Your answer

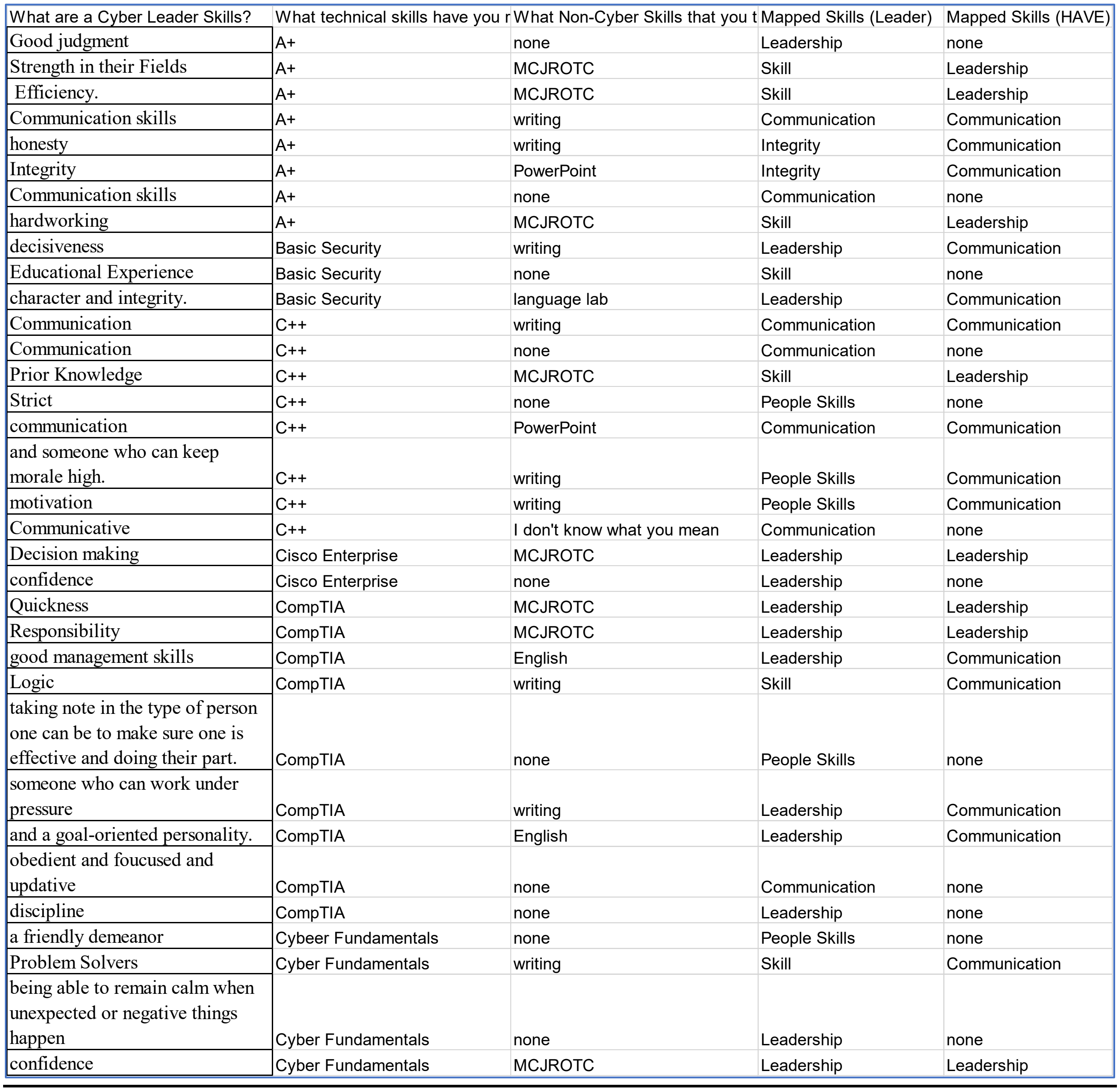
Are you being trained for your next position? How and in what focus areas/priorities? *

Your answer

What skillset did you have upon recruitment? Are those skills still being utilized or advanced? *

Your answer

Appendix 4 – FCPS Survey Results



What are a Cyber Leader Skills?	What technical skills have you r	What Non-Cyber Skills that you t	Mapped Skills (Leader)	Mapped Skills (HAVE)
Good judgment	A+	none	Leadership	none
Strength in their Fields	A+	MCJROTC	Skill	Leadership
Efficiency.	A+	MCJROTC	Skill	Leadership
Communication skills	A+	writing	Communication	Communication
honesty	A+	writing	Integrity	Communication
Integrity	A+	PowerPoint	Integrity	Communication
Communication skills	A+	none	Communication	none
hardworking	A+	MCJROTC	Skill	Leadership
decisiveness	Basic Security	writing	Leadership	Communication
Educational Experience	Basic Security	none	Skill	none
character and integrity.	Basic Security	language lab	Leadership	Communication
Communication	C++	writing	Communication	Communication
Communication	C++	none	Communication	none
Prior Knowledge	C++	MCJROTC	Skill	Leadership
Strict	C++	none	People Skills	none
communication	C++	PowerPoint	Communication	Communication
and someone who can keep morale high.	C++	writing	People Skills	Communication
motivation	C++	writing	People Skills	Communication
Communicative	C++	I don't know what you mean	Communication	none
Decision making	Cisco Enterprise	MCJROTC	Leadership	Leadership
confidence	Cisco Enterprise	none	Leadership	none
Quickness	CompTIA	MCJROTC	Leadership	Leadership
Responsibility	CompTIA	MCJROTC	Leadership	Leadership
good management skills	CompTIA	English	Leadership	Communication
Logic	CompTIA	writing	Skill	Communication
taking note in the type of person one can be to make sure one is effective and doing their part.	CompTIA	none	People Skills	none
someone who can work under pressure	CompTIA	writing	Leadership	Communication
and a goal-oriented personality.	CompTIA	English	Leadership	Communication
obedient and foucused and updative	CompTIA	none	Communication	none
discipline	CompTIA	none	Leadership	none
a friendly demeanor	Cybeer Fundamentals	none	People Skills	none
Problem Solvers	Cyber Fundamentals	writing	Skill	Communication
being able to remain calm when unexpected or negative things happen	Cyber Fundamentals	none	Leadership	none
confidence	Cyber Fundamentals	MCJROTC	Leadership	Leadership

leading by example	Cyber Fundamentals	MCJROTC	Leadership	Leadership
The experience of leading and managing a big group.	Cyber Fundamentals	digital art	Leadership	Communication
resilience	Cyber Fundamentals	English	Leadership	Communication
Leaders	Cyber Fundeamentals	none	Leadership	none
Delegation	FANUC coding	none	People Skills	none
Confidence and Determination	FANUC coding	MCJROTC	Leadership	Leadership
They have to know how everyone works	FANUC coding	none	People Skills	none
Integrity	Intro to Programming	language lab	Integrity	Communication
Knowledge	Java	none	Skill	none
Courage	Java	writing	Leadership	Communication
helpful	Java	none	People Skills	none
influence	Java	PowerPoint	People Skills	Communication
Interest	Java	girl scouts	Skill	Leadership
Cyber	Java	leadership	Skill	Leadership
The qualities for a successful organization are good communication and good skills and experience.	Java	leadership	Communication	Leadership
Listens to all arguments	network management	none	Communication	none
commitment	network management	writing	Leadership	Communication
self ownership	network management	language lab	Leadership	Communication
Consistency	Network Mgmt	English	Leadership	Communication
that the person can control a situation and stay calm when under pressure	Network Operations	English	Leadership	Communication
communication skills	Network Operations	none	Communication	none
Courage	networking	PowerPoint	Leadership	Communication
technical skill	none	eagle scout	Skill	Leadership
Leadership qualities needed are decisive decision making	none	none	Leadership	none
Integrity	Python 1	debate team	Integrity	Communication
commitment	Python 1	language lab	Leadership	Communication
experience	Python 1	none	Skill	none
Skillful	Python 1	none	Skill	none
and Self-awareness	Python 2	MCJROTC	People Skills	Leadership
technical skill	Python 2	none	Skill	none
not Biased or exposed to pressure	Python1	MCJROTC	People Skills	Leadership
Communication	Pytohn 2	none	Communication	none
communication	SQL	PPS	Communication	Leadership
leadership	SQL	PPS	Leadership	Leadership
and having different goals.	SQL	PPS	Leadership	Leadership
personality	SQL	none	People Skills	none
Knowledge	tehncial skills	English	Skill	Communication
empathy	VEX coding	PowerPoint	People Skills	Communication
Timely	web design	debate team	Leadership	Communication
People skills	Web Design	writing	People Skills	Communication
Good Explanations	web desing	debate team	Communication	Communication
Encouraging	web graphice	none	People Skills	none
honesty	Web Media	leadership	Integrity	Leadership