REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
05-09-2018	Master's of Military Studies	Sep 2017 - Apr 2018

4. TITLE AND SUBTITLE

THE MARINE EXPEDITIONARY UNIT INFORMATION SECTION: ESTABLISHING INFORMATION SUPERIORITY AT THE TACTICAL LEVEL AND BEYOND

5a. CONTRACT NUMBER
N/A

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
N/A

6. AUTHOR(S)
O'Melia, Christopher, 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)
Dr. Richard Dinardo

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 operationalization of the information environment by belligerent states and threat actors across the range of military operations has violated individual and state sovereignty around the world. The enemy has gained the initiative seizing key terrain within the global network of information systems. A strong reactive defense can no longer be the standard to preserve US national security within the information environment. If the United Stated is to dominate within the information environment, it must train, man, equip, and employ the Marine Expeditionary Unit to establish regional information superiority within geographic combatant commands. The 21st century MAGTF must operationalize the information environment and employ all capabilities within, as a supporting arm to achieve physical and cognitive advantage thereby preserving US national security and sovereignty.

15. SUBJECT TERMS

Information Environment Operations; MEF Information Group; Cyber Warfare; Information Warfare; Marine Expeditionary Unit

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**	UU	28	USMC Command and Staff College
Unclass	Unclass	Unclass			**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:
THE MARINE EXPEDITIONARY UNIT INFORMATION SECTION: ESTABLISHING INFORMATION SUPERIORITY AT THE TACTICAL LEVEL AND BEYOND

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

AUTHOR:
MAJOR CHRISTOPHER J. O'MELIA
UNITED STATES MARINE CORPS

AY 2017-18

Mentor and Oral Defense Committee Member: Richard L. DiNardo
Approved: Richard L. DiNardo
Date: 9 May 2018

Oral Defense Committee Member: Matthew Fegan
Approved: Matthew Fegan
Date: 9/May/2018

EXECUTIVE SUMMARY

Title: The Marine Expeditionary Unit Information Section: Establishing Information Superiority at the Tactical Level

Author: Major Christopher O'Melia, United States Marine Corps

Thesis: If the United Stated is to dominate within the information environment, it must train, man, equip, and employ the Marine Expeditionary Unit to establish regional information superiority within geographic combatant commands. The 21st century MAGTF must operationalize the information environment and employ all capabilities within, as a supporting arm to achieve physical and cognitive advantage thereby preserving US national security and sovereignty.

Discussion: The information environment is an unrestricted space which allows for the cognitive freedom of action to all actors. The enemy utilizes this unrestricted access to limit cross domain freedom of maneuver. The purpose of this paper is to develop a concept of employment for Marine Expeditionary Unit Information Environment Operations. This paper will analyze and deconstruct current national and strategic information operations and cyber warfare doctrine to identify the critical capabilities and requirements for the employment of Information Operations as a supporting arm. In conclusion, I hope to develop a concept for the employment of information environment operations by the Marine Expeditionary Unit.

Conclusion: The information environment is an unrestricted space which allows for the cognitive freedom of action to all actors. The enemy utilizes this unrestricted access to limit freedom of maneuver across all domains and dimensions. To dominate within this environment, the 21st century MAGTF must operationalize the information environment and employ all capabilities within, as a supporting arm to conventional maneuver and fires. Although the Marine Air Ground Task Force Information Environment Operations Concept of Employment provides framework for MAGTF operations within the IE, currently the operating concept does not establish the subordinate task organization to integrate these concepts within Marine Expeditionary Unit or Special Purpose MAGTF. The Marine Corps ability to influence, out-cycle, and dominate adversaries in the information environment requires the:

1. Develop a subordinate MAGTF Information Environment Task Organization – MIS Capabilities provide the MEU commander tools to be applied in politically sensitive, contested, or restricted areas where conventional forces may not be acceptable.
2. Establish authorities to enable employment of IRCs at the MEU level - Enabling authorities for the offensive and defensive employment of IRC to the MEU commander will allow for a timely agile response to global emerging threats and contingencies thus providing decision time for the Combatant Commander, and President.
3. Develop IE Operations Doctrine – Updated MAGTF Information Environment Operations doctrine will align personnel, systems, equipment, and training, enabling information operations to be applied as a supporting arm within all MAGTF organizations.
4. Integrate Information Related Capabilities into MEU Pre-deployment Training – The MEU commander and staff must integrate Information and cyber training into the MEU pre-deployment training.

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.

LIST OF ILLUSTRATIONS

TABLE OF CONTENTS

Page

PREFACE

The purpose of this paper is to develop a concept of employment for Marine Expeditionary Unit Information Environment Operations. This paper will analyze and deconstruct current national and strategic information operations and cyber warfare doctrine to identify the critical capabilities and requirements for the employment of Information Operations as a supporting arm. In conclusion, I hope to develop a concept for the employment of information environment operations by the Marine Expeditionary Unit.

INTRODUCTION

The global propagation of the internet and digital information has proven to be the most powerful tool to initiate social, military, and geopolitical change. Nation states, radical insurgent groups, and individuals have gained complete parity in access to the tools and platforms to achieve global influence within the information environment. Information Environment Operations and Cyberspace Operations are two distinct operating concepts which take place in the information environment. While cyber operations are considered an operational capability of IE operations, cyberspace is an independent "fifth domain" with distinct cyber missions as effects can extend beyond the information environment. Joint Publication 3-13, *Information Operations*, recognizes the information environment operations as strategic resource vital to national security and success on the battlefield.[1]

In 2009 the Secretary of Defense directed the establishment of Cyber Command (USCYBERCOM) as a sub-unified command under United States Strategic Command (USSTRATCOM).[2] The primary objective of Cyber Command is to integrate the cyberspace operations capabilities of the services and agencies in support of the National Security objectives. Service components responded to the Secretary of Defense direction by establishing component commands: Fleet Cyber Command, U.S. Army Cyberspace Command (ARCYBER), and Air Force Cyberspace Command (AFCYBER).[3] Marine Forces Cyberspace Command (MARFORCYBER) was established on October 2009. MARFORCYBER's mission, is to plan, coordinate, integrate, synchronize, and direct the Marine Corps' full spectrum of cyberspace operations. These operations support MAGTF, joint, and combined cyberspace requirements that enable freedom of action across all warfighting domains.

Within the past seven years USCYBERCOM and service component commands have developed a cyber force which enhances cross domain offensive and defensive capabilities to

preserve sovereignty and national security.[4] Although there have been many advancements with the development of a cyber force, the Marine Corps is still deficient in fully integrating the capability as a supporting arm down to the tactical level. The September 2016 Marine Corps Operating Concept: *How an Expeditionary Force Operates in the 21st Century* identified the information technology gap as, "The Marine Corps is currently not organized, trained, and equipped to meet the demands of a future operating environment characterized by complex terrain, technology proliferation, information warfare, the need to shield and exploit signatures, and an increasingly non-permissive maritime domain."[5] Arguably, the two elements of the future operating environment which are most detrimental to military operations and national security are technology proliferation and information warfare. These two elements have been synthesized to describe the Information Operations Environment (IOE). The June 2016 *Department of Defense Strategy for Operations in the Information Environment*, provides the strategic guidance for how the DOD intends to operationalize the information environment operations to, "affect the decision-making and behavior of our adversaries and designated others to gain advantage across the range of military operations."[6]

Background – Operationalizing the Information Environment in the MAGTF

A Marine Expeditionary Unit is a forward-deployed Marine Air Ground Task Force capable of continuous operations in support of the President and Geographic Combatant Commanders. The MEU embarked on an Amphibious Ready Group provides the commander a versatile credible capability to deter, gain access, shape, and promote stability. The MEU capabilities include: amphibious operations to respond to crisis, limited contingency operations, establishing conditions for follow-on forces, and support to special operations forces. The unique capabilities of a MEU allow for interoperability with joint, combined, and special forces. [7]

The 21st century MAGTF is reliant on digital information, networks, and systems. These open and closed systems broadcast enormous electronic signatures, require significant spectrum and bandwidth, and are under continuous attack. Adversaries target classified information, degrade networks, distort information, and disable communications systems. Ultimately, the enemy aims to deny freedom of maneuver across all domains and dimensions. The Department of Defense 2016 *Strategy for Operations in the Information Environment* describes the complex landscape of the information environment as:

> This networked environment has enabled both state and non-state actors to employ activities in or through the IE to effectively achieve their objectives. They use various capabilities to exploit, disrupt, and disable command and control systems and other critical infrastructure; to disseminate propaganda and disinformation; to foster internal dissent; to recruit and solicit financing; and to promote legitimacy for their actions while discrediting the legitimacy of others. Although we can expect potential state adversaries to offer sophisticated challenges through aggressive operations in the IE, new forms of technology and communication have lowered the barriers of entry for non-state actors. These actors, and their supporters and surrogates, can now access the IE with ease and at relatively low cost, using it to advance their objectives and influence audiences around the globe.[8]

Marine Expeditionary Units are at the front lines of the information operations environment war. Command and control, communications, networks, and targeting systems are all susceptible to attack. The MEU is the ideal platform in which to employ information environment operations to promote regional stability. Operationalizing the information environment from a sea-based forward presence will disrupt the enemy's employment of information related capabilities denying freedom of maneuver within the cognitive, physical and information domains. Currently, the MEU is not equipped, or task organized to conduct full spectrum operations within the information environment without significant support from the Marine Information Group, MARFORCYBER, and/or national agencies. This deficiency within the MEU is a critical gap which threatens regional stability and national security.[9]

Thesis

The operationalization of the information environment by belligerent states and threat actors across the range of military operations has violated individual and state sovereignty around the world. The enemy has gained the initiative seizing key terrain within the global network of information systems. A strong reactive defense can no longer be the standard to preserve US national security within the information environment. If the United Stated is to dominate within the information environment, it must train, man, equip, and employ the Marine Expeditionary Unit to establish regional information superiority within geographic combatant commands. The 21st century MAGTF must operationalize the information environment and employ all capabilities within, as a supporting arm to achieve physical and cognitive advantage thereby preserving US national security and sovereignty.

DEFINING THE INFORMATION ENVIRONMENT

Key Terms and Definitions

The **Marine Air-Ground Task Force (MAGTF)** is the Marine Corps principal organizational construct for conducting missions across the range of military operations.[10]

The **Information Environment (IE)** is the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information.[11]

Information Operations (IO) is the integrated employment during military operations of information-related capabilities (IRCs), in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision making of adversaries and potential adversaries while protecting our own. IO integrates the application of force and the employment of information with the goal of affecting the perception and will of adversaries. The integration of IRCs for

effect can be compared to fire support coordination, in which a targeting methodology synchronizes and employs various capabilities to generate desired effects. It is the integration and synchronization of IRCs that enables desired effects in and through the IE at specified times and locations.[12]

Information-Related Capabilities are the tools, techniques or activities that affect any of the three dimensions of the information environment.[13]

The **Physical Dimension** is composed of the command and control systems and supporting infrastructure. It enables organizations to conduct operations across air, land, sea and space. It consists of physical platforms and networks and is the easiest to measure. Combat power is traditionally measured in this domain.[14]

Within the **Information dimension**, information is collected, processed, stored, disseminated, displayed and protected; command and control of modern military forces is communicated, and commander's intent is conveyed.[15]

The **Cognitive Dimension** encompasses the mind of the decision maker and the target audience where people think, perceive, visualize and decide. It is the most important of the three dimensions. Numerous factors affect this dimension, among them are leadership, cohesion, morale, training, experience, situational awareness, public opinion, perceptions, media, public information and rumors.[16]

MAGTF Information Operations is the integrated planning and employment of MAGTF, Naval, Joint, and Interagency information capabilities, resources, and activities that enhance the Marine Corps single-battle concept and provide defensive, offensive, exploitative effects and support in order to operate, fight and win in and through a contested information environment.[17]

Information Superiority is defined as 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. Information superiority is not static; during operations, all sides continually attempt to secure their own advantages and deny useful information to adversaries.[18]

Cyberspace is a global domain within the information environment consisting of the interdependent network of IT infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.[19]

INFORMATION ENVIRONMENT OPERATIONS IN THE MAGTF

The MEF Information Group (MIG)

On 6 July 2017, Lieutenant General Robert S. Walsh, Deputy Commandant, Combat Development and Integration published the *Marine Air Ground Task Force Information Environment Operations Concept of Employment* to, "improve the MAGTF's ability to coherently plan and execute integrated actions in and through the information environment."[20] This concept of employment established the framework for the organization of the MEF Information Group (MIG) and provided guidance to support further development of concepts and capabilities.

The purpose of the MIG is to operationalize the information environment as a maneuver space, enabling planning, coordination, and mission execution. The mission of the MIG is to, "coordinate, integrate and employ IE Ops capabilities in order to ensure the MAGTF Commander's ability to facilitate friendly forces maneuver and deny the enemy freedom of action in the information environment. Provide communications, intelligence, supporting arms

liaison, and law enforcement capabilities in support of MAGTF operations."[21]

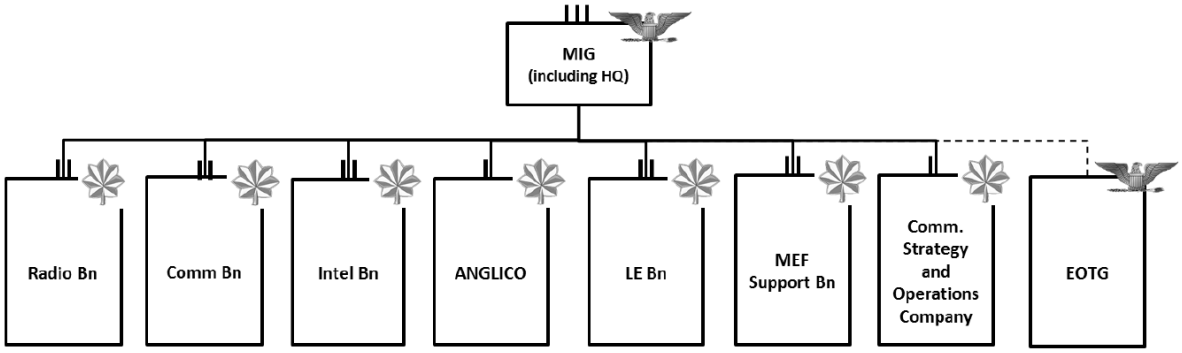

Figure 1. Marine Expeditionary Force Information Group Task Organization

The MIG is designated as a subordinate command of the MEF command element focused on the planning, coordination, and execution of information environment operations within the MEF area of interest. The MIG is an O-6 command comprised of subordinate commands which enable the execution of information operations across the MEF battlespace. The MIG commander is responsible for ensuring the seven IE Ops functions are integrated in support of the MAGTF CONOPS and scheme of maneuver. Based on designated mission requirements, assigned tasks, and commanding general direction and priorities, the MIG commander determines command relationships to fulfill mission requirements. The task organization of the MIG enables it to either support MEF staff tasking with its subordinate elements or can be allocated the authority as a major subordinate element main effort to achieve objectives. [22]

The MIG COC enables functional integration of information environment operations into the MAGTF and Joint Force. Connectivity through Information Battle Management and Control System (IBMCS), enable unity of effort in the integrating IE operations through the single battle concept. Furthermore, integration with subordinate C2 nodes within MAGTF C2 centers including the MEF COC, Fires and Effects Coordination Center (FECC), TACC, Direct Air

Support Center (DASC), and Intelligence Operations Center (IOC), permits IE operations to be employed as a combined arm in unison with conventional maneuver and fire support systems.[23]

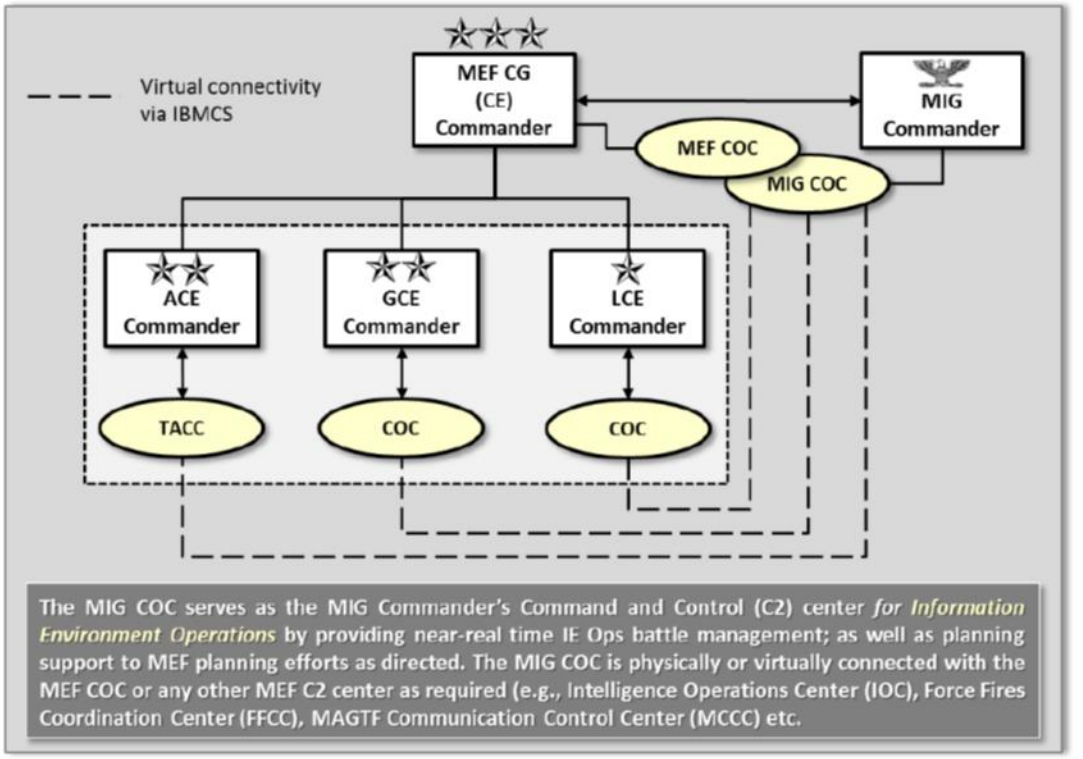

Figure 2. MIG Command and Control Relationship

Currently, there is no guidance or framework directing the formation of subordinate information environment organizations to integrate the seven functions of Information Environment Operations into the Marine Expeditionary Brigade, Special Purpose MAGTF, or Marine Expeditionary Unit. The establishment of the Marine Expeditionary Unit Information Section will enable nested cross domain freedom of maneuver as well as deny, degrade, disrupt, destroy, and manipulate (D4M) enemy systems within the information environment thus enabling national and regional security. The following section proposes a concept of employment for the Marine Expeditionary Unit Information Section (MIS).

Marine Expeditionary Unit Information Section (MIS)

The MEU Information Section is a subordinate element of the Marine Expeditionary Force Information Group. It is composited for MEU and SPMAGTF deployment rotations from MIG subordinate commands and thus its mission and capabilities are nested with geographic command and national strategic objectives. The mission of the MEU Information Section is to coordinate, integrate, and employ IE Ops capabilities within assigned area of operation in order to ensure the MEU Commander's ability to enable friendly forces maneuver and deny the enemy freedom of action in the information environment. Additionally, the MIS provides communications, intelligence, supporting arms, reconnaissance, and special operations liaison in support of MAGTF operations.[24]

The MEU Information Section is established as a permanent subordinate command within the MEU Command Element (CE) responsible for planning, coordinating, and executing information environment operations in support of the MEU across the assigned area of operation. Functional integration of IE operations is the responsibility of the MEU commander and is delegated by authority, as directed, to the MIS commander. The MIS is composited from attachments of the subordinate commands of the MIG and is structured to integrate and fulfill the seven functions of information environment operations at the operational and tactical level. The MIS capabilities are determined by the authorities assigned by the MEF commander, Secretary of Defense, or the President of the United States. MIS subordinate elements which support IE operations include the Radio section, Communications section, Intelligence Section, and the Communication Strategy and Operations Section. Recon company and the Special Operations Force Liaison Element (SOFLE) will provide support to IE operations as directed.[25]

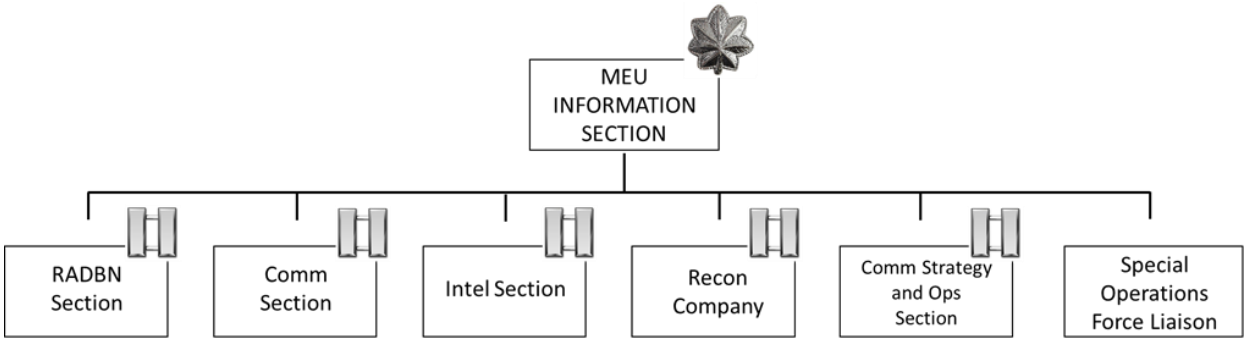

Figure 3. Marine Expeditionary Unit Information Section

The MIS is retained as a subordinate command within the CE to ensure operational, strategic, and joint capabilities are integrated across all phases and within all areas of the MEU battlespace. Furthermore, if additional authorities, cross-boundary coordination, and/or additional capabilities are required, the MEU staff and commander can leverage higher headquarters, joint headquarters, and national level agencies to support MEU information environment operations. Based on the mission priorities, task organization, tasks, and commander's guidance, the MIS commander directs subordinate command relationships. In assigning these relationships, the MIS commander may direct MIS subordinate elements to support the MEU command element and Major Subordinate Element (MSE) operational requirements and/or provide IE Ops forces and capabilities to MSEs.[26]

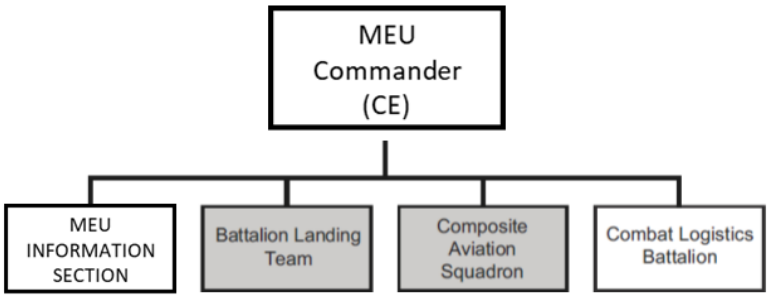

Figure 4. MIS Relationship to MSE

The MIS HQ is organized with personnel to provide IE Ops planning and execution support as directed by the MEU commander. During planning and execution, the MIS S-3 provides future and current operations personnel to support MEU and MSC operational planning teams. The MIS HQ element establishes a MIS COC to synchronize cross domain IE capabilities across all elements of the MAGTF, joint, and combined forces. Additionally, the MIS COC provides personnel to the force fires and effects coordination center (FFEC) to integrate and deconflict information related capabilities in support of conventional maneuver forces and fires.

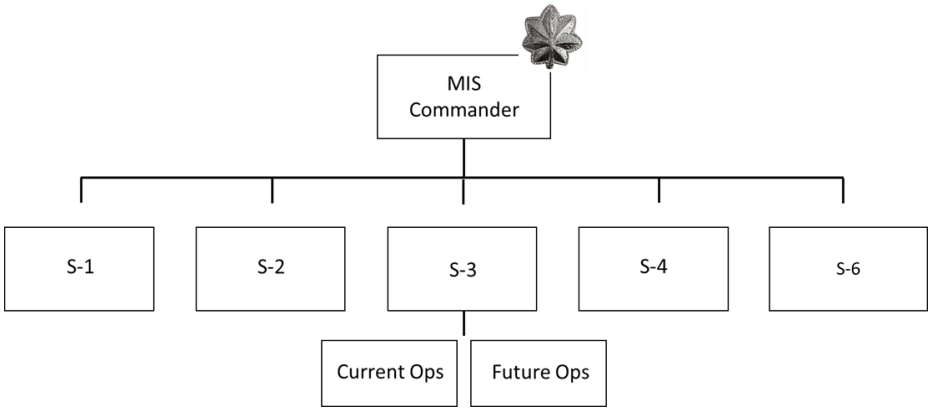

Figure 5. MIS Staff Sections

MEU Information Section – Integration into the MAGTF Operations

Information Environment Operational Capabilities provide the MEU commander tools to be applied in politically sensitive, contested, or restricted areas where conventional forces may not be acceptable. Functional integration of IE operations occurs across all planned phases of an operation (shape, deter, seize the initiative, dominate, stabilize, and enable civil authority).

Information Related Capabilities require extensive planning, coordination, and lead time to ensure effects are deconflicted, assets are aligned, and approval is granted by the appropriate authority. As a forward deployed contingency force, MEU planners must ensure that Information Related Capabilities are embarked, regionally aligned, and/or are supported by reach back

through military, civilian, and/or national organizations.[27] Information Related Capabilities must be templated as part of the standard MEU mission profiles to allow for expedient approval in support of amphibious mission profiles and contingency operations.

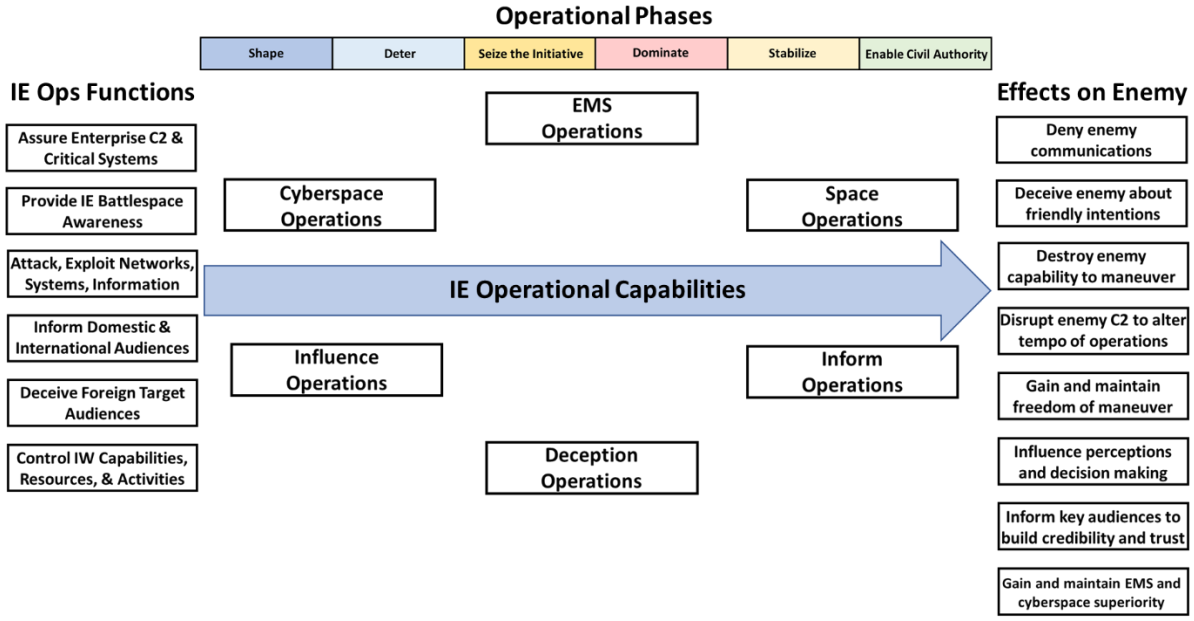

Figure 6. IE Operations Functions, Capabilities, and Effects

Functions

Function #1: Assure Enterprise Command and Control Systems and Critical Systems

Intelligence running estimate information enables planning, real time network management, and defense actions. The command and control system architecture is established to support the MEU concept of operations both afloat and ashore. Intelligence running estimate information enables planning, real time network management, and defensive actions. The MIS assures the C2 systems enable the MEU commander maintains command and control over assigned forces and to maintain freedom of action across all warfighting domains.[28]

The MIS conducts electromagnetic spectrum operations which encompasses electronic warfare (EW) and spectrum management. Furthermore, the MIS is responsible for the planning,

coordination, and deconfliction of spectrum with EMS-dependent adjacent units and capabilities such as Signals Intelligence (SIGINT) and cyberspace operations, and space operations.[29]

Function #2: Provide Information Environment Battlespace Awareness

This function synthesizes data, information, and intelligence across the physical, informational, and cognitive domains to identify threats, vulnerabilities, and opportunities. The S-2 and/or IOC provides the MIS COC with threat intelligence and indications and warnings (I&W) regarding technical, organizational, or human targets, target system, target command and control networks and nodal dependencies, threat cyberspace operations capabilities and actions, threat space capabilities and actions, threat EMSO capabilities and actions, battle damage assessments (BDA), and re-attack recommendations.[30] The MIS COC provides running estimate overlays which include the analysis of threat, environmental, and friendly force information relevant to IE Operations.[31]

Function #3: Attack and Exploit Networks, Systems and Information

The MIS employs cyberspace operation capabilities to conduct: (1) Department of Defense information network (DODIN) operations, (2) defensive cyberspace operations (DCO), and (3) offensive cyberspace operations (OCO).[32] Signal Intelligence Support Teams (SSTs), Electronic Warfare Support Teams (EWSTs), and MARFORCYBER Combat Mission Teams enable the MIS to conduct full spectrum cyber operations. Information related capabilities exploit and attack enemy networks, systems, signatures, and information to deny, degrade, disrupt, destroy and manipulate the enemy. Planning, coordination, and deconflictions is achieved through the Force Fires and Effect Coordination Center.[33]

Function #4: Inform Domestic & International Audiences

The Communications Strategy and Operations Section of the MIS provides personnel and planners to provide accurate, timely, and relevant communications with domestic and foreign audiences to build understanding and support for operational objectives. Additionally, communications are utilized to reinforce alliances and deter adversaries. The MIS Communications Strategy and Operations Section plans, coordinates, and deconflicts effects through the Force Fires and Effect Coordination Center.[34]

Function #5: Influence Foreign Target Audiences

The Communications Strategy and Operations section integrate Influence Operations (psychological operations (PSYOP), military deception (MILDEC), operations security (OPSEC), counterintelligence (CI) operations, counter-propaganda operations and public affairs (PA) operations) into the MAGTF concept of operations. Influence Operations are ultimately designed to shape perceptions in the IE of both the adversary and/or other relevant actors. Influence effects are applied through the targeting process and are coordinated and deconflicted through coordinates, and deconflicts effects through the Force Fires and Effect Coordination Center.[35]

Function #6: Deceive Foreign Target Audiences

The Communications Strategy and Operations section plans, coordinates, and ensures MAGTF deception actions are nested under higher level joint plan. The MIS COC coordinates the timing and tempo of deception actions in support of tactical-level commanders and ensures deception actions are deconflicted through the force fire and effects coordination Center with other MAGTF operations which may affect or be affected by deception actions.[36]

Function #7: Control of IE Operations Capabilities, Resources and Activities

The MEU Information Section commander utilizes the MIS COC, FFEC, and IOC to track and assess information related capabilities in support of the MAGTF concept of operations. Measures of Performance and Measures of Effectiveness ensure the MIS is to rapidly adapt capabilities to maintain information superiority.[37]

Activities

IE Shaping and Deterring Activities

The MEU will conduct information environment operations in support of an OPLAN or Theater Campaign Plan. Information Related Capabilities are employed to deter adversaries and potential adversaries from threatening US and allied objectives, interests, and security. The MIS will integrate efforts across the joint, combined, and interagency force. With dedicated resources, the MEU Information Section can apply IRCs immediately to address contingencies and emerging threats providing decision time for the Combatant Commander, and President.[38]

IE Seizing the Initiative and Dominating Activities

During these phases the MEU is conducting full spectrum information environment operations. IE Operational Capabilities are employed across multiple lines of operation as a supporting arm to conventional fires and maneuver. Information Superiority is obtained during these phases to enable cross domain freedom of maneuver. Although IRCs may be focused to support MAGTF operations, IE operations and associated capabilities are strategic assets and may be pulled to support national strategic objectives.[39]

IE Stabilizing and Enable Civil Authority Activities

During these phases the MEU Information Section is employing IRCs in support of Civil Military Operations, Inform Operations, and Civil Affairs. Support to combat operations will be

sustained as required to enable security. Cross domain freedom of maneuver ensures accurate and timely information is promulgated throughout the area of operation. The MIS will assist in building host nation capacity and capability to permit civil authority to maintain security over the information environment. In the transition to Phase V, the MIS transfers security responsibilities of the information environment to the host nation.[40]

Authorities

The dynamic, complex, and nuanced nature of IE operations is such that any application of operational authorities requires a comprehensive and detailed legal valuation of authority and/or legality of specific actions.[41] The sophistication of multinational operations can extend IRC package approval timelines as each nation has its own laws, policies, and processes for approving plans[42] The *Operational Law Handbook* specifies the titles and directives which enable the employment of IRCs:

> "The authority to employ IRCs is rooted foremost in Title 10, United States Code (USC). While Title 10, USC, does not specify IO separately, it does provide the legal basis for the roles, missions, and organization of DOD and the Services. Title 10, USC, Section 164, gives command authority over assigned forces to the CCDR, which provides that individual with the authority to organize and employ commands and forces, assign tasks, designate objectives, and provide authoritative direction over all aspects of military operations."[43]
>
> "The DOD and Chairman of the Joint Chiefs of Staff (CJCS) directives delegate authorities to DOD components. Among these directives, DODD 3600.01, Information Operations, is the principal IO policy document. Its joint counterpart, Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3210.01, Joint Information Operations Policy, provides joint policy regarding the use of IRCs, professional qualifications for the joint IO force, as well as joint IO education and training requirements. Based upon the contents of these two documents, authority to conduct joint IO is vested in the CCDR, who in turn can delegate operational authority to a subordinate JFC, as appropriate."[44]

Authorities do not currently exist to develop and employ IRCs at the MEU level. Authorities for tactical IE operations are deliberately granted and managed at the strategic level.

Enabling authorities for the offensive and defensive employment of IRC will allow for a timely agile response to global emerging threats and contingencies. Information Related Capabilities must be templated as part of the standard MEU mission profiles to allow for expedient approval in support of amphibious mission profiles and contingency operations.

RECOMMENDATIONS

Develop a subordinate MAGTF Information Environment Task Organization – The MEU is a national strategic capability forward postured and continuously deployed to address global military and contingency requirements. MEU MSEs are often tactically employed to achieve mission requirements. MIS capabilities provide the MEU commander tools to be applied in politically sensitive, contested, or restricted areas where conventional forces may not be acceptable. The MIS will allow the conduct of full spectrum information environment operations in support of all three levels of war. Information related capabilities will establish conditions for larger MEF or Joint IE operations. Additionally, the MIS will integrate fully into MAGTF planning and execution. Effects based IRCs must be employed as a supporting arm to achieve combined arms effects thus enabling maneuver in the cognitive, information, and physical domains.

Establish authorities to enable employment of IRCs at the MEU level – Information Related Capabilities must be templated as part of the standard MEU mission profiles to allow for expedient approval in support of amphibious mission profiles and contingency operations. Enabling authorities for the offensive and defensive employment of IRC to the MEU commander will allow for a timely agile response to global emerging threats and contingencies. If authorities are unable to be delegated to the MEU level, support relationships with authorized units must be established to ensure timely support.

Develop IE Operations Doctrine – The United States cyber policy to preserve and defend open internet to promote the spread of democratic values, has shaped the information and cyber policies of the Department of Defense and subordinate service components.[45] Current information and cyber doctrine does not exist to provide a common frame of reference across the DOD, standardize operations, and facilitate readiness. MCWP 3-32 *MAGTF Information Operations* is not sufficient to establish the doctrinal foundations for the employment of Information Environment Operations within the MAGTF. Updated MAGTF Information Environment Operations doctrine will align personnel, systems, equipment, and training, enabling information operations to be applied as a supporting arm within all MAGTF organizations. Information / Cyber doctrine will inform the leaders of capabilities and requirements ensuring synergy in planning, integration, and employment of IRCs in support of MAGTF operations.

Develop a Networked Mesh of Interoperable Command and Control Systems – Current command and control systems afloat are not sufficient to support employment of information environment operations in an expeditionary environment. The Navy/Marine Corps team must develop a networked mesh of interoperable agile command and control systems afloat to enable a distributed MEU, MEB, and MEF to establish cross domain information superiority to enable cognitive and conventional maneuver. Amphibious ready groups supported by AGEIS technologies would be an essential component to operate within and defeat anti-access area-denial (A2AD) systems. This concept is illustrated in Figure 7.

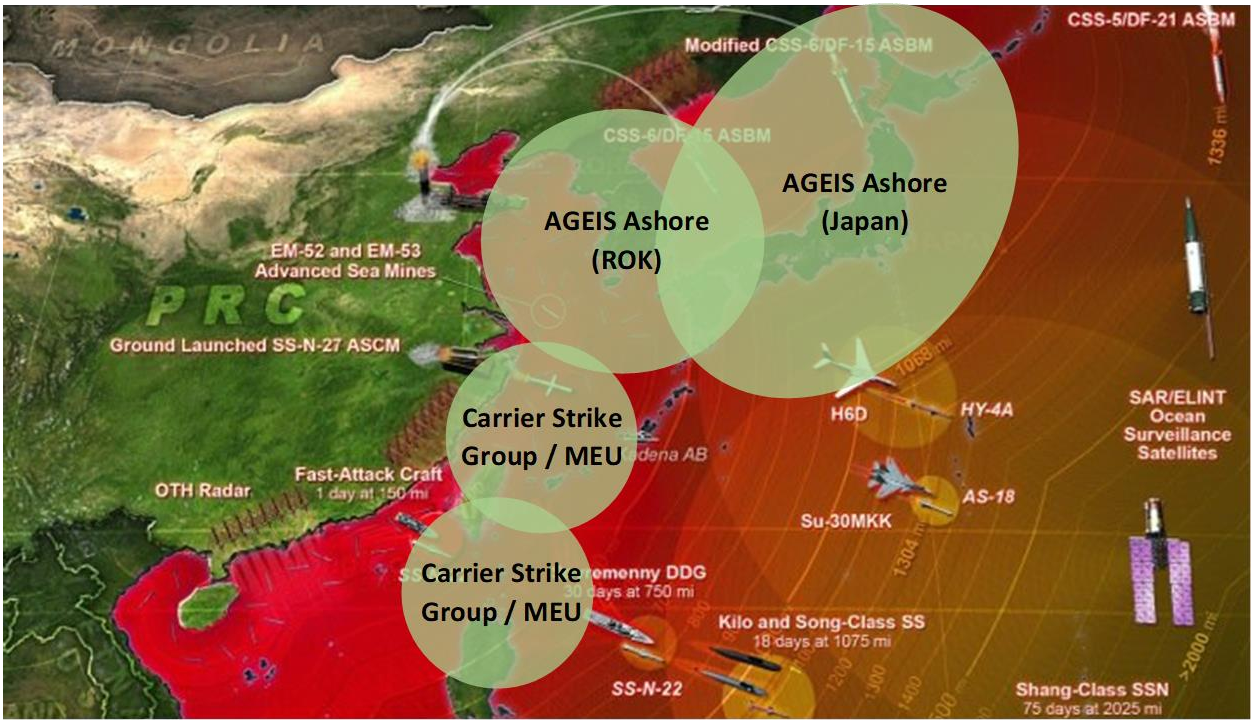

Figure 7. Distributed C2 Systems Enabling IE Ops in A2AD Environment

Integrate Information Related Capabilities into MEU Pre-deployment Training– The Marine Expeditionary Unit does not currently train to employ IRCs in support o MAGTF operations. Expeditionary Operations Training Group must develop, integrate, and evaluate information and cyber training into the MEU pre-deployment training. IRC effects must be integrated into targeting boards and deconflicted through the Fires and Effects Coordination Center as a supporting arm. IRCs must be employed immediately to secure MEU C2 systems during training to ensure that all Marines understand their responsibility to security and defense.

CONCLUSION

The information environment is an unrestricted space which allows for the cognitive freedom of action to all actors. The enemy utilizes this unrestricted access to limit freedom of

maneuver across all domains and dimensions. To dominate within this environment, the 21st century MAGTF must operationalize the information environment and employ all capabilities within as a supporting arm to conventional maneuver and fires. The subordinate task organization does not currently exist to integrate the recommended concepts within Marine Expeditionary Unit or Special Purpose MAGTF. The Marine Corps ability to influence, out-cycle, and dominate adversaries in the information environment is predicated on the development of the following initiatives:

1. Develop a subordinate MAGTF Information Environment Task Organization – MIS Capabilities provide the MEU commander tools to be applied in politically sensitive, contested, or restricted areas where conventional forces may not be acceptable.
2. Establish authorities to enable employment of IRCs at the MEU level - Enabling authorities for the offensive and defensive employment of IRC to the MEU commander will allow for a timely agile response to global emerging threats and contingencies thus providing decision time for the Combatant Commander, and President.
3. Develop IE Operations Doctrine – Updated MAGTF Information Environment Operations doctrine will align personnel, systems, equipment, and training, enabling information operations to be applied as a supporting arm within all MAGTF organizations.
4. Integrate Information Related Capabilities into MEU Pre-deployment Training – The MEU commander and staff must integrate Information and cyber training into the MEU pre-deployment training.

The *Marine Air Ground Task Force Information Environment Operations Concept of Employment* was the first step to operationalize IE ops within the MAGTF. Recognizing the

importance that the information environment will play in future conflicts, in the summer of 2017 the United States Marine Corps established Deputy Commandant of Information (DCI), a three-star billet, will serve as the coordinating body for the development and integration of information warfare capabilities into all aspects of MAGTF operations. There is no doubt that the United States Marine Corps will continue to lead the effort to operationalize the information environment thus enabling the joint force to preserve national security and sovereignty within every dimension and domain.

LIST OF ACRONYMS

ACE – Aviation Combat Element
ACO – Airspace Control Order
ANGLICO – Air Naval Gunfire Liaison Company
AOI – Area of Interest
AOR – Area of Responsibility
ARFOR – Army Forces Component Command
ATC – Air Traffic Control
ATO – Air Tasking Order
B2C2WG – Boards, Bureaus, Centers, Cells, Working Groups
BDA – Battle Damage Assessment
BLOS – Beyond Line of Sight
BMC2 – Battle Management and Control
BN – Battalion
C2 – Command and Control
CA – Civil Affairs
CAC2S – Common Aviation Command and Control System
CAO – Civil Affairs Operations
CCIR – Commanders Critical Information Requirement
CCMD – Combatant Command
CE – Command Element
CEWCC – Cyberspace and Electronic Warfare Coordination Cell
CHOP – Change in Operational Control
CI – Counterintelligence
CMO – Civil Military Operations
COA – Course of Action
COC – Combat Operations Center
COE – Concept of Employment
CommStrat – Communication Strategy and Operations
CONOPS – Concept of Operations
CONPLAN – Concept Plan
COP – Common Operational Picture
CTP – Common Tactical Picture
DASC – Direct Air Support Center
DCI – Deputy Commandant of Information
DCO – Defensive Cyberspace Operations
DCO-IDM – Defensive Cyberspace Operations Internal Defense Measures
DCO-RA – Defensive Cyberspace Operations Response Actions
DI – Digital Interoperability
DODIN – Department of Defense Information Network
DOTMLPF-P – Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, Facilities, Policy
EA – Electronic Attack
EMI – Electromagnetic Interference

EMS – Electromagnetic Spectrum
EMSO – Electromagnetic Spectrum Operations
EMSOC – Electromagnetic Spectrum Operations Center
EW – Electronic Warfare
EWCA – Electronic Warfare Control Authority
EWST – Electronic Warfare Support Team
EXORD – Execution Order
FDO – Foreign Disclosure Officer
FECC – Fires and Effects Coordination Center
FECC – Force Fires Coordination Center
FRAGO – Fragmentary Order
GCE – Ground Combat Element
HN – Host Nation
HQ – Headquarters
HHQ – Higher Headquarters
IBMCS – Information Battle Management and Control Service
IE – Information Environment
IM – Information Management
IMO – Information Management Officer
I&W – Indications and Warnings
IO – Information Operations and/or Influence Operations
IOC – Intelligence Operations Center
ISO – In support of
ISR – Intelligence Surveillance and Reconnaissance
IE Ops – Information Environment Operations
JEMSOC – Joint Electromagnetic Spectrum Operations Center
JFLCC – Joint Force Land Component Command
JFMCC – Joint Force Maritime Component Command
JTF – Joint Task Force
JTFHQ – Joint Task Force Headquarters
KLE – Key Leader Engagement
LCE – Logistics Combat Element
LE – Law Enforcement
LNO – Liaison
MACCS – Marine Air Command and Control System
MAGTF – Marine Air Ground Task Force
MARFOR – Marine Forces Component Command
MAW – Marine Aircraft Wing
MCCC – MAGTF Communications Control Center
MCDP – Marine Corps Doctrinal Publication
MCPP – Marine Corps Planning Process
MEB – Marine Expeditionary Brigade
MEF – Marine Expeditionary Force

NOTES

[1] Chairman of the Joint Chiefs of Staff, *Joint Publication 3-13, Information Operations*, (Washington, DC:

Office of the Chairman of the Joint Chiefs of Staff, 20 November 2014),

[2] US Strategic Command, "US Cyber Command Mission Statement," last modified September 30, 2016, http://www.stratcom.mil/Media/Factsheets/Factsheet-View/Article/960492/us-cyber-command-uscybercom/.

[3] Headquarters United States Marine Corps, *Marine Corps Concepts and Programs 2013*, (Washington, DC: Headquarters US Marine Corps, 2013), 32.

[4] Paul Szoldra, "How the US military is beating hackers at their own game," *Business Insider*, last modified May 24, 2016, http://www.businessinsider.com/us-military-cyberwar-2016-5.

[5] Headquarters United States Marine Corps, *Marine Corps Operating Concept: How an Expeditionary Force Operates in the 21st Century*, (Washington, DC: Headquarters US Marine Corps, September 2016), 4.

[6] US Department of Defense, *Strategy for Operations in the Information Environment*, Washington, DC: Office of the Secretary of Defense, June 2016, 8.

[7] Headquarters United States Marine Corps, *Marine Corps Order 3120.9C*, Policy For Marine Expeditionary Units, (Washington, DC: Headquarters US Marine Corps, August 2009), 4.

[8] US Department of Defense, *Strategy for Operations in the Information Environment*, (Washington, DC: Office of the Secretary of Defense, June 2016), Forward.

[9] U.S. Marine Corps Retools Strategy As Tech Threats Mushroom, Loren Thompson, Contributor, Forbes Jan 13, 2017 @ 11:34 AM https://www.forbes.com/sites/lorenthompson/2017/01/13/u-s-marine-corps-retools-strategy-as-tech-threats-mushroom/2/#2d5c3379509f.

[10] Headquarters United States Marine Corps, *Amphibious Ready Group and Marine Expeditionary Unit Overview*, (Washington, DC: Headquarters US Marine Corps, 2012), 2.

[11] US Department of Defense, *Strategy for Operations in the Information Environment*, (Washington, DC: Office of the Secretary of Defense, June 2016), 3.

[12] Ibid., 3.

[13] Chairman of the Joint Chiefs of Staff, *Joint Publication 3-13, Information Operations*, (Washington, DC: Office of the Chairman of the Joint Chiefs of Staff, 20 November 2014), I-3.

[14] Headquarters US Marine Corps, *MCWP 3-32 Marine Air-Ground Task Force Information Operations*, (Quantico, VA: Combat Development and Integration, May 2016), 1-3.

[15] Ibid., 1-3.

[16] Ibid., 1-4.

[17] Headquarters US Marine Corps, *MAGTF Information Environment Operations Concept of Employment*, (Quantico, VA: Combat Development and Integration, July 6, 2017), 1.

[18] Chairman of the Joint Chiefs of Staff, *Joint Publication 3-13, Information Operations*, (Washington, DC: Office of the Chairman of the Joint Chiefs of Staff, 20 November 2014), GL-3.

[19] Chairman of the Joint Chiefs of Staff, *Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms*, (Washington, DC: Office of the Chairman of the Joint Chiefs of Staff, 31 October 2009), 58.

[20] Headquarters US Marine Corps, *MAGTF Information Environment Operations Concept of Employment*, (Quantico, VA: Combat Development and Integration, July 6, 2017), Forward.

[21] Ibid., 4.

[22] Ibid., 4.

[23] Ibid., 7.

[24] Ibid., 4.

[25] Ibid., 5-6.

[26] Ibid., 7.

[27] Headquarters US Marine Corps, MCWP 3-32 *Marine Air-Ground Task Force Information Operations*, (Quantico, VA: Combat Development and Integration, May 2016), 2-5.

[28] Headquarters US Marine Corps, *MAGTF Information Environment Operations Concept of Employment*, (Quantico, VA: Combat Development and Integration, July 6, 2017), 11.

[29] Headquarters, Department of the Army, *ATP 6-02.70 Techniques for Spectrum Management Operations*, (Washington, DC, December 2015), Chap 1.

[30] Headquarters US Marine Corps, *MAGTF Information Environment Operations Concept of Employment*, (Quantico, VA: Combat Development and Integration, July 6, 2017), 12.

[31] Ibid., 12.

[32] Chairman of the Joint Chiefs of Staff, *Joint Publication 3-13, Information Operations*, (Washington, DC: Office of the Chairman of the Joint Chiefs of Staff, 20 November 2014), II-9.

[33] Headquarters US Marine Corps, *MAGTF Information Environment Operations Concept of Employment*, (Quantico, VA: Combat Development and Integration, July 6, 2017), 12.

[34] Chairman of the Joint Chiefs of Staff, *Joint Publication 3-61, Public Affairs*, (Washington, DC: Office of the Chairman of the Joint Chiefs of Staff, 19 August 2016), III-23.

[35] Headquarters US Marine Corps, *MCWP 3-32 Marine Air-Ground Task Force Information Operations*, (Quantico, VA: Combat Development and Integration, May 2016), 3-1-3-3.

[36] Chairman of the Joint Chiefs of Staff, *Joint Publication 3-13.4, Military Deception*, (Washington, DC: Office of the Chairman of the Joint Chiefs of Staff, 26 January 2012), I-1-I-4.

[37] Chairman of the Joint Chiefs of Staff, *Joint Publication 3-0, Joint Operations*, (Washington, DC: Office of the Chairman of the Joint Chiefs of Staff, 17 January 2017), V-12.

[38] Chairman of the Joint Chiefs of Staff, *Joint Publication 3-13, Information Operations*, (Washington, DC: Office of the Chairman of the Joint Chiefs of Staff, 20 November 2014), IV-11.

[39] Ibid., IV-11

[40] Ibid., IV-12

[41] Ibid., III-1

[42] Ibid., III-3

[43] Headquarters, Department of the Army, *Operational Law Handbook*, International And Operational Law Department The Judge Advocate Generals Legal Center & School, U.S. Army: Charlottesville, VA, 2015,136.

[44] Ibid.,136.

[45] Matthew Flynn, *US Cyber Policy: Defending Openness*, http://newconflict.org/us%20cyber%20policy.html

BIBLIOGRAPHY

Carr, Jeffery. *Cyber Warfare*. Sebastopol: O'Reilly Media, 2012.

Carnegie Endowment for International Peace. *The Military Doctrine of the Russian Federation, Approved by Russian Federation presidential edict, February 5, 2010 (Translated)*.

Washington, DC: Carnegie Endowment for International Peace, 2010: http://carnegieendowment.org/files/2010russia_military_doctrine.pdf.

Chairman of the Joint Chiefs of Staff. *Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms*. Washington, DC: Office of the Chairman of the Joint Chiefs of Staff, 31 October 2009.

Chairman of the Joint Chiefs of Staff. *Joint Publication 3-13, Information Operations*. Washington, DC: Office of the Chairman of the Joint Chiefs of Staff, 20 November 2014.

Chairman of the Joint Chiefs of Staff. *Joint Publication 3-0, Joint Operations*. Washington, DC: Office of the Chairman of the Joint Chiefs of Staff, 17 January 2017.

Chairman of the Joint Chiefs of Staff, *Joint Publication 3-13.4. Military Deception*. Washington, DC: Office of the Chairman of the Joint Chiefs of Staff, 26 January 2012.

Chairman of the Joint Chiefs of Staff. *Joint Publication 3-61, Public Affairs*. Washington, DC: Office of the Chairman of the Joint Chiefs of Staff, 19 August 2016.

Combat Development and Integration United States Marine Corps. *Marine Air Ground Task Force Information Environment Operations Concept of Employment.* Quantico, Virginia, 6 July 2017.

Connell, Michael and Vogler, Sarah. *Russia's Approach to Cyber Warfare.* Washington, DC: CNA Analysis and Solutions, March 2017.

US Department of Defense. *Information Operations*. JP 3-13. Washington, DC: Department of Defense, November 20, 2014.

Dimitrakopoulou, Sophia and Dr. Liaropoulos, Andrew. "Russia's National Security Strategy to 2020: A Great Power in the Making." *Caucasian Review of International Affairs* 4 (2010): http://cria-online.org/10_4.html.

European Union Delegation to the United Nations. *Report of the Independent Fact Finding Mission on the Conflict in Georgia*. New York: European Union Delegation to the United Nations, September 2009: http://eu-un.europa.eu/report-of-the-independent-international-fact-finding-mission-on-the-conflict-in-georgia/.

Giles, Keir. *The Next Phase of Russian Information Warfare*. New York: NATO Strategic Communications Centre of Excellence, 2016.

Headquarters, Department of the Army. *ATP 6-02.70 Techniques For Spectrum Management Operations*. Washington, DC, December 2015.

Headquarters, Department of the Army. *Operational Law Handbook*. International And Operational Law Department The Judge Advocate Generals Legal Center & School, U.S. Army: Charlottesville, VA, 2015.

Headquarters United States Marine Corps. *Amphibious Ready Group and Marine Expeditionary Unit Overview*. Washington, DC: Headquarters US Marine Corps, 2012.

Headquarters US Marine Corps. *MCWP 3-32 Marine Air-Ground Task Force Information Operations*. Quantico, VA: Combat Development and Integration, May 2016.

Headquarters US Marine Corps. *MAGTF Information Environment Operations Concept of Employment*. Quantico, VA: Combat Development and Integration, July 2017.

Headquarters United States Marine Corps. *Marine Corps Concepts and Programs 2013*. Washington, DC: Headquarters US Marine Corps, 2013.

Headquarters United States Marine Corps. *Marine Corps Operating Concept: How an Expeditionary Force Operates in the 21st Century*. Washington, DC: Headquarters US Marine Corps, September 2016.

Headquarters United States Marine Corps. *Marine Corps Order 3120.9C Policy for Marine Expeditionary Units*. Washington, DC: Headquarters US Marine Corps, August 2009.

Kramer, Franklin, D., Stuart H. Starr, and Larry K. Wentz, ed. *Cyberpower and National Security*. Dulles, Virginia: NDU Press and Potomac Books, 2009.

Maldre, Patrik. *The Russian Cyber Threat: Views from Estonia*. Washington, DC: Center for European Policy Analysis, May 18, 2016. http://cepa.org/The-Russian-Cyber-Threat-Views-from-Estonia 18 May 2016.

Manwaring, Max G. *The Complexity of Modern Asymmetric Warfare*. Norman: University of Oklahoma Press, 2012.

Schoen, Douglas E., Kaylan, Melik. *The Russia-China Axis*. New York: Encounter Books, 2014.

Stiennon, Richard. *Surviving Cyber War*. Plymouth, UK: The Scarecrow Press, 2010.

US Department of Defense. *Strategy for Operations in the Information Environment*, Washington, DC: Office of the Secretary of Defense. June 2016

Zetter, Kim. *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. New York: Crown Publishers, 2014.