REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ORGANIZATION.

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
04-06-2016	Master's of Military Studies	SEP 2015 - APR 2016

4. TITLE AND SUBTITLE

Marine Corps Cyberspace Operations:
The Need for Change

5a. CONTRACT NUMBER
N/A

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
N/A

6. AUTHOR(S)
Patterson, Jeffrey, J, Major, USMC

5d. PROJECT NUMBER
N/A

5e. TASK NUMBER
N/A

5f. WORK UNIT NUMBER
N/A

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

8. PERFORMING ORGANIZATION REPORT NUMBER
N/A

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)
Gary D. Brown

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

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

In order to optimize USMC cyberspace capabilities and capacity developments, the Marine Corps must advocate paradigm change, revise current doctrine, restructure its cyber forces, and reform current training models. The DoD's doctrinal acceptance of cyberspace as the fifth warfighting domain, influenced the Marine Corps' dogmatic approach towards capabilities development which led it to inneffectively obligate equities to all three sub-functions of cyberspace operations. The Marine Corps should consider cyberspace in relation to the larger information environment (IE) framework in order to better synchronize cyberspace operations and information operations. It can do so through a few near- and mid-term practical steps with regards to doctrine, training, and organization. Articulating cyberspace's relationship within the IE, will result in more practically organized MAGTF cyberspace forces, more proficient practitioners, and better integrated cyberspace operations as important parts of information operations. These results optimize the capability and capacity of Marine Corps cyberspace forces and posture the service to counter the most probable future security threats.

15. SUBJECT TERMS
cyber, cyberspace; Marine Corps; cyberspace doctrine; cyber force structure, cyber force organization

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			USMC Command and Staff College
Unclass	Unclass	Unclass	UU	36	19b. TELEPHONE NUMBER *(Include area code)* (703) 784-3330 (Admin Office)

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

MASTER OF MILITARY STUDIES

TITLE:
Marine Corps Cyberspace Operations:
The Need for Change

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

AUTHOR:
Major Jeffrey J. Patterson

AY 15-16

Mentor and Oral Defense Committee Member: Gary D Brown
Approved: GARY D BROWN
Date: 6 Apr 16

Oral Defense Committee Member: Matthew Flynn
Approved:
Date: 4/6/16

J.W. Gordon 4/6/16

Executive Summary

Title: Marine Corps Cyberspace Operations: The Need for Change

Author: Major Jeffrey Patterson, United States Marine Corps

Thesis: In order to optimize USMC cyberspace capabilities and capacity developments, the Marine Corps must advocate paradigm change, revise current doctrine, restructure its cyber forces, and reform current training models.

Discussion: The information age promulgated endless amounts of new terminology, phrases, and concepts into DoD cyberspace lexicon. The Defense Department's doctrinal acceptance of cyberspace as the fifth warfighting domain, influenced the Marine Corps' dogmatic approach towards capabilities development. Misinformed paradigms led the Marine Corps to obligate equities to all three sub-functions of cyberspace operations. The Marine Corps service-level objectives and milestones pursued organic capabilities in the so-called cyberspace domain, just as it had the land, sea, and air domains. These inefficient pursuits caused duplicative DoD efforts and structures. However, there are likely more efficient ways to achieve effects in cyberspace operations. The Marine Corps should consider cyberspace in relation to the larger information environment (IE) framework in order to better synchronize cyberspace operations and information operations. It can do so through a few near- and mid-term practical steps with regards to doctrine, training, and organization.

Conclusion: The Marine Corps must recognize flaws in current paradigms, advocate for doctrinal change, restructure its cyber forces, and revise current training models. Articulating cyberspace's relationship within the IE, will result in more practically organized MAGTF cyberspace forces, more proficient practitioners, and better integrated cyberspace operations as important parts of information operations. These results optimize the capability and capacity of Marine Corps cyberspace forces and posture the service to counter the most probable future security threats.

DISCLAIMER

THE OPINIONS AND CONCLUSIONS EXPRESSED HEREIN ARE THOSE OF THE INDIVIDUAL STUDENT AUTHOR AND DO NOT NECESSARILY REPRESENT THE VIEWS OF EITHER THE MARINE CORPS COMMAND AND STAFF COLLEGE OR ANY OTHER GOVERNMENTAL AGENCY. REFERENCES TO THIS STUDY SHOULD INCLUDE THE FOREGOING STATEMENT.

Tables

Page

Table of Contents

Page

Preface

As a Marine Communications Officer, cyberspace operations is a particularly important topic to me. Observations about Marine Corps cyberspace operations over the last twelve years provided sufficient desire for my analysis of the current service-level approach towards cyberspace capabilities development. My analysis was informed by books and articles written in academia, but centered primarily on U.S. Governmental topics and reports. Specifically, an examination of critical DoD and USMC cyberspace related doctrine and future operating concepts, led to the conclusions in this paper. I hope this conceptual framework can be of use to Marine Corps cyberspace communities of interest, and the service writ large, by encouraging dialogue on the topics included within this analysis.

I would like to personally acknowledge the tremendous support and constructive criticism provided to me by my mentors, Dr. Gary Brown and Dr. Matthew Flynn. The invaluable insight gained during the Cyber Warfare course was also instrumental in developing my thoughts on the subject. I would also like to thank my military and civilian faculty advisors, LtCol (USAF) Michael Mcmellon, and Dr. Douglas Streusand for their continual support throughout the year, as well as the entire Marine Corps University staff and the wonderfully helpful ladies of the Leadership Communications Skills Center (LCSC). Lastly, but just as importantly, I would like to thank my wife, Stephanie, and four children for their tremendous amount of patience, while I saw the project through to its conclusion.

I. INTRODUCTION

Cyberspace networks proliferated exponentially since the internet's first commercial e-mail service in 1983.[1] In fact, computing technologies are now so ubiquitous, that more people on the planet own a cellphone than a toothbrush, yet the intricacies and utility of cyberspace is still perplexing to most, including the Department of Defense (DoD).[2] If the Marine Corps believes that cyberspace operations are synonymous with communications, then its current trajectory is satisfactory. However, the Marine Corps seems to recognize that cyberspace is an inherently unique and potentially powerful medium to affect warfighting. In order to optimize Marine Corps cyberspace capabilities and capacity, it must advocate paradigm change, revise current doctrine, restructure its cyber forces, and reform current training models. This analysis will discuss the implications of accepting these four recommendations and explain why the DoD must articulate cyberspace's true relationship with the larger Information Environment (IE). The resultant effects would be optimally organized MAGTF cyberspace forces, more proficient practitioners, and better integrated effects with information operations (IO) across the Range of Military Operations (ROMO).

II. LITERATURE REVIEW

The conclusions and recommendations outlined in this analysis centered on examination of cyber-related national strategy, military doctrine, and future operating concepts. The analysis derived from synthesizing relevant cyberspace themes in U.S. Executive Branch security strategies, joint Department of Defense doctrinal publications, and Marine Corps service level planning guidance. U.S. Government strategic security documents, congressional research reports, and congressional testimony formed the bedrock for analyzing cyberspace themes in national security. Examination of future operating concepts stemmed from officially published

materials, briefs, and developmental materials about USMC intentions in cyberspace. The current trend in DoD doctrine recognizes three missions of cyberspace operations, and categorizes cyberspace as the fifth warfighting domain. Books, articles, and professional journals aided in understanding additionally important cyberspace debates, and provided context of the intellectual progression of the cyberspace field within academia. However, while these sources were useful in garnering insight, framing opinions, and correlating theories, they were ancillary factors in shaping the paper's scope, conclusions, and recommendations.

III. FLAWED CYBERSPACE PARADIGMS AND STRATEGIES

The Marine Corps must advocate change in cyberspace paradigms in order to enhance the shared understanding cyberspace's character and its potential effects on warfighting. The President, Secretary of Defense, Chairman of the Joint Chiefs of Staff, and Commandant of the Marine Corps, all recognize the growing importance of cyberspace to U.S. national security. However, the last several decades of unprecedented cyberspace advancements propagated an endless flotsam of terminology, concepts, and doctrine into DoD lexicon that obfuscates its true utility. Popular theories culminated in the DoD's belief that cyberspace is the 5th warfighting domain (in addition to the land, sea, air, and space domains).[3] On the contrary, cyberspace is not a domain at all. The DoD's conclusion is a grave mistake considering that the White House implored the services not to characterize cyberspace as a warfighting, military, or operational domain.[4] Both the National Security Strategy and National Security Presidential Policy Directive-54 on cyber security, refrained from calling cyberspace a domain as well. Instead, the Obama administration refers to cyberspace as a shared space that enables the free flow of information.[5]

While cyberspace is fundamentally an avenue to exchange information and deliver effects, it is not analogous to the other four domains. Some may argue that it is far from clear what practical difference this declaration will make to Marine Corps cyberspace capabilities and capacity. However, the widespread fallacy of the "domain" qualifier drove the thinking of many military practitioners and planners, and permeates numerous doctrinal DoD publications, service strategies, and future operating concepts. The military's definition of the cyberspace domain also inflates the already recognized Merriam-Webster definition, which is "a subdivision of the internet consisting of computers or sites usually with a common purpose (as providing commercial information) and denoted in Internet addresses by a unique abbreviation (as com or gov)".[6] The inapt definition is more than just descriptive; it altered the Marine Corps approach to cyberspace capabilities development and informs and instructs their employment. It ushered the Marine Corps onto a path towards developing capabilities as it had in the sea, land, and air domains—on a dogmatic quest for organic capability and capacity. This impracticality will be discussed in greater detail in Sections IV and V.

The Marine Corps recognizes the joint service definition of cyberspace which is: "A global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[7] Like layers of an onion, the DoD describes cyberspace as encompassing Physical Network Layers, Logical Network Layers, and Cyber-Persona layers. Additionally, Joint Doctrine categorizes three cyberspace operations (CO) missions: Offensive Cyberspace Operations (OCO), Defensive Cyberspace Operations (DCO), and Department of Defense Information Network (DoDIN) Operations.[8] These explanations of warfighting's newest technological

capability are appropriate. However, the joint description of cyberspace as a so-called *domain* is too vast and ambiguous. Analogies are regularly drawn between cyberspace and the other four warfighting domains as if they were nearly synonymous. Thus far, the parallels are incongruent and thoroughly unconvincing.

First, cyberspace has too few traits in common with the other domains. Whereas boundaries in the other four domains can be delineated by geographic, oceanographic, atmospheric, and astronomical features, cyberspace boundaries cannot. Furthermore, tanks, ships, planes, and satellites are not considered *parts* of the land, sea, air or space domains. Nor are intangible information conduits such as sonar, radar, or radio waveforms considered *parts* of the other domains. They are objects *within* those domains or paths for information exchange within the electromagnetic spectrum (EMS). Yet, the DoD accepts physical hardware such as routers, servers, switches, and computers, as well as intangible wireless protocols within the EMS, such as 802.11, as *parts* of the cyberspace domain. Many boundaries in the logical layers or cyber-persona layers of cyberspace are similarly superficial.

Similarly, if one accepts the JP 3-12 definition of cyberspace, then why did the military consider previously profound technological inventions as natural advancements in the evolution of communications? The Guttenberg press revolutionized the way written information was exchanged through its use of movable type. The telegraph revolutionized the speed at which messages could be transmitted. The earliest telephones enabled instantaneous two-way voice communications. Wireless broadcasting technologies such as Radio and TV enabled mass communication on previously unthinkable scales. Radio transceivers permitted ad-hoc networks for information exchange. Consider just some of the "interdependent networks of information technology infrastructures…computer systems, and processors and controllers" necessary in

these communications mediums. Printing press machines, extensive networks of copper cable infrastructure, telephony switchboards, hub & spoke series of broadcasting towers, and countless receivers and transmitters were all resident pieces of hardware in the physical layers of these systems. The logical layers of these systems encompassed invisible elements such as electromagnetic waveforms used in broadcasting or the electrical signals within the public switched telephone network circuitry. Arguably, there were even "persona" layers in the form of authors pen names, radio DJ pseudonyms, and celebrity screen names. Other than the complexity of the internet—which is to be expected—there there are far more similarities to these mediums than there are differences.

Although cats have analogous characteristics to humans (such as two eyes and a nose), cats are not synonymous to human beings. There is *meaningful* difference. Likewise, just because there are analogous characteristics between cyberspace and the other domains, does not mean that the nature of the cyberspace domain is synonymous to the others. In fact, it is so different that noted cyberspace author Lawrence Lessig posits that "Cyberspace has no intrinsic nature. It is as it is designed."[9] But whether or not cyberspace has a true nature is beyond the scope of this paper. The point is that cyberspace is fundamentally and meaningfully different than the other four domains. While the air/space, land, and sea are composed of naturally occurring elements in the form of gases, solids, and liquids, cyberspace is the only man-made arena architected around programmed code, and unobservable in physical form. Once programed, computers communicate in algorithmic languages, and routinely in the absence of direct human interaction (whether intentionally or because of neglect). But the communication takes place for the same fundamental reason—information exchange. Cyberspace does not change communications theory, as defined by the Marine Corps in MCDP-1.

MCDP 6 summarizes communications theory as "any method or means of conveying information from one person or place to another to improve understanding."[10] Cyberspace operations allow communications theory to happen in practice. Consider the conceptual element of information itself. The differences in previous communications media and the modern internet is certainly discernable, but not substantive. For example, few could argue that packet switching is exponentially more efficient than circuit switching. Packets can travel thousands of miles hundreds of times faster than the blink of a human eye.[11] This is dramatically different than pre-Guttenberg era manuscript duplication, to say the least. Cyberspace's efficiency, speed, and widespread accessibility make it unique, but there was a time when the Marine Corps rightly understood that inventions were fundamentally mediums for information exchange (even if the information being delivered is malicious code). Humans are still the centrally defining element within the systems. Even cyberspace operations occur within the joint targeting cycle, it is human ability that creates, utilizes, and destroys the systems.

Like previously disruptive technologies, the pervasive allure of cyberspace yields misled conclusions. Foremost is a commonly held DoD belief that *information superiority* can be achieved in cyberspace, just as one achieves *air superiority* in air warfare.[12] The joint military definition of information superiority is "The operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. See also information operations."[13] Believing that one can achieve uninterrupted (meaning 100%) information flow, while prohibiting enemy information exchange is illogical—even ludicrous. Because of the ad-hoc and self-healing nature of computer networks, there will almost always be alternative avenues for information exchange, especially in the most interconnected countries.[14] The best that any rational actor can hope for in

cyberspace is to gain an advantage in operational tempo over your adversary through faster rates of information exchange. It is not done by completely eliminating disruptions. MCDP 1-0 acknowledges that the nature of war will include fog and friction (in this case potential network disruptions or prohibitive actions from the adversary).[15]

Because the technological complexities of cyberspace are nearly unimaginable, the Marine Corps is not postured to dominate in cyberspace. EF-21 recognizes that "While the Marine Corps may operate on and from the sea, in and from the air, and on the land, it is not optimized to dominate any domain. Rather, it is optimized to be expeditionary…"[16] The same recognition must occur in cyberspace. Like previously alluring technological promises, the DoD's quest to chase viable cyberspace strategies is leading the Marine Corps towards mistaken investments in force structure, capabilities procurement, and doctrine/concept development. The Marine Corps must advocate for more practical ideas to develop its cyberspace capabilities and generate cyberspace capacity through an economy of force. Subsequent sections will address specific recommendations on how this can be done through doctrinal revision, organizational restructuring, and training reforms. Before examining the Marine Corps' strategy for developing cyberspace capacity and capability, it is helpful to examine key strategic themes in national security documents that guide the DoD's overall approach, and to explain the role of doctrinal publications.

The National Military Strategy (NMS) outlines broadly stated goals for the DOD to achieve the tenets of the National Security Strategy (NSS). Variations of the term "cyber" are referenced nineteen separate times within the NSS, while the NMS mentions it another ten instances. Broadly summarized, the NSS and NMS recognize the shared state and private sector necessity for an open, interoperable, secure, and reliable Internet, and the corresponding interdependence

of our economic, safety, and healthcare networks. Defending the integrity of the internet through cybersecurity practices supports the goal of assuring access to shared spaces. Central sub-themes include concepts of attack mitigation through attribution and network resiliency. The strategies also discuss the growing sophistication of adversarial cyber capabilities, Department of Homeland Security (DHS) efforts to protect critical cyber systems and physical infrastructure, the expansion of cyberspace cooperation with military allies to confront potential threats in cyberspace, and the need for reliable and secure DoD networks. Of note, the Chinese and North Korean governments were specifically condemned for their role in U.S. cyber espionage and attacks, respectively.[17] Coincidentally, the NSS was published approximately the same time as the Justice Department's indictment of five members from the Chinese People's Liberation Army for their role in cyber activities against the U.S.[18]

The *Department of Defense Cyber Strategy*, published in April of 2015, by the Office of the Secretary of Defense, provides greater granularity for the Department of Defense's cyber mission by specifying five strategic goals for DoD cyberspace missions and outlining specific objectives to meet the stated activities and missions. Secretary Carter specifically emphasizes the three core cyber missions central to the overall strategy in the foreword of the document: to defend DoD networks, systems, and information; defend the U.S. homeland and U.S. national interests against cyberattacks of significant consequence; and support operational and contingency plans.[19] So, how did the strategy affect the way the Marine Corps structured its efforts to develop service-level objectives and milestones in support of generating cyberspace capabilities and capacity? Unsurprisingly, the DoD immediately established organizations (such as U.S. Cyber Command) and focused on the production of joint doctrinal publications (such as JP 3-12, *Cyberspace Operations)* before it fully understood or could accurately articulate the

problem. As action-biased organizations, each service began developing subordinate concepts and plans without appreciating the nuances of what they were trying to achieve. Instead of exercising operational art and applying doctrinally sound operational design elements such as *ends, ways,* and *means* approaches towards a synchronized strategy, it was as if the DoD's mantra was "Build it first and we'll figure out what *it* is later."[20]

There is a near-causal correlation between the DoD's doctrine and the Marine Corps' approach to cyberspace capabilities development. Because of extensive lead time requirements associated with numerous planning cycles, doctrine and future operating concept strategies are nearly inseparable. National strategies guide the biennial Unified Command Plan, which specifies requirements, informs service-level campaign strategies, and influences future operating concepts investments. Doctrine is supposed to explain how the services fight *today*, while operating concepts and vision are expressions of how the services may organize and fight in the *future*. However, future operating concepts are rooted in currently accepted paradigms, and guide how the Marine Corps developed operational objectives and milestones for cyberspace capabilities and capacity.

IV. USMC CYBERSPACE DOCTRINAL FRAMEWORK

The DoD must revise incongruent doctrine in order to ensure cyberspace operations (CO) are more thoroughly integrated with information operations (IO). As explained in the previous section, cyberspace is, at its core, a part of the larger IE. Joint publications on IO and CO correlate inherent relationships between the two types of operations, yet the Marine Corps has been largely unable to conflate the doctrine well enough to practically implement the theories. According to *The DoD's Dictionary of Military and Associated Terms*, doctrine is "Fundamental principles by which military forces or elements thereof guide their actions in support of national

objectives. It is authoritative but requires judgment in application."[21] The definition implies that doctrine should provide a degree of clarity and unified direction for its users.

Instead of thoroughly integrated into operations, IO are routinely afterthoughts in military planning even when history illustrates why this approach is foolish. U.S. military COIN operations provide frequent and ample evidence of pendulum swing attempts aimed at understanding cultures or "winning hearts and minds". JP 3-13, *Information Operations* and JP 3-12, *Cyber Operations* are two centrally important doctrinal documents that attempt to govern IO and CO unification. The joint chiefs of staff published *Information Operations* in 2012 and *Cyberspace Operations* in 2013. In 2014, it updated *Information Operations* in order to specify that measures of performance should be assessed for information-related capabilities [IRCs], including cyberspace operations. JP 3-13 describes cyberspace operations as an information related capability (IRC). IRCs are "Tools, techniques, or activities using data, information, or knowledge to create effects and operationally desirable conditions within the physical, informational, and cognitive dimensions of the information environment." [22] Acknowledging that cyberspace operations affect physical, informational, and cognitive dimensions of the IE, is not contentious. Nor is accepting cyberspace operations or MISO, as IRCs. However, as previously discussed, accepting that cyberspace is a domain, makes the terms *dimensions* and *domains*, unnecessarily ambiguous. Simplifying doctrinal terms can guide the Marine Corps towards more optimal (and better integrated) solutions.

The Marine Corps' lack of unified direction for cyberspace operations stems from the misguided DoD approach to doctrine development. It is clearly evident in a candid interview statement from Col Breazile, a former Commander of Marine Corps Communication-Electronics

School and current Director of the Command and Control/Cyber & Electronic Warfare Integration Division [C2/CEWID] within CD&I, who stated:

> We've got organizational issues, we've got command and control issues, we've got acquisition issues, we've got manpower and training issues…The number one issue that we see up front is the way we do command and control in the cyberspace operations...So the Commandant wanted us to get after nailing down some of these issues—what are some things we can do now immediately to change our organization to kind of fix us and align us properly so that we as an institution can move forward smartly with building capacity and capabilities within cyberspace?[23]

This statement highlights the Marine Corps' frustration as it grapples to come to terms with cyberspace as a warfighting domain and the desire to harness the potential effects of cyber power. The divergence in cyberspace terminology caused unintended consequences for achieving unified directions in USMC cyberspace. In an attempt to enhance cyberspace operations and intelligence-related IRCs, the Marine Corps created an Assistant Deputy Commandant for Information Warfare (ADC IW) position.[24] This organizational construct assigned the CG, ADC IW as a subordinate Commander to the CG, MCCDC and was designed to enhance cross-functional coordination between the Director of Intelligence (DIRINT) and the Director of C4. However, there are no inherent operational authorities in the construct, nor is there even a formally recognized DoD definition for information warfare. In fact, the term was deliberately eradicated from doctrine years ago (presumably because it never gained a shared acceptance of what the concept actually was). In spite of this, it did not prevent the existence of at least eight separate IW organizations across the other three services as well as DIA.[25]

Furthermore, the 2014 Cyber and Electronic Warfare Coordination Cell (CEWCC) concept, appears to be nothing more than a half-hearted attempt to "operationalize" integrated cyberspace and EW capabilities. Its stated intent is to "lay the foundation for how the Marine Corps will continue to operationalize the cyberspace domain and electromagnetic spectrum (EMS) as interrelated 'maneuver' spaces through which military advantages can be gained or lost."[26]

However, based on the meager investment of manpower (2-5 planners per MEF), the Marine Corps seems to be dipping it toes in the water thinking it will learn how to swim.[27] There are no organic Marine Corps cyberspace formations under the operational control of a CEWCC, nor are there existing plans to create them. This statement also seems to imply that cyberspace is really a subset of the EMS. There are, however, conceptual ideas within the IO communities of interest to create IW Battalion formations in the Marine Corps.[28] However, they are pre-embryotic at this point in time, and do not merit an extended discussion.

There are a few practical ways for the DoD to alleviate doctrinal challenges associated with understanding cyberspace. First, the Marine Corps must accurately characterize cyberspace for what it is. Historical precedence of technological revolutions in military affairs (RMAs), such as airplanes, can help remind the Marine Corps that alluring inventions have not fundamentally altered the nature of war. Accurately characterizing cyberspace as medium for information and effects—albeit with potentially profound applications—can help drive deliberately articulated end-states in operational planning. It must eradicate the recognition of cyberspace as a "domain" from its doctrine. This point will not be belabored again here. Secondly, the Marine Corps organize to achieve a symbiotic relationship between IO and CO. Section V covers this in more detail. Lastly, the DoD and Marine Corps must practice the operational design methodology of *ends, ways,* and *means* when developing and revising doctrine. Doing so would guide the Marine Corps in applying concepts and synchronizing efforts in order to maximize its cyberspace capability and capacity.

According to JP 3-0, the *Ends* must answer "What are the objectives and desired end state?"[29] Expeditionary Force-21 is the conceptual vision for how the Marine Corps will organize and fight in the increasingly chaotic future environment. It asserts that the rapid proliferation of

technology has led to unprecedented interconnectedness and increased the likelihood of transnational security threats that undermine U.S. interests abroad. It also recognizes that "Advances in information technology and cyberspace capabilities create both opportunities and challenges."[30] There are numerous cyberspace "*ends"* explicitly outlined for the Marine Corps in EF-21. All of them emphasize the importance of cyberspace integration with the other warfighting functions. The implied end state is to exploit cyberspace opportunities in order to maintain a military advantage over likely U.S. adversaries.

How does the Marine Corps ensure that its "*ways"* will achieve its future end state? The *ways* should answer "What sequence of actions is most likely to achieve those objectives and end state?" For an answer, it is useful to examine the *United States Marine Corps Service Campaign Plan (USMC SCP)* and its associated appendix K, the *Marine Corps Information Enterprise (MCIENT) Strategy.* Headquarters Marine Corps, C4 (HQMC, C4) Directorate published the MCIENT Strategy in 2010 to "influence enterprise Force Development priorities by providing the Marine Corps' single, top level Information Enterprise objectives that inform future capability decisions, supporting plans, concepts, and programming initiatives."[31] Keeping in mind the five missions outlined in the *DOD Cyber Strategy* as a framework, the *MCIENT Strategy* specifies thirteen strategic objectives designed to maximize tenants of cyberspace capacity and capabilities. Twelve of the objectives are largely related to development of the telecommunications architecture itself (i.e. Developing, expanding, and distributing enterprise resources). Most pertinent to the scope of this discussion is Strategic Objective 4.6: Man, Train, and Equip the Force for the MCIENT.[32] Considering that the MCIENT was published four years prior to the USMC SCP, the Marine Corps clearly put the cart before the horse.[33] Marine Corps communications and cyberspace operations development trajectories were already set in motion.

Annexes to the *SCP* (such as the *MCIENT* and *MCISR-E)* should attempt to be more symbiotic in nature. The better integrated warfighting functions are, the likelier the Marine Corps meets the *ends* and objectives its describes in EF-21. Commanders should come to expect integrated processes, systems, staffs, and effects (including actions and activities in cyberspace).

Lastly, the Marine Corps must match *means* to practical and sustainable initiatives. *Means* must answer "What resources are required to accomplish that sequence of actions?"[34] *The* Mission statement of the SCP articulates that "From fiscal year 2014 through fiscal year 2022, Deputy Commandants (DC), Directors, and Commanders will take required actions to develop, organize, train, equip, and provide Marine forces to meet CCDR requirements, provide for the national defense, and posture the Marine Corps forces for the future security environment".[35] The SCP's mid-range goals and intermediate objectives guide subordinate Departments and Commands in matching resources with stated objectives. The current state of Marine Corps cyberspace capability and capacity does not indicate effective resourcing.

The Marine Corps should continually reassess its strategy for measures of performance and measures of effectiveness. As conditions in the international security environment change, the Marine Corps should ensure that its operational strategies are soundly nested within the national level security and cyberspace operations architecture by reviewing its service level strategies at least every two years to incorporate in-stride refinements to goals and intermediate objectives, as necessary. Based upon impractical cyberspace future operating concepts, it is doubtful that the service is currently doing so. Else, the Marine Corps would have would have reached far different solutions.

Existing USMC doctrine indicates a lack of holistic approaches in cyberspace. For example, MCWP 3-40.3, *MAGTF Communications System* is largely incongruent with JP 6-0, *Joint*

Communications System. In fact, there is not a single instance of the word cyberspace in the Marine Corps publication, while it is mentioned an astounding 97 times in the joint publication! Either the Marine Corps believes communications are completely synonymous to cyberspace operations, or it needs to update its doctrine to synchronize its own actions and objectives. Marine Corps communications encompass two of three cyberspace operations activities (DCO and DoDIN Operations), yet there is no Marine Corps equivalent publication to JP 3-12, *Cyberspace Operations.* Since there are numerous references to cyberspace operations throughout EF-21, the MCIENT strategy, and the SCP, omissions of "cyberspace" do not appear deliberate.[36] The Marine Corps should remedy this fact by developing an equivalent Marine Corps doctrinal publication to JP 3-12, *Cyberspace Operations* and to make clear distinctions on the employment of USMC cyber capabilities in support of cyberspace operations.

Joint Publications make a fairly convincing case that these are three distinct operations within the cyberspace operational construct. DCO and DoDIN largely exist to enable Command and Control (C2) for friendly forces and enable information exchange. While the Marine Corps' current 06XX career field possesses adequate capability and capacity to conduct these missions, they are typically not well synchronized across all warfighting functions. The Marine Corps must also come to terms with whether it not it intends to develop capable, sustainable, and viable OCO capabilities resident to Marine Corps forces. If it intends to, it must identify who will conduct this mission, how it will generate the capacity to do so, and how professionalize and sustain proficiency of the force. Specific cyberspace forces training and education reform is discussed in Section VI.

V. **USMC CYBER FORCE ORGANIZATIONAL FRAMEWORK**

As the DoD's smallest service (comprised of only 14% of its active duty personnel)—and in light of budgetary constraints—making wise cyberspace capacity decisions is imperative for the Marine Corps. The Marine Corps must economize its forces around capabilities to meet the most probable future security threats. Generally speaking, Marines are currently categorized by functional area (known as Primary Military Occupational Specialties) and separated into organizations along operating forces and supporting establishment fault lines. The operating forces, such as the Fleet Marine Forces (FMF), are employed throughout the globe in support of Combatant Command (COCOM) or unified functional commands (such as USSOCOM) requirements. Their responsibilities typically include the planning, installation, operation, and maintenance (PIOM) of Marine Corps cyber-related networks and systems. Elements within the supporting establishment typically establish cyber policy, provide functional area oversight, and establish service-level strategies to train, man, and equip Marine Corps forces. Marine Corps Force-level commands (such as U.S. Marine Corps Forces Cyber Command or U.S. Marine Corps Forces Special Operations Command), have responsibilities to conduct both roles (train, man, equip, as well as employ).

The Marine Corps operating forces continue to organize based on obsolete Cold War era operating constructs. Most functionally aligned organizations were created during the infancy (or even well before) the proliferation of the internet. For example, infantry forces are assigned to the Ground Combat Element, aviation elements to the Air Combat Element, and logistics elements to the Logistics Combat Element. Within each element (to include the MEFs), Combat Service (CS) and Combat Service Support (CSS) capabilities are also organized by function. Most notably, the Communication Battalions (the USMC's largest operating force cyberspace units) have not meaningfully reorganized since their establishment circa 1989, under what is now

II Marine Headquarters Group (only 6 years after the Internet was even evented).[37] The histories of the Intelligence and Radio Battalions (also functionally aligned and related to cyberspace) share similar lineages. Forces and their respective functions are only composited and integrated, once they are assigned specific missions (i.e. Marine Expeditionary Units or Special-Purpose MAGTFs). During an era characterized by disaggregated operations, the functionally aligned constructs do not demonstrate the age-old adage "train as you fight". Although the Communication Battalions exclusively provide DoDIN operations and DCO for Marine Expeditionary Forces (MEFs), the necessity to understand OCO capabilities is crucial. According to the Unified Command Plan, the national command authority assigns cyberspace forces to combatant commanders based on the envisioned cyber forces necessary for the mission.[38] If OCO were authorized in support of a MAGTF operation (whether as a standalone service or in support of a larger JTF), task-organized teams from USCYBERCOM would provide those functions. Hence, there is not a necessity to retain organic OCO capabilities within a MAGTF.

The current functional alignment of operational force cyberspace-related units are not conducive to meeting the employment challenges posed by asymmetric threats in the future operating environment, as described by EF-21 (such as necessity for Company Landing Teams). The Marine Corps should consider minor structural revisions, particularly in the MEF Headquarters Groups (MHG). If recent employment of Special Operations Forces (SOF) is any indication, future deployments will require smaller and more tightly-integrated cyber force and intelligence detachments, capable of supporting disaggregated operations. The overall question of how to best achieve economy of cyber forces is still largely unresolved, but the necessity to reorganize existing forces for the information age is readily apparent. Crisis response or irregular

warfare against asymmetrical threats will be the new normal in future security environments. If the Marine Corps does not posture its cyberspace forces to exploit informational advantages at the Company level (as *EF-21* intends), it will surely sacrifice relevant opportunities to those who can (such as SOF elements). The structure of the large-scale functional Battalions should be further distributed to the tactical edge at lower echelons. Even platoon-level elements rely upon cyberspace operations. One of the SCP's stated goals is "Designated SPMAGTF Crisis Response (SPMAGTF CR) command elements and SPMAGTF CR MSE's achieve tactical digital C2 capability to the Platoon-level." PP&O, CD&I, C4, MARFORCOM, MARFORPAC are designated as participating agencies.[39] Yet, there are no discernable structure changes to support this goal. In all likelihood the solution to sourcing personnel and equipment would have to come from existing T/O&E structure from within the Communication Battalions. Though the exact organizational model constructs are beyond the scope of this paper, restructuring warrants additional discussion in force structure review groups and service-level war games.

In spite of the above observations, and to the detriment of force capacity, the DoD took the opposite "Field of Dreams" approach to cyberspace capability development—"If you build it they will come." Predictably, in 2009, the former Secretary of Defense, Robert Gates ordered the creation of a subordinate unified command under USSTRATCOM that would be responsible for cyberspace operations.[40]

> USCYBERCOM plans, coordinates, integrates, synchronizes and conducts activities to: direct the operations and defense of specified Department of Defense information networks and: prepare to, when directed, conduct full spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries.[41]

The 2009 memorandum specified that the Commander would also serve as the Director of the National Security Agency. The National Security Agency leads the U.S. Government in cryptology that encompasses both Signals Intelligence (SIGINT) and Information Assurance

(IA), and enables Computer Network Operations.[42] This specification was indicative of the changing attitudes towards cyber warfare but did not necessarily unify service-level cyberspace operations. Although economy of force is a proven means of maximizing the capacity of high-demand, low-density capabilities (such as cyberspace-related MOSs), the four services set out on individual courses, apparently determined to provide four overlapping, often redundant, capabilities. The DoD postured the services to start digging their cyberspace trenches by equipping their personnel with soup ladles. The job may eventually get done, but there are more efficient ways to accomplish the task. Afraid of being excluded from potential resource venues, driven by genuine desires to procure alluring cyberspace capabilities, or perhaps just because they were directed—each service ignored economy of force maxims they knew to be true. The robustly-sized USCYBERCOM will achieve full operational capability (FOC) by 2017.[43]

Due to billet rotation schedules, available career progression opportunities, and lifelong technical training tracks, it is unreasonable to expect that the Marine Corps will yield a return on investment from USCYBERCOM. Thus far, there are no indications of increased retention or promotion rates for cyberspace personnel. These topics are discussed in greater detail later. Nor is there observable evidence to support claims of increased proficiency of cyberspace forces or tangible OCO capabilities. Even if Marines attend extensive National Security Agency (NSA) training, there is no well-recognized certification designating them as exceptionally qualified for promotion. In an era of budgetary constraints, the Marine Corps' equity contributions resulted in zero-sum gains. If the Marine Corps is expected to contribute forces to USCYBERCOM (especially during eras of fiscal austerity), there should be measurable benefits to the individual

Marines and to the service (especially while it reduces the operational capacity of FMF cyberspace capability).

The U.S. Army established a Functional Area (FA) career field for its cyberspace practitioners. In contrast, the Marine Corps did not establish an analogous Primary MOS (PMOS) career track but rather, retained separate Communications (06XX) and Intelligence (02XX) career fields. Even 065X Marines with the term "Cyber" as part of their official billet titles, exclusively conduct DCO and DoDIN operations. The Marine Corps simply does not have the capacity to replicate the Army model structure of an independent cyberspace career field, nor should it try. However, a few practical short-term solutions could be implemented.

While the recently released *CMC FRAGO 01* explicitly published the Commandant's intent to expand IO and Cyber capabilities at the MARFOR elements and MEFs, the most recent Quadrennial Defense Review indicates that major changes in tables of organization and MOS demographics are not likely to produce a statistically meaningful shift in numbers.[44] When compared to other MOSs, the billet rotation models and promotions rates for cyberspace planners and practitioners are at or below services averages. In fact, overall promotion rates for Communication Officers are routinely lower than their combat arms counter-parts.[45]Additionally, the Marine Corps solution for problems associated with retaining qualified high-demand/low-density career fields such as communications and intelligence, has been monetary incentives. Of the USMC's active duty population, 7.86% held communications-specific (06XX) Primary Military Occupational Specialties (PMOS). However, one should not misconstrue this percentage as diminutive. Communications was the second largest Enlisted MOS out of forty-two career fields (8.11% of the active duty Enlisted population) and sixth largest MOS of the thirty-eight Officer career fields (5.85% of the active duty Officer

population). If you include Ground-Electronics Maintenance (28XX) and Signals Intelligence (26XX) career fields—both of which which conduct significantly meaningful activities within the cyber mission—the cumulative number grows to 12.31% of 2015 active duty personnel.[46] See Table 1.

Total # of USMC Active Duty Personnel as of 11 March 2015 188,064 (20,926 Officers/167,138 Enlisted)						
MOS	Officers	% of AD Officers	Enslisted	% of AD Enl	Total Off/Enl	Total % of 2011 AD Pop.
06XX	1225	5.85	13553	8.11	14778	7.86
28XX	107	0.51	4741	2.84	4848	2.58
26XX	45	0.22	3467	2.07	3512	1.87
Totals	1377	6.58	21761	13.02	23138	12.31

Table 1.

Compare the above data to the fact that the Marine Corps' allocated 10.85% of its $4,750,250 funds appropriated for its FY16 Selective Reenlistment Bonus (SRB) Program towards the 06XX cyber career field (a disproportionately high amount). The goal of the SRB program is to monetarily incentivize service retention of highly qualified Marines in high-demand, but low-density career fields (which often coincides with marketable skillsets in civilian job sectors). The SRB categorizes eligible Marines into Zones A, B, or C (from those least- to those most-experienced). The $56,000 incentive allotment for eligible Zone A personnel was tied with two other MOSs for the highest quantity. Notably, the other two MOSs were Human Intelligence and SOF Critical Skills Operators—also directly associated with important cyber activities. The $59,000 "Zone B" incentive allotment was also the *single* highest amount apportioned for any MOS career field. Even more statistically significant is the fact that of the eligible populace in the Zone C category, the 06XX career field accounted for a staggering 44.11% of the available funds.[47] All of the aforementioned analysis is to say that the Marine Corps understands the need to recruit and retain highly skilled individuals with cyber-related job skills and experience, but is consistently ineffective at doing so.

While these efforts are laudable, they do not address the systemic issues associated with force rotations, freedom of innovation, or career progression opportunities (several critical factors of job satisfaction). Because of technical nature of many cyberspace operations, the profession requires a lifelong commitment from its practitioners—an impracticality for the majority of personnel in the Marine Corps. While monetary incentive may help hemorrhaging personnel capacity, they do not yield additional capability. The USMC desire to investment in human capital is a worthy pursuit. However, money is better invested in training and educational opportunities for its personnel.

However, hope is not lost for the Marine Corps cyberspace community. The Marine Corps can benefit from a few practical short- and mid-term actions. Intelligence and Communications Marines assigned to MARFORCYBER, USCYBERCOM, who successfully complete advanced level cyberspace-related curriculums and 36 month tours of duty, should be awarded an Additional MOS (AMOS) designator and denoted as "specially qualified" for future promotion (thereby incentivizing service at these commands). MARFORSOC already adopts this model through its use of the 8071 AMOS designation of Special Operations Capabilities Specialist-Communications (SOCS-C). Although Marines agree to extended 48 or 60 month tours because of extensive on the job training requirements, there is currently no incentivizing mechanism to serve at MARFORCYBER, USCYBERCOM, or MARFORSOC. In fact, due to spending four years in a command with comparatively limited time for Command opportunity, it may actually hinder Officer careers. The AMOS assignment would be a cost-effective means of talent management and could aide in matching ideally suited candidates for follow-on assignments (much like the Army SOF model). In addition to assigning AMOSs, these personnel should be considered for reoccurring assignments at those commands in order to maximize the return on

investment for uniquely qualified skillsets. Increased opportunity for promotion and advanced training may yield higher job satisfaction amongst given populations (which is a critical factor in retention). An alternative approach is to abandon USMC equities in OCO altogether. Thereby reconstituting capacity into back into the Fleet Marine Forces.

The Marine Corps should integrate capabilities at the lowest possible tactical levels in order to adapt to the changing security environment. For example, it could readily combine its Marine Headquarters Group (MHG) Battalions into integrated units in order to capitalize on the combined effects of intelligence, communications, and radio battalion C4ISR assets. This also affords integrated training opportunities, thereby maximizing the effects of integration (to include cyberspace capabilities). The Marine Corps cannot profess to "train how we fight", if it is not persistently organized to do so. Communications teams must design networks around information exchange requirements, sensors must be emplaced in concert with priority intelligence requirements, electromagnetic spectrum effects must be considered with consideration to friendly forces. Teams should not aggregate and disaggregate only during real-world contingencies, they should practice with one another on a frequent basis during routine exercises and training.

The Marine Corps must meet cyberspace capability and capacity objectives outlined in the USMC SCP through effective organizational structure and professionalization of cyberspace forces. The HQMC C4 Director is the lead Office of Primary Responsibility (OPR) for five specified goals and three intermediate objectives within the document. MARFORCYBER is tasked as the OPR for an additional two goals. To summarize, C4 is tasked with: improving cyber proficiency through training, workforce readiness, and policy revision; enabling distributed MAGTF C2 via increasing access, interoperability, and reach back capabilities of the Marine

Corps Enterprise Network (MCEN) garrison and tactical domains; and enhancing the MCEN flexibility by distributing enterprise services and sharing collaborative resources. MARFORCYBER is tasked with: achieving full operational capability (FOC) of the USMC portion of the Cyber National Mission Force in support of USCYBERCOM; and developing cyber range requirements in support of training and testing for the cyber mission force.[48] This section will discuss capacity-related issues, while Section VI will focus on capability-related issues. Capacity-related concepts are enabled by recruitment, retention, and talent management while capability-related concepts are enabled by professionalization and talent development.

VI. USMC CYBERSPACE TRAINING & EDUCATION FRAMEWORK

The USMC must reform its cyberspace training models in order to increase proficiency, thereby maximizing capabilities. The importance of professionalizing cyberspace forces is obviously merited. The Marine Corps must develop curriculum that educates its Communication and Intelligence professionals about inter-service and interagency OCO capabilities and the process for requesting external capability support, while it focuses its organic training efforts exclusively on DCO and DoDIN Ops. This maximizes the integrated affects of OCO, when authorized, while preserving the capacity for the vast majority missions conducted in cyberspace: OCO and DoDIN operations. The potential time and money savings on training, manning, and equipping the currently redundant service capabilities is readily apparent. Given the systemic conditions of USMC promotions, rotations, and organization mentioned in Section V, this is the most practical and efficient training and educational model for the Marine Corps. As previously noted, MAGTF elements typically perform operational level objectives in support of a Geographic Combatant Command (whether acting as a JTF or performing service-specific functions). If a MAGTF was expected to conduct OCO under Presidential or National Executive-

level authorities, it would be augmented with additional forces. Furthermore, because of the global nature of cyberspace, many OCO functions could be employed from the United States.

Civil-military relations theorist Samuel Huntington described a profession as "a peculiar type of functional group with highly specialized characteristics."[49] He described what the Marine Corps calls lifelong learners—professionals whose expertise stems from prolonged education and experience. Marine Corps cyberspace operational capability is primarily achieved through the professionalization of its cyberspace forces. This critical concept is enabled through effective talent development. Headquarters Marine Corps, Training and Education Commands must ensure the Marine Corps meets it cyberspace capability objectives outlined in the USMC SCP. This section will briefly discuss means of achieving capability end states.

Manpower expenditures (such as personnel salaries) are the single-highest operating costs for the Marine Corps. Like the SOF Truth that "Humans are More Important Than Hardware", *EF-21* boasts that the individual Marine is the bedrock of the Corps.[50] The Commandant regularly notes the importance of lifelong learning concepts and invests in its career progression opportunities for both its Officer and Enlisted Marines. Notably, the USMC maintains the lowest average age of its members among all of the services. Because of this reality, and due to the highly technical nature of the cyberspace career field, the Marine Corps will always be at a significantly disadvantaged status in maintaining qualified cyberspace personnel and developing cyber capabilities.

The Marine Corps does not seem to seem to appreciate the reality of its quantitative constraints. Though it does not appear to be developing separate cyberspace operator career fields, it continues to commit significant personnel structure to MARFORCYBER and USCYBERCOM. In the current zero-sum gain environment, large personnel contributions to

these organizations make little practical sense, especially if they are retained only at equal (or lesser) rates than their FMF counterparts. Furthermore, they detract from the ability to sustain organic cyberspace support to critical USMC organizations, such as standing SPMAGTFs or newly emerging Marine Expeditionary Brigade concepts. If the Marine Corps intends to retain credible crisis-response forces, it must divest from committing significant personnel expenditures to bloated Headquarters staffs such as USCYBERCOM. If the Marine Corps intent is truly to integrate the so-called cyberspace domain to have effects across all of the warfighting functions, then the continued stove-piped efforts in the 06XX and 26XX training communities are also not indicative of this claim.[51] The Marine Corps never established a "Cyber" PMOS career track as the Army did with its cyberspace functional area (FA). It simply renamed many of its computer network specialists and chief billets. Truly professionalizing the cadre requires much more than this. If the Marine Corps desired tactical cyberspace capabilities resident within the MAGTFs, it must make committed investments to establish a cyber PMOS career tracks. Or perhaps the Marine Corps did so out of its recognized lack of capacity. Either way, the Marine Corps must decide if it intends to create tactical cyber capabilities at the expense of current capacity. It cannot sustain both a fiscally austere and personnel-constrained environment.

Rather than make significant (and unlikely) systemic policy changes (to USMC promotions and rotation models, for example), the Marine Corps must establish practical and achievable cyberspace capabilities goals. It must significantly divest from current active duty contributions to USCYBERCOM and MARFORCYBER. Instead of attempting to develop and sustain OCO capabilities, Marine Corps cyberspace practitioners must understand how to request and employ assets through USCYBERCOM. Especially considering strategic level OCO, while MAGTFs are traditionally operationally focused elements and employed in support of a Joint Force

Commander (JFC) or for crisis response. The Marine Corps should deliberately limit its operational focus on a narrower subset of cyberspace capabilities. The existing PMOS structure and career progression courses for 06XX does seem to indicate that the Marine Corps intends to focus on DoDIN Operations and DCO, rather than pursue organic OCO capabilities for the MAGTF. Considering the relatively minimal OCO mission, this is probably a wise decision. The Marine Corps could still combine organizational adaptations with refined training models, to most efficiently use its finite cyberspace resources.

Though there are career progression opportunities at every phase in a military professional's career, Officer PMOS roadmaps are rarely (if ever) prescribed. Entry-, career-, and mid-level career progression courses, frequently focus within respective PMOS communities of interest. The Marine Corps should give serious thought to communication and intelligence training and educational continuums in order to capitalize on numerous functional area merges happening in cyberspace. For example, it should mirror, as much as practical, the Expeditionary Warfare School, and Command and Staff College models in its PMOS training venues. Early inter-service exposure and training opportunities would provide increased understanding of sister-service capabilities and limitations, as well as eliminate potential redundancies across services. The Marine Corps could develop cyber warfare integration courses with an intended target audience of 06XX, 28XX, and 26XX Officers and senior Staff Non-Commissioned Officers. The course could introduce integration concepts that help Commanders gain tactical advantages in cyberspace, without completely overhauling entry-level PMOS structure (which would be a costlier and time-consuming process). For example, the USMC should understand how to request and unique information related capabilities (such as OCO), rather than try and train towards

sustaining unrealistic standards. As previously mentioned, duties and in cyberspace career fields do not lend well to part-time responsibilities.

If the above initiatives proved effective, longer term considerations could include tying these career progression courses into promotion considerations, or even establishing integration-specific MOS's that specialize in cyberspace operations, EMS, and intelligence targeting cycles employed in the CEWCCs (beyond the 8834 AMOS). Although DoDIN operations and DCO would still be the focus of effort for the 06XX community, OCO exposure would help the community orient on the adversary's cyberspace environment from the enemy perspective and help in the Intelligence Preparation of the Operational Environment (IPOE) during steady state operations. This would enhance Computer Network Operations (CND/CNO/CNE) by combining elements from various cyber-related communities. The intent would be complimentary—but not duplicative—efforts between the SIGINT and Communications communities. Integrated schooling and training would have the secondary benefit of furthering professionalization of Marines' careers by providing early exposure to other warfighting functions which expand their repertoire. Talent development tracks and careful talent management also help overcome challenges associated with retention of qualified personnel. Investing in a Marine's career demonstrates that the service is committed to their professional development.

There are currently several notable examples of the USMC investing the intellectual rigor developing its cyberspace capabilities. Marine Corps Enterprise Network (MCEN) unification, Information Management Officer (IMO) advocacy, and numerous Information Technology (IT) acquisitions initiatives (such as Universal Needs Statements and emergent Programs of Record) are positive measures of progress.[52] IMO advocacy is a significant steps towards integrating and unifying over 90 major software applications that span six warfighting functions, with existing

communications systems, computer hardware, and networks.[53] The tangential effort towards a "Seamless MCEN" transition will create a single user identity (both in garrison and while deployed) that enables a member to rapidly deploy while retaining access to individual and organizational data.[54] However, creating trained operators and organizing forces for employment is tantamount to the success of these initiatives. After all, systems without trained professionals who can exploit the technologies for combat effect, become the proverbial "self-licking ice cream cone." They serve no purpose. The C4 Operational Advisory Group (OAG) recently proposed recommended changes to Training Command (TCOM) for the 06XX and 28XX career fields. Both MOS communities are attempting to resolve the crux of creating a more proficient "network centric" Marine by implementing changes to several career development tracks. Traditional Radio Operators (0621s) are being presented computer networking concepts in order to keep pace with technologies and Technical Controllers (2821/2823s) are transitioning away from legacy multiplexing devices in favor of Internet Protocol-based hardware, such as routers. What is more, the task-saturated 065X community (Cyber Marines) is now parceled into Cyber Network, Cyber Systems, and Cyber Security Military Occupational Specialties. TCOM approved significant revisions to training and career tracks for twenty individual PMOS's in the cyber community and curriculum revisions are continuously in progress.[55] C4 should further refine and capitalize upon enterprise services, such as the Marine Corps Enterprise Information Technology Services (MCEITS) program of record, and regionalized cloud computing environments, such as those enabled by the Marine Information Technology Support Centers (MITSC).[56] This economizes Marine cyber forces for other emerging requirements, while simultaneously assuring Commanders timely access to needed information. Maintaining a light

personnel footprint is also particularly important in politically sensitive areas of operation where minimizing visibility of military presence is paramount.

VII. CONCLUSION

It is not entirely clear at this point in time exactly how the Marine Corps should organize its cyberspace forces to meet future security threats. However, it is abundantly clear that there is not a single warfighting function or MOS that does not not somehow operate within some layer of the cyberspace domain (whether knowingly or not) and the need to restructure is already here. Cyber operations are so ubiquitous, that conserving the Marine Corps' finite cyber-capable resources (whether money, personnel, or equipment) is an operational imperative. As the DoD's smallest service, the Marine Corps cannot afford to straddle the fence on its position to pursue cyberspace capability or capacity. It must decide between the two, if it is to perform either function effectively. The Marine Corps must reject currently popular cyberspace maxims, advocate for doctrinal change, restructure its cyber forces, and revise current training models. This ensures a comprehensive approach to integrating cyberspace operations with other warfighting functions and across the range of military operations.

Notes

[1] Peter Singer and Alan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know*, (New York: Oxford University, 2014), 19.

[2] http://60secondmarketer.com/blog/2011/10/18/more-mobile-phones-than-toothbrushes/

[3] U.S. Joint Chiefs of Staff, *Cyberspace Operations*, Joint Publication 3-12, (Washington, DC: Doctrine for the Armed Forces of the United States, February 2013), V.

[4] The White House, *Guidance Regarding the Use of "Domain" in Unclassified and Public Statements,* draft memorandum, 14 March 2011.

[5] The White House, *The National Security Strategy of the United States of America* (Washington, DC, 2015), 12. https://www.whitehouse.gov/sites/default/files/docs/2015_national_security_strategy.pdf

[6] http://www.merriam-webster.com/

[7] U.S. Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms*, JP 1-02 (Washington, DC: Joint Chiefs of Staff, 8 November, 2010 [As Amended Through 15 November, 2015]), 58.
[8] U.S. Joint Chiefs of Staff, *Cyberspace Operations*, I-3.
[9] Lawrence Lessig, *Code Version 2.0*. (New York, NY: Basic Books a member of the Perseus Books Group, 2006), 317.
[10] Headquarters US Marine Corps, *Command and Control*, MCDP 6, (Washington, DC: Headquarters US Marine Corps, 4 October, 1996), 94.
[11] Michael Lewis, *Flash Boys*: *A Wall Street Revolt* (New York, NY: W.W. Norton and Company, 2014), 9-10.
[12] U.S. Joint Chiefs of Staff, *DoD Dictionary of Military Terms*, *10*.
[13] U.S. Joint Chiefs of Staff, *DoD Dictionary of Military Terms*, 115.
[14] James Cowie, "Internet Infrastructure: Virtual Meets Reality," (PowerPoint presentation. renesys, MORE-IP, Amsterdam, 23 May, 2013).
[15] Headquarters US Marine Corps, *Warfighting*, MCDP 1, (Washington, DC: Headquarters US Marine Corps, 20 June, 1997), 3-20.
[16] Headquarters, US Marine Corps, *Expeditionary Force 21*, (Washington DC: Headquarters Marine Corps, 2014), 5.
[17] The White House, *The National Security Strategy*, 12-13.
[18] The Department of Defense, *The DoD Cyber Strategy*, (Washington, DC: Office of the Secretary of Defense, April 2015), 12.
[19] The Department of Defense, *The DoD Cyber Strategy*, 5.
[20] U.S. Joint Chiefs of Staff, *Joint Operations*, Joint Publication 3-0, (Washington, DC: Doctrine for the Armed Forces of the United States, 11 August 2011), II-4.
[21] U.S. Joint Chiefs of Staff, *DoD Dictionary of Military Terms*, 71.
[22] Joint Chiefs of Staff, *Information Operations*, JP 3-13 (Washington, DC: Joint Chiefs of Staff, 27 November, 2012 [As Amended Through 20 November, 2014]), I-4.
[23] Marine Corps Cyber Task Force Stood Up, Will Report to Commandant This Summer by Meghan Epstein, 28 April 2015. http://news.usni.org/2015/04/28/marine-corps-cyber-task-force-stood-up-will-report-to-commandant-this-summer
[24] Deputy Commandant for CD&I, "ADC Information Warfare," (PowerPoint presentation. Headquarters Marine Corps, C4 OAG, Quantico, VA, 27 October, 2015). Current Organizational Chart Located at http://www.mccdc.marines.mil/
[25] U.S. Joint Chiefs of Staff, *DoD Dictionary of Military Terms*, A-6, A-64, A103, A-125.
[26] Headquarters, US Marine Corps, Deputy Commandant for Combat Development and Integration, *MAGTF Cyber and Electronic Coordination Cell (CEWCC) Concept*, *1*.
[27] Headquarters, US Marine Corps, CD&I, *CEWCC Concept, 8-17*.
[28] Marine Corps Information Operations Center, "Marine Corps Information Operations," (PowerPoint presentation, Command & Staff College, Quantico, VA, 11 February 2016).
[29] U.S. Joint Chiefs of Staff, *Joint Operations*, II-4.
[30] Headquarters, U.S. Marine Corps, *Expeditionary Force-21*, 8.
[31] Headquarters, US Marine Corps, C4, *MCIENT*, 7.
[32] Headquarters, US Marine Corps, C4, *MCIENT*, 25.
[33] Headquarters, US Marine Corps, C4, SCP & *MCIENT*,.
[34] U.S. Joint Chiefs of Staff, *Joint Operations*, II-4.

[35] Headquarters, US Marine Corps, PP&O, *United States Marine Corps Service Campaign Plan 2014-2022*, (Quantico, VA Headquarters US Marine Corps, 21 May, 2014), 11-12.
[36] U.S. Joint Chiefs of Staff, *Joint Communications Systems*, Joint Publication 6-0, (Washington, DC: Doctrine for the Armed Forces of the United States, June 2010), I-1.
[37] 8th Comm Bn History/Lineage public website
[38] Unified Command Plan
[39] Headquarters, US Marine Corps, PP&O, *USMC SCP*, 33.
[40] Robert M. Gates, *Establishment of a Subordinate Unified U.S. Cyber Command Under U.S. Strategic Command for Military Cyberspace Operations*, Secretary of Defense Memorandum (Washington, DC
[41] https://www.stratcom.mil/factsheets/2/Cyber_Command/
[42] https://www.nsa.gov/about/mission/index.shtml
[43] Headquarters, US Marine Corps, Service Campaign Plan, 29.
[44] For the scope of this discussion, the Marine Corps Total Force Structure (MCTFS) database was utilized to gather organizational information (such as Tables of Organization baseline numbers) in order to gather a partial view of Marine Corps cyber fore allocation, and make useful baseline comparisons.
[45] Assistant Secretary of the Navy, Manpower & Reserve Affairs, Precept Convening the Fiscal year 2017 U.S. Marine Corps Major Promotion Selection Board and Captain Continuation Selection Board, FYs 2011 - 2015.
[46] As of 11 March, 2015 the total active duty population of the United States Marine Corps was 188,064 (20,926 Officers and 167,138 Enlisted). https://marinecorpsconceptsandprograms.com/almanac
[47] Commandant of the Marine Corps. MARADMIN: Fiscal Year 2016 (FY16) *Selective Reenlistment Bonus (SRB) Program and Broken Service SRB (BSSRB) Program*.
[48] Headquarters, US Marine Corps, PP&O, *USMC SCP*, 19, 22-23, 29-30, 33.
[49] Samuel Huntington, *The Soldier and the State*, (Cambridge, Massachusetts: The Belknap Press of Harvard University Press, 1985), 7.
[50] Headquarters, U.S. Marine Corps, *Expeditionary Force-21,* 44.
[51] Bob Price, "06xx Modernization OPT," (PowerPoint presentation. Headquarters Marine Corps, C4, Washington, DC, 27 October, 2015).
[52] Carlin Curtis, "Seamless MCEN," (PowerPoint presentation. Headquarters Marine Corps, C4, Washington, DC, 28 October, 2015).
[53] Steve Knott, "Information Management Advocacy," (PowerPoint presentation. Headquarters Marine Corps, C4, Washington, DC, 27 October, 2015).
[54] Carlin Curtis, "Seamless MCEN".
[55] Bob Price, "06xx Modernization OPT".
[56] Headquarters, US Marine Corps, C4, *Marine Corps Information Enterprise Strategy, Appendix 2*, 14.

Bibliography

Primary Materials

Breazile, Gregory. "Fall OAG Brief 2015: HQMC C4 OAG 'C4 Capability Development'." PowerPoint presentation. Headquarters Marine Corps, Capabilities Development

Directorate, Quantico, VA, 27 October, 2015.

Commandant of the Marine Corps. FRAGO 01/2016: *Advance to Contact*. Headquarters Marine Corps, Washington, DC, 19 January 2016.

Curtis, Carlin. "Seamless MCEN." PowerPoint presentation. Headquarters Marine Corps, C4, Washington, DC, 28 October, 2015.

Deputy Commandant for CD&I. "ADC Information Warfare." PowerPoint presentation. Headquarters Marine Corps, C4 OAG, Quantico, VA, 27 October, 2015.

Flynn, George J. LtGen, DC CD&I "Statement Concerning Operating in the Digital Domain: Organizing the Military Departments for Cyber Operations." Congressional testimony for the Subcommittee on Terrorism, Unconventional Threats and Capabilities of the House Armed Services Committee, United States Congress, Washington, DC, September 23, 2010.

Groen, Mike. "Director of Intelligence USMC." PowerPoint presentation. Command and Staff College, Marine Corps University, Quantico, VA, January, 2016.

Headquarters, US Marine Corps. *Expeditionary Force 21*. Washington DC: Headquarters Marine Corps, 2014.

Headquarters, US Marine Corps. *Command and Control*. MCDP 6-0. Washington, DC: Headquarters US Marine Corps, 4 October, 1996.

Headquarters, US Marine Corps. *MAGTF Communications Systems*. MCWP 3-40.3. Washington, DC: Headquarters US Marine Corps, January, 2010.

Headquarters, US Marine Corps, C4. *Marine Corps Information Enterprise Strategy. MCIENT w/ Appendices*. Washington, DC: Headquarters US Marine Corps, December, 2010.

Headquarters, US Marine Corps, Deputy Commandant for Combat Development and Integration. *MAGTF Cyber and Electronic Coordination Cell (CEWCC) Concept*. Quantico, VA: Headquarters Marine Corps, 1 May 2014.

Headquarters, US Marine Corps, PP&O. *United States Marine Corps Service Campaign Plan 2014-2022*. Quantico, VA Headquarters US Marine Corps, 21 May, 2014.

Knott, Steve. "Information Management Advocacy." PowerPoint presentation. Headquarters Marine Corps, C4, Washington, DC, 27 October, 2015.

Marine Corps Information Operations Center. "Marine Corps Information Operations." PowerPoint presentation. Command & Staff College, Quantico, VA, 11 February 2016.

Price, Bob. “06xx Modernization OPT.” PowerPoint presentation. Headquarters Marine Corps, C4, Washington, DC, 27 October, 2015.

Joint Chiefs of Staff, *Cyberspace Operations*. JP 3-12. Washington, DC: Joint Chiefs of Staff, 5 February, 2013.

Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms*. JP 1-02. Washington, DC: Joint Chiefs of Staff, 8 November, 2010 (As Amended Through 15 November, 2015).

Joint Chiefs of Staff, *National Military Strategy of the United States of America*. Washington, DC: Joint Chiefs of Staff, June, 2015.

The White House. *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World.* Washington, DC, 2011. https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

The White House. *The National Security Strategy of the United States of America.* Washington, DC, 2015. https://www.whitehouse.gov/sites/default/files/docs/2015_national_security_strategy.pdf.

The White House. *Guidance Regarding the Use of “Domain” in Unclassified and Public Statements.* draft memorandum, 14 March 2011.

United States Army. *Understanding Narrative: The Battle of the Narrative and the Operations Process*. Ft Meade, MD: Asymmetric Warfare Group, 2013.

U.S. Department of Defense. *Computer Network Defense*. Directive O-8530.1-M, December 2003.

U.S. Department of Defense. *Department of Defense Cyberspace Policy Report*. Washington, DC: Office of the Secretary of Defense, November 2011.

U.S. Department of Defense. *Department of Defense Strategy for Operating in Cyberspace*. Washington DC: U.S. Department of Defense, July 2011.

U.S. Department of Defense. *NETOPS for the Global Information Grid (GIG).* Instruction 8410.02, December, 2008.

U.S. Department of Defense. *Management of the Department of Defense Information Enterprise.* Directive 8000.01, February, 2009.

U.S. Department of Defense. *Secretary of Defense Memorandum, Establishment of a Subordinate Unified US Cyber Command Under US Strategic Command for Military Cyberspace Operations (U).* Washington, DC: U.S. Department of Defense, December 2006.

U.S. Department of Defense. *Department of Defense Strategy for Operating in Cyberspace*. Washington DC: U.S. Department of Defense, July 2011.

U.S. Joint Chiefs of Staff. *Cyberspace Operations*. Joint Publication 3-12. Washington, DC: Doctrine for the Armed Forces of the United States, February 2013.

U.S. Joint Chiefs of Staff. *Information Operations*. Joint Publication 3-13. Washington, DC: Doctrine for the Armed Forces of the United States, February 2006.

U.S. Joint Chiefs of Staff. *Joint Operations*. Joint Publication 3-0. Washington, DC: Doctrine for the Armed Forces of the United States, 11 August 2011.

U.S. Joint Chiefs of Staff. *Joint Communications Systems*. Joint Publication 6-0. Washington, DC: Doctrine for the Armed Forces of the United States, June 2010.

U.S. Joint Chiefs of Staff. *National Military Strategy for Cyberspace Operations*. Washington, DC: Doctrine for the Armed Forces of the United States, December 2006. http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-023.pdf.

Secondary Materials

Alexander, Keith B., "Warfighting in Cyberspace." Joint Forces Quarterly, no. 46 (3rd Quarter 2007).

Center for Naval Analyses, Support to the Cyber Task Force: Cyberspace Operations Workforce Development: Arlington, VA. https://www.dtic.mil/DTICOnline/downloadPdf.search?collectionId=tr&docId=ADB408931

Clausewitz, von Carl. *On War,* edited with an introduction by Anotal Rapoport. London, England: Penguin Books, 1982.

Cowie, James. "Internet Infrastructure: Virtual Meets Reality." PowerPoint presentation. renesys, MORE-IP, Amsterdam, 23 May, 2013.

Elliott, Michael C., "Operational Command and Control of Joint Task Force Cyberspace Operations." (research paper, Newport, RI: U.S. Naval War College, Joint Military Operations Department, 2008).

Gates, Robert M. *Establishment of a Subordinate Unified U.S. Cyber Command Under U.S. Strategic Command for Military Cyberspace Operations,* Secretary of Defense Memorandum. Washington, DC: Department of Defense, 2009.

Huntington, Samuel. *The Soldier and the State*. Cambridge, Massachusetts: The Belknap Press of Harvard University Press, 1985.

Lewis, Michael. *Flash Boys*: *A Wall Street Revolt*. New York, NY: W.W. Norton and Company, 2014.

Laity, Mark. "NATO and the Power of the Narrative." In *Information at War: From China's Three Warfares to NATO's Narratives.* London: Legatum Institute, 2015.

Lessig, Lawrence. *Code Version 2.0.* New York, NY: Basic Books a member of the Perseus Books Group, 2006.

Murphy, Dennis M. "Attack or Defend: Leveraging information and Balancing Risk in Cyberspace." Military Review (May-June 2010): 88-96.

Nissen, Thomas E. "Social Media, Cross-Media, and Narratives." In *#TheWeaponizationofSocialMedia @Characteristics_of_Contemporary_Conflicts.* Copenhagen: Royal Danish Defense College, 2015.

Reveron, Derek S., ed. *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World.* Georgetown University Press, 2012. Pp. 246.

Singer, Peter and Alan Friedman. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. New York: Oxford University, 2014.

Springer, Paul J. *Cyber Warfare*. Santa Barbara, CA: ABC-CLIO, 2015.

The Department of Defense. *The DoD Cyber Strategy.* Washington, DC: Office of the Secretary of Defense, April 2015.

Zalman, Amy. "A Battle of Narratives." *IO Journal, Vol 2, Issue 3* (August 2010): 3-10.