# REPORT DOCUMENTATION PAGE

*Form Approved*
*OMB No. 0704-0188*



| 1. REPORT DATE *(DD-MM-YYYY)* | 2. REPORT TYPE | 3. DATES COVERED *(From - To)* |
|---|---|---|
| 15-04-2019 | Master of Military Studies (MMS) thesis | AY 2019-2020 |

**4. TITLE AND SUBTITLE**

The Expeditionary Information Warfare Commander: A Composite Warfare Design to Synthesize Navy and Marine Corps Information Competencies

**5a. CONTRACT NUMBER**
N/A

**5b. GRANT NUMBER**
N/A

**5c. PROGRAM ELEMENT NUMBER**
N/A

**6. AUTHOR(S)**
Reed, Jessica, A, Lieutenant Commander, USN

**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)**

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

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

**13. SUPPLEMENTARY NOTES**

**14. ABSTRACT**

This paper proposes implementing a permanently designated Information Warfare Commander (IWC) within the Expeditionary Composite Warfare Command (CWC) design. Background discusses the disparate ways that military services and government agencies conceptualize information in struggle to optimize its application. Historic summary presents the organizational evolution of responsibility to information related capabilities and connects these points to the apparent present lack of formal structure that could facilitate Navy-Marine Corps multi-dimensional, cross-domain, coordination of information operations in contribution to composite expeditionary operations. Next, it presents the Navy and Marine Corps information communities, as they currently operate in parallel, in comparison and contrast to the steps already taken to incorporate permanent IWCs into Carrier Strike Group (CSG) design. The proposed design presents a notional organizational body and addresses DOTMLPF-P considerations. It discusses enduring criticisms and shortfalls observed in the CSG IWC model and additional obstacles to incorporating the IWC concept into the naval expeditionary force organization.

**15. SUBJECT TERMS**

Composite Warfare; Expeditionary Information Warfare Commander, IWC; Operations in the Information Environment, OIE; Information Operations, IO; joint all-domain; naval integration.

| 16. SECURITY CLASSIFICATION OF: | | | 17. LIMITATION OF ABSTRACT | 18. NUMBER OF PAGES | 19a. NAME OF RESPONSIBLE PERSON |
|---|---|---|---|---|---|
| a. REPORT | b. ABSTRACT | c. THIS PAGE | | | USMC Command and Staff College |
| Unclass | Unclass | Unclass | UU | 40 | 19b. TELEPHONE NUMBER *(Include area code)*<br>(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 Expeditionary Information Warfare Commander: A Composite Warfare Design to Synthesize Navy and Marine Corps Information Competencies

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

**AUTHOR:**

Lieutenant Commander Jessica Reed
United States Navy

AY 2019-20

---

Mentor and Oral Defense Committee Member: Dr. John Gordon
Approved: //Signed//
Date: 15 April 2020

Oral Defense Committee Member: LtCol Jude Shell
Approved: //Signed//
Date: 15 April 2020

Oral Defense Committee Member: CDR Jose Berrios
Approved: //Signed//
Date: 15 April 2020

## Executive Summary

**Title:** The Expeditionary Information Warfare Commander: A Composite Warfare Design to Synthesize Navy and Marine Corps Information Competencies

**Author:** Lieutenant Commander Jessica A. Reed, United States Navy

**Thesis:** Organizational design designating a dedicated expeditionary Information Warfare Commander (IWC) can synthesize and direct disparate Navy and Marine Corps information competencies within the expeditionary Composite Warfare construct.

**Discussion:** Decision makers are relentlessly emphasizing the critical role that information plays in all operations across the conflict continuum. Information is the connective tissue that will enable Joint Forces to achieve joint all-domain operations. Joint mastery of information's complex nuances will require deconflicting variable concepts of information; revolutionary transformations in organizational mindsets and structures to facilitate pacing with information threats; and overcoming operational stovepipes to synthesize information competencies for scalable, agile, and most importantly, interoperable maneuver throughout the information environment.

**Conclusion:** Approaching operations across the conflict continuum from a multi-dimensional perspective is a gradual, organizational change process. Information community professionals are uniquely equipped to model and advocate institutionalizing the multi-dimensional mindset necessary to achieving all-domain operations. Dedicating a full-time information professional to the IWC role within Composite Warfare Command design emphasizes Navy and Marine Corps commitment to tactical and operational information function integration.

DISCLAIMER

## *Illustrations*

Page

## *Preface*

As the United States strives to optimize its National Security posture in the information age, philosophical themes recognizing information as a critical enabler to seizing and maintaining competitive advantages repeat themselves. Unfortunately, the breadth of the information operating environment complicates the Joint Force's ability to agilely coordinate disparate information resources in order to optimize information effects across multiple dimensions, within all domains, and throughout the conflict continuum. The Navy and Marine Corps have taken strides, in parallel, to synthesize planning and coordination of information operations across their respective forces. In 2019, the *38th Commandant of the Marine Corps Planning Guidance* explicitly directed the Marine Corps to integrate the expeditionary force in readiness back into the Fleet via naval Composite Warfare doctrine. Information, with its robust and diverse applicability, is an obvious avenue for multi-point, Navy-Marine Corps integration.

This Master of Military Studies (MMS) paper advocates for the implementation of a permanently designated Information Warfare Commander (IWC) within the Expeditionary Composite Warfare Command (CWC) design. Background will discuss the disparate ways that military services and government agencies conceptualize information in struggles to optimize its application. In brief historic summary, it will present the organizational evolution of responsibility to information related capabilities and connect these points to the apparent present lack of formal structure that could facilitate Navy-Marine Corps multi-dimensional, cross-domain coordination of information operations in contribution to composite expeditionary operations. Next, it will present the Navy and Marine Corps information communities, as they currently operate in parallel, identifying counterparts for coordination and integration in comparison and contrast to the steps already taken to achieve the incorporation of permanent

IWCs into Carrier Strike Group (CSG) CWC design. Finally, this MMS will conclude with a design for a full-time IWC within the expeditionary CWC organization. The design will present a notional organizational body and addresses afloat and ashore coordinated supporting-supported task and function considerations. It will also identify and address enduring criticisms and shortfalls observed in the CSG IWC model and additional obstacles to incorporating the IWC concept into the naval expeditionary force organization.

While writing this paper, I received assistance from a variety of people. At the Marine Corps University Command and Staff College (MCU CSC), Quantico, my mentors Dr. John Gordon and LtCol Daniel Micklis, were invaluable in their guidance and counsel during the preparation of this paper. Their guidance made this a far better paper. My Marine Corps intelligence community mentor, LtCol Jude Shell, was a crucial sounding board motivating me to design a way to more thoroughly integrate Navy and Marine Corps information talent. My Navy military faculty advisor, CDR Stephen Kelley, provided sage council and support that kept me grounded in the service of which I am so proud to be a part. My conference group civilian and military faculty advisors, Dr. Craig Hayden and Col(sel) David Emmel, were outstanding instructors during my time at MCU CSC. My Navy Information Warfare Community mentor, CDR Jose Berrios who provided critical Navy perspective to further legitimize the defense of my thesis. My Operations in the Information Environment instructor Mr. Jim McNieve for keeping me connected with the wealth of information and subject matter expertise at the Marine Corps Information Operation Center and beyond. Lastly, CAPT(sel) Don Wilson and LT Katie Hendrickson from Amphibious Squadron 8; and Capt Brady Bustin and Capt Justin McNeely from II Marine Information Group, all for challenging some of my assumptions and validating others, with insight provided from their current, downrange perspectives.

## *Table of Contents*

Page

# INFORMATION: AN EVOLUTIONARY DEFINITION AND ROLE

*"The advent of the internet, the expansion of information technology, the widespread availability of wireless communications, and the far-reaching impact of social media have dramatically impacted operations and changed the character of modern warfare…The elevation of Information to a joint function impacts all operations and has implications across doctrine, organization, training, materiel, leadership and education, personnel, facilities and policy [DOTMLPF-P]…"*[1]

– **Gen James Mattis, USMC(ret), 26th Secretary of Defense**

The complexity and speed, both tangibly and cognitively, with which information flows is presenting unprecedented challenges to military operators' abilities to observe, orient, decide and act to achieve objectives in an amorphous globalized context. Joint mastery of information's complex nuances will require deconflicting variable concepts of information; revolutionary transformations in organizational mindsets and structures to facilitate pacing with information threats; and overcoming operational stovepipes to synthesize information competencies for scalable, agile, and most importantly, interoperable maneuver throughout the information environment. This design is not a proposal to introduce numerous additional information personnel into the existing tactical level Naval Expeditionary Force organization. Instead, it merely aims to regroup and pair information competencies within the existing organization to consolidate field grade leadership under the advisory guidance and advocacy of a dedicated command authority capable of facilitating further coordination between otherwise disparate functions. Organizational design designating a dedicated expeditionary Information Warfare Commander (IWC) can synthesize and direct disparate Navy and Marine Corps information competencies within the expeditionary Composite Warfare construct.

Hyperconnectivity[i] in today's global environment has driven decision makers to relentlessly

[i] From Wikipedia: "Hyperconnectivity is a term invented by Canadian social scientists, Anabel Quan-Haase and Barry Wellman, pertaining to person-to-person and person-to-machine communication in networked organizations and networked societies. It refers to the use of multiple means of communication, such as email, instant messaging, telephone, face-to-face contact and Web information services." https://en.wikipedia.org/wiki/Hyperconnectivity#cite_note-1

emphasize the critical role that information plays in all operations across the conflict continuum. Arguably, not since logistics has an element to military operations become recognized as so diversely scoped and universally essential. The current *National Security Strategy of the United States* (NSS) discusses information as a critical element subject to global competition. The NSS implicitly identifies acts of "information warfare" putting information in context as a weaponized tool that United States (U.S.) adversaries are persistently exploiting and manipulating to malign ends. It also describes U.S. efforts thus far to counter these actions as "tepid and fragmented," partly due to a "lack of sustained focus."[2] The *National Defense Strategy of the United States* (NDS) echoes the same tone and particularly discusses the Joint Force's need to gain and maintain the information advantage. Specifically, the NDS cites Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) as a foundational capability in the Joint Force Global Operating Model.[3] It frames the resilient, survivable, federated networks and information ecosystems and capabilities for gaining and exploiting information, that comprise C4ISR, as the ways and means to seizing the information advantage that U.S. leaders so desperately seek.[4]

Contextualizing information into a framework for joint military operations is a dynamic, expansive and ongoing process. Information's role in doctrine is broadly associated with discerning and influencing behaviors and decision processes. The information instrument of power is variably identified as a function,[5] a warfare domain,[6] an environment,[7] and both an aggregate of operations across multiple dimensions and a dimension in-and-of itself. [8] Information's imprecise doctrinal identity only makes starkly apparent the fact that a common understanding of information does not exist. Moreover, despite its indisputable essentiality since the advent of the information age, information endures as an enigmatic concept that U.S. joint

national defense entities rigorously strive to doctrinize in the interests of unifying information related tasks and purposes across the conflict continuum. Repetitious U.S. government efforts to precisely characterize the expanding nature of information has resulted in a series of fallaciously vague, derivative definitions. Given information's vast and abstract nature, U.S. government efforts to subcategorize information framework into components is understandable. After all, the U.S. government must inevitably assign manageable spheres of responsibility and expertise. Unfortunately, amidst the continuous evolution of the information framework, evident in the brief history that follows, assigning responsibility to synthesize and apply informational power presently remains hampered by disparate, stovepiped endeavors across the military service branches, defense organizations and government agencies.

Long before conceptualization of the information environment; cyberspace operations; space-based technologies; or even the doctrinization of information operations (IO), information existed as an undefined entity interwoven into all operations. There are certainly examples of information's influence dating back even to revolutionary America. But as a starting point here, one can consider history's most global conflicts, World Wars I and II. Although at the time, not defined as Electromagnetic Spectrum Operations (EMSO) or Electronic Warfare (EW); disruption, denial, and exploitation of adversary communications networks certainly occurred during World War I. Operation Fortitude, the elaborate Military Deception (MILDEC) campaign that protected Allied D-Day intentions in World War II, remains an exemplar of cognitive operations for modern joint MILDEC operators and planners to study and emulate.[9]

The paradigm shift marked by the rise of maneuver warfare theory introduced a more holistic approach to warfighting. The Joint Force found Gulf War I successes in innovatively pairing traditional physical destruction of enemy Command, Control, and Communications and

sensor objectives with physical and cognitive, soft-kill objectives by way of EW, MILDEC, Operations Security (OPSEC), and Psychological Operations (PSYOP). The Joint Chiefs labeled this forward leaning hybrid of tactical, operational and strategic thinking, which aimed to isolate the adversary's command structure from its combat means, as Command and Control Warfare (C2W).[10] Concurrently, the Navy treated space and EW (SEW) as its tactical C2W node. This point is addressed in more detail in the Naval composite warfare discussion, but goes to highlight that EW, MILDEC, OPSEC, PSYOP, C2 and Space operations were all regarded as Information Related Capabilities (IRC) collectively grouped into the IO competency. When awareness of cyberspace threats became exponentially more apparent in the late 90's, joint planners also added cyber to the IRC mix.[11] Operation Iraqi Freedom (OIF) and Operation Enduring Freedom (OEF) ushered in an era of counter insurgency operations and U.S. military efforts to win over "hearts and minds" in the interests of stability and nation building. This resurrected cognitive IOs such as influence and other forms of public diplomacy that were prevalent during the Cold War.

Finally, in 2013, the Secretary of Defense (SECDEF) formally defined IO as "the integrated employment, during military operations, of 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."[12] Ambiguous SECDEF language was consistent with the definition provided in joint military IO doctrine the year prior. Both documents also provided similar, but different, and conspicuously non-all-inclusive lists of IRCs. In doctrinal reinforcement to the IO capabilities identified in the operational history, joint doctrine and 2013 SECDEF guidance explicitly identify Cyber, Military Information Support Operations (MISO)[ii], influence activities, Civil Military Operations (CMO), and Public Affairs (PA) as IRCs.[13] Of

[ii] MISO replaced PSYOP in 2011 but was re-designated as merely a subcategory among the functions performed by PSYOP personnel in 2017.

note, no doctrine has been specific enough to define IRCs in a way that distinguishes them from any other type of capability.[iii]

Much like IRC, the definition of the Information Environment (IE) is also notoriously imprecise. Remove "information" and "The aggregate of individuals, organizations, and systems that collect, process, disseminate, or act [on information],"[14] describes any function within an operating environment. There is only one environment, and it is contrived to attempt to distil information apart from it. Placing emphasis on the information inextricably intwined throughout the environment is an intellectual exercise in regarding the environment from the broader perspective of human (cognitive), data (informational) and tangible (physical) dimensions simultaneously.[15] In 2016, via the *DoD Strategy for Operations in the Information Environment,* the Department of Defense made a deliberate effort to strategically addressed the necessity to coordinate operations from this heightened, multi-dimensional perspective.

Cyber and space are routinely categorized as subsets of the information environment because it is nearly impossible to understand them without taking on the multi-dimensional, information perspective. Conversely, it remains relatively inconsequential to myopically regard the traditional air, land and sea domains exclusively from a physical dimension perspective. The EMS, which conceptually proceeded the relevancy of both space and cyber in the operating environment, is similarly subcategorized under the information banner. In 2018, 15 months after the Joint Force established information as the seventh joint function, the Secretary of the Navy doctrinally recognize the EMS environment as a distinctive battlespace on par with sea, air, land, space and cyber.[16] While this was just a unilateral Naval initiative, this was still a win by some measures, because it brought another characteristically multi-dimensional element to the

[iii]JP3-13 defines IRC as, "A tool, technique, or activity that affects any of the three dimensions of the information environment." This is the definition accepted for the purposes of this MMS, despite vagueness made even more apparent in the discussion of the Information Environment.

forefront. Eventually, the attributes regarded from a multi-dimensional perspective will outnumber those that still are not. Once the Joint Force achieves institutionalization of multi-domain operations theory, even air, land, and sea will naturally be regarded as more than merely physical domains. However, angst, controversy, and resistance to change indicates that there is still significant room for progress. What the Joint Force is willing to categorize as information is a gage for the force's aptitude for integrated, multi-dimensional thought, because in IO, "it is not the ownership of the capabilities and techniques that is important, but rather the integrated application."[17]

The fractured elements of the organization and command structure to manage Operations in the IE (OIE) has also undergone several cycles of expansion and contraction. During the Cold War, President Eisenhower commissioned the United States Information Agency (USIA). USIA's scope was acutely centered on public diplomacy. USIA was the lead organization responsible for U.S. government messaging intended for foreign audiences.[18] Budget constraints and a domestic climate with gradually increasing skepticism towards public diplomacy drove USIA functions to be absorbed by the State Department and the USIA disestablished in 1999.[19]

In regards to EMSO elements of information, in 1980, the Secretary of Defense established the Joint Electronic Warfare Center (JEWC). The JEWC merged with the Joint Command and Control Warfare Center (JC2WC) to collectively become the Joint Information Operations Center (JIOC).[20] However, despite the merger, JEWC continues to exist as a branch organization leading Joint EMSO initiatives that consolidate EW IRCs, separate from C2W and other IO niches. Nevertheless, the collective JIOC was nested under Strategic Command (STRATCOM) authority with sub-unified Space and Cyber Command IRCs. In 2018, Cyber was elevated to functional Unified Combatant Command status, with Space following as a new

geographic Unified Combatant Command in 2019. 2019 also marked the establishment of the U.S. Space Force. Despite revolution in military affairs declarations for Space[21] and Cyber bolstering their maturation into disciplines broad and complex enough to merit their own combatant commands, they remain nested under the information umbrella that loosely correlates global domains. It is a peculiar mystery that by Naval standards, the EMS is also a global domain, distinct from cyber and space, but still nested with them as IE terrain.

The primary challenge behind mastering information's complexities in order to create discrete advantages is acceptance of its amorphous nature. If information encompasses the physical domain, what makes sea, air or land any less informational than cyber or space? All capabilities have potential for being classified as an IRC. Subordination of the JIOC to STRATCOM suggests an inherently strategic association for IRCs, but IRCs are too common and pervasive across the Range of Military Operations (ROMO) for this to be so. Instead, information is the miscellaneous category for all globally interconnected activities occurring across the human (cognitive), data (informational) and tangible (physical) dimensions.[22] Any military decision maker or operator truly adopting a multi-domain, multi-dimensional perspective should be hard pressed to define what within a generic operating environment is *not* an IE consideration. It would be most ideal for this proposal to first, have a stronger consensus on professional disciplines within the Navy and Marine Corps definitively focused on information matters as a primary line of effort. However, a myriad of variables and historic baggage of organizational cultures contributing to inherently incongruent structures requires an approach with an underlying key assumption. For the intents and purposes of this proposal, all C4ISR, EMS, cryptologic, cyber, space, meteorological and oceanographic (METOC) science, law enforcement, and inform and influence competencies are deemed information centric.

## COMPOSITE WARFARE: NAVAL MULTI-DOMAIN TACTICAL COMMAND ORGANIZATION

*"We [Navy operators] are in multi-domain every single day…If we didn't sign up and say it's something new, I apologize."*[23]

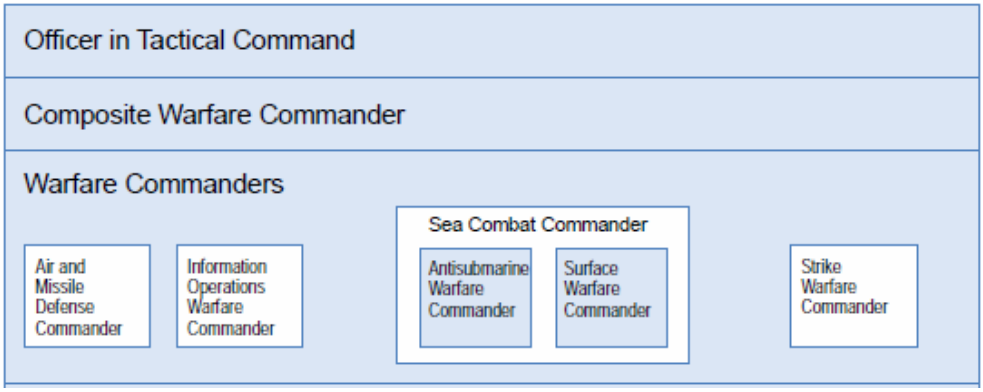
**- Richard V. Spencer, 76th Secretary of the Navy**

*"Marine Corps integration into the Fleet via composite warfare will be a prerequisite to the successful execution of amphibious operations: Marines cannot be passive passengers en route to the amphibious objective area…Marines must contribute to the fight alongside our Navy shipmates from the moment we embark."*[24]

**- General David H. Berger, 38th Commandant of the Marine Corps**

Even as conceptual understanding of domains continues to expand, multi-domain integration remains an elusive necessity for military operations. Strategic Command Commander, Vice Admiral Charles Richard, asserted that "thinking about land, air, sea, cyber and space as separate domains [was] obsolete."[25] These comments are only a relatively recent assertion of a philosophy that senior military decision makers have expressed since sea-land and air-sea battle theories recognizably became inadequate to address Anti-Access and Area Denial (A2AD) challenges that contested U.S. force presumptions of superiority in the traditional domains.[26] To regain advantage, decades of Capstone Concepts for Joint Operations have persistently emphasized a need for an exquisitely interoperable C4ISR architecture. The most current venture for the culmination of this vision is the Joint "all-domain operations" concept.[27] Information, encompassing cyberspace; the EMS; global satellite enabled connectivity between physical domains; and relationship enabled influence over human cognition, is ostensibly the connective tissue expected to crosscut traditional domain silos and enable agile C2 and maneuverability of all-domain capabilities.

Maritime tactical organizational structure was designed long ago to facilitate such cross-domain collaboration and integration. Doctrinally, at the maritime tactical level this has been the Composite Warfare Command (CWC) structure.[28] Balancing simplicity with functional diversity, from its inception, Navy composite warfare doctrine distinguished commanders for Surface Warfare (SW), Anti-Submarine Warfare (ASW), Air and Missile Defense (AMD), Strike Warfare (STW) and Information Operations Warfare (IW) for mission command authority over respective mission areas. Figure 1 is a generic depiction of the composite warfare structure.



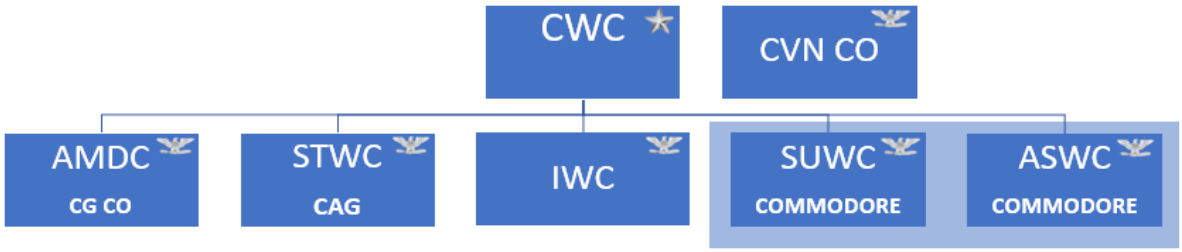

Of note, the Information Operations Warfare Commander (IWC) evolved from the Space and Electronic Warfare Commander (SEWC) that Navy introduced into doctrine in 1990. The Chief of Naval Operations redesignated the SEWC as the Command and Control Warfare Commander (C2WC) in 1993 to align similar, but not entirely interchangeable descriptive terminology, with joint doctrine terminology.[29] This terminology evolution further reflects the controversial difficulty that joint forces persistently face in decisively classifying IRCs apart from other distinct functions or domains, particularly C2. When activity levels and mission complexity is considered "manageable," the surface and subsurface commanders are commonly fused together

under the oversight of a dual-hatted Sea Combat Commander (SCC).[30] The SCC consolidation is particularly common and logical for task forces, such as traditional Amphibious Ready Group-Marine Expeditionary Unit (ARG/MEU) Amphibious Task Forces (ATF), that have minimal to no organic surface ASW assets to command.

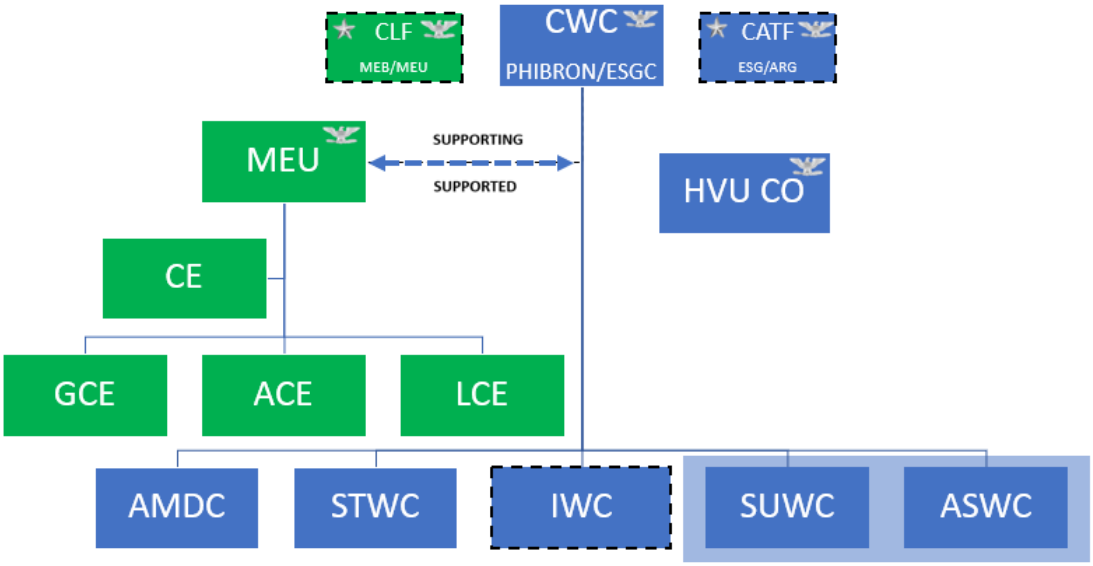
Generic CWC design is functionally more befitting to a Carrier Strike Group (CSG) structure than an ATF structure. In CSG CWC organization, there is a static CWC for all the respective "domain" commanders to support. The O-6 commodore is the stakeholder for planning and employment of sea combat (surface and subsurface) and AMD assets. The commodore traditionally benefits from collaborating with, peer O-6, Carrier (CVN) and Carrier Air Wing (CVW) commanders, who are key stakeholders with respective TACON authority over the CVN and the CVW that the CVN primarily supports. Until 2016, when Navy established a full-time IWC position on CSG staffs, the CVN CO was commonly collaterally designated the IWC.[31]

After-action reporting from the test case IWCs,[32] as well as the initial cadre of IWCs screened and assigned as full time IWCs, reveals that it was a welcomed change to have designated subject matter experts with, what the NSS might recognize as, a "sustained focus"[33] on broad information mission competencies. Full-time IWCs mitigated the fact that CVN CO's are persistently preoccupied with commanding 5,000+ crew, nuclear powered aircraft carriers.[34] Figure 2 depicts the CSG CWC design. Rather than the CWC being the single point of integration, mission command authority at the warfare commander level facilitates cross-domain synchronization and mission priority deconfliction prior to decisions making it to the CWC. Achieving tactical integration at lower levels within the CWC design enables the CWC to remain operationally oriented

on Joint Force Maritime Component Commander (JFMCC), Fleet Marine Force (FMF) and higher command level concerns.




Unfortunately, the CSG CWC design breaks down a bit in traditional amphibious force organizations because of the parallel but distinct and incongruent command organizations of the Amphibious Task Force (ATF) and the Amphibious Landing Force (LF). In ARG/MEU tradition, the responsible O-6s to fuse the CWC and MEU elements together typically include the MEU Commander, designated as the CLF; the Amphibious Squadron (PHIBRON) Commodore, dual hatted as the CATF and CWC; and the High Value Unit (HVU) CO multi-hatting as SCC, AMDC, STWC, and IWC. Figure 3 shows the ARG/MEU CWC design. In the case of an ESG or Littoral Combat Group, the CWC may be elevated to an embarked Flag or General Officer.



Notably, Task Force 58, a contingency task force stood up during OEF, was an unorthodox but successful example of a Marine General Officer ashore assuming the CATF designation. CWC authority remained with the PHIBRON commodore, but still, some questioned the decision to designate a Marine General Officer as CATF. Task Force 58 was tremendously successful and now serves as an example of doctrinal flexibility and a Joint Commander's capability to effectively lead cross-service components as circumstances may call.[35] Operation Orders (OPORD) may designate COs of assigned subordinate units or additional ESG staff as AMDC and/or ASWC. Unfortunately, the binary simplicity of the CATF-CLF supported-supporting relationship, most driven by the geographic disposition of the MEU either afloat or ashore, fails to facilitate continuously dynamic cross-domain supported-supporting nuances. Furthermore, information, as an inherently multi-domain function, commonly transcends operational perspectives limited to physical objectives.

## NAVY INFORMATION WARFARE COMMUNITY

*"Our collective IW capabilities to assure command and control, provide predictive battlespace awareness, and deliver integrated IW fires will be integral to all plans and operations – not a 'bolt-on' capability after the fact."*[36]

– **Vice Admiral Brian Brown, Naval Information Forces Commander**

In 2009, the U.S. Navy established the Information Dominance Corps, which later transitioned becoming the Information Warfare (IW) community that exists today. Navy chartered the IW community in order to isolated information as a warfare area distinct from air, surface, subsurface and expeditionary; with the intention of more effectively and collaboratively leading and managing Navy personnel possessing extensive skills in information-intensive fields.[37] The IW community officer corps is comprised of the intelligence, cryptologic, Meteorological and Oceanographic, information professionals and cyber warfare engineers. Intelligence, cryptologic, information technician and aerographic specialists make up the Navy

IW community enlisted force. Figure 4 identifies professionals in the Navy IW community. Additionally, the Chief of Naval Operations (CNO) established a deputy Chief of Naval Operations for Information Warfare (N2N6) with oversight over this consolidated intelligence and networks and communications directorates. The N2N6 assumed responsibility for providing end-to-end accountability for Navy information requirements, investments, capabilities and forces.[38]

**Information Warfare Officer (IWO)**
Information Professional (IP)
Cryptologic Warfare (CW)
Intelligence (INTEL)
Meteorology/Oceanography (METOC)
Cyber Warfare Engineer

**Enlisted Information Warfare Specialist (IW)**
Information Systems Technician (IT)
Cryptologic Technician (CT)
Intelligence Specialist (IS)
Aerographer's Mate (AG)

Despite having an N2N6, the Navy did not establish an information type commander (TYCOM) to administratively consolidate disparate manning, training and equipping efforts by the "information force" until 2014.[39] This was in stark contrast to Air, Surface, Subsurface, Expeditionary, Special Operations Warfare, and Military Sealift communities which all had TYCOM administrative oversight. Additionally, the Navy did not establish an information warfare development center for producing information warfare community tactics, techniques and procedures until 2017.[40] As of this writing, Navy IW personnel are commonly dispersed and under the tactical and administrative authority of non-information force commands.

Skillsets markedly excluded from the doctrinal Navy IW community at present include public affairs officers, mass communications specialists, electronic technicians, sonar technicians, operations specialists, fire controlmen, masters at arms and security professionals.

These areas of expertise are arguably critical enablers to strategic communications; remote sensing maintenance, operations, exploitation and targeting; and signatures management (SIGMAN) enforcement. Of note, cognitive force protection, in the form of OPSEC, which safeguards friendly force critical information, is commonly collaterally assigned to personnel within the IW community despite characteristically being an all-hands effort.

Force protection is a separate function from information. Law enforcement elements of force protection operate under rules and authorities for gathering and actioning information that are complimentary, but distinct from other IRCs; namely, intelligence (to include counterintelligence), which is also doctrinally a separate function from information. [41] Ensuring that conflicts of interest do not arise in actioning some forms of information is one possible reason for categorizing force protection and law enforcement activities apart from other IRCs. This specialty is only identified for consideration as an addition to the Navy IW community because Navy law enforcement personnel equivalents within the Marine Corps are incorporated into Marine Information Group (MIG) design. However, it is equally possible that the Marine Corps law enforcement's association to MIGs is merely an artifact from its association to the Command Element of Marine headquarters groups prior to their conversions into MIGs rather than true consideration of law enforcement as an IRC.

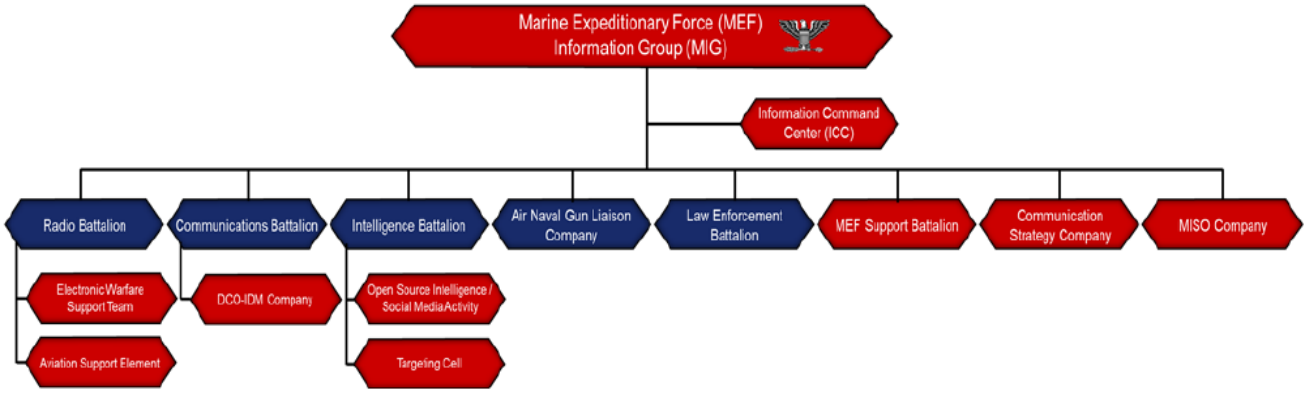
## MARINE EXPEDITIONARY FORCE INFORMATION GROUP

*"While the notion of operating in and through the information environment may not be new or unfamiliar, what is new is our approach to achieving decision in battle by incorporating a large number of rapidly advancing multifunctional information capabilities into MAGTF operations."*[42]

**- Lieutenant General Robert Walsh, Deputy Commandant for Combat Development and Integration**

In 2017, the U.S. Marine Corps (USMC) issued a concept of employment for Marine Air Ground Task Force (MAGTF) information environment operations. The same year, the USMC redesignated its MEF Headquarters Groups as Marine Expeditionary Force Information Groups

(MIG) and established its first Deputy Commandant for Information (DC I), responsible for integrating, aligning and advocating for Operations in the Information Environment. The information centric force organizations consolidated under MIGs include radio, communications, intelligence and law enforcement battalions; and air naval gun liaison, communications strategy and Military Information Support Operations (MISO) companies.[43] Figure 5 depicts the MIG and MEF Command Element organization. In 2019, the 37th Commandant of the Marine Corps signed a directive recognizing information as the seventh Marine Corps warfighting function, aligning to joint doctrine that elevated information to a function nearly two years prior.




At the time of this writing, MIGs doctrinally remain enmeshed with legacy MEF Headquarters Group roles that may or may not be explicitly information centric. MIGs are command element headquarters that are significantly enhanced by personnel specializing in fields that the Marine Corps designates information centric. Information empire brokers could make a case for all C2, and thus all command elements, being inherently information centric. Historic tendencies to interchange EW and other IRCs with C2 certainly supports this argument. However, the fact that C2 is a function separate and distinct from information, [44] potentially makes this argument a slippery slope. As the MIG concept matures and the Marine Corps acclimates to the new paradigm that "information is combat power,"[45] the Marine Corps may

eventually need to break information out into a truly separate and distinct MAGTF combat element.

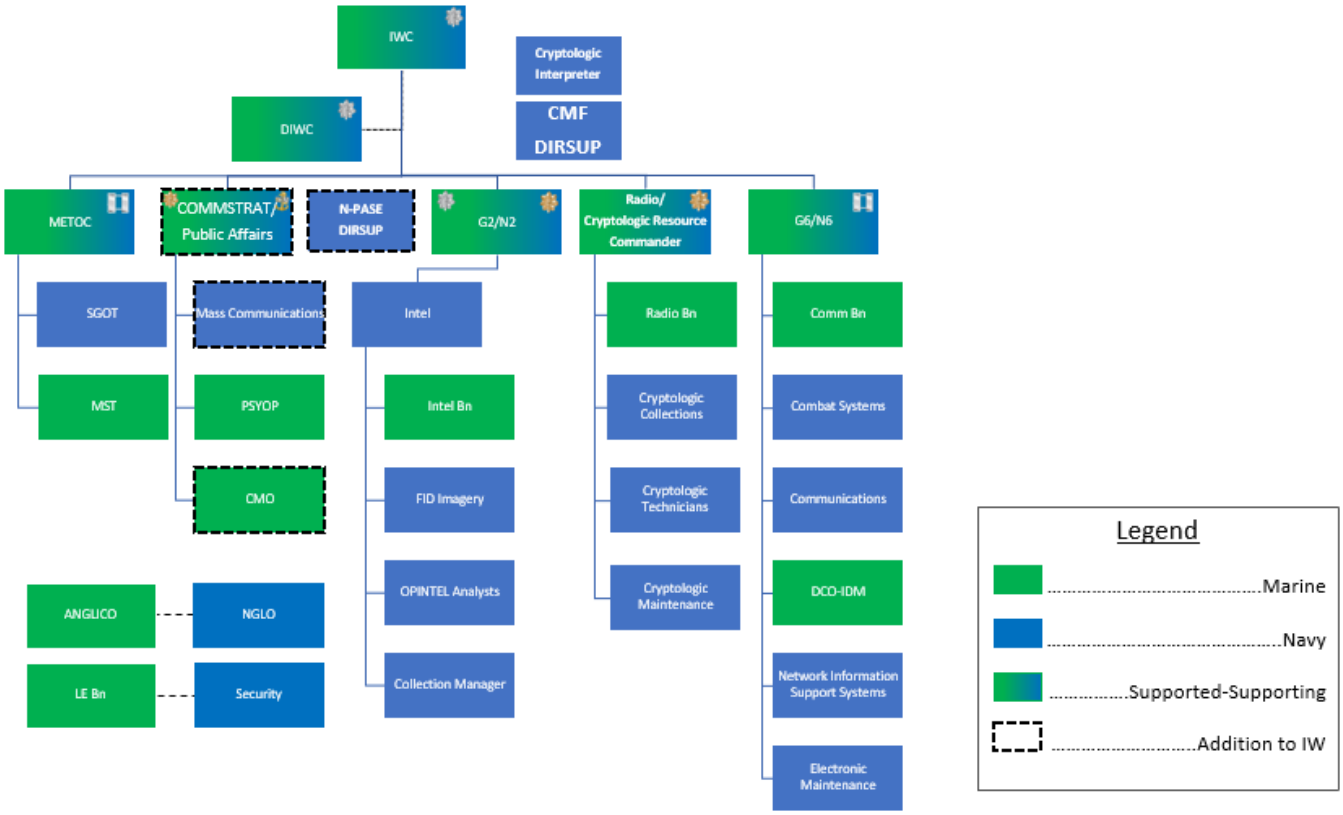
## NAVAL EXPEDITIONARY INFORMATION WARFARE COMMANDER DESIGN

*"There is nothing more difficult to take in hand, more perilous to conduct, or more uncertain in its success than to take the lead in the introduction of a new order of things*."[46]

**- Niccolo Machiavelli**

Navy and Marine Corps leadership expects Sailors and Marines to be co-equal partners in a composite Naval expeditionary force. With information implicitly regarded as the pinnacle multi-dimensional operations competency, it is only fitting that those professionals most versed in multi-domain approaches lead and model this change. Secretary Mattis foreshadowed the elevation of information having implications across the DOTMLPF-P spectrum. This design inherently addresses organization and personnel, and doctrine was discussed at length in previous sections. The remainder of this section addresses remaining DOTMLPF-P considerations.

At the 2019 Information Warfare Senior Leadership Symposium, the Marine Corps highlighted the importance of identifying blue/green counterparts in every capability.[47] The information body of professionals that would notionally fall under the direction of a Naval Expeditionary IWC, as depicted in figure 6, illustrates that direct blue/green counterparts may either augment (rather than pair) sister service counterparts, or branch off into coordination with several different counterparts because of incongruent functional specialty groupings between the two forces. Blue/green gradient blocks depict supported-supporting tactical command relationships flexible for dynamic line of effort priorities. Ideally, positional leadership authority is complimentary between the services (i.e. A Marine Corps deputy IWC would complement a Navy IWC or vice versa). However, both components shall maintain administrative control of their own personnel at all times.




While on-the-job qualification requirements are certainly inevitable; for optimal operational proficiency, joint training simulations and wargaming, as well as cross service coordination, during pre-deployment phases of readiness, should commence as early as possible in training and readiness cycles to normalize integrated operations. IWCs are expected to have a reasonable level of expertise by nature of their experience and seniority. Still, it would be prudent to standardize a training pipeline for prospective IWCs and deputies that included expeditionary warfare commander overview education as well as IW or OIE overview education from the appropriate sister service.

Integration efforts for the information body of professionals will compliment functions each service performs individually and expand the distribution of labor more evenly across the integrated information force. Additionally, it will incorporate underutilized capabilities and resources to enhance the agility and lethality of the composite naval force. Many innovative,

blue/green integrated concepts of operations involving IRCs have been successfully implemented and need only to be captured and formalized. Preferably, formalization would be achieved within organization and TTP doctrine vice local standard operating procedures or best practices.

Integrating Marine Corps and Navy tactical information organizations enable Marines to take more active roles in afloat maritime activities including: shaping operations, influence operations, and underway force protection, which are all achieved through projecting a pattern of life consisting of bold and unpredictable forward presence throughout the global commons. This concept is difficult for many to accept because of the abstract and continuous nature of information related objectives that expand the expeditionary paradigm to include penetrating adversary A2AD restrictions in the cognitive and information, as well as physical dimensions. Traditionalists tend to regard this degree of sea control as an entirely Navy mission. However, despite the arbitrary nature of physical boundaries in these dimensions, physical deployment of military forces remains essential to these operations, making them every bit as expeditionary as forcible entry and other "traditional" expeditionary force missions defined in MCDP 3.[48] Just as Navy has projected its power ashore via gunfire support, land attack cruise missiles, air power strikes, and various non-kinetic effects; supporting Marine Corps expeditionary capabilities are necessary when Marine forces are deployed afloat either in concentrated force transit or dispersed in a maritime Expeditionary Advanced Base Operations (EABO) capacity. When the Marine Corps asks what Fleet Commanders and the Navy need from the Marine Corps[49] an emphatic answer from the information perspective is, expeditionary support enabling force protection and maneuver, particularly of L-class (amphibious) ships, within the cognitive and informational dimensions as well as the physical.

From a materiel perspective, Marine Corps EW Support Teams can employ Electronic Attack (EA) and Electronic Support (ES) force protections assets, particularly during chokepoint transits. Proof of this concept was demonstrated by Kearsarge ARG/MEU when it positioned a MRZR all-terrain vehicle equipped with a Light Marine Air Defense Integrated System (LMADIS) on the Kearsarge flight deck for counter Unmanned Aerial Systems (UAS) protection during a 2019 Suez Canal transit.[50] Later the same year, implementing identical countermeasures, Boxer ARG/MEU successfully downed two encroaching Iranian UAS during a Strait of Hormuz transit.[51] Major General David Coffman, Director of Expeditionary Warfare for the CNO, attested to seeing a Marine Light Armored Vehicle (LAV) employed afloat in similar fashion to LMADIS "because it had better sensors than the ship did to find small boats."[52] This demonstrates how an embarked Marine Corps LAV is adaptable as an ES and close-in-weapon defense capability in maritime Fast Attack Craft (FAC) or Fast Inland Attack Craft (FIAC) threat environments. Given appropriate precautions against EA fratricide, Marine Corps EA capabilities may also be useful aids for own force EM signal suppression during critical SIGMAN vulnerability periods.

Optimized personnel, materiel and facilities management potentially enhances inform, influence and public diplomacy functions. Communications Strategy (CommStrat) Marines could pair with embarked Navy Public Affairs and Mass Communications personnel, to include Navy Public Affairs Support Element (N-PASE)[53] direct support augments, to perform production and dissemination of internal and external media. With intelligence analyst support, this blue-green team could be the primary executor of standing Visual Information (VI) tasking as well as kneeboard and reconnaissance (RECCE) guide production by employing combat camera Marine skills during opportune VI collections attained via on-call Ship's Nautical or

Otherwise Photographic Interpretation and Examination (SNOOPIE) evolutions. Lastly, Civil Affairs Marines and Navy Cryptologic Interpreters, when assigned, could enrich the CommStrat and public affairs planning and execution of Key Leader Engagements occurring both at sea and ashore.

Marine Corps social media trend analysis and other open source, publicly available information monitoring activities could enhance cognitive dimension maritime domain awareness. Near real-time analytic insight into trending commercial and leisure social network activity in foreign operating areas could provide indications and warnings of active adversary stand-off targeting and observable measures of effectiveness of freedom of navigation and maritime power projection activities. PSYOP Marines could benefit from shipboard audio-visual studio and print production facilities in enhancement to their organic material capabilities which are adaptable for dual purpose use communications to both inform friendly audiences and influence or deceive foreign relevant actors. Integrating Navy and Marine Corps inform and influence activities under consolidated leadership would serve to ensure timely and consistent messaging across various relevant actor audiences.

Military LE is a critical enabler to some information activities because it may take disciplinary measures against U.S. military personnel discovered, via technical intelligence surveillance means, to be in violation of lawful military directives. In contrast, unless there is express consent, Executive Order 12333 precludes military intelligence professionals from acting against unauthorized activities by U.S. military personnel, when the activities are discovered via technical foreign intelligence surveillance means.[54] This nuance has compelled many ATFs to ensure that LE personnel accompany operators of technical intelligence surveillance equipment when they conduct own force monitoring scans. This way, LE is present to take immediate legal

recourse against personnel who violate operational EM SIGMAN policy. Embarked Marine Corps LE personnel could easily augment Navy Master at Arms personnel operating in this capacity.

Marine Corps ANGLICO and LE could also augment several other force protection lines of effort afloat. ANGLICO could augment Naval Gunfire Liaison (NGLO) personnel responsible for initiating SNOOPIE events and employing flare, dazzler and lethal crew served weapon defenses against close-quarter UAS, FAC and FIAC threats. The supplementary manpower that an embarked MEU provides generally enhances afloat force protection by enabling more robust own force monitoring, battlespace awareness and application and verification of forms of SIGMAN even beyond active EM suppression. For example, additional afloat force protection measures that embarked Marine Corps personnel could enhance also include but may not be limited to maintenance and application of passive countermeasure system materials, rigging of deceptive lighting, or distributed EABO generated EM and acoustic signal decoys.

Over the horizon management of the Naval Tactical Grid and correlation into the Joint All Domain C2 network, as orchestrated by an IWC, would enable Marine Corps elements distributed ashore to minimize the hardware infrastructure and EMS footprints necessary for mission success. MEU elements could potentially improve integrated data and communication network connectivity while maintaining low probability of intercept connectivity with the afloat Supporting Arms Coordination Center (SACC) for reachback. Broader network integration would empower IWCs to provide greater responsiveness to LCE needs, Naval Surface Fire Support, and request and coordination assistance for theater and national ISR and targeting assets. Additionally, these elements could passively benefit from a robust integrated fires network likely to include C2 of autonomous platform technologies. IWC oversight of operational

intelligence processes could improve deconfliction of intelligence priorities in support to battlespace awareness and targeting, both laterally between other tactical warfare commanders and upwards between CWCs and operational and strategic level authorities. An authoritative representative, versed in C4ISR administrative processes and distinctly focused on synthesizing organic blue/green ISR resources in conjunction with managing tactical Tasking, Collection, Processing, Exploitation and Dissemination (TCPED) architecture, may enhance theater and national level mission support to CLFs and otherwise dispersed expeditionary advanced base operators.

In regard to policy, cascading effects of some IRCs can be difficult to predict and contain. For this reason, authorities for IRCs likely to have impacts beyond the tactical level are maintained at operational or strategic command levels. Offensive Cyber Operations, Joint MILDEC, and Deception in Support of OPSEC are three examples of OIE that could be tactically useful, if not for attribution, strategic implication, joint coordination, and deception fratricide concerns saddling tactical operators with impractically lengthy and complicated approval chains. In the near future, O-5 and O-6 IWCs are unlikely to receive delegated mission command authority over these IRCs. However, compelling advocacy to a component or combatant command Flag or General Officer, from an O-5 or O-6 composite warfare equivalent to an AMDC, entrusted with the authority to fire tactical Tomahawk Land Attack Missiles, or a nuclear submarine CO entrusted with low-yield nuclear weapons batteries release, is likely to command more urgency than an identical capabilities request coming from a niche professional Junior Officer tucked away in an underappreciated staff headquarters branch office. One can certainly argue that if authorities reside at echelon II and higher command levels, that is where IWCs and other information professionals are needed most. This is the primary reason that the

Navy Information TYCOM is also advocating to establish IWCs within the Maritime Operations Centers around the world.[55] However, an effort to incorporate IWCs at the echelon II level alone ignores the necessity to bridge the gap between tactical and operational level needs.

An embarked full-time IWC enables information equities to have consistent and equitable consideration on par with other operation functions during tactical cross-domain coordination. The first PHIBRON IWC test case is currently underway.[56] Navy Personnel Command screening of volunteers for a second trial have stalled due to manpower constraints that require an O-5 billet coding offset to be negotiated between the Information Warfare community and the Surface Warfare community in order to support sustainable, standardized manning.[57]

Like preliminary iterations of full time IWCs within CSG CWC design, consistency in mission execution is not expected. The Navy may try repurposing a variety of different billets before determining a standard. Similarly, between the three MIGs, the Marine Corps is varying its distribution of forces and specialized personnel to identify a favorable balance of MIG personnel embarked, in garrison and temporarily assigned as needed to FMF and Fleet MOC headquarters. Using applicable lessons learned from CSG IWC afloat program development and present and future expeditionary IWC trial cases will reveal optimal ways forward. Continued emphasis on cross service planning and coordination prior to embarkation will also improve overall preparedness for more thorough and seamless MIG and Navy IW community integration.

It is unreasonable to expect an IWC to be a subject matter expert of every IRC under his or her purview. Just as a MEU commander is reliant upon support from and cross-coordination between subordinate air, ground and logistics combat element commanders; or a CAG commander is reliant on leadership and expertise from his or her squadron commanders, the IWC is meant to be the senior tactical level authority representing the body of IRCs within the

ATF. Passionate debate persists over whether information professionals should be masters of their niche specialties or jacks of all IRCs. Critics of the concept that favors the later believe that transforming information into a profession of generalists will hinder development to a level of exceptionalism in any given niche.[58] However, if information is truly the multi-dimensional connective tissue enabling all operations, as it presents itself to be, if nothing else information professionals ought to be the "masters" of integration. Joint forces continue striving to achieve a universal integrative paradigm, but approaching the fifth decade of multi-domain doctrine revisions suggests that physical domain traditionalists have yet to completely buy-in.

## EXPEDITIONARY IWC: THE NAVAL INTEGRATION WARFARE COMMANDER

*"Therefore, in [OIE], it is not the ownership of the capabilities and techniques that is important, but rather their integrated application in order to achieve a Joint Force Commander's end state*."[59]

**- JP 3-13, *Information Operations***

Ultimately, designated IWCs within the expeditionary CWC organization would be uniquely positioned and empowered to orchestrate tactical level coordination of IRCs as an integrating authority for Navy and Marine Corps information competencies. This design establishes formal leadership that compliments and aligns to Navy and Marine Corps integration efforts for OIE that are already progressing. It addresses Marine Corps planning guidance explicitly endorsing Marine Corps integration into CWC and implicitly emphasizing innovative force design that supports multi-dimensional approaches enabling seamless all-domain operations. This design outlines DOTMLPF-P considerations and provides specific examples of tactical and operational integration that could benefit from informed IWC oversight. IWCs would model multi-dimensional approaches within their competencies and be knowledgeable advocates bridging gaps between tactical and operational level tasks and functions prone to operational and strategic level effects. Due to the broad, dynamic, and complex nature of OIE, it

would be most efficient for the coordination of tactical level information related actions to have dedicated, full-time oversight. Making IWC a collateral duty requirement of a ground, air or surface specialist has proven to be inadequate and perpetuates the antiquated paradigm that regards information as merely a supplementary function. Designating a dedicated IWC can synthesize and direct disparate Navy and Marine Corps information competencies within the expeditionary Composite Warfare construct.

---

[1] James Mattis, Secretary of Defense, memorandum for record, September 15, 2017.
[2] The White House, *The National Security Strategy of the United States of America* (Washington, DC, 2017), 35, https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf
[3] US Department of Defense, *National Defense Strategy of the United States of America*, (Washington, DC, 2018), 7, https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf
[4] US Department of Defense, National Defense Strategy, 6.
[5] SECDEF Memo Sep 15, 2017.
[6] National Defense University, Joint Vision 2020, (Washington, DC, National Defense University Institute for National Strategic Studies, 2000), 6, 21, 28, 31-32. https://apps.dtic.mil/dtic/tr/fulltext/u2/a526044.pdf
[7] US Department of Defense, *Strategy for Operating in the Information Environment*, (Washington, DC, 2016), https://dod.defense.gov/Portals/1/Documents/pubs/DoD-Strategy-for-Operations-in-the-IE-Signed-20160613.pdf
[8] US Joint Chiefs of Staff, *Information Operations*, JP 3-13 (Washington, DC: Pentagon, 27 November 2012 incorporating change 1 20 November 2014), 18, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13.pdf
[9] Roger Hesketh, *Fortitude: The D-Day Deception Campaign* (New York: Overlook Press, 2000)17-27; 351-361.
[10] Dan Struble. "What is Command and Control Warfare?" *Naval War College Review* 48, no. 3 (Jul 1, 1995): 89-98. p90, 92. https://www.jstor.org/stable/44642810
[11] US Cyber Command, "U.S. Cyber Command History," accessed December 16, 2019. https://www.cybercom.mil/About/History/
[12] US Department of Defense, *Information Operations*, DODD 3600.01, May 2, 2013, https://fas.org/irp/doddir/dod/d3600_01.pdf
[13] US Joint Chiefs of Staff, *Military Information Support Operations Supplement to the Joint Strategic Capabilities Plan*, CJCSI 3110.05F, April 7, 2017.
[14] U.S. Joint Chiefs of Staff. *Department of Defense Dictionary of Military and Associated Terms*, JP 1-02, 8 November 2010 as amended through 15 February 2016, 116,
[15] US Joint Chiefs of Staff, JP 3-13, 19-20.
[16] US Secretary of the Navy, *Electromagnetic Battle Space*, Instruction 2400.3, October 5, 2018. https://www.secnav.navy.mil/doni/Directives/02000%20Telecommunications%20and%20Digital%20Systems%20Support/02-400%20Visual%20Information%20Services/2400.3.pdf
[17] US Joint Chiefs of Staff, JP 3-13, 22.
[18] Nicholas Cull, *The Cold War and the United States Information Agency: American Propaganda and Public Diplomacy, 1945-1989*, (Cambridge: Cambridge University Press, 2008), 101-102.
[19] Cull, The Cold War and the USIA, 482-485.
[20] Leigh Armistead, ed., *Information Operations: Warfare and the Hard Reality of Soft Power* (Washington, DC 2004), 165-167.
[21] Colin Gray and John Sheldon, "Space Power and the Revolution in Military Affairs," *Airpower Journal* 13, no. 3 (1999) 23-38.
[22] US Joint Chiefs of Staff, JP 3-13, 19-20.
[23] Sydney J. Freedberg Jr, "All Service Sign on to Data Sharing – But Not to Multi-Domain," *Breaking Defense*, February 8, 2019, https://breakingdefense.com/2019/02/all-services-sign-on-to-data-sharing-but-not-to-multi-domain/
[24] U.S. Marine Corps, *38th Commandant's Planning Guidance* (Washington, DC, 2019), 10, https://www.hqmc.marines.mil/Portals/142/Docs/%2038th%20Commandant%27s%20Planning%20Guidance_2019.pdf?ver=2019-07-16-200152-700

[25] Cheryl Pellerin, "STRATCOM: Integrating Space With Other Warfare Domains is Key to Deterrence," *DOD News*, March 23, 2017, https://www.defense.gov/Explore/News/Article/Article/1127620/stratcom-integrating-space-with-other-warfare-domains-is-key-to-deterrence/
[26] U.S. Department of Defense, *Service Collaboration to Address Anti-Access & Area Denial Challenges*, Air-Sea Battle Office, May 2013, https://archive.defense.gov/pubs/ASB-ConceptImplementation-Summary-May-2013.pdf
[27] Colin Clark, "Gen Hyten On the New American Way of War: All-Domain Operations," *Breaking Defense*, February 18, 2020, https://breakingdefense.com/2020/02/gen-hyten-on-the-new-american-way-of-war-all-domain-operations/
[28] US Joint Chiefs of Staff, *Joint Maritime Operations*, JP 3-32, 8 June 2018, 40-42, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_32.pdf?ver=2019-03-14-144800-240
[29] Dan Struble. "What is Command and Control Warfare?" *Naval War College Review* 48, no. 3 (Jul 1, 1995): 89-98. https://www.jstor.org/stable/44642810
[30] US Joint Chiefs of Staff, JP 3-32, 41.
[31] Kelly Aeschbach RDML(sel), *Information Warfare Self Sync*. PowerPoint presentation. Naval Information Forces, Suffolk, VA, 14 December 2016, slide 9, https://sites.google.com/site/idcsync/documents
[32] Bryan Braswell, "Evolving the Information Warfare Commander." *CHIPS*, July-September 2010. https://www.doncio.navy.mil/CHIPS/ArticleDetails.aspx?ID=9422
[33] The White House, *The National Security Strategy*, 35.
[34] Cliff Bean CAPT and Henry Stephenson CAPT, *Proceedings Podcast Episode 69 - is IW a Warfare Command.* By Bill Hamlet, *Proceedings* podcast audio: 2019. https://soundcloud.com/naval-institute/proceedings-podcast-episode-66-is-iw-a-warfare-command
[35] Michael Valenti, *The Mattis Way of War: An Examination of Operational Art in Task Force 58 and 1st Marine Division*, (Fort Leavenworth, Kansas: US Army Command and General Staff College Press, an imprint of the Combat Studies Institute Press, 2016) 21-26, https://www.armyupress.army.mil/Portals/7/combat-studies-institute/csi-books/the-mattis-way-of-war.pdf
[36] George Lammons, "10 Years Later NAVIFOR Expects Increased Fleet Integration," *CHIPS*, (October-December 2019), https://www.doncio.navy.mil/CHIPS/ArticleDetails.aspx?id=12934
[37]Chief of Naval Operations, The Information Dominance Corps, OPNAVINST 5300.12, October 6, 2009, https://cryptome.org/dodi/opnav-5300-12.pdf
[38] ADM Gary Roughead, 29th Chief of Naval Operations to VADM David Dorsett, Director of Naval Intelligence, memorandum, June 26, 2009. https://sites.google.com/site/idcsync/documents
[39] Deputy Chief of Naval Operations for Information, *Information Dominance Engagement Area No. 37: Information Dominance Type Commander (TYCOM)*, March 7, 2014, https://sites.google.com/site/idcsync/documents
[40] Megan Shutka LCDR, "Naval Information Warfighting Development Center Enters Initial Operational Capability," *Navy News Service*, March 29, 2017, https://www.navy.mil/submit/display.asp?story_id=99564
[41] US Joint Chiefs of Staff, JP 3-0, 53.
[42] Headquarters US Marine Corps, *Marine Air Ground Task Force Information Environment Operations Concept of Employment*, Deputy Commandant for Combat Development and Integration CONEMP, 6 July 2017, 3, https://www.trngcmd.marines.mil/Portals/207/Docs/wtbn/MCCMOS/FINAL%20MAGTF%20IE%20OPS%20CoE%202017-07-06.pdf?ver=2017-11-16-090225-057
[43] Marine Corps Information Plans and Strategy Division, *Deputy Commandant for Information OIE Overview Brief*, (Marine Corps University, Quantico, VA, October 9, 2019), PowerPoint presentation.
[44] US Joint Chiefs of Staff, *Joint Operations*, JP 3-0 (Washington, DC: Pentagon, 17 January 2017 incorporating change 1 22 October 2018), 53-54, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_0ch1.pdf?ver=2018-11-27-160457-910
[45] MCIP&S Division, *OIE Overview Brief*, PowerPoint.
[46]Brainy Media Inc, "Brainy Quote," world's largest quotation website, copyright 2001-2020, https://www.brainyquote.com/quotes/niccolo_machiavelli_131418
[47] Deputy Commandant for Information, *Road to 2025* (Information Warfare Senior Leadership Symposium, Leesburg, VA, June 3, 2019) PowerPoint presentation. https://www.milsuite.mil/book/groups/navy-information-dominance-outreach/content?filterID=contentstatus%5Bpublished%5D%7Ecategory%5B2019-information-warfare-senior-leader-symposium-iwsls%5D
[48] Headquarters US Marine Corps, *Expeditionary Operations*, MCDP 3 (Washington, DC: Headquarters US Marine Corps, April 4, 2018), 38-42, https://www.marines.mil/News/Publications/MCPEL/Electronic-Library-Display/Article/899839/mcdp-3/
[49] U.S. Marine Corps, *Commandant's Planning Guidance*, 4.

[50] Shawn Snow, "Here's Why the Corps Strapped a Counter-Drone System to the Deck of a Warship in the Suez Canal," *Marine Corps Times*, January 31, 2019, https://www.marinecorpstimes.com/news/your-marine-corps/2019/01/31/the-corps-strapped-a-new-counter-drone-system-to-the-deck-of-a-warship-transiting-the-suez-canal-heres-why/
[51] Gidget Fuentes, "Boxer ARG, 11th MEU, rap Up 5th, 7th Fleet Deployment," *USNI News*, November 26, 2019, https://news.usni.org/2019/11/26/boxer-arg-11th-meu-wrap-up-5th-7th-fleet-deployment
[52] Snow, *Marine Corps Times.*
[53]Navy News Service, "Navy Public Affairs Support Element," About NPASE, accessed February 25, 2020, https://www.navy.mil/local/npasehq/ABOUT.asp
[54] United States Intelligence Activities, Executive order 12333 (1947) https://fas.org/irp/offdocs/eo/eo-12333-2008.pdf
[55] Lammons, *CHIPS*, "10 years Later NAVIFOR Expects Increased Fleet Integration."
[56] Christopher Dumas LCDR, January 14, 2020, Letter from CAPT Adam Porter, "CPR-3 O-5 IWC Afloat Opportunity," *MILSUITE*, U.S. Navy Intelligence Officer Detailing, https://www.milsuite.mil/book/thread/225013
[57] Greg Gabriel CDR, email message to author, February 20, 2020.
[58] Henry Stephenson CDR, "Masters or Jacks? Treating the Information Dominance Corps as A General Warfare Competency Risks Weakening the Skill Sets of its Specialists," *Proceedings* 140, no. 10 (October 2014), 58-63, https://www.usni.org/magazines/proceedings/2014/october/masters-or-jacks
[51] US Joint Chiefs of Staff, JP 3-13, 22.

**Glossary of Acronyms**

| | |
|---|---|
| ACE | Air Combat Element |
| AMDC | Air and Missile Defense Commander |
| ANGLICO | Air Naval Gunfire Liaison Company |
| ARG | Amphibious Ready Group |
| ASWC | Anti-Submarine Warfare Commander |
| ATF | Amphibious Task Force |
| A2AD | Anti-Access and Area Denial |
| CATF | Commander Amphibious Task Force |
| CLF | Commander Landing Force |
| CMF | Cyber Mission Force |
| CMO | Civil Military Operations |
| CNO | Chief of Naval Operations |
| CE | Command Element |
| CO | Commanding Officer |
| COMMSTRAT | Communications Strategy |
| CSG | Carrier Strike Group |
| CVW | Carrier Air Wing |
| CWC | Composite Warfare Command(er) |
| C2 | Command and Control |
| C2W | Command and Control Warfare |
| C4ISR | Command, Control, Communications, Computers, Intelligence, Surveillance, Reconnaissance |
| DC I | Deputy Commandant of the Marine Corps for Information |
| DCO-IDM | Defensive Cyber Operations – Internal Defensive Measures |
| DDGO | Deputy Director of Global Operations |
| DESRON | Destroyer Squadron |
| DIRSUP | Direct Support |
| DOTMLPF-P | Doctrine, Organization, Training, Materiel, Leadership and education, Personnel, Facilities and Policy |
| EABO | Expeditionary Advanced Base Operations |
| EMSO | Electromagnetic Spectrum Operations |
| ESG | Expeditionary Strike Group |
| EA | Electronic Attack |
| EW | Electronic Warfare |
| FAC | Fast Attack Craft |
| FIAC | Fast Inland Attack Craft |
| FID | Fleet Intelligence Detachment |
| GCE | Ground Combat Element |
| HVU | High Value Unit |
| IE | Information Environment |
| IO | Information Operations |
| IRC | Information Related Capability |
| ISRA | Intelligence, Surveillance, and Reconnaissance Agency |
| IW | Information Warfare |

| | |
|---|---|
| IWC | Information Warfare Commander |
| JC2WC | Joint Command and Control Warfare Center |
| JEWC | Joint Electronic Warfare Center |
| JFMCC | Joint Force Maritime Component Commander |
| JIOC | Joint Information Operations Center |
| LCE | Logistic Combat Element |
| LE | Law Enforcement |
| MAGTF | Marine Air-Ground Task Force |
| MEB | Marine Expeditionary Brigade |
| MEF | Marine Expeditionary Force |
| MEU | Marine Expeditionary Unit |
| MIG | Marine Information Group |
| MILDEC | Military Deception |
| MISO | Military Information Support Operations |
| MMS | Master of Military Studies |
| MST | METOC Support Team |
| NDS | National Defense Strategy |
| NGLO | Navy Gunfire Liaison Officer |
| NSS | National Security Strategy |
| N2N6 | Deputy Chief of Naval Operations for Information Warfare |
| OCO | Offensive Cyber Operations |
| OEF | Operation Enduring Freedom |
| OIE | Operations in the Information Environment |
| OIF | Operations Iraqi Freedom |
| OPORD | Operation Order |
| OPSEC | Operation Security |
| PA | Public Affairs |
| PHIBRON | Amphibious Squadron |
| PSYOP | Psychological Operations |
| RECCE | Reconnaissance |
| ROMO | Range of Military Operations |
| SACC | Supporting Arms Coordination Center |
| SCC | Sea Combat Commander |
| SGOT | Strike Group Oceanography Team |
| SECDEF | Secretary of Defense |
| SEWC | Space and Electronic Warfare Commander |
| SIGMAN | Signature Management |
| SNOOPIE | Ship's Nautical or Otherwise Photographic Interpretation and Examination |
| STRATCOM | Strategic Command |
| STWC | Strike Warfare Commander |
| SUWC | Surface Warfare Commander |
| SW | Surface Warfare |
| TCPED | Tasking, Collection, Processing, Exploitation, and Dissemination |
| UAS | Unmanned Aerial System |
| U.S. | United States |

| | |
|---|---|
| USIA | United States Information Agency |
| VI | Visual Information |

## BIBLIOGRAPHY


Aeschbach, Kelly RADM(sel). *Information Warfare Self Sync*. PowerPoint presentation. Naval Information Forces, Suffolk, VA, 14 December 2016. https://sites.google.com/site/idcsync/documents

Armistead, Leigh, ed. *Information Operations: Warfare and the Hard Reality of Soft Power*. Washington, DC, 2004.

Atherton, Kelly. "Marine Jamming Jeep Sends Unknown Drone to the Deep." C4ISRNET, 18 July 2019. https://www.c4isrnet.com/unmanned/2019/07/18/marine-jamming-jeep-sends-unknown-drone-to-the-deep/.

Braswell, Bryan. "Evolving the Information Warfare Commander." CHIPS, July-September 2010. https://www.doncio.navy.mil/CHIPS/ArticleDetails.aspx?ID=9422.

Cull, Nicholas John. *The Cold War and the United States Information Agency: American Propaganda and Public Diplomacy, 1945-1989*. Cambridge: Cambridge University Press, 2008.

Dan Struble. "What is Command and Control Warfare?" *Naval War College Review* 48, no. 3 (Jul 1, 1995): 89-98. https://www.jstor.org/stable/44642810.

Deputy Chief of Naval Operations for Information. *Information Dominance Engagement Area No. 37: Information Dominance Type Commander (TYCOM)*. March 7, 2014. https://sites.google.com/site/idcsync/documents

Deputy Commandant for Information. *Road to 2025*. PowerPoint presentation. Information Warfare Senior Leader Symposium, June 3, 2019. https://www.milsuite.mil/book/groups/navy-information-dominance-outreach/content?filterID=contentstatus%5Bpublished%5D%7Ecategory%5B2019-information-warfare-senior-leader-symposium-iwsls%5D

Gray, Colin and John Sheldon. "Space Power and the Revolution in Military Affairs." *Airpower Journal* 13, no. 3 (1999): 23-38.

Headquarters U.S. Marine Corps. *Marine Air Ground Task Force Information Environment Operations Concept of Employment*. Washington D.C.: Headquarters U.S. Marine Corps, July 6, 2017.

Headquarters U.S. Marine Corps. *Expeditionary Operations.* MCDP 3. Washington D.C., April 4, 2018. https://www.marines.mil/News/Publications/MCPEL/Electronic-Library-Display/Article/899839/mcdp-3/

Hesketh, Roger Fleetwood. *Fortitude: The D-Day Deception Campaign*. 1st ed. Woodstock, N.Y: Overlook Press, 2000.

Lammons, George. "10 Years Later NAVIFOR Expects Increasing Fleet Integration." CHIPS, 24 October 2019. https://www.doncio.navy.mil/CHIPS/ArticleDetails.aspx?id=12934

Marine Corps Information Plans and Strategy Division. *Deputy Commandant for Information OIE Overview Brief*. PowerPoint presentation. Marine Corps University, Quantico, VA, October 9, 2019.

Mattis, James, Secretary of Defense. Memorandum for Record, 15 September 2017.

Roughead, Gary ADM, Chief of Naval Operations, U.S. Navy to VADM David Dorsett, Director of Naval Intelligence. Memorandum, 26 June 2009. https://mrr.dawnbreaker.com/portals/phase3/opnav-resource-sponsors/opnav-n2-n6/

Stephenson, Henry CDR. "Masters or Jacks? Treating the Information Dominance Corps as A General Warfare Competency Risks Weakening the Skill Sets of its Specialists." *Proceedings* 140, no. 10 (October 2014), 58-63, https://www.usni.org/magazines/proceedings/2014/october/masters-or-jacks

Struble, Dan. "What is Command and Control Warfare?" *Naval War College Review* 48, no. 3 (Jul 1, 1995): 89-98. p90, 92. https://www.jstor.org/stable/44642810

The White House. *The National Security Strategy of the United States of America*. Washington DC, December 2017. https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf

U.S. Department of Defense. *Information Operations (IO).* Directive 3600.01, May 2, 2013 with Chg 1. https://www.hsdl.org/?abstract&did=800802

U.S. Department of Defense. *National Defense Strategy of the United States of America.* Washington, DC, January 19, 2018. https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf

U.S. Department of Defense. *Service Collaboration to Address Anti-Access & Area Denial Challenges*. Air-Sea Battle Office, May 2013. https://archive.defense.gov/pubs/ASB-ConceptImplementation-Summary-May-2013.pdf

U.S. Department of Defense. *Strategy for Operating in the Information Environment*. Washington, DC, June 13, 2016. https://dod.defense.gov/Portals/1/Documents/pubs/DoD-Strategy-for-Operations-in-the-IE-Signed-20160613.pdf

U.S. Fleet Forces Command. *Strike Group and Staff Tactical Training Continuum*, COMUSFLTFORCOM/COMPACFLTINST 1500.49C, February 1, 2019.

U.S. Joint Chiefs of Staff. *Joint Vision 2020.* Washington, D.C., 2000. https://apps.dtic.mil/dtic/tr/fulltext/u2/a526044.pdf

U.S. Joint Chiefs of Staff. *Department of Defense Dictionary of Military and Associated Terms*, JP 1-02. Washington, DC: Pentagon, 8 November 2010 as amended through 15 February 2016. https://fas.org/irp/doddir/dod/jp1_02.pdf

U.S. Joint Chiefs of Staff. *Information Operations*, JP 3-13. Washington, DC: Pentagon, 27 November 2012 with Change 1 20 November 2014. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13.pdf

U.S. Joint Chiefs of Staff. *Joint Maritime Operations.* JP 3-32. 8 June 2018. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_32.pdf?ver=2019-03-14-144800-240

U.S. Joint Chiefs of Staff. *Joint Operation.* JP 3-0. 17 January 2017 with Chg 1 22 October 2018. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_0ch1.pdf?ver=2018-11-27-160457-910

U.S. Joint Chiefs of Staff. *Military Information Support Operations Supplement to the Joint Strategic Capabilities Plan*. CJCSI 3110.05F, April 7, 2017.

U.S. Marine Corps. *38th Commandant's Planning Guidance*. Washington, DC: 2019. https://www.hqmc.marines.mil/Portals/142/Docs/%2038th%20Commandant%27s%20Planning%20Guidance_2019.pdf?ver=2019-07-16-200152-700

U.S. Secretary of the Navy. *Electromagnetic Battle Space*. Instruction 2400.3. October 5, 2018. https://www.secnav.navy.mil/doni/Directives/02000%20Telecommunications%20and%20Digital%20Systems%20Support/02-400%20Visual%20Information%20Services/2400.3.pdf

Valenti, Michael L. *The Mattis Way of War: An Examination of Operational Art in Task Force 58 and 1st Marine Division*. Fort Leavenworth, Kansas: US Army Command and General Staff College Press, an imprint of the Combat Studies Institute Press, 2016. https://www.armyupress.army.mil/Portals/7/combat-studies-institute/csi-books/the-mattis-way-of-war.pdf