Pi Shaped Officers:

Developing Naval Officers to Lead in the
Converged Cyberspace and Electromagnetic Spectrum Domains

By:
LCDR Brian L. P. Schulz, USN
Federal Executive Fellow
Duke University
29 April 2016

The views and opinions expressed here are the author's alone and do not reflect the views and opinions of the U.S. Navy or Duke University.

Abstract

The Chief of Naval Operations has acknowledged the rise of the Electromagnetic Spectrum and Cyberspace in modern Naval Warfare. These two critical areas are now considered their own domains, on par with sea, air, land, and space. They are a linchpin to every other domain and future Naval Operations depend on assured access and maneuverability in these two domains. The Navy Cryptologic Warfare Officer Community, too, has evolved from the SIGINT-centric community of WWII, assuming the roles of Electronic Warfare and Cyberspace Operations as they emerged. After a decade of turbulence, in which the strategic direction of the community was ever changing, the goals of the community today are clear; built on the foundation of Signals Intelligence, Electronic Warfare, and Cyberspace Operations as core competencies.

This paper explores the emergence of the Electromagnetic Spectrum and Cyberspace as warfighting domains and the evolution of the Navy Cryptologic Warfare Officer Community. It analyzes the results of a recent survey of 277 Officer and presents a recommended manpower strategy to ensure the Navy is properly aligned to meet future challenges within the Electromagnetic Spectrum and Cyberspace.

List of Acronyms

AFCEA	Armed Forces Communication and Electronics Association
AFSC	Air Force Specialty Code
AM	Amplitude Modulation
ARPA	Advanced Research Projects Agency
C2	Command and Control
C3F	Commander Third Fleet
C5F	Commander Fifth Fleet
C10F	Commander Tenth Fleet
CNO	Chief of Naval Operations
COMINT	Communications Intelligence
CSO	Cyberspace Operations
DCNO	Deputy Chief of Naval Operations
DCO	Defensive Cyber Operations
DoD	Department of Defense
DODIN	Department of Defense Information Network
EA	Electronic Attack
ELINT	Electronic Intelligence
EMMW	Electromagnetic Spectrum Maneuver Warfare
EMS	Electromagnetic Spectrum
EP	Electronic Protect
ES	Electronic Warfare Support
EW	Electronic Warfare
FCC	Fleet Cyber Command
FFC	Fleet Forces Command
FISINT	Foreign Instrumentation Signals Intelligence
FM	Frequency Modulation
GPS	Global Positioning System
IC	Intelligence Community
IP	Information Professionals

IS	Intelligence Squadron
IT	Information Technology
JO	Junior Officer
JP	Joint Publication
MOS	Military Occupational Specialty
NIOC	Navy Information Operations Command
NNWC	Naval Network Warfare Command
NPC	Navy Personnel Command
NRL	Navy Research Laboratory
NSG	Naval Security Group
NSWC	Navy Special Warfare Command
OCO	Offensive Cyber Operations
OPSEC	Operational Security
RADAR	Radio Detection and Ranging
RF	Radio Frequency
SIGINT	Signals Intelligence
U.S.	United States
VADM	Vice Admiral

List of Figures

Table of Contents

I. Introduction

Last spring (2015), the Chief of Naval Operations (CNO) released the Cooperative Strategy for 21st Century Seapower (CS-21), outlining the latest strategic vision for the United States (U.S.) Navy. In this document, the CNO stated that "the Sea Services have historically organized, trained, and equipped to perform four essential functions: deterrence, sea control, power projection, and maritime security. Because access to the global commons is critical, this strategy introduces a fifth function: all domain access. This function assures appropriate freedom of action in any domain—the sea, air, land, space, and *cyberspace*, as well as in the *electromagnetic spectrum*… *the electromagnetic-cyber environment is now so fundamental to military operations and so critical to our national interests that we must treat it as a warfighting domain on par with sea, air, land, and space*."[i] In this simple statement, the CNO set Naval Warfare on a new trajectory. The domains of the Electromagnetic Spectrum (EMS) and Cyberspace had been doctrinally elevated to the level of the traditional domains of sea, air, land, and space when considering the future operations of the U.S. Navy.

The U.S. Navy invests millions of dollars into training and retaining the best pilots to take-off and land on ships at sea, nuclear power experts to provide the required power to deployed submarines and aircraft carriers, and special warfare experts to carry out difficult and sensitive operations around the globe. If the EMS and Cyberspace truly are critical to the U.S. Navy, then the Officers focused on these areas, similar to their pilot, submariner, and special warfare counterparts, should enjoy the highest levels of training, clearly articulated career expectations and requirements to ensure advancement, and continued skill development to meet the challenges presented in these domains. The U.S. Navy must improve in these areas, as they are in direct competition with the other branches of service, the Intelligence Community (IC), the whole of government, and both domestic and international private industry for personnel with the required skills and education to operate in these critical domains. And this competition is fierce, with 46% of private and government organizations are reporting that they have a problematic shortfall of cybersecurity personnel among their employees.[ii]

The purpose of this paper is three-fold. We will explore the genesis and rise of the EMS and Cyberspace to the elevated levels we see today. We will examine the identity of these EMS Jedi's and Cyber warriors within the officer ranks of the U.S. Navy today. And we will analyze if the Navy is properly posturing and grooming these Officers as Junior Officers (JOs) to assume future senior leadership positions in the Navy's Cyberspace and EMS domains.

II. Background

A. Defining Key Terms

1. Electromagnetic Spectrum (EMS)

NASA defines the EMS as "the full range of frequencies that characterize light."[iii] DoD further defines the EMS as "the range of frequencies of electromagnetic radiation from zero to infinity. It is divided into 26 alphabetically designated bands."[iv] The EMS is a natural occurring domain, similar to the land, sea, air, and space domains. Scientists have researched the EMS for centuries, so definitions and understanding of the complex EMS is relatively concise and relatively straightforward. While new technologies continue to be invented to utilize the EMS, the EMS itself does not change. This is not the case with the man-made, continually evolving domain of Cyberspace, which we will look at in the next section. A graphical representation of the entire EMS is included below.

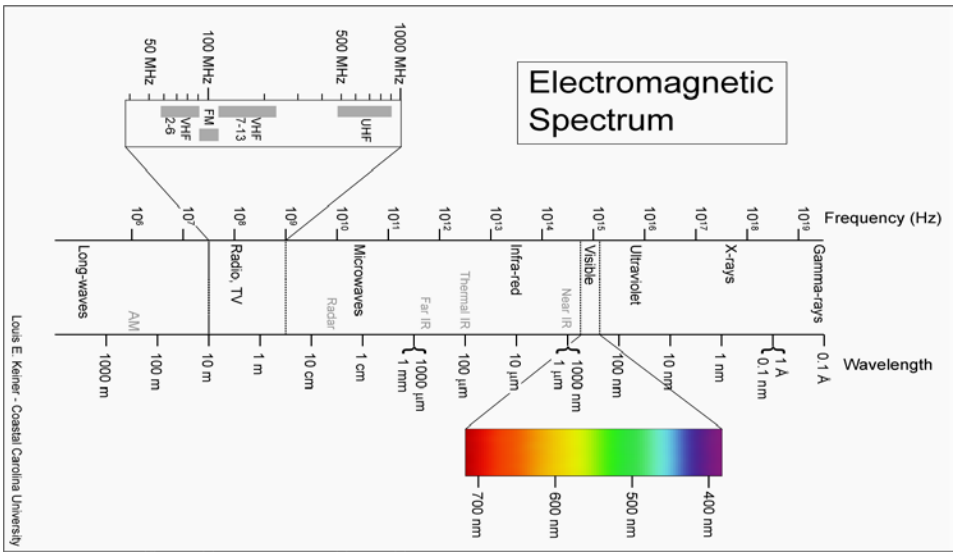

Figure 1: Electromagnetic Spectrum (EMS) [v]

Specific portions of the EMS have greater applicability and interest to DoD than others. The Radio Frequency (RF) and Microwave portions of the EMS house major communication types, including maritime signals and navigation aids, Amplitude Modulation (AM) and Frequency Modulation (FM) radios, cellular phones, Global Positioning System (GPS), satellite communications, WiFi/802.11, WiMax/802.16, Bluetooth/802.15, and Radio Detection and Ranging (RADAR), all of which are of significant interest to the DoD. Increased commercial technology across the RF band of the EMS has made proper cooperation and management within the EMS critical to prevent interference among users, especially in these critical areas of communication, positioning, navigation, and RADAR. A graphical representation of the RF band of the EMS is included below.

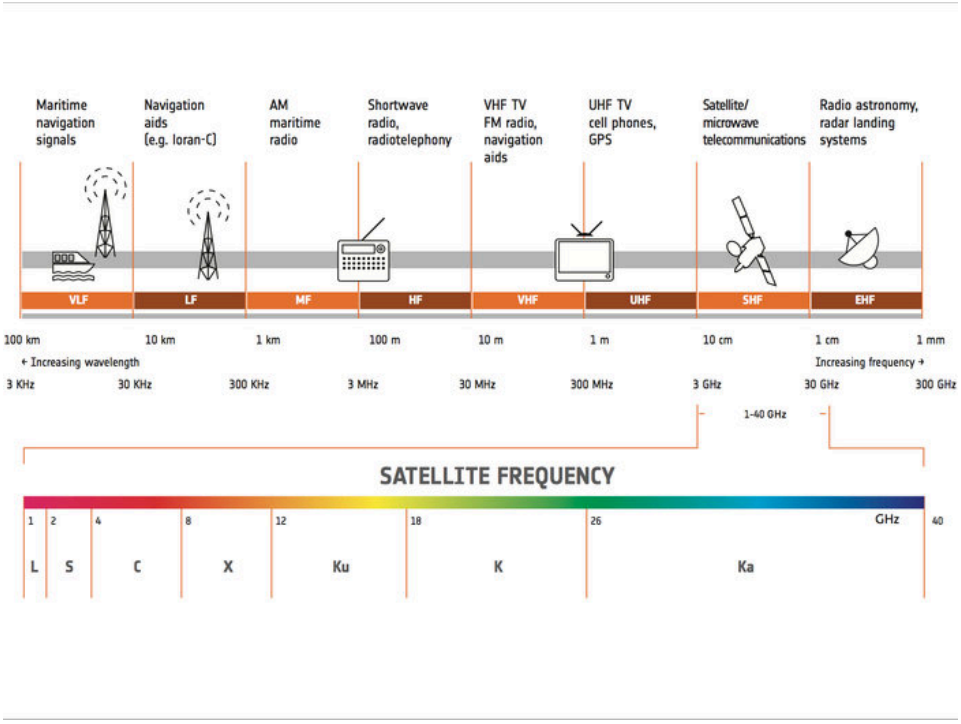

Figure 2: Radio Frequency (RF) Band [vi]

2. Cyberspace

Where the EMS is a naturally existing domain with clear scientific data and definitions, Cyberspace is a man-made domain, and as such, a concise coherent

definition is more elusive. We will examine the conception and evolution of Cyberspace below to see how the current definitions of this domain have evolved.

When researchers at the Advanced Research Projects Agency (ARPA) invented the precursor to the Internet back in 1969, few, if any, imagined how it would change the world in the coming half-century. The experimental tool used by scientists and researchers to share data and information evolved into the complex global network of computers, systems, and data that now make up the Internet and to some extent a portion of Cyberspace we have today.[vii]

Many modern, leading researchers and authors in the arena of Cyberspace have developed their own definitions, all slightly nuanced, and all subject to scrutiny. In one of the seminal works on the subject, Clarke and Knake defined Cyberspace as "all of the computer networks in the world and everything they connect and control. It is not just the Internet… Cyberspace includes the Internet plus lots of other networks of computers that are not supposed to be accessed from the Internet."[viii] Valeriano and Maness took exception to this definition, primarily because Clarke and Knake used their definition to identify a weakness in air-gapped (off the network) computers. They also criticized the narrow term 'computer networks' that Clarke and Knake used, offering that they should have used the broader 'microprocessor' term instead to incorporate expansion beyond computers.[ix] They point the reader to a separate work by Nye, who provided a more inclusive and robust definition, stating that Cyberspace "includes the Internet of networked computers but also intranets, cellular technologies, fiber-optic cables, and spaced based communications."[x] Singer and Friedman provide a unique side-bar to this definition in a discussion of locality and governance, specifically that "Cyberspace may be global, but it is not stateless or a global commons."[xi] Valeriano and Maness amplify Singer and Friedman's idea by identifying that Cyberspace remains the domain of states and is governed by institutions and networks, citing the Internet Corporation for Assigned Names and Numbers (ICANN) as an example.[xii]

In Joint Publication (JP) 3-12 released in 2013, the U.S. DoD took a stand and clearly defined Cyberspace, calling it "the global domain within the information environment consisting of the interdependent network of information technology

infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[xiii] This is a definition that Clarke, Knake, Valeriano, Manness, Nye, Singer, and Friedman could all agree on.

Having established working descriptions of the EMS and Cyberspace, we will take a closer look at how and why these ideas evolved within DoD as warfighting domains.

B. Rise of the EMS and Cyberspace within DoD

1. Rise of the EMS as a Warfighting Domain

Operations within the EMS are not new. The Navy utilized the EMS from its discovery in 1888, using it to communicate with ships at sea. In 1922, the Navy Research Laboratory (NRL) discovered the ability to use radio waves to detect moving objects at sea, creating RADAR, and operationally employing it throughout WWII. Since that time, DoD has furthered its use of the EMS to include navigation, communications, communications jamming, and infrared seekers for weapons, creating the opportunity for intelligence-gathering and warfare within the EMS.[xiv]

Signals Intelligence (SIGINT) is intelligence derived from electronic signals and systems, to include communications systems, RADARS, and weapons systems.[xv] SIGINT contains the three subsets of Communications Intelligence (COMINT), Electronic Intelligence (ELINT), and Foreign Instrumentation Signals Intelligence (FISINT).[xvi] COMINT is the "technical information and intelligence derived from foreign communications by-other-than-the-intended recipients,"[xvii] ELINT is "technical and geolocation intelligence derived from foreign non-communications electromagnetic radiations emanating from other-than-nuclear detonations or radioactive sources,"[xviii] and FISINT is "intelligence derived from the intercept of foreign electromagnetic emissions associated with the testing and operational deployment of non-US aerospace, surface, and subsurface systems, to include but not limited to telemetry, beaconry, electronic interrogators, and video data links."[xix]

Electronic Warfare (EW) is an accepted DoD doctrinal term and has been practiced since WWII. EW is "military action involving the use of electromagnetic and directed energy to control the EMS or to attack the enemy."[xx] It includes the subdivisions

of Electronic Attack (EA), Electronic Protection (EP), and Electronic Warfare Support (ES). EA is “the use of EM energy, directed energy, or anti-radiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability,” EP consists of “actions taken to protect personnel, facilities, and equipment from any effects of friendly or enemy use of the electromagnetic spectrum that degrade, neutralize, or destroy friendly combat capability,” and ES is “to search for, intercept, identify, and locate or localize sources of intentional and unintentional radiated EM energy for the purpose of immediate threat recognition, targeting, planning and conduct of future operations.”[xxi]

While operations within the EMS are not new, the level of emphasis on operations within the EMS have increased. In 2013, the CNO stated for the first time that "we're using the electromagnetic spectrum as a domain and as a means."[xxii] “Means” in this statement is in reference to the strategic planning ideas of “ends” (what is going to be accomplished), “ways” (how it will be accomplished) and “means” (who/what will be used to accomplish it). The Deputy Chief of Naval Operations (DCNO) for Information Dominance (N2/N6) followed up the CNO’s comments later that month, outlining the new concept of Electromagnetic Spectrum Maneuver Warfare (EMMW) as an operational approach to optimize and maintain supremacy across the EMS. The goal of EMMW is for the U.S. to collect on adversary data and adversary signals across the EMS to inform the friendly network, while simultaneously selecting and manipulating the friendly network presence and emissions in efforts to deceive, jam, or deny an adversary within the EMS.[xxiii] In a 2015 presentation at the Armed Forces Communications and Electronics Associations (AFCEA) Industry Day, the CNO’s Director of Integrated Fires showed the maturity of EMMW, outlining the four key objectives of this new warfare model, to include “Battlespace Awareness, Assured Command and Control, Maneuver, and Integrated Fires,”[xxiv] using the same terms associated with typical physical domains to describe operations in the EMS.

EMS operations, to include EW, EMMW, and SIGINT, are conducted from deployed ships. The new operating concept of EMMW does not change the manpower required to complete these operations, but strives to unify the efforts conducted by various

personnel on the ship or aircraft. Every ship will have a designated Ship's EW Officer onboard, responsible for all EW operations of the platform.[xxv] EW equipped aircraft will have the same. These Officers will lead the EMS operations and enlisted personnel onboard conducting these operations.

2. Rise of Cyberspace as a Warfighting Domain

The ascent of Cyberspace to its current level of significance as an operational domain for the U.S. Navy was not an instantaneous phenomenon, but rather a natural bi-product of the growth in Cyberspace in the Information Age.

The U.S. DoD released the National Military Strategy for Cyberspace Operations in 2006, defining Cyberspace as "characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures,"[xxvi] and specific strategic priorities included gaining and maintaining the initiative to operate within adversary decision cycles and integrating cyber capabilities across the full range of military operations using Cyberspace.[xxvii] In 2011, the DoD released the Strategy of Operating in Cyberspace, providing strategic initiatives for operations in Cyberspace, to include highlighting the importance of cybersecurity, employing new concepts to protect DoD networks and systems, and most significantly the strategic objective that "DoD will treat Cyberspace as an operational domain to organize, train, and equip so that DoD can take full advantage of Cyberspace's potential."[xxviii] These 2006 and 2011 strategy documents laid a foundation for Cyberspace as an independent domain.

Cyberspace provides an incredible capability in communication, command and control (C2), and associated intelligence functions, while simultaneously creating potential vulnerabilities for enemy or nefarious action within Cyberspace. These capabilities and vulnerabilities in Cyberspace mirror the physical domain and the ideas of Cyberpower, Cyberwar, and Cyberconflict have been developed to explain them further. Valeriano and Maness explore each in detail, providing analysis and criticism of the leading experts' writings on these topics.

Cyberpower is the ability to apply control and influence in Cyberspace, focusing on the combination of a nation's offensive capabilities, defensive capabilities, and dependence in and on Cyberspace. Cyberpower is strategic in nature and is a high/macro level component of a nation state. Strong nations traditionally have the most Cyberpower, but Valeriano and Maness point out that Cyberspace provides a unique asymmetric component that allows smaller states, and even non-state actor groups and individuals, to compete with traditionally large states in this domain with minimal investment.[xxix]

Arqilla and Ronfeldt coined the idea of Cyberwar back in 1993, when they wrote on the topics of "Netwar and Cyberwar."[xxx] At the time, their writing was considered fantastic and futuristic, but has actually turned out to be amazingly predictive. They suggested that Cyberwar would be fought exclusively between militaries, while Netwars would be a more asymmetric engagement with non-states and irregular forces. The contemporary realization of these two ideas has proven more challenging, as a clear line of distinction between state, state-sponsored, and non-state actors in Cyberspace is not always clear. However, their main thesis holds true: conflict will "increasingly depend on and revolve around information and communications."[xxxi] Nye further describes Cyberwar as "hostile actions in Cyberspace that have effects that amplify or are equivalent to major kinetic violence."[xxxii]The 2007 Cyberwar in Estonia demonstrated the kinetic effects of Cyberwar.[xxxiii]

Valeriano and Maness choose to use the term Cyberconflict instead of Cyberwar to be inclusive of lower-level cyber operations and interactions that do not rise to the level of the Nye Cyberwar definition used above. Specifically, they define Cyberconflict as the use of "Cyberspace for malevolent and/or destructive purposes in order to impact, change, or modify diplomatic or military interactions between entities."[xxxiv] The distinction they choose here separates Cyberconflict from other actions that occur in Cyberspace that could be defined as crime or espionage. Similar to what you would see in any physical domain, the power projection available in Cyberspace ranges from espionage to conflict to acts of war.

DoD Cyberspace Operations (CSO) cover the range of Cyberconflict and Cyberwar to ensure U.S. Cyberpower. CSO can be broken into Offensive Cyber

Operations (OCO), Defensive Cyber Operations (DCO), and DoD Information Network (DODIN) Operations. OCO are operations "intended to project power by the application of force in or through cyberspace," DCO are "passive and active cyberspace operations intended to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities, and other designated systems," and DODIN Operations are "operations to design, build, configure, secure, operate, maintain, and sustain DoD networks to create and preserve information assurance on the DoD information."[xxxv]

CSO covers the range of articulated DoD primary cyber missions, which include to "defend DoD networks, systems, and information; defend the U.S. homeland and national interest against Cyber-attacks of significant consequence; and to provide cyber support to military operational and contingency plans."[xxxvi] All services are being called to provide forces to the newly coined "Cyber Mission Force" with 133 Cyber Mission Teams operational by 2018. These teams will include 13 National Mission Teams to defend the U.S. and its interests against Cyber-attacks, 68 Cyber Protection Teams to defend priority DoD networks and systems, 27 Combat Mission Teams to support operational plans and operations of the Combatant Commands, and 25 Support Teams to support the National and Combat mission teams.[xxxvii] The Navy is responsible for manning 40 of 133 Cyber Mission Force teams.[xxxviii] These teams will be made up of both Officers and Enlisted Sailors conducting CSO. Unlike the EMS operations discussed in the previous section, CSO will traditionally be conducted from shore facilities vice onboard various deployed naval platforms. That said, every deployed Navy ship will have Naval Officers from the Information Professionals (IP/1820) Officer Community and/or enlisted Information Technology (IT) specialists to "operate, maintain, secure, plan and acquire the Naval network and the systems that support Navy operations and business processes." [xxxix]

3. Convergence of the EMS and Cyberspace

In the previous sections, we reviewed the rise of the EMS and Cyberspace to their current levels as warfighting domains. In addition to their rise, there has also been a convergence of the EMS and Cyberspace and a resultant convergence of CSO and EW.

The EMS is a critical component of military and civilian computer networks and Cyberspace. Whether on a college campus, at a local coffee shop, or on a ship at sea, the wireless network provides access, mobility, and connectivity. While Cyberspace is the "Internet, telecommunications networks, computer systems, and embedded processors and controllers,"[xl] depending on the network design, these networks are part of the EMS. An 802.11 WiFi signal or a fiber optic line where data exists in visible light are examples where the EMS is the backbone enabling Cyberspace. The iPhone accessing the Internet through the Verizon LTE network? The EMS. And the ship at sea sending and receiving an uplink and downlink to a satellite overhead? Also the EMS. The two are fully intertwined. A recent DoD Spectrum Workshop briefing identified the difficulty to determine where Cyberspace ends and the EMS begins, and vice versa, calling the "EMS the physical environment in which Cyberspace exists" and highlighting the technical convergence that exists between wire connections, wireless connections, and optical connections between systems and networks.[xli]

Senft elaborates on this convergence in an operational sense, discussing the parallels that exist between CSO and EW, with both based on similar principles of attack, defense, and support. He goes on to establish the parallel between OCO and EA as offensive/attack capabilities, as both are a use of force with an intent to degrade, neutralize, or destroy a target. DCO and EP are both defensive in nature, looking to protect data, networks, systems, and equipment. DODIN Operations and ES do not align as neatly; where DODIN operations consist of the design, building, and maintenance of friendly networks, ES is searching the EMS for energy to allow for future operations and planning. Both are supporting other aspects of EW and CSO. DODIN operations provide the foundation for DCO, as well as the platform for OCO. ES provides the indications and warning for future EP as well as target identification for future EA.[xlii] Senft refers to work by Rohret and Jiminez at the Joint Information Operations Warfare Center (JIOWC), which further describes this convergence, specifically showing how the use of the RF portion of the EMS enables and delivers CSO effects. In addition, synchronized CSO maximizes EW effects.[xliii] The below graphic shows the convergence of not only the EMS and Cyberspace, but the subsequent overlap and convergence of SIGINT, EW, and CSO.

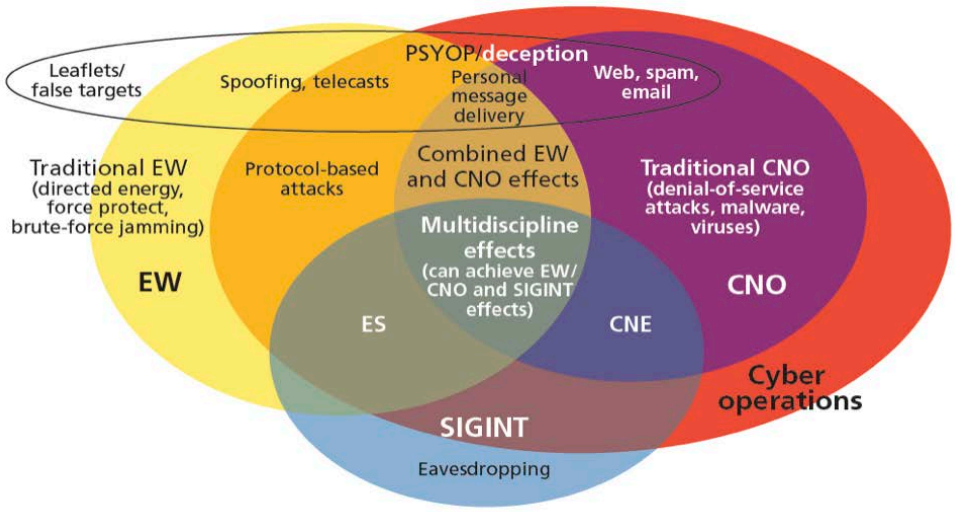

Figure 3: Convergence of EW, SIGINT, and CSO[xliv]

III. Navy Cyberspace and EMS Operations

Many communities throughout the U.S. Navy are active within the EMS and Cyberspace. Surface Warfare Officers and Submarine Officers are responsible for the sea domain, yet are dependent on the EMS and Cyberspace. The same is true for Navy Pilots and Flight Officers operating in the air domain, but directly dependent on and operating in the EMS and Cyberspace domains. Conversely, the U.S. Navy Cryptologic Warfare Officer Community is responsible for operations in the EMS and Cyberspace, but utilize the other domains and partner with other Communities to conduct these operations.

A. Navy Cryptologic Officer Community Overview

The defined and articulated function of the U.S. Navy Cryptologic Warfare Officer Community is to conduct Signals Intelligence (SIGINT), Electronic Warfare (EW) and Cyberspace Operations (CSO) across the converged EMS and Cyberspace.[xlv] We have already seen how this Triad of core competencies (SIGINT, EW, and CSO) fall squarely within the EMS and Cyberspace Domains which the CNO has deemed critical.

Vice Admiral (VADM) Jan Tighe, the U.S. Navy Cryptologic Warfare Officer Community Leader, surmises that “we deliver effects IN (sic) the converged domain

(EW/Cyber) and enable effects in other warfare domains (SIGINT). Our operations are both offensive and defensive. We hunt and engage adversaries in the converged domain."[xlvi] In the next section, we will look briefly at the origins and evolution of this critical U.S. Navy Warfare Officer Community.

B. Navy Cryptologic Officer Community Evolution

The Cryptologic Warfare Officer Community can trace its ancestry to the 19th century, when the first wireless transmission was sent from a Navy ship, simultaneously creating a capability and vulnerability in the EMS. From a simple radio transmission, the fields of SIGINT and cryptanalysis were born. In 1948, the Navy established a formal Navy Cryptologic officer designator and enlisted rating, and in 1950 the Naval Security Group (NSG) was established as the headquarters for all Navy Cryptologic personnel conducting SIGINT and EW operations for the U.S. Navy.[xlvii] The next 50 years saw relative stability within the Navy Cryptologic Community, with Cryptologic Officers adapting and evolving to meet the challenges of emerging electronic, communication, and information technology.

In 2005, Cryptologic Officers were renamed Information Warfare Officers, to reflect the inclusion of Information Operations, which included Computer Network Operations, as a core responsibility. Also in 2005, the NSG was disestablished after 55 years and Naval Network Warfare Command (NNWC) became the parent organization for the new Information Warfare Officer community.[xlviii] NNWC was established as the operational authority to coordinate all information technology, information operations, and space requirements for the Navy[xlix], so aligning newly named Information Warfare Officers under NNWC was a forward-leaning effort to recognize the convergence of the EMS and Cyberspace within the Information Domain.

In 2009, the CNO and Department of the Navy established the Information Dominance Corps (IDC), combining the Information Warfare Officer community with Intelligence, Meteorology, Information Professionals, and Space Cadre Officers. This move was done in effort to consolidate all Navy communities conducting information related operations to increase both efficiency and effectiveness for the individual

communities as well as for the newly formed aggregate. In 2010, the US 10th Fleet (C10F) was established (actually recommissioned, as it originally existed from 1943-1945, focused on meeting the anti-submarine threat in WWII[l]), Fleet Cyber Command (FCC) was established, and the dual-hatted C10F/FCC assumed responsibilities from NNWC for the Navy's Cryptologic, Information Operations, Cyberspace, EW, and Space missions.[li]

The decision to have a numbered fleet (C10F) responsible for these critical missions highlighted the Navy's emphasis on operations in the EMS and Cyberspace and their dedication to the principle of Information as a true warfighting domain. In the 2010 Navy Vision for Information Dominance, it was clear that the Navy now viewed "Information as a weapon" that would be used "in warfare and as warfare."[lii] And in the 2012 Human Capital Strategy for C10F/FCC, it was deemed critical to "dominate the modern information-related disciplines of intelligence, cyber, networks, space, oceanography, meteorology, and electronic warfare."[liii]

In 2016, the IDC was re-designated as the Information Warfare Community (IWC) to reflect "the rising influence of global information systems and the increasing rate of technological change and adoption… this transition also aligns Information Warfare as a predominant warfare area."[liv] As a result of this decision by the CNO, the former Information Warfare Officer community had to be renamed, with the return to heritage of Cryptology as Cryptologic Warfare Officer Community, adopting the Cryptologic moniker from the community's original establishment in the 1950's.

Hericlitus is credited with saying "the only thing that is constant is change."[lv] That is an appropriate statement for the Cryptologic Warfare Community from 2005-2016. The Cryptologic Warfare Community was evolving for a decade, driven by commercial technological innovation and the Navy's response to those innovations. In an effort to provide clear direction amidst the turbulence of change, Cryptologic Warfare Officer Community leadership released the Cryptologic Community Foundational Principles in 2011 to identify the core values and guiding principles for the community.

C. Navy Cryptologic Warfare Community Foundational Principles

Five years ago, the Cryptologic Warfare Officer Community realized the need to develop a strategy to define and refine the focus of the community that was in the middle of a significant period of change. The result was the 2011 Cryptologic Community Foundational Principles. This document was authored by a collective within the community and approved by every flag rank Cryptologic Warfare Officer.

The articulated intent of the document was to "unify the efforts of the Cryptologic Community," clearly defining the community's aim to "deliver value by deliberately developing deep, specialized expertise across our core skills, taking collective ownership of the same and overtly demonstrating commitment to our stated values."[lvi] These core skills were defined as SIGINT, Computer Network Operations (now known as CSO), and EW across the EMS and network, in global Navy, Joint, and National environments.

Within these core competencies, the Foundational Principles offered that Cryptologic Warfare Officers will provide timely Indications and Warning (I&W) and targeting information, deliver non kinetic effects and enable kinetic action, and integrate national and tactical information.[lvii] The document showed great foresight, aligning with the CNO's 2015 CS-21, specifically highlighting that "SIGINT, CNO, and EW comprise a 'main battery' in the future of warfare" and that "threats, consequence, and vulnerability across the cyberspace domain and information market are increasing in complexity, frequency, urgency, and potency."[lviii]

The Foundational Principles document also presents the benefits of maintaining these core competencies in one community. The convergence of the EMS and Cyberspace domains has created a "continuum of protocol and spectrum… bridging the RF to Internet Protocol (IP) gap,"[lix] and thus Cyberspace Operations and SIGINT are closely linked with similar tools, processes, procedures, and skillsets.

This document, even though it is five years old, is still the lasting articulation from Cryptologic Warfare Officer Community leadership defining the core competencies and operations for a U.S. Navy Cryptologic Warfare Officer. The core values outlined have been referenced as lately as March 2016 by the Cryptologic Warfare Officer Community Leader. She clearly reiterated the mission of the Cryptologic Warfare Officer Community,

stating that “on behalf of Maritime and Joint Commanders, we execute Cryptologic Warfare, which encompasses Signals Intelligence, Cyberspace Operations, and Electronic Warfare Operations in order to deliver effects through sea, air, land, space, and cyber domains at all levels of war.”[lx] So it is clear the principles are still considered valid and relevant. As such, it is rational that the cadre of Officers providing “specialized expertise across our core skills”[lxi] adhere to the guidance and direction from this document. But is it truly followed? Are Cryptologic Warfare Officers truly demonstrating specialized expertise in a core skill area?

IV. Generalist versus Specialist

The Cryptologic Warfare Officer Community is one of the most technologically demanding fields within the U.S. Navy. As previously discussed, it has continued in a state of perpetual flux for the last 15 years as commercial technological innovation and the rise of telecommunications and the Internet have evolved. We have discussed the three core competencies desired within a Navy Cryptologic Officer- namely SIGINT, CSO, and EW expertise. And we have seen how the Foundational Principles specifically call for” specialized expertise across our core skills.”[lxii]

So what does an “optimal” Navy Cryptologic Officer look like? Is it the CSO expert who is fluent in multiple programing languages and has completed multiple tours in CSO, becoming a true specialist and expert? Or is it the Systems Engineer who has completed tours across the core competencies in CSO and SIGINT and EW, with a lesser depth of expertise in one area but more breadth and shallower expertise across all three? The challenge of defining an ideal employee make-up is not unique to this problem. In the larger Human Resources (HR) realm of management theory, this challenge is viewed as the Generalist vs Specialist debate and is seen across sectors of private industry.

A. Review of the Generalist vs Specialist Debate

HR theory has evolved significantly over the last 30 years. Leading business researcher Josh Berson outlines the evolution of HR, going back 30+ years. Up through the 1980’s, the personnel department of an organization was responsible for hiring new employees and ensuring that compensation occurred. In the 1990’s, companies used

HR departments to develop more competitive recruiting, workforce training, and workforce strategic development.. Another transition occurred in the 2000's, into what today is called Talent Management.[lxiii]

Talent Management is an "organization's commitment to recruit, retain, and develop the most talented and superior employees available in the job market."[lxiv] This is a divergence from traditional personnel department and HR strategies where significant focus was on the hiring of new employees, but development and management once they were in the organization was lacking. Leading experts on this subject point out that "industry's greatest challenge by far is to rectify the under-development, under-utilization and ineffective management and use of its most valuable resources- its young managerial and professional talent."[lxv]

In the case of a Cryptologic Warfare Officer, part of this Talent Management challenge is defining and developing the skills required from the Officers themselves. Specifically, whether the Cryptologic Warfare Officer community wants their Officers to be specialists or generalists. Specialists are focused on a specific domain that is narrower in scope, and they have deep technical skills in a particular area. Generalists are focused across multiple domains, with a broader scope and working-level knowledge and competency in multiple areas.[lxvi]

Many organizations struggle to determine which type of employee (generalist or specialist) is best for optimizing an organization. Whereas traditionally it was encouraged to demonstrate specialty on a job application due to the cost involved in training specific specialties, many organizations now follow a cost-saving trend of hiring multi-tasking employees, which tends to more generalist tendencies.[lxvii] Some generalist vs specialist bias appears to buck conventional wisdom.

Google is a technologically advanced company. Their products involve significant coding and technical work, so one would naturally opine that they are a company of specialists. In fact the opposite is true. In a Harvard Business Review interview, Google's CEO stated they are actually looking for "generalists as opposed to specialists." [lxviii] His reasoning is that a dynamic indsutry, like Google, requires a more generalist mindset due

to conditions always changing. He also notes that specialists bring more of a bias when solving problems and are more rigid in their thinking of solutions.[lxix]

One survey suggests that specialists are becoming more generalist in nature, despite the fact that they were hired specifically for their specialty skills.[lxx] This convergence of the generalist and specialist is creating a new, morphed type of employee, called the generalizing-specialist, the specializing-generalist, or the versatilist. As the names indicate, a generalizing-specialist is a specialist who develops generalist tendencies while maintaining their specialty, where a specializing-generalist is a generalist who develops a specialization. Versatilists are defined as applying their depth of skill to a widening scope of situations, constantly building new skills, competencies, relationships, and assuming new roles.[lxxi]

As seen below, a generalist can be represented by a horizontal line spread across a broad number of topics without depth, and a specialist is conversely represented by a vertical line showing depth in a single area, but lacking breadth of general knowledge. This new converged worker is then represented by a T shape in the image below.

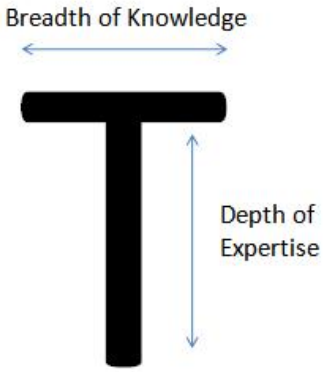

Figure 4: The T-Shaped Employee [lxxii]

This idea of a T shaped employee is not new. David Guest is credited as first coining this idea back in 1991. He wrote that “this type of rounded personality is also sought in other branches of the same theory, which prizes individuals known as T-shaped People.”[lxxiii] Others have expounded on this idea with variations such as “Hybrids”[lxxiv] and

"Versatilist."[lxxv] These "Generalizing Specialists" or "Master Generalists" are able to maintain a depth of expertise in a specific field while developing breadth of general knowledge to collaborate across other disciplines[lxxvi], or as Wu, Zou, and Kong put it, "broadly learning and weaving across disciplines (top of the T) and going deeply into understanding engineering concepts (vertical branch of the T)."[lxxvii]

Irving and Grasso emphasized the importance of these employees to the engineering disciplines, looking for "cathedral builders" vice mere "brick layers"[lxxviii], problem definers vice mere problem solvers, with a depth of their field as well as a basic understanding of adjacent and connecting fields, to address the novel and complex problems they will encounter.[lxxix] [lxxx] And according to Bill Buxton, when you have a team of these T-shaped individuals working together, their cross bars (horizontal) overlap due to their common language and breadth, while their combined pillars (vertical) span numerous areas of expertise, covering the domain of any problem you are addressing.[lxxxi]

As we have already seen, the Cryptologic Community Foundational Principles call for Cryptologic Warfare Officers to develop "deep, specialized expertise across our core skills"[lxxxii] and VADM Tighe, the community leader, has emphasized her stance that these core competencies remain resident in one community. But what is the true level of expertise desired? The statement itself, "expertise across our core skills"[lxxxiii] is challenging, simultaneously indicating a depth and breadth of expertise. Without further amplification and explanation of expectations, these principles actually lead to confusion among Cryptologic Warfare Officers.

V. U.S. Navy Cryptologic Warfare Officer Survey

A. Survey Background

Using Qualtrics software, I created a survey targeting U.S. Navy Cryptologic Warfare Officers in the grade of O1 (Ensign) to O4 (Lieutenant Commander). This rank target was intentional. Once promoted to O5 (Commander), Cryptologic Warfare Officers are immediately screened for an O5 Operational Milestone assignment and subsequently screened the following year for O5 Command opportunity. Per the 2016 Navy Personnel

Command (NPC) approved community briefs, 80% of newly promoted O5 Cryptologic Officers are screened for this milestone opportunity, with 16% screened for O5 Command the following year.[lxxxiv] Due to the short window between the time of promotion to O5 and these screening boards, the foundation of expertise, qualifications, and performance on which these boards' decisions are made occurs over the approximately 15 years spent at the O1-O4 level. As such, it is critical these Officers have a clear understanding of Cryptologic Warfare Community expectations during this period.

My principal aim with this survey was to gain insight into the adherence to and interpretation of the Cryptologic Community Foundational Principles document by the targeted survey audience. I focused on the Foundational Principles document itself, as well as the portion that discussed the idea of specialized expertise across the communities' core skills. I introduced the term "generalist" as a counter-term to "specialist." As previously discussed, specialists are focused on a specific domain, narrower in scope, with deep technical skills and a particular area. Generalists are focused across multiple domains, with a broader scope and working level knowledge and competency in multiple areas.[lxxxv]

I distributed the survey to the Cryptologic Warfare Officer community through email distribution to the Executive Officers at eight Navy Information Operation Commands (NIOCs) and to the senior Cryptologic Warfare Officers stationed with Naval Special Warfare Command (NSWC), Navy Fleet Forces Command (FFC), Commander, Third Fleet (C3F), and Commander, Fifth Fleet (C5F) to facilitate distribution to Officers attached with the NSW community and on Surface platforms around the world. This method ensured distribution to those Officers who met the community and rank requirement, as opposed to posting the link in social media forums, which might have gained a wider distribution, but risked losing control of the distribution. The survey was password protected and included a control question about the participant's Officer Community and rank that would end the survey if the user did not meet the requirements for participation. In addition, survey participation was limited to one completion opportunity per IP address, to reduce fraud potential. The survey was active for one

month beginning 19 January 2016 and there were 277 respondents. A copy of the Survey in its entirety is included in Appendix 1.

B. Survey Results

Two key questions from the survey were focused on determining if Cryptologic Warfare Officers had read the Cryptologic Community Foundational Principles and if they had clear guidance from Cryptologic Warfare Community leadership regarding a desire for Cryptologic Warfare Officers being specialists or generalists.

Have you read the 2011 Cryptologic Community Foundational Principles?

#	Answer		Response	%
1	YES		161	58%
2	NO		116	42%
	Total		277	100%

Do you feel you have received clear guidance from Information Warfare Community leadership regarding the expectation of being a Generalist vs being a Specialist as an Information Warfare Officer (1810/681X)?

#	Answer		Response	%
1	YES		74	27%
2	NO		203	73%
	Total		277	100%

Almost half of the Cryptologic Warfare Officers surveyed indicated they had not read the document which was produced to provide strategic guidance on the core competencies required for the Cryptologic Warfare Community. More curious was that an even greater number that felt they were not given clear guidance from community leadership regarding expectations as a specialist or generalist, with almost 75% indicating they did not feel they had received clear guidance. These two questions indicate that there is a communication problem between the Cryptologic Warfare Community leadership and the Officers who participated in this survey regarding expectations of performance in the core competencies.

These results mentioned above indicate that the surveyed Cryptologic Warfare Officers would then be confused as to the direction of the community and expectations for career progression. However, the survey indicated that over 60% felt that they actually did know the needed jobs required to be promoted to O5.

Do you feel confident that you know what jobs are required for you to be promoted to O5 (CDR) as an Information Warfare Officer (1810/681X) and be competitive for Command as an O5?

#	Answer		Response	%
1	YES		178	64%
2	NO		99	36%
	Total		277	100%

These results are surprising when compared to the question of how many had read the Foundational Principles and felt they had received clear guidance from senior Community leadership. If they aren't reading the Foundational Principles, where are these Junior Officers garnering the information that made them feel comfortable that they knew what jobs would allow them to promote to O5 and compete for a Command position?

When I asked survey participants what they thought the Cryptologic Community desired, a specialist or generalist, they overwhelmingly (over 80%) thought the Community desired a generalist. However, when then asked about what they personally thought the ideal model should look like in the future, less than 10% thought it should be one that was generalist dominated.

Do you feel the Information Warfare Community desires an Information Warfare Officer (1810/681X) to be a specialist or generalist?

#	Answer		Response	%
1	SPECIALIST		52	19%
2	GENERALIST		225	81%
	Total		277	100%

If you were creating the model for the future Navy Information Warfare (1810/681X) Officer, would you advocate for them to be Specialists or Generalists?

#	Answer		Response	%
1	SPECIALIST		108	39%
2	GENERALIST		25	9%
3	A COMBINATION (I.E. A SIGINT EXPERT WITH EXPERIENCE IN CYBER AND OR EW)		144	52%
	Total		277	100%

This disparity is remarkable. These responses indicate that there is a great divide between what these Officers felt the community *currently values* in a Cryptologic Officer as compared to what they felt the community *should value* in the future. This is also in conflict with what the community articulated that they *do value*, as outlined in the Foundational Principles.

The response to the initial question about whether these officers felt that community leadership desired them to be generalists or specialists was surprisingly weighted to perception that they desired generalists, despite language in the Cryptologic Community Foundational Principles to the contrary. In the second question, the idea of a generalizing-specialist or versatilist was presented for the first time, to gauge interest and support for that concept.

Lastly, there was a strong reported bias that Officers felt the Community valued the Cyber core competency over those of SIGINT and EW.

9. Do you feel that the Navy Information Warfare Community values one of the core competencies over the others for an Information Warfare Officer (1810/681X)?

#	Answer		Response	%
1	NO, I FEEL ALL HAVE EQUAL VALUE		54	20%
2	YES, SIGINT		60	22%
3	YES, CYBER		155	56%
4	YES, EW		6	2%
	Total		275	100%

This perception is understandable, due to the emphasis that the Navy has placed on CSO over the last five years. However, with the CNO's recent focus on the EMS, the emergence of the EMMW operational concept, and the convergence of Cyberspace and the EMS, the EW core competency is a critical area of emphasis. As previously discussed, the EMS is the backbone of Cyberspace and EW and CSO will be fully intertwined moving forward. In addition, the continued importance of the foundational core competency of SIGINT as an enabler of both EMMW and Cyberspace operations, as well as kinetic targeting, cannot be overstated.

VI. Recommendations

Department of the Navy and Cryptologic Warfare Community leadership have been clear: Cyberspace and the EMS are critical new warfighting domains. CSO and EMMW are growth areas for the U.S. Navy. The EMS and Cyberspace have converged and will be intertwined moving forward. Navy Cryptologic Warfare Officers have responsibility to execute Cyberspace Operations and EMMW, directly in line with Cryptologic community core competencies of Cyber, SIGINT, and EW. Based on the results of the survey discussed above, Cryptologic Warfare Officers do not have a clear understanding of expectations for regarding specialization and community core competencies. Below are three recommendations to improve and overcome the perceptions identified in the survey to meet the critical challenges in the Cyberspace and EMS domains.

A. Maintain the Core Competency Triad

In her most recent memorandum to the Cryptologic Warfare Officer community, VADM Tighe voiced her support for maintaining the core competency Triad of SIGINT, EW, and CSO within the Cryptologic Warfare Officer community. Specifically, she stated that "our value is rooted in our ability to leverage technology to solve problems in the converged domains and deliver operationally relevant effects. We deliver effects IN the converged domain (EW and Cyber) and enable effects in other warfare domains (SIGINT)."[lxxxvi] This reiterates the more technical explanation provided in the Foundation Principles document, that "EMS and cyberspace domains have converged… there is a continuum of protocol and spectrum bridging the RF to IP gap… CNE (Cyber) and SIGINT are closely linked… with similar tools, processes, procedures, and skillsets."[lxxxvii] The Navy should continue to keep this Triad of SIGINT, EW, and Cyber together to optimize Navy operations in the converged EMS and Cyberspace domains and to prevent the confusion seen in the other services. Army and Air Force officers conduct operations in the EMS and Cyberspace domains, but unlike the Navy, their Officers conducting these operations are divided within three communities instead of under one singular community.

The Air Force has broken this Triad apart among their officers. They have four different Air Force Specialty Code (AFSC) designations for Officers conducting EW, SIGINT, and CSO. Air Force EW Officers fall within the 12RX Reconnaissance/Surveillance/Electronic Warfare Combat Systems Officer AFSC. This AFSC is similar to the Navy's Naval Flight Officer (NFO) community, responsible for conducting navigation and EW operations on various aircraft. The Air force does not have a unique AFSC for SIGINT Officers; rather, Air Force SIGINT Officers are 14NX Intelligence Officers who have completed additional training or are stationed at an Air force Intelligence Squadron (IS) that is responsible for conducting SIGINT operations. Air force Cyberspace Officers were recently broken into 17DX Network Operations and 17SX Cyber Warfare Operations[lxxxviii], leading to consternation and confusion within the Air Force. Examining the two new AFSC's, Lee points out that both communities "operate cyberspace weapon systems to various degrees." But looking further at the descriptions of the two AFSCs, a 17DX Officer is responsible for "designing, building, configuring,

securing, operating, maintaining and sustaining" the environment, and a 17SX is responsible for "offensive cyber operations and defensive cyber operations."[lxxxix] This confusion is compounded due to the fact the Air Force also assigns 33SX Communications and Information Officers duties listed as "network systems operations… computer network defense and electronic protection… systems engineering and architecture design… plan, design, build, manage and maintain communications and information systems architectures."[xc] These 33SX duties seem to conflict and duplicate the duties of the 17DX Officer.

The Army is similar to the Air Force in some regards; they have also broken the EW, SIGINT, and CSO specialties into multiple Military Occupational Specialties (MOS). Army EW Officers fall under the 30A Information Operations Officer MOS, coupling EW along with Operational Security (OPSEC), Psychological Operations, Deception, and Public Affairs under the Information Operations moniker.[xci] Like the Air Force, the Army does not have a specific SIGINT Officer MOS. Rather, an Army SIGINT Officer is a 35O Military Intelligence Officer that has received additional training and assignment.[xcii] In 2015, the Army created the new 17A Cyber Officer MOS to focus specifically on the Cyberspace domain, with the Commandant of the Army Cyber school pointing out the new community's objective to "conduct defensive cyber operations, offensive cyber operations and electronic warfare."[xciii] Now the 17A Cyber Officer MOS is clearly responsible for CSO, however both the 17A MOS and the 30A MOS now both claim to conduct forms of EW. Additionally, there has been no change to the Army 25O Signal Officer MOS, where those Officers remain responsible for "planning, installing, integrating, operating and maintaining the Army's voice, data and information systems, services and resources."[xciv] This is similar to the distinction in the Navy between the Information Professional (IP) Officer responsible for network service and the Cryptologic Warfare Officer responsible for CSO. There is cooperation and obvious overlap, predominantly in the DCO and DODIN Operations role, but a clear line of distinction that the Navy and Army maintain is critical.

To avoid confusion and mission overlap, the Navy should keep the Triad of EW, SIGINT, and CSO as core competencies of the Cryptologic Warfare Officer and not break them apart among different communities.

B. Pi Model

We discussed the conflict between a specialist and generalist earlier, ending with the idea of a "Generalizing Specialist" or "T" shaped employee who is able to maintain a depth of expertise in a specific field while developing breadth of general knowledge to collaborate across other disciplines.[xcv] We also discussed the call from the Cryptologic Community Foundational Principles for Cryptologic Warfare Officers to develop "deep, specialized expertise across our core skills."[xcvi] I offer that a U.S. Navy Cryptologic Warfare Officer should not merely follow the T shape model we previously discussed, but rather evolve further into what I call a Pi (π) shaped Officer. A graphical representation is included below.

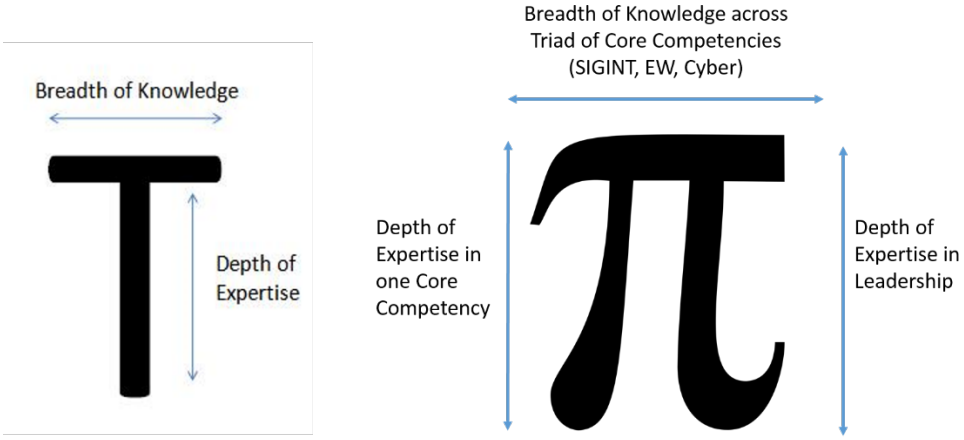

Figure 5: T and Pi Shaped Employee/Officer

This Pi-shaped Officer model builds on the concept of the T shaped employee, but with two vertical legs of specialization, one in a core competency and the other in leadership, while maintaining the horizontal line of breadth of expertise across the other core competencies as well as the various Navy platforms and domains. It would be easy to suggest that all Officers should be leaders, so this second leg is irrelevant. However, from my experience, unless an expectation or requirement is clearly articulated, it will not be fully met. The final result is a team of these Pi shaped officers, which will allow, as

Buxton stated earlier, “their cross bars (horizontal) overlap due to their common language and breadth, while their combined pillars (vertical) span numerous areas of expertise, covering the domain of any problem you are addressing.”[xcvii] Using this construct, Junior Officers will grow into senior Pi-shaped Officers, ready to face all the problems in the converged warfighting domains of the EMS and Cyberspace.

The Cryptologic Warfare Officer community is unique, and fortunate, that it is able to hand-select the Officers that are gained or hired annually. Applicants are screened and Officer Candidates are selected based on a proven specialty from academic and/or previous job experience in a technical Science Technology Engineering and Math (STEM) field. As such, they join the community from day one, already with a short vertical leg of specialization. While this specialization is normally not in a specific field of CSO, EW, or SIGINT, it is a STEM specialization that is foundational to one of those core competencies.

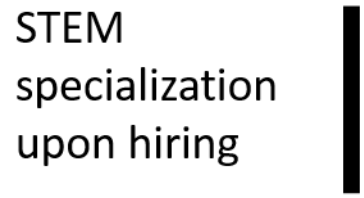

Figure 6: Cryptologic Warfare Officer at Accession (ENS/O1)

Once the new Cryptologic Warfare Officer is hired, they enter into initial training, consisting of a Cryptologic Warfare Officer Basic Course and a broader Information Warfare Community introduction course. These training courses develop breadth across the Core Competencies and lead into the Cryptologic Warfare Officer’s first assignment. In addition, new Cryptologic Warfare Officers receive leadership training during these basic courses to prepare them for their pending role as a Division Officer upon their first assignment. The resultant shape of a Cryptologic Warfare Officer as they enter into their first operational assignment has two vertical lines and a horizontal line in various stages of growth, but is far from the Pi shaped Officer they will grow into.

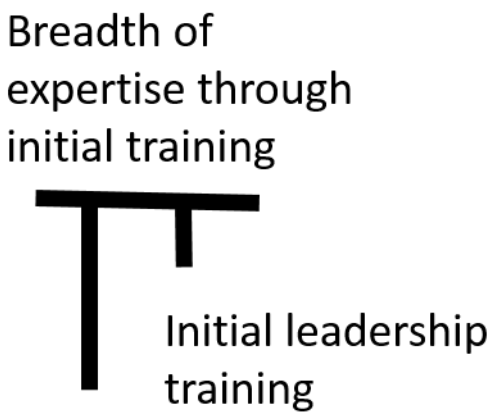

Figure 7: Cryptologic Warfare Officer upon Initial Training Completion (ENS/O1 ~6 months)

At their first assignment, a Cryptologic Warfare Officer will continue to develop into a Pi shaped Officer. They will develop depth in one of the core competencies through the operational requirements of their first job. These jobs vary depending on assignment location, but all are rooted in one of the core competencies of SIGINT, CSO, or EW. They will be afforded the opportunity to grow their horizontal breadth across all core competencies through the Cryptologic Warfare Officer basic qualification and Information Warfare Officer Warfare Qualification program. These are both rigorous qualification programs designed to test and evaluate the learned skills of a new Cryptologic Warfare Officer. Lastly, they will develop their leadership vertical leg as they assume the responsibility of leading as a Division Officer. This vertical leg will grow through the interaction with Sailors and Chiefs, the leadership and mentorship of their Department Head, and the collaboration with other Division Officers. At the end of this first assignment, a successful Cryptologic Warfare Officer should begin to resemble the Pi shaped Officer that will continue to grow and strengthen throughout the rest of their career.

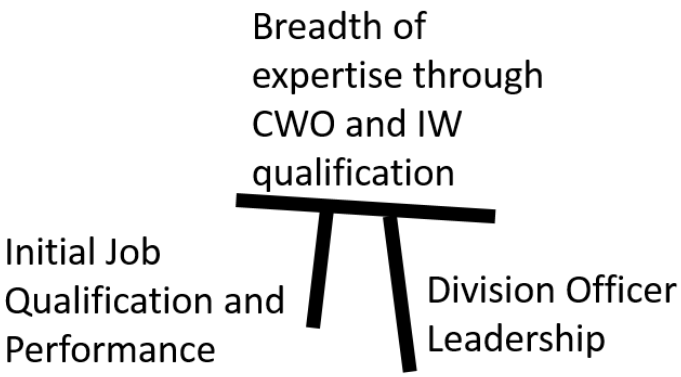

Figure 8: Cryptologic Warfare Officer upon Completion of First Assignment (LTJG/O2 ~3yrs)

Upon completion of initial assignment, the Cryptologic Warfare Officer will be assigned to a tactical assignment onboard a ship, submarine, aircraft squadron, Navy Special Warfare (NSW) unit or Cyber Team. This will allow for growth, both in a core competency, as well as in increased breadth of knowledge of all core competencies and upon different Navy platforms. The typical Officer will have completed 5-6 years of service and have earned the rank of LT/O3 after this second tour. The Officer will then be sent to the Naval Postgraduate School (NPS) to obtain a Master's Degree in Computer Science, Electrical Engineering, or Cyber Systems and Operations. The articulated community aim is for 100% of Cryptologic Warfare Officers to complete this Master Degree program to deepen his/her core competency knowledge and understanding from an academic sense. Upon completion of the Master's program, they will complete a utilization tour, using the academic knowledge learned and deepening their core competency knowledge. Cryptologic Warfare Officers should finish this assignment at the 10-11 year mark, as a newly selected LCDR/O4, if performance in all the aforementioned jobs to this point met the Navy standard of "superior performance."

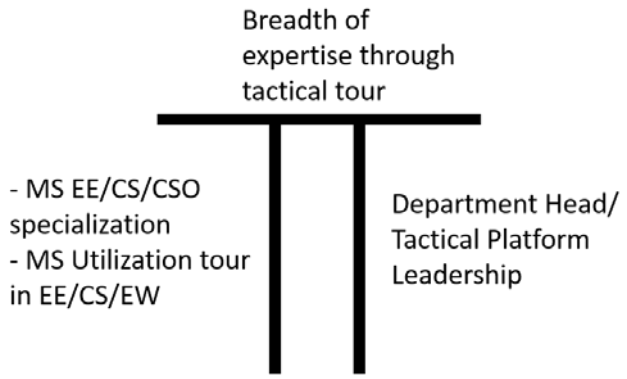

Figure 9: Cryptologic Warfare Officer upon Selection to LCDR/O4 (~10-11 years)

As an O4, the Cryptologic Warfare Officer will have the opportunity to complete an operational milestone assignment, once again growing in breadth and depth in various SIGINT, Cyber, and EW capacities with strike groups, submarine squadrons, NSW commands, fleet and joint staffs, and cyber units. They will also have the opportunity to serve as Department Heads and Executive Officers, further refining their leadership vertical leg while also continuing education through the Information Warfare Community mid-career course, expanding their horizontal breadth line. At the end of their time as an O4/LCDR, a Cryptologic Warfare Officer will have obtained a fully developed Pi-shape, having substantial depth in at least one core competency and as a leader, as well as great breadth of knowledge across all core competencies, the IWC writ large, and the U.S. Navy.

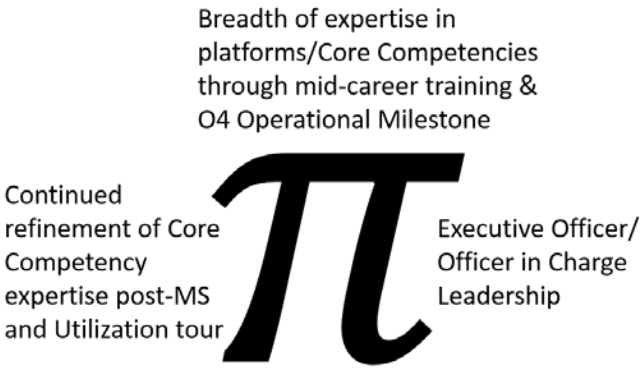

Figure 10: Cryptologic Warfare Officer as a Senior LCDR/O4 (~15-16 years)

C. Foundational Principles 2.0

As a result of the progress that has taken place over the last five years, to include the recognition of the Cyberspace and EMS domains and further development of their convergence, it is time for the Cryptologic Warfare Officer Community to re-write the foundational principles. With the evolution of the Information Dominance Corps into the Information Warfare Community and the former Information Warfare Officer Community reverting back to their Cryptologist roots as Cryptologic Warfare Officers, the new version will eliminate all confusion on nomenclature and community inclusion. In addition, it will allow the opportunity to remove other outdated terms and replace them with new doctrinally accepted terms, such as replacing Computer Network Operations (CNO) with CSO and the inclusion of OCO, DCO, and DODIN Operations.

As recently as 11 March 2016, the Cryptologic Warfare community leader reemphasized the core competencies of the community, so that portion will remain constant.[xcviii] But as the survey I completed for this research demonstrated, there is not full clarity on expectations when it comes to these core competencies. The community leadership can take this Foundational Principal re-write as an opportunity to clearly articulate a stance on the generalist vs specialist model for Cryptologic Warfare Officers and articulate the vision of the Pi shaped 'generalizing specialist'. In addition, as the cadre of Flag rank leadership within the Cryptologic Warfare Officer community has changed since 2011, this will be an opportunity for the new Flag officers to demonstrate support for these Foundational Principles, like their predecessors did.

Once the new Foundational Principles document has been signed, it is imperative that it is widely distributed and digested. As my survey indicated, almost half the surveyed Officers had not read the Foundational Principles and, even more importantly, felt they had not received clear guidance from Community leadership in this issue. That must and can improve. Onus will reside with the individual Officer to read the new document, senior leadership within the Cryptologic Warfare Officer community can ensure widest distribution and encourage dialogue on the document. The Cryptologic Warfare Officer

community should utilize all available mediums for dissemination, to include list-serves, email, Facebook, Twitter, and a community blog.

In addition to communication among the Cryptologic Warfare Officer community, this document and the language and guidance within should be the bedrock for future communication to Navy promotion boards, in the form of community input to the Promotion Board Convening Order signed by the Secretary of the Navy. The same guidance being provided to shape an Officer's career planning should be provided to the promotion board determining that Officer's advancement eligibility. Community leadership, to include the Officer Community Manager, must ensure the guidance articulated to the community is properly reflected in the Convening Order used by the voting members of a promotion/selection board in order to verify that those Officers who are following the community guidance and performing well are the ones being selected and promoted by the boards.

Rewriting the Cryptologic Community Foundation Principles will afford Community leadership to demonstrate a renewed commitment to the Core Competency Triad (SIGINT, EW, CSO) and provide an avenue for clear articulation of expectations in the area of specialization vs generalization. The correct messaging and dissemination of this document will ensure its widest distribution and adherence.

VII. Conclusion

The CNO has acknowledged the rise and importance of the EMS and Cyberspace in modern Naval Warfare. These two critical areas are now considered their own domains, on par with sea, air, land, and space. They are a lynchpin to every other domain and future Naval Operations depend on assured access and maneuverability in these two domains.

The Cryptologic Warfare Office Community, too, has evolved from the SIGINT-centric community of WWII, assuming the roles of EW and Cyberspace Operations as they emerged. After a decade of turbulence, in which the strategic direction of the community was ever changing, the goals of the community today are clear; built on the foundation of SIGINT, EW, and CSO as core competencies.

Embracing this, the Cryptologic Warfare Officer community has the opportunity to clearly define the expectations for all Cryptologic Warfare Officers conducting SIGINT, EW, and Cyberspace operations in the converged EMS and Cyberspace domains. Correctly establishing a balanced generalizing specialist (Pi shaped) Officer model will allow for the development of Officers at the O1-O4 level to meet the senior leadership and Command responsibilities at the O5 and above level, ensuring the Cryptologic Warfare Officer community has the cadre of Officers with the depth and breadth of knowledge and experience to meet the challenges of today and anticipate the challenges of tomorrow.

Appendix 1

1. ***Do you feel confident that you know what jobs are required for you to be promoted to O5 (CDR) as an Information Warfare Officer (1810/681X) and be competitive for Command as an O5?***
    a. ***Yes***
    b. ***No***

2. ***Do you feel the Information Warfare Community desires an Information Warfare Officer (1810/681X) to be a specialist or generalist?***
    a. ***Specialist***
    b. ***Generalist***

3. ***If you were creating the model for the future Navy Information Warfare (1810/681X) Officer, would you advocate for them to be Specialists or Generalists?***
    a. ***Specialist***
    b. ***Generalist***
    c. ***A Combination (ie a SIGINT expert with experience in Cyber)***

4. ***Have you read the 2011 Cryptologic Community Foundational Principles?***
    a. ***Yes***
    b. ***No***

5. ***Do you have a documented specialty (AQD) in MORE THAN ONE of the Cryptologic Community core competencies (Cyber/EW/SIGINT)?***
    a. ***One documented specialty***
    b. ***Two documented specialties***
    c. ***Three documented specialties***

6. ***Have you had MULTIPLE (2+) tours in ONE of the Cryptologic Community core competencies (Cyber/EW/SIGINT)?***
    a. ***Two tours in one competency***
    b. ***Three or more tours in one competency***
    c. ***No***

7. ***Based on the mentorship and career advice you have received, do you feel it is more career enhancing for you to Complete multiple tours in one core competency or complete a single tour in multiple core competencies***
    a. ***Complete multiple tours in one core competency***
    b. ***Complete a single tour in multiple core competencies***

8. ***Do you feel you have received clear guidance from Information Warfare Community leadership regarding the expectation of being a Generalist vs being a Specialist as an Information Warfare Officer (1810/681X)?***
    a. ***Yes***
    b. ***No***

9. ***Do you feel that the Navy Information Warfare Community values one of the core competencies over the others for an Information Warfare Officer (1810/681X)?***
    a. ***No, I feel all have equal value***
    b. ***Yes, SIGINT***
    c. ***Yes, Cyber***
    d. ***Yes, EW***

BIBLIOGRAPHY

- Apprentice Academy.(2014). "T-Shaped: How To Be An Adaptable, Collaborative & Valuable Employee." January 20, 2014. From http://theapprenticeacademy.co.uk/blog/t-shaped-how-to-be-an-adaptable-collaborative-valuable-employee/

- Arquilla, John, and Ronfeldt, David. (1993). "Cyberwar is Coming!" RAND Corporation.

- Arquilla, John, and Ronfeldt, David. (1997). "In Athena's Camp: Preparing for Conflict in the Information Age." RAND Corporation.

- Bersin, Josh. (2007). "Talent Management Changes HR." From http://joshbersin.com /2007/06/talent-management-changes-hr/

- Branch, Ted. (2016). "Information Dominance Corps Re-designated Information Warfare Community." Navy Administrative Message 023/16.

- Buxton, Bill. (2009). "Innovation Calls For I-Shaped People." Business Week- Bloomberg Business. July 13, 2009.

- Carter, Ash. (2015). "2015 DOD Cyber Strategy." Washington DC.

- Clarke, Richard, and Knake, Robert. (2011). "Cyberwar: The Next Threat to National Security and What to do About It." Harper Collins Publisher. New York.

- Crane, Helen. (2013). "Specialists or generalists: what do employers really want?" The Guardian. November 5, 2013

- Department of Defense. (2011) "Department of Defense Strategy for Operating in Cyberspace." Washington DC. 2011.

- Department of the Navy. (2010). "The U.S. Navy's Vision for Information Dominance." Washington DC.

- Department of the Navy. (2012). "Navy Information Dominance Corps Human Capital Strategy 2012-2017." Washington DC.

- Editor HR Review. (2013). "UK workers specialist skills are under threat." HR Review. October 28, 2013.

- European Space Agency. (2013). "Satellite Frequency Bands." From http://www.esa.int/ spaceinimages/Images/2013/11/Satellite_frequency_bands

- Fleet Cyber Command Public Affairs. (2010). "Navy Stands Up Fleet Cyber Command, Reestablishes U.S. 10th Fleet." Department of the Navy. January 29, 2010. From http://www.navy.mil/submit/display.asp?story_id=50954

- Freedberg, Sydney. (2014). "Navy Forges New EW Strategy: Electromagnetic Maneuver Warfare." Breaking Defense. October 10, 2014. From http://breakingdefense.com/2014/10/ navy-forges-new-ew-strategy-electromagnetic-maneuver-warfare/

- Frith, Teresa. (2005). “Cryptology Officers Get New Name; Boss.” Department of the Navy. October 14, 2005. From http://www.navy.mil/submit/display.asp?story_id=20384

- Grasso, Domenico, and Burkins Melody. (2010). “Holistic engineering education: Beyond technology.” NewYork. Springer.

- Greenert, Jonathan. (2013). “Wireless Cyberwar, The EM Spectrum, And The Changing Navy.“ Breaking Defense. April 3, 2013. From http://breakingdefense.com/2013/04/adm-greenert-wireless-cyber-em-spectrum-changing-navy/

- Greenert, Jonathan, and Dunford, Joseph, and Zukunft, Paul. (2015). Cooperative Strategy for 21st Century Seapower (CS-21). Washington DC.

- Guest, David. (1991). “The hunt is on for the Renaissance Man of computing.” The Independent. London. September 1991.

- Heathfield, Susan. (2014). “What is Talent Management- Really?” From http://humanresources.about.com/od/successionplanning/g/talent-management.htm

- Holstead, Joseph. (2013). “A Short History of US Navy Information Warfare.” CHIPS: The Department of the Navy Information Technology Magazine.

- HR in Asia Team. (2014). “Talent Archetypes: Specialists, Generalists and Versatilists.” HR in Asia. From http://www.hrinasia.com/recruitment/talent-archetypes-specialists-generalists-and-versatilists/

- Irving, Carl. (1998). “Well-educated Bricklayers? Two new colleges hope to produce broadly trained engineers.” National Center for Public Policy and Higher Education- Cross Talk. 1998.

- Joint Publication 1-02. (2016). “Department of Defense Dictionary of Military and Associated Terms.” Washington DC.

- Joint Publication 3-12. (2013). “Cyberspace Operations.” Washington DC.

- Joint Publication 3-13.1. (2007). “Electronic Warfare.” Washington DC.

- Lee, Robert. (2015). “Disruptive by Design: Saving the Air Force Cyber Community.” SIGNAL Magazine. February 2015.

- Mann, Andi. (2014). “Specialists vs. Generalists.” August 25, 2014. From http://devops.com /2014/08/25/specialists-vs-generalists-enterprise-devops/#!prettyPhoto

- Michaels, Ed, and Handfield-Jones, Helen, and Axelrod, Beth. (2001). “The War for Talent.” Harvard Business Press.

- Morello, Dianne. (2005). “Versatilist: Gartner says Technical Aptitude No Longer Enough To Secure Future for IT Professionals.” From http://www.gartner.com/press_releases/asset_ 139314_11.html.

- Navy Personnel Command, Department of the Navy. (2016). “FY-17 Active Duty Line Community Brief.”

- Nye, Joseph. (2011). “Nuclear Lessons for Cyber Security?” Strategic Studies Quarterly. Winter.

- Pace, Peter. (2006). “National Military Strategy for Cyberspace Operations.” From http://www.au.af.mil/au/awc/awcgate/awc-doct.htm

- Palmer, Colin. (1990). “Hybrids— a critical force in the application of information technology in the nineties.” Journal of Information Technology.

- Palmieri, Margaret. (2015). “Electromagnetic Maneuver Warfare.” AFCEA. 2015. http://www.afcea.org/events/navyday/15/documents/IndustryDay_2015_EMW_Palmierirelea sable.pdf

- Penn-Hall, Luke. (2016). ”The Cybersecurity Skills Shortage.” From http://thecipherbrief.com /article/techcyber/cybersecurity-skills-shortage

- Pike, John. “History of the Naval Security Group.” From http://fas.org/irp/agency/navsecgru/ history.htm

- Rehman, Scheherazade. (2013). “Estonia’s Lessons in CyberWarfare.” US News and World Report.

- Richelson, Jeffery. (2013). “National Security Agency Tasked with Targeting Adversaries' Computers for Attack Since Early 1997, According to Declassified Document.” April 26, 2013. From http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/

- Rogers, Michael and other Navy Information Warfare Officer Community Leaders. (2011). “Cryptologic Community Foundational Principles.” Copy available at http://seanheritage.com/ blog/project/cryptologic/

- Rohret, David, and Jimenez, Abiud. (2012). “*Convergence of Electronic Warfare and Computer Network Exploitation/Attacks Within the Radio Frequency Spectrum*.” Proceedings of the International Conference on Information Warfare.

- Schmidt, Eric. (2014). “How Google Manages Talent.” Harvard Business Review Podcast. September 2014.

- Seffers, George. (2015). “U.S. Army Builds Cyber Branch One Step at a Time.” SIGNAL Magazine. April 2015.

- Senft, Michael. (2016). “Convergence of Cyberspace Operations and Electronic Warfare Effects.” The Cyber Defense Review.

- Singer, P.W., and Friedman, Allan. (2014). “Cyber Security and Cyber War: What everyone needs to know.” Oxford University Press.

- Tighe, Jan. (2016). “COMTENTHFLT Letter.” From http://www.stationhypo.com/2016/02/iw-designator-name-change-survey.html#more).

- Tighe, Jan. (2016). “The Evolution of Navy Cryptology.” Memorandum from Fleet Cyber Command. From http://www.stationhypo.com/2016/03/the-evolution-of-navy-cryptology-guest.html?showComment=1457708516764#c6708247651519625745

- U.S. Department of Defense. “Department of Defense Cyber Strategy.” http://www.defense.gov/News/Special-Reports/0415_Cyber-Strategy

- U.S. Fleet Cyber Command/U.S. 10th Fleet Public Affairs. (2014). “Building the Navy’s Portion of the Cyber Mission Force.” CHIPS: The Department of the Navy Information Technology Magazine

- University of Central Florida. (2016). “Florida Solar Energy Center Electromagnetic Spectrum.” http://www.fsec.ucf.edu/en/education/k-12/curricula/sm3/documents/SM3-11-ElectromagneticSpectrum_WebVersion.pdf

- Valeriano, Brandon, and Maness, Ryan. (2015). “Cyber War vs Cyber Realities.” Oxford University Press.

- Wu, Jingshan, and Zou, Xiaodong, and Kong, Hanbing. (2012). “Cultivating T Shaped Engineers for the 21st Century.” American Society for Engineering Education.

---

[i] Greenert, Jonathan, and Dunford, Joseph, and Zukunft, Paul. Cooperative Strategy for 21st Century Seapower (CS-21). Washington DC. 2015

[ii] Penn-Hall, Luke.” The Cybersecurity Skills Shortage.” http://thecipherbrief.com/article/techcyber/cybersecurity-skills-shortage (accessed March 29, 2016)

[iii] NASA Goddard Space Flight Center. “Dictionary.” https://web.archive.org/web/20150204035224/http://imagine.gsfc.nasa.gov/docs/dict_ei.html (accessed March 29, 2016).

[iv] Joint Publication 1-02. “Department of Defense Dictionary of Military and Associated Terms.” Washington DC. 2016. Pg 74

[v] University of Central Florida, “Florida Solar Energy Center Electromagnetic Spectrum.” http://www.fsec.ucf.edu/en/education/k-12/curricula/sm3/documents/SM3-11-ElectromagneticSpectrum_WebVersion.pdf (accessed March 29, 2014)

[vi] European Space Agency. “Satellite Frequency Bands.” http://www.esa.int/spaceinimages/Images/2013/11/Satellite_frequency_bands (accessed March 29, 2016)

[vii] Carter, Ash. “2015 DOD Cyber Strategy.” Washington DC. 2015. Pg 5.

[viii] Clarke, Richard, and Knake, Robert. “Cyberwar: The Next Threat to National Security and What to do About It.” Harper Collins Publisher. New York. 2011. Pg 70

[ix] Valeriano, Brandon, and Maness, Ryan. “Cyber War vs Cyber Realities.” Oxford University Press. 2015. Pg 22.

[x] Nye, Joseph. “Nuclear Lessons for Cyber Security?” Strategic Studies Quarterly. Winter. 2011. Pg 19.

[xi] Singer, P.W., and Friedman, Allan. “Cyber Security and Cyber War: What everyone needs to know.” Oxford University Press. 2014. Pg 14.

[xii] Valeriano, Brandon, and Maness, Ryan. “Cyber War vs Cyber Realities.” Oxford University Press. 2015. Pg 23.

[xiii] Joint Publication 3-12. “Cyberspace Operations.” Washington DC. 2013. Pg 6.

[xiv] Greenert, Jonathan. “Wireless Cyberwar, The EM Spectrum, And The Changing Navy.“ Breaking Defense. April 3, 2013. http://breakingdefense.com/2013/04/adm-greenert-wireless-cyber-em-spectrum-changing-navy/ (accessed March 29, 2016).

[xv] National Security Agency. “Signals Intelligence.” https://www.nsa.gov/sigint (accessed March 29, 2016).
[xvi] Joint Publication 1-02. “Department of Defense Dictionary of Military and Associated Terms.” Washington DC. 2016. Pg 223.
[xvii] Ibid. Pg 50.
[xviii] Ibid. Pg 81.
[xix] Ibid. Pg 98.
xx Joint Publication 3-13.1. “Electronic Warfare.” Washington DC. 2007. Pg. 108.
xxi Ibid. Pg 108.
xxii Metzger, Julianne. “CNO Speaks to Electronic Warfare and Information Operations Professionals.” http://www.navy.mil/submit/display.asp?story_id=77340 (accessed March 29, 2016)
xxiii Freedberg, Sydney. “Navy Forges New EW Strategy: Electromagnetic Maneuver Warfare.” Breaking Defense. October 10, 2014. http://breakingdefense.com/2014/10/navy-forges-new-ew-strategy-electromagnetic-maneuver-warfare/ (accessed March 29, 2016).
[xxiv] Palmieri, Margaret. “Electromagnetic Maneuver Warfare.” AFCEA. 2015. http://www.afcea.org/events/navyday/15/documents/IndustryDay_2015_EMW_Palmierireleasable.pdf (accessed March 29, 2016).
[xxv] Department of the Navy. “Ship’s Electronic Warfare Officer.” http://www.cool.navy.mil/usn/officer/nobc_desc/nobc9282_desc.htm (accessed March 29. 2016).
xxvi Pace, Peter. “National Military Strategy for Cyberspace Operations.” http://www.au.af.mil/au/awc/awcgate/awc-doct.htm (accessed March 29, 2016).
xxvii Richelson, Jeffery. “National Security Agency Tasked with Targeting Adversaries' Computers for Attack Since Early 1997, According to Declassified Document.” April 26, 2013. http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/ (accessed 29 March 2016).
xxviii Department of Defense. “Department of Defense Strategy for Operating in Cyberspace.” Washington DC. 2011.
[xxix] Valeriano, Brandon, and Maness, Ryan. “Cyber War vs Cyber Realities.” Oxford University Press. 2015. Pg 27.
[xxx] Arquilla, John, and Ronfeldt, David. “Cyberwar is Coming!” RAND Corporation. 1993.
[xxxi] Arquilla, John, and Ronfeldt, David. “In Athenas Camp: Preparing for Conflict in the Information Age.” RAND Corporation. 1997. Pg 275.
[xxxii] Nye, Joseph. “Nuclear Lessons for Cyber Security?” Strategic Studies Quarterly. Winter. 2011. Pg 21.
[xxxiii] Rehman, Scheherazade. “Estonia’s Lessons in CyberWarfare.” US News and World Report. January 14, 2013.
[xxxiv] Valeriano, Brandon, and Maness, Ryan. “Cyber War vs Cyber Realities.” Oxford University Press. 2015. Pg 32.
[xxxv] Joint Publication 3-12. “Cyberspace Operations.” Washington DC. 2013. Pg 69.
[xxxvi] U.S. Department of Defense. “Department of Defense Cyber Strategy.” http://www.defense.gov/News/Special-Reports/0415_Cyber-Strategy (Accessed 29 March 2016).
[xxxvii] Ibid
xxxviii U.S. Fleet Cyber Command/U.S. 10th Fleet Public Affairs. “Building the Navy’s Portion of the Cyber Mission Force.” CHIPS: The Department of the Navy Information Technology Magazine. October- December 2014.
xxxix United States Naval Academy. “Special Duty: Information Professional 1820.” http://www.usna.edu/CyberCenter/_files/documents/idc/1820_IP_Community_Info_Sheet_Jan12.pdf (accessed March 29, 2016).
xl Joint Publication 3-12. “Cyberspace Operations.” Washington DC. 2013. Pg 6.
xli Department of the Navy. “Networks and EMS (NES) Roadmap
Navy EW and Cyber Convergence .” https://cryptome.org/2013/07/cyber-war-racket-0026.pdf (accessed March 29, 2016).
xlii Senft, Michael. “Convergence of Cyberspace Operations and Electronic Warfare Effects.”The Cyber Defense Review. January 4, 2016.
[xliii] Rohret, David, and Jimenez, Abiud. “*Convergence of Electronic Warfare and Computer Network Exploitation/Attacks Within the Radio Frequency Spectrum*.” Proceedings of the International Conference on Information Warfare. 2012. Pg 245.
[xliv] Senft, Michael. “Convergence of Cyberspace Operations and Electronic Warfare Effects.”The Cyber Defense Review. January 4, 2016.

xlv Tighe, Jan. "COMTENTHFLT Letter." February 12, 2016. http://www.stationhypo.com/2016/02/iw-designator-name-change-survey.html#more (Accessed March 29. 2016).
xlvi Ibid
xlvii Pike, John. "History of the Naval Security Group." http://fas.org/irp/agency/navsecgru/history.htm
xlviii http://www.doncio.navy.mil/CHIPS/ArticleDetails.aspx?ID=4677 (accessed March 29, 2016).
xlix Frith, Teresa. "Cryptology Officers Get New Name; Boss." Department of the Navy. October 14, 2005. http://www.navy.mil/submit/display.asp?story_id=20384 (accessed March 29, 2016).
l Fleet Cyber Command Public Affairs. "Navy Stands Up Fleet Cyber Command, Reestablishes U.S. 10th Fleet." Department of the Navy. January 29, 2010. http://www.navy.mil/submit/display.asp?story_id=50954
li Holstead, Joseph. "A Short History of US Navy Information Warfare." CHIPS: The Department of the Navy Information Technology Magazine. July-September 2013.
lii Department of the Navy. "The U.S. Navy's Vision for Information Dominance." Washington DC. May 2010. Pg 3 and Pg 6.
liii Department of the Navy. "Navy Information Dominance Corps Human Capital Strategy 2012-2017." Washington DC. 2012. Pg 4.
liv Branch, Ted. "Information Dominance Corps Redesignated Information Warfare Community." Navy Administrative Message 023/16. February 2, 2016.
lv Mpanga, David. "Ebrace Change: It is the Only Constant in Life." April 19, 2014. http://www.monitor.co.ug/OpEd/Commentary/Embrace-change---It-is-the-only-constant-in-life/-/689364/2284692/-/v54581z/-/ (accessed April 28, 2016).
lvi Rogers, Michael and other Navy Information Warfare Officer Community Leaders. "Cryptologic Community Foundational Principles." 2011. Pg 3.
lvii Ibid. Pg 8.
lviii Ibid. Pg 4.
lix Ibid Pg. 4.
lx Tighe, Jan. "The Evolution of Navy Cryptology." Memorandum from Fleet Cyber Command. March 11. 2016. http://www.stationhypo.com/2016/03/the-evolution-of-navy-cryptology-guest.html?showComment=1457708516764#c6708247651519625745 (accessed March 29, 2016).
lxi Rogers, Michael and other Navy Information Warfare Officer Community Leaders. "Cryptologic Community Foundational Principles." 2011. Pg 3.
lxii Ibid. Pg 3.
lxiii Bersin, Josh. "Talent Management Changes HR." June 1, 2007. http://joshbersin.com/2007/06/talent-management-changes-hr/ (accessed March 29. 2016).
lxiv Heathfield, Susan. "What is Talent Management- Really?" Dece,mber 16, 2014. http://humanresources.about.com/od/successionplanning/g/talent-management.htm (accessed March 29, 2016).
lxv Michaels, Ed, and Handfield-Jones, Helen, and Axelrod, Beth. "The War for Talent." Harvard Business Press. 2001. Pg 95.
lxvi HR in Asia Team. "Talent Archetypes: Specialists, Generalists and Versatilists." HR in Asia. April 24, 2014. http://www.hrinasia.com/recruitment/talent-archetypes-specialists-generalists-and-versatilists/ (accessed March 29, 2016).
lxvii Crane, Helen. "Specialists or generalists: what do employers really want?" The Guardian. November 5, 2013. http://www.theguardian.com/careers/careers-blog/specialist-generalist-what-do-employers-want (accessed March 29, 2016).
lxviii Schmidt, Eric. "How Google Manages Talent." Harvard Business Review Podcast. September 2014. https://hbr.org/2014/09/how-google-manages-talent/ (accessed March 29, 2016).
lxix Ibid.
lxx Editor HR Review. "UK workers specialist skills are under threat." HR Review. October 28, 2013. http://www.hrreview.co.uk/hr-news/strategy-news/uk-workers-specialist-skills-are-under-threat/49215 (accessed March 29, 2016).
lxxi HR in Asia Team. "Talent Archetypes: Specialists, Generalists and Versatilists." HR in Asia. April 24, 2014. http://www.hrinasia.com/recruitment/talent-archetypes-specialists-generalists-and-versatilists/ (accessed March 29, 2016).

lxxii Apprentice Academy. “T-Shaped: How To Be An Adaptable, Collaborative & Valuable Employee.” January 20, 2014. http://theapprenticeacademy.co.uk/blog/t-shaped-how-to-be-an-adaptable-collaborative-valuable-employee/ (March 29, 2016).
lxxiii Guest, David. “The hunt is on for the Renaissance Man of computing.” The Independent. London. September 1991.
lxxiv Palmer, Colin. “Hybrids— a critical force in the application of information technology in the nineties.” Journal of Information Technology, 1990. Pg 232-235.
lxxv Morello, Dianne. “Versatilitst: Gartner says Technical Aptitude No Longer Enough To Secure Future for IT Professionals.” 2005. http://www.gartner.com/press_releases/asset_139314_11.html. (accessed March 29, 2016).
lxxvi Mann, Andi. “Specialists vs. Generalists.” August 25, 2014. http://devops.com/2014/08/25/specialists-vs-generalists-enterprise-devops/#!prettyPhoto (accessed March 29, 2016).
lxxvii Wu,Jingshan, and Zou, Xiaodong, and Kong, Hanbing. “Cultivating T Shaped Engineers for the 21st Century.” American Society for Engineering Education. 2012.
lxxviii Irving, Carl. “Well-educated Bricklayers? Two new colleges hope to produce broadly trained engineers.” National Center for Public Policy and Higher Education- Cross Talk. 1998.
lxxix Grasso, Domenico, and Burkins Melody. “Holistic engineering education: Beyond technology.” New York. Springer. 2010.
lxxx Wu,Jingshan, and Zou, Xiaodong, and Kong, Hanbing. “Cultivating T Shaped Engineers for the 21st Century.” American Society for Engineering Education. 2012.
lxxxi Buxton, Bill. “Innovation Calls For I-Shaped People.” Business Week- Bloomberg Business. July 13, 2009.
lxxxii Rogers, Michael and other Navy Information Warfare Officer Community Leaders. “Cryptologic Community Foundational Principles.” 2011. Pg 3.
lxxxiii Ibid. Pg 3.
lxxxiv Navy Personnel Command, Department of the Navy. “FY-17 Active Duty Line Community Brief.”2016. Pg 31.
lxxxv HR in Asia Team. “Talent Archetypes: Specialists, Generalists and Versatilists.” HR in Asia. April 24, 2014. http://www.hrinasia.com/recruitment/talent-archetypes-specialists-generalists-and-versatilists/ (accessed March 29, 2016).
lxxxvi Tighe, Jan. “COMTENTHFLT Letter.” February 12, 2016. http://www.stationhypo.com/2016/02/iw-designator-name-change-survey.html#more (Accessed March 29. 2016).
lxxxvii Rogers, Michael and other Navy Information Warfare Officer Community Leaders. “Cryptologic Community Foundational Principles.” 2011. Pg 4.
lxxxviii Department of the Air force. “Officer AFSC Classifications.” November 20, 2012. http://www.af.mil/AboutUs/FactSheets/Display/tabid/224/Article/104484/officer-afsc-classifications.aspx (accessed March 29, 2016.)
lxxxix Lee, Robert. “Disruptive by Design: Saving the Air Force Cyber Community.” SIGNAL Magazine. February 2015.
xc Powers, Rod. “United States Air Force Commissioned Officer Job Descriptions.” http://usmilitary.about.com/od/officerjobs/a/33xx.htm (accessed March 29, 2016).
xci Department of the Army. “Military Occupational Specialties (MOS)- Jobs for Officers only .” http://army.com/info/mos/officers (accessed March 29. 2016).
xcii Ibid
xciii Seffers, George. “U.S. Army Builds Cyber Branch One Step at a Time.” SIGNAL Magazine. April 2015.
xciv Department of the Army. “Military Occupational Specialties (MOS)- Jobs for Officers only .” http://army.com/info/mos/officers (accessed March 29. 2016).
xcv Mann, Andi. “Specialists vs. Generalists.” August 25, 2014. http://devops.com/2014/08/25/specialists-vs-generalists-enterprise-devops/#!prettyPhoto (accessed March 29, 2016).
xcvi Rogers, Michael and other Navy Information Warfare Officer Community Leaders. “Cryptologic Community Foundational Principles.” 2011. Pg 3.
xcvii Buxton, Bill. “Innovation Calls For I-Shaped People.” Business Week- Bloomberg Business. July 13, 2009.
xcviii Tighe, Jan. “The Evolution of Navy Cryptology.” Memorandum from Fleet Cyber Command. March 11. 2016. http://www.stationhypo.com/2016/03/the-evolution-of-navy-cryptology-guest.html?showComment=1457708516764#c6708247651519625745 (accessed March 29, 2016).