REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
05-04-2019	Master of Military Studies Research Paper	AUG 2018 - JUN 2019

4. TITLE AND SUBTITLE
Of One Mind: Decision Superiority through Unifying Maritime Operations in the Information Environment

5a. CONTRACT NUMBER
N/A

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
N/A

6. AUTHOR(S)
Jeffery H. Robichaux, 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)
N/A

10. SPONSOR/MONITOR'S ACRONYM(S)
N/A

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

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for Public Rlease; Distribution is Unlimited

13. SUPPLEMENTARY NOTES
N/A

14. ABSTRACT
Service-specific thinking about operations in the information environment (OIE) must adapt to achieve seapower in the 21st century. The aim of future maritime operations is to gain and maintain decision superiority in the contested operations of the littorals. To achieve decision superiority, a Maritime Task Force (MTF) must control the information environment. The Navy and Marine Corps currently defines and fights in the IE differently and there is no Navy-Marine Corps unity of effort associated with OIE beyond a circumstantial ad hoc structure. The MTF cannot fight in the future Operating Environment without an integrated OIE C2 structure. This analysis uses a seven-function OIE framework to provide a recommendations by which the senior leadership of each service can categorize information-related capabilities (IRCs) to assist in developing the C2 structure necessary to conduct OIE. Ultimately, unity of effort in the information environment will ensure information superiority and enable decision superiority over a peer adversary.

15. SUBJECT TERMS
Information Operations, Decision Superiority, Information Superiority, Information Warfare, Operations in the Information Environment, Unity of Effort, United States Navy, United States Marine Corps

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			19b. TELEPHONE NUMBER *(Include area code)*

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: Of One Mind: Decision Superiority through Unifying Maritime Operations in the Information Environment

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

AUTHOR:

Major Jeffery Robichaux
United States Marine Corps

AY 2018-19

Mentor and Oral Defense Committee Member: JD Work
Approved: _____
Date: 5 April 2019

Oral Defense Committee Member: Matthew Flynn
Approved: _____
Date: 4/5/19

Scott F. Stebbins
Col USMC

Valerie A. Jackson
Col USMCR
20190405

Table of Contents

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.

EXECUTIVE SUMMARY

Title: Of One Mind: Decision Superiority through Unifying Maritime Operations in the Information Environment

Author: Major Jeffery Robichaux, United States Marine Corps

Thesis: How the Navy and Marine Corps conducts integrated operations in the information environment requires modifications to achieve the essential unity of effort necessary to gain and maintain decision superiority.

Discussion: The aim of future maritime operations is to gain and maintain decision superiority in the contested operations of the littorals. To achieve decision superiority, a Maritime Task Force (MTF) must control the information environment. The Navy and Marine Corps currently defines and fights in the IE differently and there is no Navy-Marine Corps unity of effort associated with Operations in the Information Environment (OIE) beyond a circumstantial ad hoc structure. A seven-function OIE framework provides a recommended baseline by which the senior leadership of each service can categorize information-related capabilities (IRCs). Understanding these IRCs and how they can be employed are vital to commanders as they fight by, with, and through information.

Conclusion: The MTF cannot fight in the future Operating Environment without an integrated OIE C2 structure. Service-specific thinking must adapt to achieve seapower in the 21st century. More importantly unity of effort in the information environment will ensure information superiority and enable decision superiority over a peer adversary.

Preface

How to conduct Information Operations has been the subject of considerable debate in the last 20 years. Since 2015, the Navy and Marine Corps have made significant realignment to manpower and organizational structure to meet the demands of the future fight in the information environment. However, the nature of independent Navy and Marine Corps debate resulted in limited service-specific changes but lacked integration. The essence of Operations in the Information Environment is not just a means of fighting—it is a way of maneuvering. While this may seem an abstruse distinction, the difference is the most important factor. Achieving decision superiority means that fighting in the highly contested maritime environment of the littorals requires commanders to use information to out think and out decide their adversaries.

After reading comments by the Chief of Naval Operations, Admiral John Robertson, it became clear that the goal of conducting Operations in the Information Environment is to achieve decision superiority. For the Navy and Marine Corps team to outpace the enemy's decision cycle and attain Sea Power and Power Projection they both first gain unity of effort. Throughout three MEU deployments, working together with my navy counterparts, I have come to appreciate the Navy's Sea Power. Unfortunately, during these deployments there was a scarcity of discussion regarding integrating Information-Related Capabilities. Even after deployments there is limited knowledge captured in after-action reports and in most cases that information is classified.

This paper aims to explore how the United States Navy and Marine Corps can achieve unity of effort when conducting Operations in the Information Environment and transition from an informal conversation during planning to a formal planning process. To conduct my research, I divided it into three parts: first, defining Operations in the Information and Maritime

Environments; secondly, how the United States Navy and Marine Corps are organized to fight in the IE; and finally, recommending how integration of information-related capabilities can occur using a seven-function framework to organize these capabilities. In some respects, my suggestions may match the general recommendations made in the 2017 MAGTF Information Environment Operation Concept of Employment. However, my recommendation are not all-encompassing but serve as examples of potential information-related capabilities that can be integrated today.

In the course of writing this paper, I have received assistance from a variety of people at all levels of the Marine Corps. At the Marine Corps University Command and Staff College (MCU CSC), Quantico, my mentors Dr. Matthew Flynn and Mr. J.D. Work, have been invaluable in their guidance in counsel during the preparation of this paper. Their efforts made this a far better paper. My Civilian and Military faculty advisors, Dr. Jorge Benetiz and LTC Paul Armstrong (USA), have been outstanding instructors and guidance counselors during my time at MCU CSC. Also, in Quantico, Dr. Benjamin Jensen, who was the original driver behind tackling the emerging topic of Information Operations. Major Sara Wood for her advice and extremely generous time commitment to proofreading this paper. Across the Marine Corps, Colonel Scot Stebbins, Majors David Burton and Dave Hanes have been sources of support.

Finally, I wish to thank my wife Jessica for her tireless support, which I have been the lucky beneficiary of throughout my Marine Corps career. To my children, Jullian, Aiden, and Anna-Grace, I hope that this paper inspires you to pursue your dreams even if it seems out of reach. Lastly, an extended thanks to my parents, for raising me to be disciplined and studious above all else.

Introduction

"There may be a good chance that the substantive issues of information warfare will not be addressed until the United States is actually engaged in an information war."[1]

-Richard Jensen, 1997

Through the 1990s the United States global technology advantage demonstrated their ownership of the information environment (IE) and made that clear to the world in the First Gulf War. The United States employed airborne command and control (C2) platforms and sensors to develop battlespace awareness and utilized electronic warfare to jam Iraqi C2 nodes. Therefore, Richard Jensen's information war had already occurred, yet the United States missed the opportunity to capitalize on this advantage beyond this success. In contrast, Chinese officials took note of how far their military lagged behind the United States in the IE—so much so that they called the First Gulf War *zhongda biange*, "the great transformation."[2] Accordingly, China and other peer competitors have significantly advanced their understanding and capabilities in the IE. While the US military recognizes the need to continue the emphasis on operations in the IE, it still debates what this means and how to best integrate planning and execution.

Today's military must be able to compete in a digitally interoperable operating environment (OE) that the Marine Corps Operating Concept characterizes as "complex terrain, technology proliferation, information warfare (IW), the need to shield and exploit signatures, and an increasingly non-permissive maritime domain."[3] Furthermore, Chief of Naval Operations, Admiral John Richardson, says, "What has emerged is a much more challenging scenario, where the first considerations for fleet action must account for maneuver[ing]—not only in the physical world on, under, and over the seas, but also in the virtual world—the electromagnetic spectrum, space, and cyberspace. When naval forces do get moving in the physical world, they will be made more capable when networked together, and their success will depend very much on achieving and maintaining decision superiority."[4] Therefore, a composited Navy and Marine

Corps team, or what can be called the Maritime Task Force (MTF) commander, must improve unity of effort to gain the information advantage resulting in battlefield decision superiority.[5]

Decision superiority is being able to out-decide your adversary in a given amount of time and making the most informed decision, a sentiment that shadows John Boyd's recognition that information dictates a time-based strategy.[6] To achieve decision superiority, a commander must attain a position of competitive advantage in the IE. However, the MTF is not manned, trained, equipped, or organized to meet the demands of the OE. How the Navy and Marine Corps conducts integrated operations in the information environment requires modifications to achieve the essential unity of effort necessary to gain and maintain decision superiority.

In addition to recommending modifications to achieve unity of effort, this analysis suggests how the MTF can integrate information-related capabilities (IRCs) across an IE functional framework. The recommendations stem from first analyzing operations in the information and maritime environments and then examining how the United States Navy and Marine Corps currently fights in the IE. If these recommendations are incorporated in the future OE, then an integrated MTF conducting operations in the IE can ensure the commander has decision superiority. Decision superiority allows the United States to recapture the central role of the IE—a critical aspect to win the next fight.

I. Defining the Information Environment and its Operations

Information Warfare (IW), in the context of Deception and Psychological Operations, is utilized throughout history. Still, the first American document that introduced the term IW originated in a now declassified Department of Defense (DoD) Directive TS-3600.1, released in 1992.[7] Its definition focused on attacking adversary information systems using signals intelligence and command and control countermeasures (C2CM) while protecting friendly information systems.[8] The stated objective was to "attain a significant enough information advantage to enable the force overall to predominate and to do so quickly."[9] In other words, the focus was to achieve victory by making a battle unnecessary. This aligns with Eastern War theory and the writings of Sun Tzu and Mao Tse-Tung that aims at winning without fighting.[10]

While the United States was trying to determine IW's degree of distinctness, China coined the term *zhixinxiquan*, "information dominance," referring to the measurement of operational advantage the friendly force has in protecting its information capabilities while denying the enemy's capability.[11] This term and its translated definition became widely accepted in the United States military for nearly two decades. But technology advances came with a transformation of the lexicon associated with information, its location, and its usefulness on the modern battlefield. Thus, there has been a shift from measuring information dominance to obtaining information superiority. Specifically, information superiority, as defined by DOD joint publication (JP), is "the operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same."[12] Arguably, it is the ends by which IW aims to achieve.

General Ronald R. Fogleman, former Air Force Chief of Staff, was able to succinctly codify centuries of IW advantages, from the Trojan Horse to World War II codebreaking, into

the Fifth [Domain] of Warfare.[13] Previously the Land, Sea, Air, and Space represented the only domains of warfare. While the term of the last century was IW, it was evolving 21st-century military doctrine that has shifted the name from "Information Warfare" to "Information Operations (IO)" to "Operations in the Information Environment (OIE)."[14] This change was as much to do with interservice thinking as coherent logic. Dr. Christopher Paul, a social scientist with RAND Corp, says, "The Joint Concept for Operating in the Information Environment (JCOIE) and the addition of information as a joint function both require bigger changes to joint thinking and processes than just adjusting some of the relevant terminology. The joint force must consider bigger changes."[15] The ambiguity in the lexicon is one of the driving issues for lacking unity of effort in the IE. With this in mind, this research paper uses IO and OIE synonymously.

A deeper appreciation of the IE and its functions are required to understand OIE. First, it is essential to understand the environment in which information exists. JP 3-0, *Joint Operations*, says, "Information affects the perceptions and attitudes that drive the behavior and decision making of humans and automated systems." The environment in which this information exists is a crucial component of the OE. JP 3-0 further defines the IE as "numerous social, cultural, cognitive, technical, and physical attributes that act upon and impart knowledge, understanding, beliefs, worldviews, and, ultimately, actions of an individual, group, system, community, or organization."[16] The IE, represented in Figure 1, is made up of three interconnected dimensions—physical, informational, and cognitive—which continuously interact with individuals, organizations, and systems.

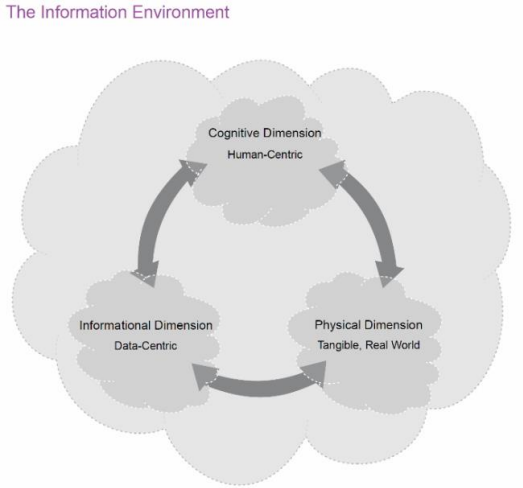

Figure 1: The Information Environment. Source: JP 3-13, Information Operations.

The JCOIE says, "This construct works well in analyzing how data flows through information systems and networks to reach a receiver but becomes problematic when trying to understand the meaning activities communicate in a pervasive and dynamic IE."[17] Ultimately, the IE perpetually exists ubiquitously or in all dimensions and across all five warfighting domains. The three dimensions, defined in Table 1, operate in a harmonized effort linking the cognitive thoughts of an individual existing in a physical environment to transmitted thoughts in the IE. JP 3-13, *Information Operations*, says, "Defining these influencing factors in a given environment is critical for understanding how to best influence the mind of the decision maker and create the desired effects."[18]

Table 1: 3 Dimensions of the Information Environment SOURCE: JP 3-13, Information Operations

Physical Dimension	C2 systems, key decision makers, and supporting infrastructure that enable individuals and organizations to create effects. It is the dimension where physical platforms and the communications networks that connect them reside.
Informational Dimension	Where and how information is collected, processed, stored, disseminated, and protected.
Cognative Dimension	The minds of those who transmit, receive, and respond to or act on information. It refers to individuals' or groups' information processing, perception, judgment, and decision making.

In these dimensions and across the warfighting domains exist a need to conduct coordinated military operations in the IE. The Marine Air Ground Task Force Information Environment Operations Concept of Employment (MAGTF IEO CoE) defines these operations as "a broad set of activities occurring in or through the IE which is conducted at the operational or strategic level to achieve operational or strategic objectives."[19] This research paper recognizes that the Joint term, OIE, does not align with the Marine Corps term IEO; however, for purposes of consistency, the term OIE will be used throughout this paper.

A set of capabilities are required to operate in the IE. The JP 3-13 defines IRCs as "tools, techniques, or activities that affect any of the three dimensions of the information environment."[20] Examples of universally accepted IRCs include information assurance, military information support operations (MISO), electronic attack, combat camera, counterintelligence, public affairs, civil-military operations, offensive cyber operations, and Key Leader Engagement (KLE). Operational capability areas group IRCs: "electromagnetic spectrum (EMS) operations, cyberspace operations, space operations, influence operations, deception operations, and inform operations."[21] These areas align with other joint doctrine publications which codify the joint principles, provides a guide to conduct operations, and recognizes authorities.

LtCol Michael Fitts, in the *Marine Corps Gazette* article, "Adding Information-Related Capabilities," says that planners underutilize the full complement of IRCs because they are not always considered a psychological effect. He continues to say that IRCs are "an often-overlooked application of integrated fires is the employment of IRCs to generate lethal and non-lethal effects that complement both maneuver and traditional means of lethal fires."[22] To that ends, IRCs are utilized to "affect the ability of the target audience (TA) to collect, process, or disseminate information before and after [making] decisions."[23] There are three types of TAs—

Key Influencers, Vulnerable Populations, and Mass Audiences—and they share information through various means.

Beyond these psychological effects, there may be desired physical effects to deny, degrade, deceive, and disrupt to accomplish compromising confidentiality, integrity, and availability of sensors, systems, and signals. "The joint force (means) employs IRCs (ways) to affect the information provided to or disseminated from the TA in the physical and informational dimensions of the information environment to affect decision making."[24] Therefore the ends of the OIE is the process to influence the physical and psychological effects of the TA. Figure 2 depicts this process.

Understanding OIE and knowing its functions helps differentiate OIE from other

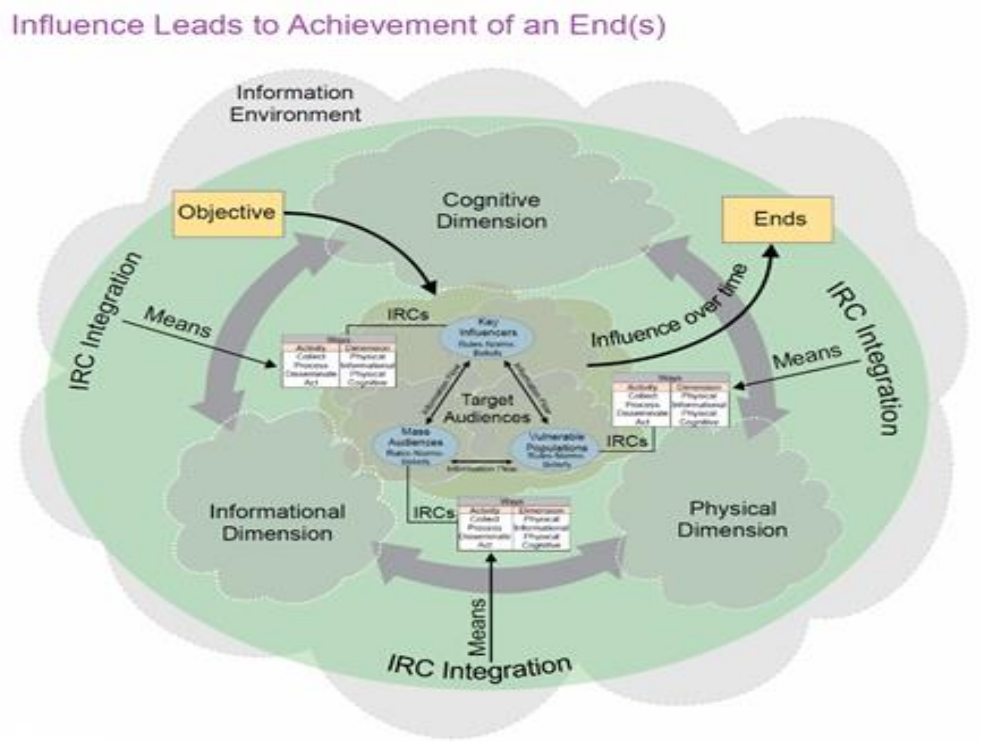

Figure 2: Complete OIE Process. Source: JP 3-13, Information Operations.

operations conducted in the OE. While these seven functions provide IE feasibility and distinguishability, they are not joint doctrine. This research paper further recognizes the seven functions may need refinements to integrate the MTF; however, decision superiority rests on

friction and chance. Unity of effort does not speak to a regimented means of TTPs but speaks more to embracing ambiguity. This allows commanders to make instinctive decisions reinforced within an IE framework and supported by IRC employment on a contested maritime battlefield.

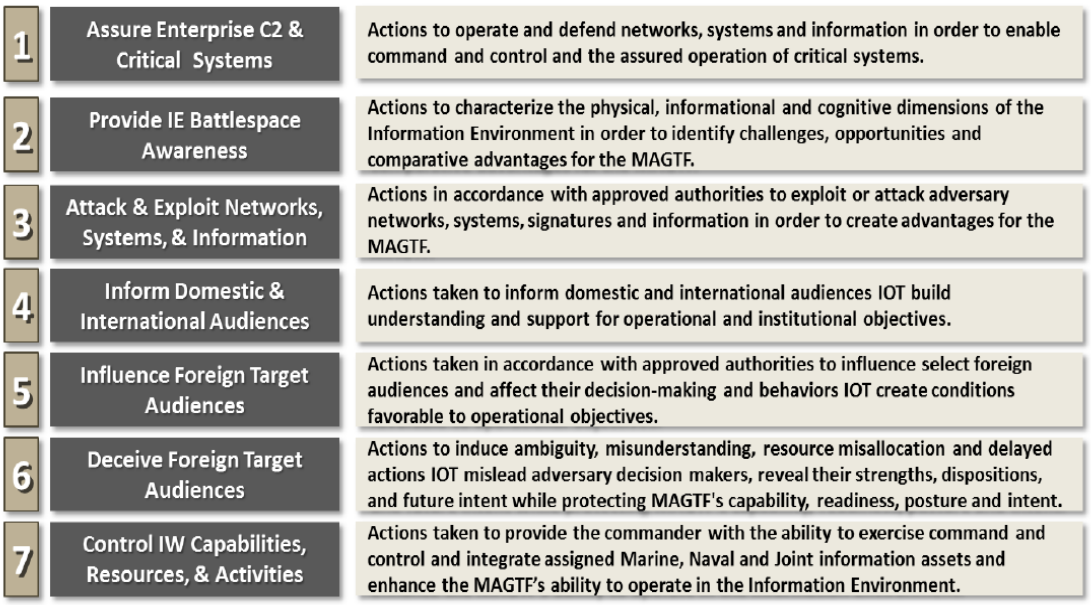

Figure 3. 7 Functions of OIE. Source: MAGTF IEO COE.

II. Defining the Maritime OE and its Littorals

The signatories of the US Constitution understood that what today is called the maritime operating environment was so critical to national interests that they required the Congress to "maintain a Navy." JP 3-32, *Command and Control of Joint Maritime Operations,* defines maritime operations as "any actions performed by maritime forces to gain or exploit command of [the] sea, sea control, sea denial, or to project power from the sea."[25] Maritime operations encompass the area on, under, or over the sea which covers 96 percent of the earth. Like the IE, it is important to understand the area where maritime operations are expected to take place.

The MTF operates in the maritime domain and its littorals. Joint doctrine defines the maritime domain as "the oceans, seas, bays, estuaries, islands, coastal areas, and the airspace above these, including the littorals."[26] Ninety percent of international trade crosses the maritime environment, and about 40 percent of the world population lives within 100 miles of a coast. The maritime environment is complex because it "encompasses the confluence of water, air, land, as well as space and cyberspace and is infinite in its variations."[27] Thus any operations in the maritime environment are intrinsically complex and often problematic.

The most complex area of this environment is operations that transition through the littorals. Joint doctrine says the littoral consists of two parts within the OE. First, "seaward: the area from the shore to the open ocean, which must be controlled to support operations ashore" and "landward: the area inland from the shore that is supportable and defendable from the sea."[28] The complexity and opportunity for conflict within the littorals are where the MTF is primed to conduct littoral operations in a contested environment (LOCE).

Today's maritime environment, specifically the littorals, are becoming increasingly more contested and without the need for physical control but through influence. The rising challenges

of anti-access/area-denial (A2/AD) weapons. A2/AD can be accomplished by hard effects (missiles or small boat ops) or soft effects (electronic-warfare (EW)). These effects require the United States to rethink how it will project military power in a contested maritime domain without the freedom of maneuver. Captain Wayne P. Hughes, USN (Ret.), and Rear Admiral Robert P. Girrier, USN (Ret.), said, "[C2] is more difficult in littoral waters because larger numbers of units must cooperate and [C2CM] must confuse or confound many more enemy vessels."[29] Littorals differ across the globe because partner nations and competitors have different operating methods in addition to the challenges in logistics, C2, and maneuver.

Surprise and small weapon engagement zones are commonplace in the littorals due to remote islands, rapidly changing subsurface environments, and neutral shipping. An MTF must seek to achieve sea control and power projection to operate from a position of advantage in this contested environment. Joint doctrine provides examples of sea control operations as destroying enemy naval forces, suppressing enemy sea commerce, and the protecting vital sea lanes.[30] Power projection is "accomplished by an amphibious raid or assault, attack of targets ashore (e.g., strike operations, close air support, naval surface fire support), operations conducted from a sea base or combinations of these."[31] LOCE occurs in both physical or IE.

With the maritime environment spanning such a large part of the globe, the United States demands its MTF to conduct LOCE. These operations nest OIE with the maritime environment. IE related considerations include space-based navigation systems, A2/AD sensor to launcher connectivity, and maritime emissions control for deception operations. Therefore, LOCE is not possible without the MTF integrating its IRCs.

III. How the Navy fights in the IE

Equally important to understanding the maritime environment is how the Navy fights and organizes to compete in the IE. The 2010 Navy Operating Concept (NOC) identifies the central idea is to use "the sea as maneuver space" to gain all-domain access or more importantly achieve seapower.[32] To do this the navy uses a combined-arms approach with "mission-tailored forces integrating sea, air, land, space, cyberspace, and information operation capabilities employed from ships and submarines; carrier-, amphibious ship- and land-based aircraft; ground vehicles; and remote sites outside the theater of operations; to achieve assigned objectives."[33] Integrating these seapower warfighting capabilities enables a commander's global awareness of the OE.

In modern naval combat, emerging hard or soft A2/AD threats dominate the ability of ships and aircraft to maneuver. Given these types of systems, it is now more than ever, important for commanders to make quick tactical calculations to reposition. These timely decisions require global awareness and an adaptive decision-making process that enables commanders to make rapid decisions in the IE. So how has the navy operated in the IE through the years?

Navy IO has roots tracing back to the beginnings of naval warfare. Military Deception (MILDEC) in support of maritime operations was vital to survival at sea. Utilizing deceptive lighting or silence to conduct a stealthy maneuver to gain an advantageous position without detection. MILDEC during amphibious operations came to light to a greater degree during World War II (WWII). In March 1943, Navy Lieutenant Douglas Fairbanks, Jr., conceptualized tactical cover and deception operations by employing small units, known as Beach Jumpers, to simulate amphibious landings with communication jammers, naval balloons, rockets, smoke generators, and radar intercept receivers thereby deceiving and confusing the enemy.[34]

Beyond WWII, the Beach Jumpers Unit, and later Fleet Composite Operational Readiness Groups (FLTCORGRU), were reactivated during the Korean and Vietnam Wars with

an additional mission to "plan and execute Psychological Operations."[35] Through the latter part of the 19th Century, a series of command mergers and name changes occurred that eventually led to the Fleet Information Warfare Center (FIWC), the Navy's IW Center of Excellence. This dramatic shift focused on defensive IW programs, such as computer incident response.

However, in the wake of the 9/11 attacks and the CNOC changing navy IO from a complementary naval warfare area to a primary naval warfare area required infrastructure realignment.[36] The merger of FIWC and Navy Security Group Activity (NGSA) resulted in Navy Information Operations Center (NIOC). In 2018, Information Warfare Training Group (IWTG) replaced NIOC. This change shifted focus to IW and training commanders in the areas of Cyber, EW, Cryptologic, Intelligence, Communications, Meteorology/Oceanography, and Space.[37]

The Deputy Chief of Naval Operations for Information Dominance (OPNAV N2/N6) is the senior office for managing intelligence, cyber, command and control, electronic warfare, battle management, oceanography and meteorology capabilities. N2/N6's mission is to "provide accountability for information-related capabilities, requirements, investments, and IE forces. N2/N6 is also tasked with directing the efforts of military and civilian professionals that make up the Information Dominance Corps and supply warfare commanders with Assured Command and Control, Battlespace Awareness, and Integrated Fires."[38] Additionally, the Navy establish Tenth Fleet with the responsibility of conducing cyberspace operations. The Navy focus is on conducting OIE, but absent is Marine Corps integration.

Navy OIE C2

Throughout US Naval history, and as new technologies emerged, a swing between centralized and decentralized C2 occurred. However, decentralized C2 achieved greater success at the maritime tactical level; thus, a framework was developed to provide guidance at the tactical level

to counter the multidimensional Soviet threat during the Cold War. The framework for decentralized C2 is the Composite Warfare Commander (CWC) construct designed to "monitor, access, plan, and direct warfare tasks."[39]

The Composite Warfare Doctrine (NWP 3-56) identifies 20 functional mission areas; however, these mission areas are expected to evolve with emerging technology and a shift in doctrinal thinking.[40] Leaders, assigned the task of CWC, range from subordinate commanders, the officer in tactical command (OTC), and functional group commanders. With the level of complexity and activity involved with the numerous mission areas in maritime operations, the CWC can retain or delegate its functions to subordinates through a tiered structure - Warfare Commanders, Functional Group Commanders, and Coordinators (Figure 4).

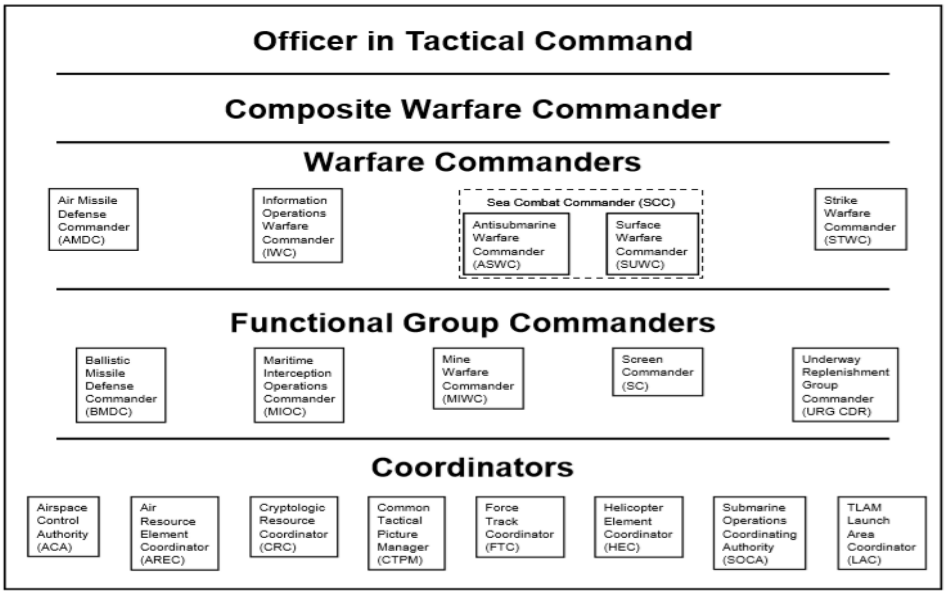

Figure 4. Composite Warfare Tiered Structure. Source: NWP 3-56 p. 1-16

The Warfare Commanders are responsible for more enduring mission areas. The Function Group Commanders perform limited scope and duration mission areas. The coordinators manage assigned resources and are limited to execute the policies of the OTC or CWC. Whereas each tiered commander may share a resource, sensor or weapon system, "only one commander may have [tactical control] of a platform at any given time."[41] Coordination of IRCs is challenging

due to the increased demand for influence across multiple mission areas.

CWC identifies an Information Operations Warfare Commander (IWC) to handle OIE. IWC responsibility is to "shape and assess the IE; to achieve and maintain information superiority; develop and execute IO plans in support of CWC objectives; and support other warfare commanders."[42] All domain access is required to provide cross-domain capabilities to enable battlespace awareness, assured C2, cyberspace operations, electronic maneuver warfare, and integrated fires.[43] The IWC functions are nested in the seven OIE Functions (Table 2).

IWC Functions	OIE Functions
1. Assist IO planning and integration.	Provide IE Battlespace Awareness
2. Assist EW planning and integration.	Provide IE Battlespace Awareness
3. Coordinate/control force electronic attack/support (EA/ES).	Attack/Exploit Networks, Systems, & Info
4. Coordinate/control offensive cyber operations (OCO).	Attack/Exploit Networks, Systems, & Info
5. Recommend the force emissions control (EMCON) profile.	Deceive Foreign Target Audience
6. Establish friendly communications security monitoring plan.	Assure Enterprise C2 & Critical Systems
7. Formulate and promulgate afloat EMS operations program.	C2 IW Capabilities, Resources, & Activities
8. Coordinate for support aircraft.	C2 IW Capabilities, Resources, & Activities
9. Coord employment of SIGINT equipment for tactical intel.	Attack/Exploit Networks, Systems, & Info
10. Direct the use of force expendable decoy resources.	Deceive Foreign Target Audience
11. Develop plans for countersurveillance, counter-influence, and counter-targeting.	Influence Foreign Target Audiences
12. Recommend defensive measures and readiness conditions.	C2 IW Capabilities, Resources, & Activities
13. Monitor operations to ensure strategic communication (SC) objective alignment.	Inform Domestic & International Audiences

Table 2. Summary of IWC Functions compared to OIE Functions.[44]

Navy Tactics, Techniques, and Procedures (TTPs) manuals identify steps for integrating these functions with an embarked Marine Corps landing force (LF); however, there is a significant disconnect between documented TTPs and reality. Unfortunately, the IWC serves only to support the Navy without reinforcing LF objectives or integrating LF IRCs. There is no MTF unity of effort associated with OIE beyond a circumstantial ad hoc structure agreed upon by the Commander of the Amphibious Task Force (CATF) and Commander of the Landing Force (CLF).

IV. How the Marine Corps fights in the IE

While the previous chapter focused on how the navy fights in the IE, it is vitally important to understand the similarities and differences in how the Marine Corps views its operations in this environment. The current fight with ISIS and Taliban, along with the previous battles with Al-Qaeda, forced the Marine Corps to recognize the importance of OIE. It is important to know how the Marine Corps is different than the Navy in the IE.

First, a review of the Marine Corps' warfighting philosophy provides an understanding of how the Marine Corps thinks about warfighting. Maneuver warfare is the Marine Corps' concept for winning on today and tomorrow's battlefields. The intention behind this concept aims to "shatter the cohesion of the enemy system… to create a situation in which the enemy cannot function."[45] The intended outcome follows the principles established in Colonel John Boyd's Observe-Orient-Decide-Act (OODA) Loop. Bill Lind, in his book *Maneuver Warfare Handbook*, says, "Maneuver means Boyd Cycling the enemy, being consistently faster through however many OODA Loops it takes until the enemy loses his cohesion."[46] In other words, maneuver warfare's goal is to achieve decision superiority.

Marine Corps' expeditionary maneuver warfare consists of five core competencies, one of them being combined arms integration.[47] The combined arms effect is accomplished through tactics, techniques, and task organization of interoperable characteristics by a variety of interdependent units.[48] The Marine Corps' Single-Battle Concept aims to achieve operational battlespace success through intense and permanent effects on other areas and events.[49] However, winning on the battlefield does not always translate to success in the IE (e.g., Vietnam).

While the Marine Corps has demonstrated resounding success across the warfighting domains utilizing maneuver warfare with combined arms effects under the semblance of a single-battle concept, it is done so sparingly in the IE. In 2017, Marine Corps' Commandant,

General Robert B. Neller highlighted the contested nature of the IE by saying, "[Marines] will have to fight not only in the domains of land, sea, and air but also in space and cyberspace. We will have to fight for and with information on the battleground of perceptions and ideas. And we will have to win the battle of electromagnetic signatures in which to be detected is to be killed."[50] General Neller is saying that fighting in the IE is as much about operations as it is about strategy.

This statement pulls at the core of the Marine Corps Operating Concept (MOC) stating that the Marine Corps must "reinvigorate [its] emphasis on maneuver warfare and integrate information warfare into [its] combined arms approach."[51] The MOC stresses that the Marine Corps is not ready for the future OE, but it must "reaffirm the primacy to conduct maneuver warfare and combined arms… and integrating the Naval Force."[52] The MAGTF provides the naval force with both unique and complementary capability to support the essential functions, specifically all-domain access. The Marine Corps' role in sea control is its ability to project power by the functions of neutralizing threats and controlling terrain in the littorals.[53] The MAGTF's single battle concept reinforces the unique ability to perform these functions across an interdependent domain approach utilizing maneuver warfare and a combined arms approach.

While the MAGTF will use the IE as maneuver space, it will also use the OIE Functions to have a combined arms effect. The Marine Corps must complete two steps in order to enhance the ability of the MAGTF to conduct OIE. First, it is essential for the Marine Corps to create a professional and versatile organization that can provide the MAGTF with combined arms effects to achieve all-domains access. Secondly, the Marine Corps must "keep pace with ever-changing technologies to succeed on a battlefield where the ability to conduct cyberspace operations is as important as the ability to perform C2, maneuver, or [conduct] fires."[54] These two actions will make the future MAGTF more capable of operating in the 21st Century.

The Marine Corps shifted its focus to reorganize and keeping pace with battlefield advancements. First, the 2017 CMC Institutional-Level Task List for Deputy Commandants and Commanders established the Deputy Commandant for Information (DCI) thereby integrating and aligning Headquarters Marine Corps, its service organizations, and its policies. DCI, as OIE advocate, directly coordinates with Plans, Policies, and Operations (PP&O) and Marine Corps Combat Development Command (MCCDC) to integrate OIE with other warfighting areas and technology advancement. DCI structure includes the Marine Corps Intelligence Activity (MCIA), Marine Corps Information Operations Center (MCIOC), and Headquarters C4. This change stands to have a significant impact on the Marine Corps establishment.

A second effect of the MOC established the Marine Corps IW Task Force tasked to "develop a conceptual and organizational construct for operating forces and supporting establishment to enable integration of IW capabilities supporting the fusion of effects for the MAGTF and [IW] organizational options and potential courses of action."[55] As a result the publication of the MAGTF IEO CoE outlined 4 steps to how the Marine Corps will change by 2025 to meet those challenges by integrating: 1) planning and executing IE operations along functional lines of effort; 2) establishing a dedicated OIE organization, the MEF Information Group (MIG), charged with integrating OIE along functional lines of effort; 3) building agile and distributed command and control capabilities; and 4.) developing a near-real-time running estimate to feed the common operational picture.[56] While this is a significant step forward in Marine Corps OIE development, like the Navy, it has not gone far enough to integrate the IE.

V. Integrating Navy and Marine Corps IRCs

While the Navy and Marine Corps share the concept of maneuver warfare through combined arms, there is not a shared concept of conducting OIE. The Navy and Marine Corps published service-specific doctrine and task organized for their respective IO forces; however, neither defined an integrated Navy and Marine Corps OIE planning process to achieve decision superiority. The integration must start with aligning IRCs to make a more efficient MTF.

Although Joint doctrine addresses an integration requirement, it lacks the process to integrate IRCs. According to the DODD 3600.01, the management of IRCs will be the responsibility of the services but "will be brought together at a specific time and in a coherent and integrated fashion for use against adversaries and potential adversaries in support of military operations."[57] Achieving an integrated MTF requires integrating the planning and execution of IRCs along a framework. While there are many different frameworks by which to incorporate OIE, this research paper recommends aligning IRCs according to the seven OIE functions. These recommendations assume the IWC construct is the IE command structure by which the MTF will conduct LOCE.

Assure Enterprise C2 & Critical Systems

Afloat forces require a networked C2 environment that is ready, responsive, and resilient. Headquarters, Marine Corps C4 (HQMC C4) department released the Marine Corps' Strategy for Assured C2. Its vision is "an assured enterprise warfighting network allowing timely and persistent information exchange in most demanding environment and circumstances realized through efficient and responsible stewardship."[58] General Neller identifies four critical characteristics—Unity, Resiliency, Interoperable, and Expeditionary—that a networked IE must possess. It is through these characteristics that IRCs for Assured C2 alignment is possible.

Unity

The first characteristic where alignment is possible is in unifying the enterprise networks such that they are prescriptive across the fleet. The Marine Corps Strategy for Assured C2 defines unification as "the term used to describe all actions associated with moving from legacy systems, processes, and organizations to a modern [network]."[59] Currently, there are numerous afloat networks at various stages of maintenance and upgrades. Unfortunately, the current navy fielding plan is not adaptive to technology changes. There is no expectation that this aspect will change because ships require lengthy and expensive overhauls to improve what was thought to be permanent C2 infrastructure. However, it is essential that future shipbuilding must include flexibility enabling C2 infrastructure modification.

Additionally, embarking Marine Corps force must reconstruct network before deployment. In the age of virtualization and cloud storage, there are logical solutions to this process that would reduce costs, increase efficiency, and improve security. DCI should dedicate resources from Headquarters C4 to solving this problem and enforce a comprehensive network architecture consistent with the quality of service garrison-based networks provide. Advancement of the naval network will position the MTF to operate in the IE.

Resiliency

The second characteristic of assured C2 ensures that afloat networks are resilient to a C2 denied or degraded environment (C2D2E). There is a growing notion that the responsibility of assured enterprise C2 and its critical systems is a function of cyberspace security. While there certainly exists a C2 network defensive approach, that approach is more of a *defense with a purpose*. This approach includes actions performed by other warfighting functions which may be

used to destroy, degrade, deny, or deceive enemy capabilities and operations targeting or affecting C2 systems and other Key Terrain-Cyber (KT-C).

An integrated planning effort to synchronize MTF Information Operations Conditions (INFOCON) and Emissions Controls (EMCON) are essential to assured C2 as well as developing a smaller signature footprint.[60] As the Navy and Marine Corps implement capabilities to maneuver in the EMS, they must also integrate concepts focused on decrease reliance and measured utilization of the same EMS capabilities. The requirement to maintain a low probability of detection (LPD) is critical to operate in the contested electromagnetic environment and maintain a defensive posture to ensure a low probability of intercept (LPI).

It must be a collaborate planning effort from both the landward and seaward forces to operate across the EMS in the maritime OE. The MTF should coordinate and deconflict EMS operations with space operations early in the planning cycle to identify communication windows in which shipboard and airborne sensors and organic transmission systems synchronize with other maritime operations. An example of integrated resiliency is a deployed reconnaissance team utilizing multi-spectrum assets during prescribed emissions windows before a raid occurs.

Additionally, there MTF must look at connectivity without the advantage of satellite communications. Beyond-Line-of-Sight systems like Free-Space Optics or Space Data's SkySat radio relay can shift or reduce the signature footprint.[61] Overreliance on satellite communications is the norm and employing emerging tech while enforcing radio discipline will create resiliency.

Interoperable

The third characteristic to improve is ensuring that enterprise networks and C2 systems are interoperable. Arguably the most challenging functional part of developing digital

interoperability, in Navy-Marine Corps' networks, is the agreements upon common hardware and software. At first glance, the networks and systems appear the same (e.g., Dell Computers with Microsoft Windows) but service specific acquisition processes prevent interoperability. The Navy and Marine Corps should share a universal application or system development cycle. However, this comes with significant bureaucracy. Therefore, the Navy and Marine Corps should sign memorandums of agreements requiring interoperability of service-specific emerging technology, and its software, primarily where it supports an integrated warfighting function.

Currently, there is no interoperability of Defensive Cyber Operations (DCO). The Navy is reliant on external support to conduct DCO whereas the Marine Corps embarks its personnel. Unfortunately, neither are permitted to perform operations across non-homogenous baselines. Marine Corps Forces Cyber (MARFORCYBER) and US Navy's Tenth Fleet's Chief Compliance Departments should develop policy authorizing embarked Cyber Defense Marines or the Navy's remotely connected operations centers to conduct active and passive DCO. The most substantial barriers to MTF interoperability are service-specific regulations and trust.

Expeditionary

The final characteristic of Assured C2 lies in the ability to power project and maintain sea control. These abilities rely on the MTF to keep a state of responsive and proactive readiness with the expectation of the force returning to a sea base. All MTF expeditionary technological solutions must have creative embarkable employment methods that support delivery by any L-Class ship or ship-to-shore connector, may it be surface or air. An example of the Marine Corps' ability to rapidly extend shipboard networks is through a MEU detachment commonly known as the Joint Task Force Enabler (JTFE). Primarily embarked on vehicles, the team can rapid

reorganize critical components into a fly-away capability. The modular equipment loadout provides the MTF with a deployable and logistically self-sustainable communications team. The JTFE is designed to establish a joint-level shore-based communications node capable to integrating up-to 500 users (limited only by deployable computer assets) with secure and non-secure voice, video and data capabilities that are interconnected with the other MAGTF elements and Navy surface ships to support an organic forward command post. The JTFE a non-standardized capability across all MAGTFs. However, the expeditionary C2 enabler concept is not lost on the waterfront communications community to provide the MTF commander.

Also, at-sea limitation restrains emerging software and applications. The Marine Corps' Strategy for Assured C2 says, "for all the focus on the Internet of Things, innovative applications, and cyber-dependent weapons systems, it is easy to overlook the fact that these capabilities often are realized only when properly networked."[62] As the military moves to a more on-demand virtual environment with cloud services the requirement is predicated on connectivity to the global backbone. It is common for the MTF to operate in C2D2E for extended periods. Therefore, network segregation is a crucial consideration for connection-oriented technology development. For systems to work in C2D2E, emerging concepts such as the Deployed Marine Corps Enterprise Network (DMCEN) and functional warfighting applications (i.e., GCSS-MC) require connectionless alternatives. New applications are not needed but additive measures, such as offline sync-enabled features, must be sourced and incorporated in existing services.

These four characteristics are the framework that sets the conditions for a ready, responsive, and resilient networked C2 environment. Expeditionary forces must consider network security and begin to think like submariners—conscious tactical decisions of emission and only emitting when required—to achieve assured C2.

Provide IE Battlespace Awareness

Captain (USN) Patrick Molenda says, “if the navy is going to be effective in electromagnetic maneuver, it must wean itself off the addiction to constant information drawn from the unit level to feed higher headquarters' insatiable demands for tactical-level situational awareness.”[63] While new technology provides greater battlespace awareness through on-demand real-time video feeds it also places higher demands on the information pull. However, new technology also ushers in the era of artificial intelligence (AI) that supports emerging technology, global awareness, and IRCs management. An AI example supporting the MTF is integration of automated logistical predictive software that forecasts maintenance failures while increasing resource replenishment.

The MTF must integrate IW capabilities through assured, adaptable, resilient, and distributed C2, under the IWC construct. This integration will provide comprehensive sensing and a shared understanding of the maritime battlespace while allowing quick assessment or predictive sustainment and mobility requirements by leveraging supporting capabilities to sense the battlefield environment and friendly situation. That friendly situation is supported by a global awareness by linking sensors and other IRCs from both the ATF and the LF’s capabilities and simultaneously cueing additional, focused sensors in a single battle concept.

Attack & Exploit Networks, Systems, & Information

Jason Healey, in his book *A Fierce Domain*, points out that Russian cyber-attacks on Ukraine and Georgian government and media outlets were used to shape the information environment. This conflict was the first integration of cyber and conventional forces creating a total land, air, sea, and cyberspace operations. The next convergence of cyber and conventional operations could occur during expeditionary operations. A contested littoral OE regulated by an enemy A2AD threat poses a severe challenge for an MTF commander, and cyber might be the answer.

In cyberspace, one central node is rarely the optimal target. Instead, the optimal targets are the critical vulnerabilities of individual critical capabilities that support the primary node. An example of a critical vulnerability may be the power station supplying power to lights along a beach landing site or creating disorganization in a port management system by which an adversary launches small attack vessels. These two examples are offensively minded approaches to support maritime operations. The same thinking should be considered each time there is an A2AD weapon system that is affecting maneuver space, a potential mitigation to this type system to conduct a cyber blockade of that area.

The concept of a cyber blockade, as explained by Dr. Alison Russel in her book by the same title, is the cyber disruption to the ingress/egress of information into a target area.[64] Just as a navy establishes a barrier to prevent access of ships to a port or beach, so too can cyber actions prevent the flow of data required to engage a weapon system. In the A2AD threat example, a cyber-attack launched at disrupting its sensor/launcher system can create a system disruption providing time and space for the MTF to maneuver through a contested environment.

Attacks on cyberinfrastructure are not limited to “soft” non-kinetic actions because a precision strike can have a similar result. Networks require connectivity through a medium or transmission system. Often those transmission systems are locally connected via cable, such as fiber optics. The use of a cabled transmission system makes it hard to penetrate but easy to break. A kinetic attack on a fiber distribution node may disconnect the grid. Alternatively, striking ground-based satellite transmission nodes would achieve the same effect.

Finally, it is important to note the need for timing is essential to all communication devices. Manipulating timing by even milliseconds on a transmission system can cause synchronization and data loss which would affect information without the effect of network

destruction. It is possible this technique would provide friendly forces with the ability to reestablish connectivity as operations move further inland. There are advantages if used to inform fighters to lay down arms in the event of a ceasefire, consider the number of Japanese on remote islands still ready to fight well into 1950 but lacked the means to be informed by the emperor. At the tactical level, it is vital to identify cyber exclusion zones where forces may want to allow or at a minimum reenable services once a disruption has occurred. Therefore, the MTF must coordinate and deconflicting the targeting cycle for attack and exploit capabilities in near-real time across the single battle concept areas and operational scheme of maneuver.

Planning, integrating, and synchronizing OIE activities across all domains shall be done in a mutually reinforcing manner. There are advantages to kinetic attacks on cyber networks, but that munition is logistical challenging in LOCE. Operations and Intel sections must together identify enemy networks and systems and decide when to utilize kinetic or cyber-munitions.

Inform Domestic & International Audiences

The JP 3-0 says "inform activities involve the release of accurate information to domestic and international audiences to put joint operations in context; facilitate informed perceptions about military operations; and counter adversarial misinformation, disinformation, and propaganda."[65] Strategic messaging is about controlling the narrative through internal coordination, providing a favorable message, and competing with alternative messaging. Tactical level operations must always be nested in strategic level messaging, and the same applies in reverse.

Foreign Humanitarian Assistance operations are critical operations where controlling the narrative is vital. When "warships" arrive off the coast of a foreign country, it is either at the request of that nation or in times of war. American adversaries are continually trying to shape international opinion by creating a narrative that is counter to humanitarian assistance. This

example provides a target rich environment where it is a matter of who controls the narrative controls the outcome. Regardless of the amount of foreign aid provided, it is vital that the MTF creates consistent, integrated Navy-Marine Corps messaging with evidence that is relatable to the local populace. Otherwise, the adversary twists the military action to a negative.

The MTF must coordinate internally to produce advantageous messaging. In the article *Fighting Against, With, and Through Narrative*, scholars say that "a clear mission narrative can help troops avoid the 'say-do gap' that often opens between actions and communications, promotes unity of effort, and diminishes the likelihood of information fratricide."[66] Combatant Commanders should provide more releasing authorities to the MTF to reduce the space between actions and the messaging thus making information immediately available to the public. Given that US forces always attempt to meet international accords, the deployment of such forces can write a narrative that brings a measure of truth to an operation—a clear US advantage.

Influence Foreign Target Audiences

MTF commanders must conduct operational design and planning with the consideration of impacts and desired effects on relevant actor perceptions, attitudes, and other behaviors. Commanders influence TAs through the timing of decisive actions, structure of employed forces, and optical parameters of an operation.[67] Peer global competitors and terrorist organizations have been relatively successful in taking advantage of social media at the tactical level to influence the narrative of public opinion by spreading biased postings backed by altered imagery.

Effective influence is attained by synchronizing the MTF narrative with an understanding of the regional and cultural OE and then distributing that narrative to the TA. Knowing your TA is a crucial enabler to conducting operations abroad, whereas MISO is responsible for influencing foreign TA.[68] JP 3-13.2 identifies the keys to effective MISO as early and continuous

planning, nested MISO, and Communications Strategy efforts, use of local capabilities and assets, and responsive approval process.[69] Like MISO, Cyber electromagnetic activities (CEMA), a combination of Cyber and EW IRCs, provide effects on voice, video, and data adversary messaging and prevent the distortion of friendly narratives. Most of CEMAs remain at a classified level but are organic or available for tasking by the MTF.

Influencing at the tactical level can also be accomplished directly by the commanders. Commanders have been operating in an environment where influencing the local leadership has had dramatic impacts on the battlefields of Iraq and Afghanistan. KLE is about building relationships to affect behaviors favorably. KLE is a process, not a one-time event. It is important for the CATF to integrate into the CLF's battlefield circulation. The MTF should show unity during KLE while also coordinating MISO and CEMA effects to influence foreign TA.

Deceive Foreign Target Audiences

The art of deception is intrinsic in a military commander's decision-making; however, the science of deception is rather undeveloped in the MTF. Sir Michael Howard says deception is the influencing of an adversary's moves while concealing your own. Thus, demands are of good security and intelligence.[70] Studying the Battle of Grozny can teach the military a lot about deception.[71] Chechens were highly successful in conducting deception operations by decoys, disguise, disinformation, and demonstrations. All their actions were to represent a larger or different force than the Russian expected while conducting false radio broadcasts and demonstrations to take advantage of their highly effective "shoot-and-scoot" methods. These methods overloaded Russian intelligence with more information than could be processed to develop a battlefield picture. This delayed response actions and often created confusion in mission-tasking orders and thus delaying Russia's ability to gain decision superiority.

Similar to Chechen actions, small mobile Navy Beach Jumper units, specialized in conducting deception operations, were able to create major amphibious assaults appear where there were only limited surface vessels. This tactic ensured the adversary was looking in the opposite direction to use a light force as a tradeoff for time as the main effort conducted sea maneuvers. This same method is achievable today with swarming techniques of Unmanned Surface Vessels (USV) by recreating an EMS footprint representing a mechanized battalion.

Nonetheless, surface maneuvers are still required, and the military lacks the technology for over-the-horizon employment of amphibious assault vehicles (AAVs)—the only currently fielded tactically armored amphibious assault vehicle. Professor Barton Whaley says deception is a low-risk endeavor and using multiple false clues can prevent one failing and add credibility to the operation.[72] Cheaper multi-purpose emerging technology for deception operations is more cost-effective than producing significant quantities of new AAVs.

Equally crucial to deception is counter-deception, which is the art of neutralizing a deceptive enemy. Either through ship maneuvers or through utilizing technology (like USV identified above), the friendly behavior may achieve the desired result of movement by the adversary. In turn, dynamic combined-arms targeting can defeat the exposed enemy without giving away the main force or the decoys. Scholars from RAND said, "deception, in all of its myriad forms, should be made a primary instrument of both force multiplication and force protection."[73] Deception is essential to decision superiority, but absent unifying deception or counter-deception IRCs presents the risk of unintentional IE fratricide.

Control OIE Capabilities, Resources, & Activities

Service agnostic, there is a natural military tendency to regard the level of war with the same level of command regardless of the temporal and spatial dimensions. The evolution of OIE does

not require a new level of command at each level of war; preferably it requires employing a mechanism to control employment capabilities, resources, and activities at that level. That control requires integration to achieve decision superiority in the maritime environment. General Martin Dempsey said, "no C2 technology has ever successfully eliminated the fog of war, but it can create the illusion of perfect clarity from a distance."[74] There is a misperception that global support will be able to reach down to control the information fight. The MTF must be capable of conducting operations in C2D2E. While there are virtually connected IRCs that are useful in influencing the OE, there must be a mechanism to control these IRCs.

JP 5-00.2 states that complex or unclear command relationships and organizations can be counterproductive to developing synergy among multinational forces. Moreover, simplicity and clarity of expression are critical.[75] A Navy-Marine Corps integrated IWC construct is a structural gap that requires a modification to the current organizational structure to solve. JP 3-13 identifies a notional Information Operations Cell that is comprised of "representatives from a wide variety of organizations to coordinate and integrate additional activities."[76] Unfortunately, an MTF does not employ this cell. DCI and N2/N6 should decide how to integrate the MTF IO cell and IRCs. The mechanism of an integrated Navy-Marine Corps IO Cell will provide the MTF with the ability to layer effects on an adversary especially ones in complex maritime environments.

Additional Recommendations

In addition to recommendations presented in the functions identified above, there are supplementary areas required to resolve this integration gap. The Navy-Marine Corps requires common lexicon, standardized training, and skilled personnel to reduce or prevent service specific barriers in the IE. These recommendations require N2/N6 and DCI level changes.

Professor Dennis M. Murphy, director of the Information in Warfare Group at the Center for Strategic Leadership, says "the US military will master information by getting the doctrine right."[77] While many tie innovations to incorporating transformative technology, an equally powerful component of innovation are the concepts that include new TTPs that enable transformative effects. Whether it is the seven functions above or something entirely different the Navy and Marine Corps must develop a framework to organize IRC effects. Furthermore, Dr. Paul says, "The codification of information as a joint function in Joint Doctrine through JP 1, JP 3-0, and the change recommendations resulting from the [OIE] Capabilities-Based Assessment, have laid out a path toward changing how the joint force thinks about the role of information in operations and how it plans the use of information in operations."[78] Consistent naming conventions ensure integration across the services. N2/N6 and DCI should adopt the term OIE and recognize IO as the complementary cognitive effect to kinetic actions in the IE.

In relation to training Per DODD 3600.01, joint exercises and training will integrate OIE.[79] During Type Commander Amphibious Training (TCAT), maritime exercises, and ARG/MEU pre-deployment training program are opportunities to integrate IRCs. All events are typically observed and evaluated by advisors/evaluators from the respective Carrier Strike Group (CSG) and the Expeditionary Operations Training Group (EOTG). The CSG and EOTG should take steps to develop integrated evaluation criteria that require the IWC to utilize IRCs to conduct desired effects during evaluation. In each capability, there are examples of immediate changes that can take effect today. Both the CSG/EOTG need senior level OIE evaluators. Similarly, embarking an integrated Navy and Marine Corps Cyber Red Team with the purpose of conducting cyber network effects that include cross-boundary or lateral attacks. The mindset of

the network must be operational to facilitate physical operations must change. MTF training in C2D2E should become the norm rather than the exception.

Another area of training is in the employment of deception which is as critical to maritime operations as basic firearms skills. The MTF should focus on signature management. Specifically, reviewing the EMS footprint during landing force operations. While identifying the signature footprint is commonplace for the navy, it is uncommon for the MTF to review EMS footprints of ship-to-shore maneuver elements. Therefore, Navy and Marine Corps amphibious training exercises there shall be a coordinated effort to identify not only the ship's signature footprint but also that of an amphibious maneuver element.

To conduct maritime OIE, the Navy and Marine Corps requires a culture that leverages its top planners, operators, and commanders. Navy and Marine Corps must put skilled leadership in the MTF, capable of planning and executing within the IWC. However, the Marine Corps' IO community should establish a defined roadmap for IO planners and enablers in whom MAGTF commanders have the confidence to integrate planning and execute operations in the IE.

Marine Corps' Captain Luke Mannion, in *Institutionalizing Information Operations*, proposed the addition of either a path for IO Officer direct accession, as a Primary Military Occupational Specialty (PMOS), or a lateral transfer MOS opened to officers beginning after their first tour.[80] Whether the above-proposed course of action or an alternative, the importance of having a defined roadmap provides additional opportunities for IO Officers to integrate the MTF. In addition to providing a path for increasing experience, it is also essential to give a deploying MAGTF the right skill set mix of enablers to support the IWC.

VI. The Critical Importance of Decision Superiority

Success in war has always required a cognitive as well as physical advantage. Placing your adversary in a position of equally unfavorable alternatives allows one force to gain that advantage via decision superiority. Regardless of strength or position, information influences the human endeavor of decision-making. OIE is a critical aspect of the next fight and examining decision superiority makes commanders rethink cognitive engagement on the spectrum of conflict. Results are not always clear, as might be the case when measuring physical effects. The fog and friction of OIE require integrated and sequenced IRCs to achieve decision superiority and gain a coordinated physical and psychological advantage. As the United States integrates land and maritime forces to plan and conduct military operations in the IE, the Navy and Marine Corps are intrinsically linked to conduct mutually supporting maneuver warfare through combined arms in the maritime environment. While both the Navy and Marine Corps have IRCs, they are not integrated and therefore operate at a decision cycle disadvantage in the digitally interoperable OE. While this paper is heavily focused on Marine Corps recommendations, achieving unity of effort requires additional navy research on how to integrate to achieve decision superiority. Unity of effort in the IE will ensure information superiority and enable decision superiority over a peer adversary in the next littoral conflict. Ultimately, service-specific thinking must adapt to achieve seapower in the 21st century.

[1] Richard M. Jensen, *Information War Power: Lessons from Air Power* (Cambridge, MA: Program on Information Resources Policy, Harvard University, Center for Information Policy Research, 1997), 82.
[2] Richard A. Clark and Robert K Knake. *Cyber War: The Next Threat to National Security and What to Do About It.* 1st Ecco Pbk. ed. (New York: Ecco, 2012), 50. *Cyber War* reveals how the Chinese underwent a critical self-examination that ultimately led them to a new strategy now known as cyber war.
[3] Headquarters United States Marine Corps, *Marine Corps Operating Concept (MOC): How an Expeditionary Force Operates in the 21st Century* (Washington, DC: 2016), 5.
[4] Admiral John Richardson, foreword to *Fleet Tactics and Naval Operations*, 3rd ed., edited by Wayne P. Hughes and Robert Girrier (The US Naval Institute Blue & Gold Professional Library, Annapolis: Naval Institute Press, June 15, 2018), XX.
[5] The non-traditional term Maritime Task Force (MTF) was develop for purposes of this paper to simplify a composited Navy and Marine Corps team operating in the littoral environment with the mission of sea control and power projection.
[6] John Boyd, USAF (Ret.) is one of the founding members of maneuver warfare. He created the Observe-Orient-Decide-Act (OODA) Loop focused on a time-based strategy to out think, out-decide, and outperform an adversary.
[7] Department of Defense, *Information Operations*, Directive, No. 3600.01 with Change 1, (Washington, DC: May 4, 2017). This directive identifies the joint definition of IO.
[8] Wayne P. Hughes and Robert Girrier, *Fleet Tactics and Naval Operations, 3rd ed*, The US Naval Institute Blue & Gold Professional Library, Annapolis Naval Institute Press, 2018. C2CM is defined as "actions taken to inhibit effective enemy C2".
[9] Department of Defense, *Information Warfare*, Directive. No. TS 3600.1, (Washington, DC: December 21, 1992) as quoted in Michael Warner, *Notes on Military Doctrine for Cyberspace Operations in the United States, 1992-2014*,Cyber Defense Review accessed March 22, 2019, https://cyberdefensereview.army.mil/CDR-Content/Articles/Article-View/Article/1136012/notes-on-military-doctrine-for-cyberspace-operations-in-the-united-states-1992/.
[10] More on Eastern War Theory and Chinese Military philosophy can be found by reading *The Art of War* by Sun Tzu and *Protracted War* by Mao Tse-Tung.
[11] Headquarters United States Army, *Information Operations*, FM 100-6, (Washington, DC: Headquarters Department of the Army, US Army, August 27, 1996), 1-9.
[12] United States, Joint Chiefs of Staff, *Information Operations*, JP 3-13, (Washington, DC: Joint Chiefs of Staff, November 20, 2014), GL-3.
[13] Ronald R. Fogleman, "Information Operations: The Fifth Dimension of Warfare," *Defense Issues* 10 (47, 1995): 1.
[14] This study recognizes there are differences in lexicon between Operations in the Information Environment (OIE) and Information Environment Operations (IEO) that the Marine Corps and Joint Concepts of Employment contradict, however the utilization of Joint terminology will provide consistency for this research. In all cases, except reference, the term IEO has been changed to OIE.
[15] Christopher Paul, "Is It Time to Abandon the Term Information Operations?," TheStrategyBridge.org, March 11, 2019, https://thestrategybridge.org/the-bridge/2019/3/11/is-it-time-to-abandon-the-term-information-operations.
[16] United States, Joint Chiefs of Staff, *Joint Operations*, JP 3-0 w/ change 1, (Washington, DC: Joint Chiefs of Staff, Oct 22, 2018), IV-1 to IV-2.
[17] United States, Joint Chiefs of Staff, *Joint Concept for Operating in the Information Environment (JCOIE)*, (Washington, DC: Joint Chiefs of Staff, July 25, 2018), 3.
[18] *Information Operations*, JP 3-13, I-3.
[19] Deputy Commandant for Combat Development and Integration, Marine Air Ground Task Force Information Environment Operations Concept of Employment (MAGTF IEO CoE), (Quantico, VA: United States Marine Corps, July 6, 2017), 22. The terms Information Environment Operations (IEO) and Operations in the Information Environment (OIE) are used interchangeably. To align with the refence, IEO is used exclusively in this paper.
[20] *Information Operations*, JP 3-32, x.
[21] *MAGTF IEO CoE*, 22.
[22] LtCol Michael L. Fitts, "Adding Information-Related Capabilities," *Marine Corps Gazette* 100, (09, 2016): 69-71.
[23] *Information Operations*, JP 3-13, I-3.
[24] Ibid, x.
[25] United States, Joint Chiefs of Staff, *Command and Control for Joint Maritime Operations*, JP 3-32, (Washington, DC: Joint Chiefs of Staff, June 8, 2018), ix.

[26] Ibid, I-5.
[27] Department of the Navy, *Naval Operations Concept 2010*, (Washington, DC: Government Printing Office, 2010), 8.
[28] United States, Joint Chiefs of Staff, *Joint Intelligence Preparation of the Operational Environment*, JP 2-01.3, (Washington, DC: Joint Chiefs of Staff, May 21, 2014), GL-6. On the seaward side of highly contested areas, such as straights and gulfs, the littorals extend from shore to shore.
[29] Hughes, et al., *Fleet Tactics and Naval Operations*, 290.
[30] *Command and Control for Joint Maritime Operations*, JP 3-32, I-3 to I-4
[31] Ibid, I-4
[32] Naval Operations Concept 2010, 13.
[33] Ibid, 56.
[34] "US Navy Beach Jumpers," accessed January 18, 2019, http://www.psywarrior.com/beach.html.
[35] Ibid.
[36] Chief of Naval Operations, "Transforming Navy Information Operations (IO)," Washington, DC, May 24, 2002, as quoted in Michael J. Todd, James A. Grant, and David A. Jessen. "It's Time to Fix Navy Information Operations." United States Naval Institute.Proceedings 142, no. 6 (06, 2016): 80-82.
[37] IWTG Mission: Advance the Fleet's IW warfighting readiness through operational based training, highly experienced IW deployers and IW mission data management in support of afloat and ashore commands delivering decisive advantages in the maritime domain. https://www.public.navy.mil/FLTFOR/iwtgnorfolk/Pages/default.aspx
[38] Joe Gradisher, "Vice Adm. Branch Takes Charge of Information Dominance and Naval Intelligence," Navy.mil, July 25, 2013, accessed March 8, 2019. https://www.navy.mil/submit/display.asp?story_id=75580.
[39] Department of the Navy, *Composite Warfare Doctrine*, Navy Warfare Publication (NWP) 3-56, (Newport, RI: September 2010), 15.
[40] Ibid, 1-4. For additional review of mission areas reference OPNAVINST C3501.2K of Jan 22, 2010.
[41] Ibid, 1-15.
[42] Ibid, 3-6.
[43] Department of the Navy, *A Cooperative Strategy for 21st Century Seapower*, (Washington, DC: March 2015), 21.
[44] For a complete list of IWC functions reference *Composite Warfare Doctrine*, NWP 3-56, 3-6.
[45] Headquarters United States Marine Corps, *Warfighting*, MCDP 1, (Washington, DC: Headquarters Marine Corps, US Marine Corps, June 20, 1997), 74.
[46] William S. Lind, *Maneuver Warfare Handbook*, Westview Special Studies in Military Affairs, New York: Westview Press, 1985, 6.
[47] The Marine Corps core competencies define its culture and its contribution to the national. Those competencies are: Warfighting Culture and Dynamic Decision-making, Expeditionary Forward Operations, Sustainable and Interoperable Littoral Power Projection, Combined Arms Integration, and Forcible Entry from the Sea; for more reference *MOC.*
[48] *Warfighting*, MCDP 1, 94.
[49] The Single Battle concept views the battlespace through three major areas - Deep, Close, and Rear fight. These areas are consistent and intertwined across all domains.
[50] Commandant of the Marine Corps, *Message to the Force 2017: Seize the Initiative*, Washington, DC: 2017, 2.
[51] *MOC*, 4.
[52] Ibid, 8.
[53] Ibid, 11.
[54] Ibid, 20. Review for a comprehensive list of the Commandant's tasks to the Marine Corps.
[55] Headquarters United States Marine Corps, *Establishment of Marine Corps Information Warfare Task Force (MCIWTF)*, (MARADMIN 596/15), Washington, DC: Headquarters US Marine Corps, November 25, 2015.
[56] *MAGTF IEO CoE*, 2.
[57] *Information Operations*, Directive, No. 3600.01 with Change 1, 2.
[58] Headquarters United States Marine Corps, *Strategy for Assured Command and Control*, (Washington, DC: March 2017), 27.
[59] Ibid, 3.
[60] The INFOCON system presents a structured, coordinated approach to defend against and react to adversarial attacks on DODN systems. For more information see Strategic Command Directive (SD) 527-1.
[61] Free-Space Optics is an emerging technology that can reduce an EMS footprint by utilizing wireless fiber optics to transmit data. Additionally, Space Data's SkySat has been in use on MEU deployments since at least 2010. For

more information see https://www.dvidshub.net/news/printable/53174. For more see https://www.spacedata.net/government/skysat/

[62] *Strategy for Assured Command and Control*, 4.

[63] Patrick Molenda, "Silence on the Net," United States Naval Institute.Proceedings 141 (05, 2015): 34-39.

[64] Alison Lawlor Russell, *Cyber Blockades*, Washington DC: Georgetown University Press, 2014, 7.

[65] *Joint Operations*, JP 3-0 w/ change 1, III-19.

[66] Christopher Paul, Kristen S. Colley, and Laura Steckman. "Fighting Against, with, and through Narrative." Marine Corps Gazette 103, no. 3 (03, 2019): 80-87, https://mca-marines.org/gazette/fighting-against-with-and-through-narrative/.

[67] According to MCWP 3-40.4, *MAGTF IO, i*nfluence is to cause other to behave in a manner favorable to US forces. https://www.marines.mil/Portals/59/MCWP%203-40.4.pdf.

[68] United States, Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms*, JP 1-02 amended, (Washington, DC: Joint Chiefs of Staff, February 15, 2016), 152, https://fas.org/irp/doddir/dod/jp1_02.pdf; JP 1-02 defines MISO as planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals in a manner favorable to the originator's objectives.

[69] United States, Joint Chiefs of Staff, *Military Information Support Operations*, JP 3-13.2 with Change 1, (Washington, DC: Joint Chiefs of Staff, December 20, 2011), I-6.

[70] Michael Howard, *Strategic Deception in the Second World War, British Intelligence in the Second World War, V. 5*, New York: Norton, 1995, ix.

[71] The Battle of Gronzy, part of the First Chechen War (Dec 1994 – Aug 1996), was a Russian victory but not without significant loss. Russians outnumbered the Chechens 60,000 to 5,000 and deception techniques assisted in leveling the battlefield. More detail on deception operations in this battle can be read in *The Art of Darkness: Deception and Urban Operations* by Gerwehr and Glenn.

[72] The concept of using multiple false clues was developed by Harvard Professor Barton Whaley. His book *Stratagem: Deception and Surprise in War* contains the analysis of land base deception operations from 1914 to 1973.

[73] Scott Gerwehr and Russell W. Glenn, *Unweaving the Web Deception and Adaptation in Future Urban Operations*, Santa Monica, CA: Rand, 2002, 59.

[74] General Martin E. Dempsey, *Mission Command White Paper*, Washington, DC: Joint Chiefs of Staff, April 2012, 7.

[75] United States, Joint Chiefs of Staff, *Joint Task Force Planning Guidance and Procedures*, JP 5-00.2, (Washington, DC: Joint Chiefs of Staff, January 13, 1999), II-1.

[76] *Information Operations*, JP 3-13, II-4.

[77] Dennis M. Murphy, "The Future of Influence in Warfare," *Joint Force Quarterly: JFQ* (64, 2012): 47-51.

[78] Christopher Paul, Kristen S. Colley, and Laura Steckman. "Fighting Against, with, and through Narrative." Marine Corps Gazette 103, no. 3 (03, 2019): 80-87, https://mca-marines.org/gazette/fighting-against-with-and-through-narrative/.

[79] *Information Operations*, Directive, No. 3600.01 with Change 1, 2.

[80] Luke F. Mannion, "Institutionalizing Information Operations," *Marine Corps Gazette* 102 (4, 2018): 49-52.

Bibliography

Clarke, Richard A, and Robert K Knake. Cyber War : The Next Threat to National Security and What to Do About It. 1st Ecco Pbk. ed. New York: Ecco, 2012.

Commandant of the Marine Corps. *Message to the Force 2017: Seize the Initiative.* Washington, DC: 2017.

Dempsey, Martin E., General. Mission Command White Paper. Washington, DC: Joint Chiefs of Staff, April 2012.

Department of the Navy. *A Cooperative Strategy for 21st Century Seapower*. Washington, DC: March 2015. https://www.navy.mil/local/maritime/150227-CS21R-Final.pdf.

Department of the Navy. *Composite Warfare Doctrine*. Navy Warfare Publication (NWP) 3-56. Newport, RI: September 2010.

Department of Defense. *Information Operations*. Directive. No. 3600.01 with Change 1. Washington, DC: May 4, 2017.

Department of the Navy. *Naval Operations Concept 2010*. Washington, DC: Government Printing Office, 2010. https://fas.org/irp/doddir/navy/noC2010.pdf

Deputy Commandant for Combat Development and Integration. *Marine Air Ground Task Force Information Environment Operations Concept of Employment* (*MAGTF IEO CoE).* Quantico, VA: United States Marine Corps, July 6, 2017. https://marinecorpsconceptsandprograms.com/concepts/mcfc-5-5-magtf-information-environment-operations-concept-employment

Fitts, Michael L., LtCol. "Adding Information-Related Capabilities." *Marine Corps Gazette* 100, (09, 2016): 69-71. https://www.mca-marines.org/gazette/2016/09/adding-information-related-capabilities.

Fogleman, Ronald R. “Information Operations: The Fifth Dimension of Warfare.” *Defense Issues* 10 (47, 1995): 1.

Gerwehr, Scott, and Russell W. Glenn. *Unweaving the Web Deception and Adaptation in Future Urban Operations*. Santa Monica, CA: Rand, 2002.

Headquarters United States Army. *Information Operations.* FM 100-6. Washington, DC: Headquarters Department of the Army, US Army, August 27, 1996. https://www.bits.de/NRANEU/others/amd-us-archive/fm100-6(96).pdf

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

Headquarters United States Marine Corps. *Strategy for Assured Command and Control.* Washington, DC: March 2017. https://www.hqmc.marines.mil/Portals/61/Marine_Corps_Strategy_for_Assured_Command_and_Control_March_2017.pdf?ver=2017-05-30-160731-940.

Headquarters United States Marine Corps. *Warfighting*. MCDP 1. Washington, DC: Headquarters Marine Corps, US Marine Corps, June 20, 1997.

Headquarters United States Marine Corps. *Establishment of Marine Corps Information Warfare Task Force (MCIWTF).* (MARADMIN 596/15), Washington, DC: Headquarters US Marine Corps, November 25, 2015.

Howard, Michael. *Strategic Deception in the Second World War*. British Intelligence in the Second World War, V. 5. New York: Norton, 1995.

Hughes, Wayne P., and Robert Girrier. *Fleet Tactics and Naval Operations*. 3rd ed. The US Naval Institute Blue & Gold Professional Library. Annapolis: Naval Institute Press, 2018.

Jensen, Richard M. *Information War Power: Lessons from Air Power*. Cambridge, MA: Program on Information Resources Policy, Harvard University, Center for Information Policy Research, 1997.

Lind, William S. *Maneuver Warfare Handbook*. Westview Special Studies in Military Affairs. New York: Westview Press, 1985.

Mannion, Luke F. "Institutionalizing Information Operations." *Marine Corps Gazette* 102, (04, 2018): 49-52. https://mca-marines.org/gazette/institutionalizing-information-operations/.

Molenda, Patrick. "Silence on the Net." *United States Naval Institute Proceedings* 141 (05, 2015): 34-39. https://search-proquest-com.lomc.idm.oclc.org/docview/1680233926?accountid=14746.

Murphy, Dennis M. "The Future of Influence in Warfare." *Joint Force Quarterly: JFQ* (64, 2012): 47-51. https://search-proquest-com.lomc.idm.oclc.org/docview/929763153?accountid=14746.

Paul, Christopher, Kristen Colley, and Laura Steckman. “Fighting Against, With, and Through Narrative.” *Marine Corps Gazette* 103, no. 3 (03, 2019): 80-87. https://search-proquest-com.lomc.idm.oclc.org/docview/2188521430?accountid=14746.

Paul, Christopher. “Is It Time to Abandon the Term Information Operations?” TheStrategyBridge.org. March 11, 2019. https://thestrategybridge.org/the-bridge/2019/3/11/is-it-time-to-abandon-the-term-information-operations.

Russell, Alison Lawlor. *Cyber Blockades*. Washington DC: Georgetown University Press, 2014.

Todd, Michael J., James A. Grant, and David A. Jessen. "It's Time to Fix Navy Information Operations." *United States Naval Institute Proceedings* 142 (06, 2016): 80-82. https://search-proquest-com.lomc.idm.oclc.org/docview/1792214913?accountid=14746.

United States. Joint Chiefs of Staff. *Department of Defense Dictionary of Military and Associated Terms.* JP 1-02 amended. Washington, DC: Joint Chiefs of Staff, February 15, 2016. https://fas.org/irp/doddir/dod/jp1_02.pdf.

United States. Joint Chiefs of Staff. *Command and Control of Joint Maritime Operations.* JP 3-32. Washington, DC: Joint Chiefs of Staff, June 8, 2018. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_32.pdf?ver=2018-07-23-161257-897.

United States. Joint Chiefs of Staff. *Information Operations*. JP 3-13. Washington, DC: Joint Chiefs of Staff, November 20, 2014. http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13.pdf

United States. Joint Chiefs of Staff. *Information Warfare: A Strategy for Peace… The Decisive Edge in War*. Washington, DC: Joint Chiefs of Staff, November 11, 1996. https://apps.dtic.mil/dtic/tr/fulltext/u2/a318379.pdf

United States. Joint Chiefs of Staff. *Joint Intelligence Preparation of the Operational Environment*. JP 2-01.3. Washington, DC: Joint Chiefs of Staff, May 21, 2014. https://fas.org/irp/doddir/dod/jp2-01-3.pdf

United States. Joint Chiefs of Staff. *Joint Operations*. JP 3-0 with Change 1. Washington, DC: Joint Chiefs of Staff, Oct 22, 2018. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_0ch1.pdf?ver=2018-11-27-160457-910.

United States. Joint Chiefs of Staff. *Joint Concept for Operating in the Information Environment (JCOIE).* Washington, DC: Joint Chiefs of Staff, July 25, 2018.

https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joint_concepts_jcoie.pdf?ver=2018-08-01-142119-830.

United States. Joint Chiefs of Staff. *Joint Task Force Planning Guidance and Procedures*. JP 5-00.2. Washington, DC: Joint Chiefs of Staff, January 13, 1999. https://www.bits.de/NRANEU/others/jp-doctrine/jp5_00_2(99).pdf

United States. Joint Chiefs of Staff. *Military Information Support Operations.* JP 3-13.2 with Change 1. Washington, DC: Joint Chiefs of Staff, December 20, 2011. https://www.bits.de/NRANEU/others/jp-doctrine/JP3-13.2C1(11).pdf.