REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
04/20/2017	Master's Thesis	SEP 2016 - APR 2017

4. TITLE AND SUBTITLE
Electronic Warfare and Cyberspace Operations: Coordination, not Convergence

5a. CONTRACT NUMBER
N/A

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
N/A

6. AUTHOR(S)
O'Shea, Devlin, R., Major, USMC

5d. PROJECT NUMBER
N/A

5e. TASK NUMBER
N/A

5f. WORK UNIT NUMBER
N/A

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

8. PERFORMING ORGANIZATION REPORT NUMBER
N/A

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

10. SPONSOR/MONITOR'S ACRONYM(S)

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

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

13. SUPPLEMENTARY NOTES

14. ABSTRACT
The continued emergence of developing technologies and associated fields has stimulated conversation and exploration as to whether greater efficiencies and more effective procedures can result from the convergence of certain EW and CO practices. The subject of converging (EW) and (CO) has achieved some resonance across the Department of Defense (DOD) since there are tangible, inextricable connections between the two fields. In evaluating the relative merits of convergence versus coordination, the actions performed in EW and CO should be judged by the same criteria as those actions performed in other combined arms in support of the GCE.

15. SUBJECT TERMS
Electronic Warfare; Cyberspace Operations; Convergence

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
					19b. TELEPHONE NUMBER *(Include area code)*
Unclass	Unclass	Unclass	UU	42	(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:

Electronic Warfare and Cyberspace Operations: Coordination not Convergence

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

AUTHOR:

Major Devlin O'Shea

AY 16-17

Mentor and Oral Defense Committee Member: MATTHEW F
Approved:
Date: 4/20/17

Oral Defense Committee Member: T W Bordas
Approved:
Date: 4/20/17

Executive Summary

Title: Electronic Warfare and Cyberspace Operations: Coordination, not Convergence

Author: Major Devlin O'Shea, United States Marine Corps

Thesis: Electronic Warfare (EW) and Cyberspace Operations (CO) should not be converged due to the negative effects on operational functionality and the development and sustainment of the Marines in those two fields. The most effective method to maximize the effects of both EW and CO is through coordination not convergence.

Discussion: The continued emergence of developing technologies and associated fields has stimulated conversation and exploration as to whether greater efficiencies and more effective procedures can result from the convergence of certain EW and CO practices. The subject of converging (EW) and (CO) has achieved some resonance across the Department of Defense (DOD) since there are tangible, inextricable connections between the two fields. EW and CO continue to be associated with each other since both functions can produce complementary effects in support of the other's environment. Marine Forces Cyberspace Command (MARFORCYBER) is interested in exploring the possibilities surrounding a potential convergence. In evaluating the relative merits of convergence versus coordination, the actions performed in EW and CO should be judged by the same criteria as those actions performed in other combined arms in support of the GCE.

Conclusion: The Marine Corps's planned creation of the Marine Corps Expeditionary Force (MEF) Information Group (MIG) and Information Warfare Coordination Center (IWCC) are the most adept method of supporting synergy and coordination between EW and CO. It is fitting that the IWCC will be employed to ease operational decisions for the commander. This combined arms construct is logical. The IWCC will maximize effects in the information environment that are complementary to maneuver forces. Ultimately, the coordination provided by the IWCC will optimize the combined arms approach in support of operational decisions and tactical actions. Although a number of factors serve to provide convergence with a superficial appeal, a predictable lack of communication between staffs and units should not serve as a catalyst to merging these distinct disciplines.

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.

Table of Contents

Page

Preface

In this paper, I intend to respond to the Request for Information levied by Marine Forces Cyberspace Command and, more broadly, to address the greater argument surrounding how initiatives such as convergence should be evaluated. As a communications officer, I have witnessed myriad proposals for realignments, convergences, and integration of communication MOSs and, as a result, have developed a certain level of skepticism. I believe that we should always have a measured approach to evaluation of certain initiatives in order to prevent decisions that are unduly influenced by the rapid evolution of these operations and technologies. Along these lines, I did not become aware of the recently drafted "MAGTF Concept of Employment for Operating in the Information Environment" until February. I was exposed to this new information during a cyberwarfare class at Command and Staff College at Marine Corps University and then during a brief from the Marine Corps Information Operations Center (MCIOC). Thankfully, the order's changes align with the coordination not convergence thesis of my paper.

I am grateful to my Master of Military Studies mentor, Dr. Matthew Flynn, for his guidance and insightful advice throughout the process. I am also grateful for my Command and Staff College military faculty advisor, LTC Joseph Janczyk (USA), for his mentorship. Finally, I owe a debt of gratitude to my parents, John and Diane O'Shea, for all of their support and encouragement.

I. Introduction

The continued emergence of developing technologies in Electronic Warfare (EW) and Cyberspace Operations (CO) has stimulated conversation and exploration as to whether efficiencies and more effective procedures can result from the convergence of EW and CO practices. The subject of converging electronic warfare (EW) and cyberspace operations (CO) has achieved some resonance across the Department of Defense (DOD) since there are tangible, inextricable connections between the two fields. EW and CO continue to be associated with each other since both functions can produce complementary effects in support of the other's environment. Marine Forces Cyberspace Command (MARFORCYBER) is interested in exploring the possibilities surrounding a potential convergence. However, EW and CO should not be converged due to the negative effects on operational functionality and the development and sustainment of the Marines in those two fields. The most effective method to maximize the effects from both EW and CO is through coordination not convergence. The actions performed in EW and CO should be viewed no differently from the actions performed in other combined arms in support of the ground combat element (GCE). Convergence provides an appealing theoretical framework, but in practice will most likely result in diminished capabilities.

The arguments for converging EW and CO generally focus on two of the three aspects of CO, offensive cyber operations (OCO) and defensive cyber operations (DCO). DOD Information Network (DODIN) operations are consistently ignored in these proposals and therefore render the convergence argument incomplete. Defensive and offensive cyber operations and the use of the electromagnetic spectrum should be closely coordinated but not converged into one entity. The *Marine Corps Operating Concept* discusses the necessity for synergy between these two approaches and how the Marine Corps must further develop its policy and practices regarding these areas.[1] The Commandant, General Neller, during a February 2017

speech to the faculty and students of Marine Corps University identified five distinct capabilities that will be increased to better combat U.S. adversaries. EW and CO were listed separately, thereby demonstrating a clear division between them and the intent that they remain separate capability sets.[2] These two entities are continuing to mature as both friendly and enemy agencies operate within them with greater regularity. EW occurs in the space, land, air, and sea domains, while CO is executed in the fifth domain that is cyberspace but frequently impacts the other four domains. These two distinctly different military operations demand specialized experts in each field to maintain superiority and produce effective results. The convergence of EW and CO could result in force manning issues and a potential loss of expertise in each field. The combination of these two unique fields may serve as a catalyst for significant changes to the Military Occupational Specialty (MOS) structures and ultimately for the dilution of the Marines' technical proficiencies, resulting in a loss of capability. Technological advancement does create proximity in these two fields but they still have distinct differences. EW impacts the transmission aspect of communications while CO focuses on architecture on either side of the transmission path.

II. Literature and Source Review

The sources utilized for this paper mainly consist of joint publications, articles describing current events involving the fields, and professional journal articles. Joint Publication 3-12 (R) Cyberspace Operations is a critical doctrinal document that outlines how the U.S. military conducts operations in cyberspace. This document's importance is based upon its relevance as the governing document for all US military interactions with friendly and enemy forces in the fifth domain. It clearly defines all relevant terms to provide a common understanding of the environment and what types of missions are available to execute. The three pillars of CO are

discussed in detail to illustrate the tremendous breadth of these mission sets. JP 3-12 (R) establishes the methods of utilization for CO with respect to other operations that are part of the joint planning process. Furthermore, this publication describes how the integration of CO into the broader planning process ensures the achievement of the commander's priorities. JP 3-12 (R) outlines fundamental principles of CO and how staffs across combatant commands and service components should coordinate with United States Cyber Command (USCYBERCOM) and other force providers. Ultimately, JP 3-12 (R) establishes the fundamental principles of CO.

Joint Publication 3-13.1 Electronic Warfare establishes the doctrine governing EW for the U.S. military. The publication quickly establishes that EW in one of the five core components of information operations and how to leverage this capability along with other aspects of information operations to achieve the most effective results. JP 3-13.1 describes the three facets of EW and how to utilize these different types of operations to attain broader objectives when incorporated in the joint planning process. An important aspect of this publication is its referencing cross-coordination between staff sections, particularly the J-2, J-3, and J-6. This is especially relevant to the themes of coordination and integration. Similarly to JP 3-12 (R), JP 3-13.1 establishes baseline principles to conduct EW operations in a joint environment to include allies and inter-agency partners.

Michael Senft's article titled "Convergence of Cyberspace Operations and Electronic Warfare Effects," published in *The Cyber Defense Review* addresses the relevant issue of converging disciplines in an attempt to produce greater effects and efficiencies. *The Cyber Defense Review* is a joint Army Cyber Institute and MARFORCYBER endeavor to provide a venue to discuss all aspects of cyberspace. An important cyberspace journals, it encourages discussion among academics, civilian professionals, and military practitioners. Senft's article

examines how the integration of EW and CO could increase the rate of success in achieving operational goals. Senft approaches his analysis from a joint perspective, but mainly focuses on the Army and Navy. He specifically speaks to the perceived Chinese and Russian integration of EW and CO under the overarching rubric of information warfare. Senft is not alone in his recognition of our adversaries' construct. Interestingly, he references the Marine Corps' Cyber Electronic Warfare Coordination Center as a desirable model for the other services to emulate. Senft's argument focuses on operational capabilities and, to some extent, command structure, but does not fully examine the personnel aspect of the proposed convergence.

The Army commissioned the 2013 Rand Corporation study titled "Redefining Information Warfare Boundaries for an Army in a Wireless World" to address its desire to systematically examine all operations linked to network operations. This publication focuses heavily on fleshing out doctrinal terms and concepts to better understand service roles and responsibilities. The authors delve deeply into the information environment and information warfare. In their construct, the disciplines of EW and CO are nested under information warfare. The chapters that specifically focus on EW and CO convergence provide a more in-depth examination than any other literature on the subject. The authors argue that operational gains will occur through the merger of the two disciplines. Also, the study does actually provide a general proposal of personnel mergers. That is critical because it is a routinely ignored aspect of convergence.

The *Handbook of Russian Information Warfare* published by the NATO Defense College provides valuable insight into the often-referenced Russian philosophy of EW and CO. This document is extremely relevant because it provides primary source information from Russian doctrine, as well as interpretation and analysis. Many authors who have examined EW and CO

frequently discuss Russia's framework for IW as a more streamlined and operationally effective process than that of the U.S. and its western counterparts. The handbook quickly demonstrates that the Russian thought process regarding IW is synergistic and acutely focused on producing effects that complement conventional efforts. This publication brings attention to the Russians' overall concept of IW employment but, it must be emphasized, does not truly advocate EW and CO convergence. The handbook describes combined arms coordination not mergers. Therefore, previous references to Russian practices require reevaluation for their accuracy in light of the handbook's analysis.

Cyber Electronic Warfare: Closing the Operational Seams by Matthew Poole and Jason Schuette published in the Marine Corps Gazette examines the relationship between the operations in the electromagnetic spectrum and cyberspace. The authors discuss the necessity for operational cohesion during the planning process and in execution. The article explains the construct of the cyber electronic warfare coordination center how it provided an effective means of coordinating with the fire support coordination center in the MAGTF Headquarters. The staff synergy resulting from this organizational model created more integrated planning among the G-sections and therefore created the conditions for greater effectiveness. The article clearly advocates for more integrated planning but recognizes the distinction between the subject matters experts' fields.

The draft "MAGTF Concept of Employment for Operating in the Information Environment (IE)," published by Marine Corps Combat Development and Integration, outlines the future creation of Marine Expeditionary Force (MEF) Information Groups and Information Warfare Coordination Centers (IWCC). The draft order explains how information warfare is a component of the more encompassing information environment operations (IE Ops) and how the

MIG will broaden and increase the cohesion of IW planning at the MEF level. The responsibilities of each subordinate unit are presented and the methodology of increasing staff interaction is described. It reflects ongoing efforts to better understand IW and CO effects on IW's evolution.

III. Cyberspace Operations

Cyberspace operations focus on objectives that reside in cyberspace, but also have the capability to affect actions across all of the domains. Cyberspace is the only domain that is not purely physical, unlike the other domains of air, land, sea, and space. The three facets of cyberspace are the physical network, logical network, and cyber persona. These three aspects of cyberspace must be understood in order to best prepare commanders for targeting options focused on key cyber terrain.

The physical network is the actual infrastructure that supports the internet and connections to various computers, servers, and other nodes. This layer is focused on geography and where the network transmits information. The physical layer crosses borders and depending the desired endpoint can rely on infrastructure that exists in multiple countries or continents. All equipment from the originating computer to the destination computers, to include all of the hardware, systems, and transmission systems comprise the physical network.[3]

The logical network is more abstract and refers to internet protocol addresses, websites hosted over different servers, and the active directory structure. These elements are the primary means of facilitating communications via the physical network. The Marine Corps Enterprise Network (MCEN) that hosts applications, active directory, and many web-based portals is an example of how the logical layer supports cyberspace operations.[4]

Cyber persona is the third and least physically tangible aspect of cyberspace. It is a person's or organization's presence and depiction on the internet. A cyber persona's level of detail and its likeness to the user employing it can greatly vary. A single individual may have multiple cyber personas. The degree of difficulty in targeting certain high value individuals is often related to their having multiple cyber personas. This construct is important since it provides perspective on the complexity of actors in this realm.

Military cyberspace operations are either offensive, defensive, or DODIN operations. OCO are bold in nature and apply force against adversaries. DCO focus on the protection of the network and elimination of potential vulnerabilities. DODIN operations revolve around the maintenance, sustainment, and improvement of the vast U.S. military network. When CO is discussed, DODIN operations are frequently overlooked but they play a vital role in the overall defense and preservation of the U.S. military network. State and non-state actors conduct thousands of attacks daily aimed at penetrating the DOD's network so it is vital that there is constant vigilance and continuous action being taken to mitigate vulnerabilities and bolster defenses.

Offensive cyberspace operations focus on aggressive action against adversarial targets. The objectives and execution of the orders are similar to those in the other domains. The military is not the only government agency that conducts OCO. In fact, due to differences between Title 10 and Title 50 of the U.S. Code, a significant amount of OCO falls outside of the DOD's realm. These laws, which were written long before the advent of cyberspace operations, should be amended in order to empower military forces to execute OCO missions. This will allow the military to seize the initiative with cyber targeting and not lose valuable time due to a reliance on intelligence officials with a myriad of competing priorities.[5] OCO is a capability set that is slowly becoming

more integrated in the joint targeting process. Operationally, the integration of these capabilities with more conventional, kinetic methods creates more synergy and effectiveness. The maturation of OCO calls for more parity with traditional targeting means in the processes and procedures. The definition of tiers and execution authority is an essential aspect of effective OCO.[6] OCO provides the force projection needed to establish a strong presence in cyberspace and create effects on the adversary's targets.

The 2008 Russian cyber-attack against Georgia provided a prime example of OCO and its employment with traditional kinetic measures. In August 2008, the Russian army engaged Georgian forces in South Ossetia. In the midst of this engagement, Russian cyber forces began Distributed Denial of Service (DDOS) attacks on Georgian media to prevent the Georgian public from becoming cognizant of the events as they were occurring.[7] The Russian efforts also halted all banking in Georgia for a period of several days. The Russian attack defaced official Georgian websites and proved to be a powerful complement to the actions against Georgian ground forces. This example illustrates how powerful OCO is and even more so when combined with actions in other domains. The Russians' ability to gain territory through conventional means combined with the disruption of the economy and degradation of official government websites deteriorated the Georgians' morale and will to fight.

Defensive Cyber Operations are a multi-faceted means of defending desired areas of a cyberspace. DCO protects infrastructure, data, systems, and interfaces. It actively counters illegal and unauthorized actions on the networks and then cooperates with intelligence activities to provide forensic information in an effort to determine the culprit. While the majority of DCO actions occur with the DODIN, there are certain actions taken to combat adversary OCO outside of the DODIN. The DOD's approach to DCO is similar to physical defenses. It relies on a multi-

tiered defense-in-depth that accounts for protection of the logical and physical infrastructure. Internal Defense Measures are the DCO activities that seek to identify threats within the DODIN and then to respond to the enemy action by stopping and quarantining the threat. DCO response actions are those maneuvers performed outside of the DODIN to directly counter an identified threat. Countermeasures are designed to reduce or eliminate a threat to the DODIN. These practices are not intended to cause significant harm or damage but are sharply focused on ending the threat from adversarial forces. This type of DCO must be in compliance with all rules of engagement (ROE) and domestic and international laws.[8] Countermeasures are a form of DCO that target potential threats through non-intrusion. These actions are similar to DCO response actions but are more proactive in nature. Countermeasures are not employed to cause destruction or loss of functionality. They specifically address malicious activity and cease once that activity has concluded. DCO's relation to EW is limited at best since most of the defenses and countermeasures are distinctly different actions than those performed for defense of the electromagnetic spectrum.

DODIN operations consist of the building, configuration, security, operation and maintenance of the DODIN.[9] The cybersecurity tenets of data confidentiality, integrity, and availability are paramount. Information Assurance and all aspects of user training is a critical component of successfully maintaining the security of the DODIN. The physical and logical security of the DODIN is critical and therefore requires constant updates and supplemental security measures. The Marine Corps and Department of Defense follow many principles of the private sector security with respect to DODIN operations and private industry's best practices influence and affect DODIN operations. For example, the DOD uses private sector patching methods and software updates to ensure vulnerability mitigation.

IV. Electronic Warfare

Electronic Warfare refers to military operations that target the electromagnetic spectrum (EM). EW is utilized to ensure friendly forces have freedom of navigation through the EW environment (EME) and also to deny the enemy's action in the EME. EW operations can originate from air, land, sea, and space through a variety of systems.[10] EW is considered to be one of five information operations (IO) core capabilities. Frequently, EW supports military deception (MILDEC). The degradation of the enemy's means to gather and process information greatly reduces his ability to perform key functions and also leads to miscalculations regarding friendly forces.[11]

There are three primary roles of EW in support of all military operations: electronic attack (EA), electronic protection (EP), and electronic warfare support (ES). EA are offensive and defensive actions taken to degrade or destroy enemy capabilities in the EME. Offensive actions are designed to pursue enemy vulnerabilities, while defensive actions prevent friendly vulnerabilities from being exploited.[12] EP focuses on actions required to deny the enemy any exploitable gaps in the EME. EP protects equipment, personnel, and facilities, and consists of spectrum management, EM hardening, and EM control. ES is directed by an operational commander to discover EM energy. The process of identifying adversarial EM activity is vital in the production of signals and signature intelligence.[13]

The electromagnetic environment consists of the full spectrum of frequencies and EM radiation. This spectrum begins with low radio frequencies and terminates with high range x-ray and gamma frequencies.[14] Electromagnetic environmental effects (E3) refers to the impact of EW on different military systems and equipment. This describes actions on all portions of EM to include EM compatibility (EMC), EM interference, EM vulnerability, EM pulse, electronic

protection (EP), and hazards of EM radiation.[15] EM compatibility refers to the method in which all devices or systems utilizing the EMS operate without degrading the other. The key tenet is preventing systems from interfering with each other while maximizing their effectiveness.[16] EM interference (EMI) is any disturbance or degradation that reduces electronic equipment's performance. This can be intentional or in many cases, it may be an accidental action due to a lack of spectrum de-confliction. EM vulnerability is the collective aspects of a system that make it susceptible to EW and therefore unable to effectively execute its tasks. EM pulse is the source of EM radiation that causes current and voltage surges.[17] Electronic protection is an EW mission designed to prevent friendly facilities, personnel and equipment from harmful EMS effects. Finally, EM radiation hazards are those detrimental effects caused by coming too close of a proximity to an antenna or transmitter.[18] EM effects are an essentially planning factor since they can ultimately degrade and disrupt operations in the EMS that will lead to mission failure.

EW is employable and effective through all of the phases of campaigns and produces effects at the tactical, operational, and strategic levels. Tactically, EW can degrade systems such as radar. At the operational level, EW prevents the massing of forces, and strategically, EW confuses and blurs the senior leaders' vision of what is occurring.[19] Further aspects of EW include control, detection, denial, deception, disruption and degradation, protection, and destruction. EMS control integrates the management of friendly systems, the degradation of the enemy's use of EMS, and the facilitation of the commander's estimate of the situation. Detection is the scanning and assessing of all threats across the spectrum. This is a critical capability that serves as the foundation for all follow-on EW activities.[20] Denial is the process of preventing the enemy from gaining information. This is generally accomplished through a multi-dimensional degradation of enemy systems. Deception is achieved through EMS disruption that creates confusion and obstacles in

the enemy's decision making cycle. Disruption and degradation reduce the enemy's capabilities through different actions in the EMS. These techniques can range from mild interference to severe capability loss and infrastructure degradation.[21] Protection is a broad term that defines all actions to include tactics, techniques, and procedures that enable friendly use of the EMS. This aspect of EW requires joint coordination and deconfliction of efforts and generally responsible use of the EMS and frequency management. EW destruction is the reduction of the enemy's system to a level of non-functionality. There are a multitude of ways to destroy an enemy's EW capability from conventional systems to cyber-attacks.[22]

In doctrine and practice, EW is closely associated with both network operations and information operations. The Global Information Grid (GIG) hosts cyberspace operations and all network operations. EW can directly impact the functionality of operations on the GIG by targeting the methods of transmission. Wireless links and satellite transmissions require use of the EMS and therefore can be susceptible to attack. The coordination between EW operations and network operations is a crucial aspect of overall defense.[23] EW, as a core component of IO, determines IO success via offensive and defensive operations. The enabling of friendly undeterred movement across the EMS and engagement of enemy EMS actions demonstrate EW's effects in support of IO.

EW is comprised of several principle activities. Countermeasures are active or passive electro-optical-infrared or radio frequency responses to enemy actions that suppress or stymie enemy actions. Electromagnetic deception consists of manipulative, simulative, and imitative means of confusing the enemy. The enemy's capabilities are degraded through misinformation that may be manifested through false EM footprints or simulations to create a false operational picture for the enemy.[24] Electromagnetic intrusion and jamming both employ EM energy to

degrade the enemy. Intrusion is more deception oriented, while jamming is directly focused on capability reduction. Electronic masking controls friendly emissions to prevent enemy detection and probing is the release of radiation into enemy systems to acquire knowledge of the capabilities. Electronic reconnaissance is similar to traditional reconnaissance in that its goals are to detect and locate the enemy to provide further assessments of capabilities.[25] Spectrum management describes the administrative and planning procedures associated with an organization so that it may optimize use of the EMS and limit its vulnerabilities.

The convergence of EW and CO has been discussed for several years in the U.S. and international defense communities. The Joint audience continues to examine efficiencies that can be gained through converging the two fields. Convergence is a term that is frequently used but it is rarely clearly defined. In most cases, those making the argument for convergence define the term as integration and elimination of any excess or overlapping capabilities. The vast majority of arguments for convergence of CNO and EW focus on OCO and EW. The combined effects stem from OCO and not from DCO or DODIN operations.

V. EW and CO Interoperability

CO and EW both provide tremendous offensive and defensive options, especially when used in conjunction with one another. While the definitions of CO and EW differ, the foundations of each have some similarities. Both disciplines have attack or offensive, protective or defensive, and support operations that seek to accomplish similar goals. These analogous, but not identical, components in EW and CO are often falsely equated through oversimplification. Offensive, protective or defensive, and support operations can implicate multiple fields in the Marine Corps and therefore caution should be exercised in making statements that depict EW and CO as entirely analogous or equivalent. The Open Source Interconnection (OSI) Model has seven layers and CO

traverses all seven.[26] Early EW primarily only operated in the first layer which is the physical connection. This is no longer the case as EW intrusion and jamming now are Internet Protocol (IP)-based. In "Convergence of Cyberspace Operations and Electronic Warfare Effects" Michael Senft references three case studies that demonstrate the necessity for CO and EW convergence. The first example refers to a tactical IP over radio system that was effectively jammed with low-levels of power. This effectively created confusion regarding the inability to transmit since there were network security measures established. The operators believed that this was in fact a system error and not a transmissions error due to jamming. The second case was an exercise where OCO and EW were employed together to attack a satellite communications network. The OCO was able to penetrate and determine the location of the satellite terminal which was subsequently jammed via EW. The third example was an attack on a mesh network that resulted in severe degradation to the point where the network operators could not determine whether they were experiencing jamming or a denial of service attack.[27] These examples illustrate the enhanced effects of CO and EW when they are employed together as combined arms. The examples display synergy between the two practices that are clearly relatable to traditional targets. For instance, the aforementioned attack on the satellite terminal that was detected through CO and then jammed through EW is comparable to a reconnaissance team discovering the location of an enemy target and then calling for either artillery or aerial delivered munitions. Both instances illustrate a close coordination of combined arms, not convergence. Senft concludes his arguments for convergence by citing the Marine Corps as a prime example of success through the Cyber Electronic Warfare Coordination Centers (CEWCC). CEWCCs were entities that integrated CO, EW, signals intelligence, spectrum management operations, and technical information operations. They were further integrated with

traditional combined arms, fire, and maneuver.[28] The CEWCC provided an entity that sought seamless EW and CO planning and execution in support of larger combined arms efforts.

VI. EW And CO Employment

Discussions of the relationship between CO and EW focus mostly on OCO. Of the three aspects of CO, it is OCO that is featured prominently, if not exclusively, when discussing integration with EW. However, OCO can only be authorized at the strategic level while the employment of EW can be approved by a tactical commander.[29] If there were a convergence, this lack of parity between the EW and CO authorities could potentially create a great deal of confusion. The full blending of EW and CO would create a conundrum for a commander in which his or her staff would be forced to determine the lines of demarcation. This certainly would not stifle OCO but might very well prove to be an impasse for what was once considered routine EW.

Furthering the notion that there are overlaps for potential convergence in EW and OCO is the utilization of digital means in both fields. The U.S. Army references digital means in doctrinal definition of a cyber-attack as, "actions that combine computer network attack (CNA, an element of Cyberwar) with other enabling capabilities (e.g., electronic attack—EA, an element of EW, physical attack; etc.) to deny or manipulate information and/or infrastructure in cyberspace."[30] The Army defines EW as "any military action involving the use of EM energy to control the EMS or to attack the adversary." These definitions point to an interrelatedness of both CO and EW. The Army's TRADOC Combined Arms Center continues to explore this phenomenon. Furthermore, TRADOC espouses the view that as technology and the means of communication become less distinguishable so will traditional barriers in CO and EW.[31] CO and EW converge at the operational level with respect to resources and capabilities. The convergence arguments presented

by the U.S. Army are very equipment and capability centric and do not fully address the shift in training, equipping, and manning that would be required.

VII. Russia's IW Model

CO and EW convergence is not unique to the United States and other nations are either already implementing or actively examining it. The 2016 Armed Forces Communications and Electronics Association (AFCEA) TechNet Conference in August provided a forum for an extensive discussion regarding CO and EW convergence with Russia's IW activities during its offensive against Georgia being cited as an example of success. The U.S. Army Cyber Center of Excellence presented how Russia has integrated its EW and CO capabilities to locate the enemy, disrupt its communications, and then attack with kinetic means.[32] The Russians' ability to synergize different types of intelligence and benefit from the effects have become a significant U.S. concern. As previously mentioned, Russia has employed combined EW and CO against Georgia and also has demonstrated success against the Ukraine. This presents a serious concern for the U.S. and invites the idea that the U.S. must build similar force and capability structure to best combat these threats. The lack of parity with Russia must be reduced and eliminated if the U.S. is to prevail according to senior Army cyber leaders.[33]

The notion that Russia is converging EW and CO is not entirely accurate. The Russians do not think in the same terms as the U.S. and its western allies with respect to CO and EW. Russia never focused on EW, CO, psychological operations, or signals intelligence as separate entities. Instead, it determined that these are all components of information warfare (IW). Russia focuses on employment of IW during all phases of conflict, especially during times of peace. The Russians place a premium on this type of engagement with adversaries due to its relatively low cost compared to conventional arms, as well as its overall effectiveness.[34] Russian doctrine does not

mention cyberspace or cyber warfare unless referring to western concepts. The Russians focus on information space and more specifically information-technical or technology and information-psychological domains. Information-technology warfare is defined as operations "to affect technical systems which receive, collect, process and transmit information, which is conducted during wars and armed conflicts." Information-psychological warfare is designed "to affect the personnel of the armed forces and the population, which is conducted under conditions of natural competition."[35] These two types of warfare are considered to be similar in this Russian model of IW. The Russians view a traditional cyber-attack in the same vein as the distribution of misinformation.

While on the surface, the Russian model of IW and its subsets appear to provide a strong argument for EW and CO convergence, this is not the case. The Russian IW model is not one of convergence but close-coordination under an overarching doctrine. The synergy of EW, CO, psychological operations, etc. is due to the Russian philosophy of combined arms. These entities that comprise IW still maintain distinct disciplines with specific, function-related tasks. The most important lesson that the U.S. should learn from the Russian model is how to produce doctrine that is more encompassing and with fewer parochial divisions. Such an approach, rather than converging the components, will create the conditions for a vast improvement in coordination and multiplication of effects. It is also worth noting that many of the discussed Russian successes are directly related to different rules of engagement and morality.[36] The totalitarian government's consistent targeting of other nations' private and state-owned business entities and its dissemination of misinformation on a vast scale via agencies of the Russian state are simply not tenable for the U.S.

VIII. Convergence Fallacy

In 2013, the Rand Corporation published an analysis for the U.S. Army titled "Redefining Information Warfare Boundaries for an Army in a Wireless World." This study frames the overarching problem as the lack of current doctrinal definition for Information Warfare. The argument for redefining terms and deconflicting joint doctrine is relatively sound but Rand's proposed model is eerily similar to the Russian model of IW. The authors propose that information operations be divided into two categories: information technical operations and inform and influence operations. EW and CO are the components of information technical operations while inform and influence operations are comprised of military information support operations (MISO) and military deception (MILDEC).[37] The study advocates consolidation in the technical realm, espousing the argument that EW's EA and EP are becoming closer to CO's OCO and DCO. The authors posit that certain types of EW attacks that are digital can be more closely aligned with OCO due to equipment overlaps. Furthermore, the study argues that EW and CO could, "and perhaps should share the same people, process, and technologies to carry out these operations to avoid duplication of effort or working at cross-purposes."[38] The study contends that spectrum personnel assigned to EW and spectrum managers normally assigned in communications units could be merged.

Both of these merger proposals grossly oversimplify these service members' responsibilities and the ease of convergence. The improvement of targeting processes is a valid goal but the argument that OCO personnel and EA personnel could be consolidated is unpersuasive. The scope of OCO exceeds that of EA and therefore broader skillsets are required for EA personnel to merge with cyber personnel. For instance, spectrum managers are responsible for ensuring friendly communications throughout the EMS. If they were to be merged with EA personnel in the spectrum field, the scope of their responsibilities would be unmanageable. The

study concludes there could be manpower gains in efficiency via cross-training. While speaking in Army doctrinal terms vice Joint doctrine, the authors essentially concede that there are limitations to what can be consolidated when addressing OCO, DCO, and DODIN operations.[39] This conclusion demonstrates the inherent complexities of consolidating responsibilities and the true breadth of CO.

IX. Coordination not Convergence

The convergence of CO and EW in the Marine Corps will not be a force multiplier or a gain of efficiency. These two fields have similarities and overlapping aspects, but ultimately are independent from one another. A complete convergence of CO and EW would convolute mission sets and reduce the expertise of those executing the missions. The Marine Corps' establishment of Command and Control (C2) and Cyber and EW Integration Division (C2/CEWID) and CEWCCs were a preliminary step in the process of addressing integration. The operative word for CO and EW should be coordination not convergence.[40] The education of staffs in how best to maximize planning from multiple fields is the most appropriate way forward for the Marine Corps. Furthermore, most convergence arguments focus solely on OCO and EW. It is important to recognize that by not addressing DCO and DODIN operations, the argument is incomplete since the majority of CO is being ignored. DCO and DODIN operations are constant in nature and require forces dedicated specifically to those missions. OCO is the one aspect of CO that should be most closely coordinated with EW. The "MAGTF Concept of Employment for Operating in the Information Environment" draft order applies the CEWCCs theme of coordination to a broader level across all facets of the MAGTF staff. The order correctly frames information as one of the four pillars of national power and describes how IE Ops and IW conducted by the military will support that pillar of power.[41] The IE spans the strategic through tactical levels and IE Ops focuses

on the strategic and operational levels. EW is described as a facet of electromagnetic spectrum operations along with electromagnetic spectrum management. The three lines of operations (LOOs) for CO align with those described in JP 3-12 (R): DODIN operations, DCO, and CO. There is a critical acknowledgement that the MAGTF will be primarily focused on DODIN operations and DCO.[42] The proposed creation of the MIG presents a more operationally focused organization equipped with the necessary staff and subordinate commands to conduct holistic IW planning. The IWCC will provide an organization that is well-equipped to maximize EW and CO through the inclusion of subject matter experts from the CO, EW, and electromagnetic spectrum management fields. The G-3 will have operational control of the IWCC which will allow lateral and intra-G-3 coordination with the Combat Operations Center (COC) and Force Fires Coordination Center (FFCC). The G-2 will retain control of the Intelligence Operations Center (IOC), and the G-6 will still be responsible for the MAGTF Communications Control Center (MCCC).[43] The formulization of these coordination and control relationships creates the necessary structure and guidance to vastly improve EW and CO coordination in support of MAGTF IW operations. This draft order supports the status quo with respect to occupational specialties while facilitating the requisite staff coordination for more synergistic operations.

Furthermore, the differences in how CO and EW are conducted and what domains they reside in are important when determining the feasibility of convergence. EW affects CO at the transport layer of the OSI model and therefore is effective, especially with the growing dependence on wireless transmission. Even with EW's greater reliance on digital technology, most CO do not affect EW capabilities. Since the emergence of technologies that operate in the EME over the last century, there has not been a call to converge other land, sea, air, or space based practices with EW. The same type of logic would apply to merge operations in the four other domains with EW.[44]

X. Effects on the Force

The arguments for CO and EW convergence generally overlook or only briefly depict the requisite force structure and personnel changes. The implementation of a significant training overhaul would be the only means to facilitate the creation of Marines who perform both EW and cyber functions. The structure of the MOSs in both fields would have to be redefined and then the appropriate changes to training platforms from entry level training through the continuum would be required. Any combination of signals intelligence MOS and Cyber MOS would almost certainly create a Marine who is less proficient in each specialty and no longer a subject matter expert. The effects of diluted MOSs and reduced skill sets would have first and second order effects that could prove crippling to the Marine Corps. Currently, EW falls under the signals intelligence field and is performed by enlisted Marines possessing several different MOSs which include Cryptologic Digital Network Operator/Analyst, Special Communications Signals Collection Operator/Analyst, Signals Intelligence Analyst, Electronic Intelligence (ELINT) Intercept Operator/Analyst, and Special Intelligence System Administrator/Communicator.[45] Cyber Network Operator and Cyber Security Technician are the two MOSs that account for CO and are part of the communications field.[46] The Special Intelligence System Administrator/Communicator has traditionally been comparable to the Cyber Network Operator and is actually permitted to request a lateral move to become a Cyber Security Technician. However, there are more technical prerequisites to become a Cyber Network Operator. The skills required for all of these MOSs are different and it is inconceivable to consider any MOS mergers. The breadth of tasks reflected in the Training and Readiness Manual for each MOS is too great to condense without losing mission-critical proficiencies.

Furthermore, Cyber Marines are not assigned permanently and exclusively to OCO

operations, DCO operations, or DODIN operations, but instead will perform all of these functions throughout their careers. Cyber Marines will inevitably perform all of these functions throughout their careers. The Marine Corps would be accepting tremendous risk if these MOSs were to be converged with signals intelligence MOSs. The creation of a hybrid MOS would detract from the proficiency of current MOSs and create a rift in the cyber community. This new MOS would be responsible for OCO and EW but would lack the knowledge of DCO and DODIN operations and therefore contribute to a lack of cohesion. Currently, retention of cyber Marines is a vexing problem for the Marine Corps and to degrade the capability of the MOS skill set would hurt not only retention but certainly recruiting as well.

XI. Conclusion

The examination of converging the disciplines of EW and CO varies depending on the authors but has attracted an international audience. As technology continues to create certain efficiencies, many are drawn to oversimplification and the desire to merge different practices in order to achieve some type of perceived advantage. The arguments for the convergence of EW and CO generally do not adequately define convergence and at times espouse coordination instead. EW and CO do have some overlapping areas but are clearly two different fields that cannot merely be merged together. The vast majority of the arguments for convergence briefly discuss DCO, omit DODIN operations, and heavily focus on OCO and EW. These omissions greatly detract from the credibility of these proposals. Furthermore, many of those positing that convergence will create greater operational gains provide neither sufficient detail as to what the newly formed cadre or organizations will look like nor specifics as to how such a reorganization will be achieved.

The focus on EW and CO asymmetry with our rivals, specifically Russia is valid to a certain degree. The Russian construct is less doctrinally divided than that of the U.S. but the Russian practices of EW and CO do not meet the threshold of convergence. Instead, they embody a closely coordinated and integrated combined arms approach in support of IW and conventional actions. The U.S. and joint community should pursue deconflicting the multiple doctrines that create unnecessary divisions but should not go beyond that point. The draft "MAGTF Concept of Employment for Operating in the Information Environment" provides the Marine Corps's attempt to eliminate historical divisions in doctrine and provide a model for the functional integration of IW's components.

Finally, one of the most glaring omissions from most arguments for convergence is any serious analysis of personnel and force structure. The "who and how" aspects of this argument are left untouched and that creates great uncertainty. The differences in the various areas of specific expertise of the Marines who operate in the EW and CO specialties absolutely must be acknowledged and addressed before these arguments for convergence can be developed beyond general, broad brush concepts.

The draft "MAGTF Concept of Employment for Operating in the Information Environment" is the most appropriate method of supporting synergy and coordination between EW and CO. Ultimately, the coordination provided by the IWCC will optimize the combined arms approach in support of operational decisions and tactical actions and it will substantially provide the putative benefits of convergence without risking the destructive disruption convergence would entail. There are many factors that drive the proponents of convergence but lack of communication between staffs and an inability to coordinate should not serve as a catalyst to merging distinct disciplines.

Endnotes

[1] Headquarters United States Marine Corps, Marine Corps Operating Concept (Washington, DC: Department of the Navy, September 2016), 24.

[2] Robert Neller, "Marine Corps University Address on Seize the Initiative" (speech, Marine Corps University, Quantico, Virginia, February 15, 2017).

[3] U.S. Department of Defense. Cyberspace Operations. JP 3-12(R). (Washington, DC: U.S. Department of Defense, February 5, 2013), I-2.

[4] Ibid, I-3.

[5] Vincent Manzo, "Deterrence and Escalation in Cross-domain Operations: Where do Space and Cyberspace Fit?," Joint Force Quarterly (3rd Quarter, July 2012), 23.

[6] Ibid, 25.

[7] Richard A. Clarke and Robert K. Knake. *Cyber War: The Next Threat to National Security and What to Do About it.* (New York: Ecco, 2010), 19.

[8] U.S. Department of Defense. Cyberspace Operations. JP 3-12(R). (Washington, DC: U.S. Department of Defense, February 5, 2013), II-3.

[9] Ibid.

[10] U.S. Department of Defense. Electronic Warfare. JP 3-13.1. (Washington, DC: U.S. Department of Defense, February 8, 2012), v.

[11] Ibid, x.

[12] Ibid, I-3.

[13] Ibid, I-4.

[14] Ibid, I-3.

[15] Ibid, I-4.

[16] Ibid, GL-7.

[17] Ibid, GL-8.

[18] Ibid.

[19] Ibid, I-6.

[20] Ibid, I-5.

[21] Ibid, I-6.

[22] Ibid.

[23] Ibid, I-7.

[24] Ibid, I-9.

[25] Ibid, I-10.

[26] Michael, Senft. "Convergence of Cyberspace Operations and Electronic Warfare Effects." *The Cyber Defense Review* (2016): 3.

[27] Michael, Senft. "Convergence of Cyberspace Operations and Electronic Warfare Effects." *The Cyber Defense Review* (2016): 4.

[28] Ibid, 5.

[29] Ibid.

[30] Isaac R. Porche III et al. "Redefining Information Warfare Boundaries For an Army in a Wireless World." (Rand Corporation. 2013), 49.

[31] Ibid, 50.

[32] George Seffers. "Russia Converges Electronic Warfare, Cyber Operations." *Signal*. (2016).

[33] Ibid.

[34] Keir Giles. *Handbook of Russian Information Warfare.* (Rome: NATO Defense College, 2016), 4.

[35] Ibid, 9.

[36] Ibid, 68.

[37] Isaac R. Porche III, Christopher Paul, Michael York, Chad C. Serena, Jerry M. Sollinger, Elliot Axelband, Endy Y. Min, Bruce J. Held. "Redefining Information Warfare Boundaries For an Army in a Wireless World." (Rand Corporation, 2013), xxi.

[38] Ibid, xxiii.

[39] Ibid, 68.

[40] Marine Corps Combat Development and Integration & Marine Corps Combat Development Command. *Command Brief.* (August 2014.), PowerPoint Presentation.

[41] Marine Corps Combat Development and Integration & Marine Corps Combat Development Command. *MAGTF Concept of Employment for Operating in the Information Environment*. Draft Order, February 22, 2017, 4.

[42] Ibid, 8.

[43] Ibid, 11.

[44] Knowles, John. "Why Two Domains Are Better Than One." *The Journal of Electronic Defense.* (2013): http://www.ecrow.org/assets/mayjed_twodomainsarebetter.pdf .

[45] Commandant of the Marine Corps, Military Occupational Specialties Manual (Short Title: MOS Manual). MCO 1200.17E, August 8, 2013, 3-121, http://www.marines.mil/Portals/59/MCO%201200.17E.pdf.

[46] Ibid, 3-111.

Bibliography

Clarke, Richard A., and Robert K. Knake. *Cyber War: The Next Threat to National Security and What to Do About it.* New York: Ecco, 2010.

Commandant of the Marine Corps, *Military Occupational Specialties Manual (Short Title: MOS Manual).* MCO 1200.17E, August 8, 2013. http://www.marines.mil/Portals/59/MCO%201200.17E.pdf

Farwell, James P. and Rohozinski, Rafael, *Stuxnet and the future of cyber war*, Survival, 2011.

Giles, Keir. *Handbook of Russian Information Warfare*. Rome: NATO Defense College, 2016.

Gould, Joe. "Electronic Warfare: What US Army Can Learn From Ukraine." *Defense News.* (2015).

Headquarters United States Marine Corps. *Marine Corps Operating Concept*. Washington, DC: Department of the Navy, September 2016.

Janczewski, Lech; Colarik, Andrew M. *Cyber Warfare and Cyber Terrorism* IGI Global (2008).

Knowles, John. "Why Two Domains Are Better Than One." *The Journal of Electronic Defense,* (Vol. 36, Issue 5 May 2013), 48.

Laird, Robbin. "C2 Modernization: An Essential Element For 21st Century Force Structure Innovation." *Second Line Defense.* (2016).

Lynn, William J. III. "Defending a New Domain: The Pentagon's Cyberstrategy", *Foreign Affairs*, Sept/Oct. 2010, pp. 97–108.

Manzo, Vincent, "Deterrence and Escalation in Cross-domain Operations: Where do Space and Cyberspace Fit?," Joint Force Quarterly (3rd Quarter, July 2012), 16-25.

Marine Corps Combat Development and Integration & Marine Corps Combat Development Command. *Command Brief*. PowerPoint Presentation. August 2014.

Marine Corps Combat Development and Integration. *MAGTF Concept of Employment for Operating in the Information Environment*. Draft Order, February 22, 2017.

Neller, Robert. "Marine Corps University Address on Seize the Initiative." Speech. Marine Corps University, Quantico, Virginia, February 15, 2017.

Poole, Matthew & Schuette, Jason, "Cyber Electronic Warfare: Closing the Operational Seams." *Marine Corps Gazette,* (Vol. 99, Issue 8 August 2015), 60-63.

Porche III, Isaac R., Christopher Paul, Michael York, Chad C. Serena, Jerry M. Sollinger, Elliot Axelband, Endy Y. Min, Bruce J. Held. "Redefining Information Warfare Boundaries For an Army in a Wireless World." Rand Corporation. 2013.

Rid, Thomas. *Cyber War Will Not Take Place.* United Kingdom. C. Hurst & Co. 2013.

Seffers, George. “Russia Converges Electronic Warfare, Cyber Operations.” *Signal*. (2016):

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

"Cyberwar: War in the Fifth Domain" *Economist*, 1 July 2010.

J.R. Wilson, “Not Your Old Timer’s Electronic Warfare.” *Military &Aerospace Electronics,* (Vol. 26, Issue 8 August 2015), 8.

U.S. Department of Defense. Cyberspace Operations. JP 3-12 (R). Washington, DC: U.S. Department of Defense, February 5, 2013.

U.S. Department of Defense. Electronic Warfare. JP 3-13.1. Washington, DC: U.S. Department of Defense, February 8, 2012.