REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
08-04-2022	FINAL	N/A

4. TITLE AND SUBTITLE
"Modernizing COCOM's: Information Warfare in the 21st Century"

5a. CONTRACT NUMBER
N/A

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
N/A

6. AUTHOR(S)

LCDR Sean Lee

Paper Advisor (if Any): **Prof John Sappenfield and LtCol Anthony Sama**

5d. PROJECT NUMBER
N/A

5e. TASK NUMBER
N/A

5f. WORK UNIT NUMBER
N/A

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Maritime Advanced Warfighting School (MAWS)
Naval War College
686 Cushing Road
Newport, RI 02841-1207

8. PERFORMING ORGANIZATION REPORT NUMBER
N/A

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

Director, Maritime Advanced Warfighting School (MAWS)
686 Cushing Road
Newport, RI 02841-1207

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

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

12. DISTRIBUTION / AVAILABILITY STATEMENT
For Example: Distribution Statement A: Approved for public release; Distribution is unlimited.
Reference: DOD Directive 5230.24

13. SUPPLEMENTARY NOTES A paper submitted to the Naval War College faculty in partial satisfaction of the requirements of the Joint Military Operations Department and the Maritime Advanced Warfighting School (MAWS). The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.

14. ABSTRACT

Modernizing COCOMs: Information Warfare in the 21st Century. Since Goldwater-Nichols, Geographic Combatant Commanders execute planning and operations supporting national strategy. Over the years, the organizational structure of the COCOM has largely remained unchanged. For some warfare areas, this has led to successful joint interoperability. New and emerging technologies, threats, and service capabilities are driving a need to modernize the joint force for information warfare. One method is to enable a new component commander, the "Joint Force Information Warfare Component Commander". By analyzing strategic competitors' information warfare advancements, service and allied information warfare efforts, and the current COCOM staff model, it becomes clear that change is necessary to fight and win in the information environment.

15. SUBJECT TERMS
Information Warfare

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
					Director, MAWS
a. REPORT	b. ABSTRACT	c. THIS PAGE		22	19b. TELEPHONE NUMBER *(include area code)*
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED			401-841-6149

Modernizing COCOMs: Information Warfare in the 21st Century

In 2014, NATO's top General, Philip Breedlove, said: "[Russia is]…waging the most amazing information warfare blitzkrieg we have ever seen in the history of information warfare".[1] In the lead-up to Russia's annexation of Crimea in 2014, Russian forces used social media, disinformation, and cyber warfare, among other information warfare capabilities, to create a manipulated information environment that shaped a narrative supporting their national political objective of seizing Crimea from Ukraine. The United States did little to counter the information campaign. In fact, the United States Government, as of this writing, has not even defined "information warfare."[2]

Since the Goldwater-Nichols act of 1986, the principal U.S. operational commanders are the geographic combatant commanders, or "COCOMs." Each COCOM is responsible for developing operational plans (OPLANs), which, in turn, generate requirements, funding, and ultimately, the ability to execute and win wars. As technology has advanced, the information environment and information warfare continue to grow in complexity and importance. However, the current operational and organizational construct within each COCOM has not kept pace to execute complex information warfare operations. For this reason, the COCOM organizational construct for planning, executing, and commanding information warfare requires a component commander.

To understand the need for an information warfare component commander, one only needs to look at the current state of IW. First, US strategic competitors are already using information warfare capabilities on a large scale to support national policy objectives across

---

[1] Peter Pomerantsev, "Russia and the Menace of Unreality: How Vladimir Putin is revolutionizing information warfare", *The Atlantic*, September 9, 2014.

[2] Catherine A. Theohary, Specialist in National Security Policy, "Defense Primer: Information Operations", Cyber and Information Operations, Congressional Research Service, Updated December 1, 2021.

every level of conflict. Second, every service component in the DoD, and many allies and partners of the US, are already building and developing significant information warfare capabilities and new service-level organizations to execute information warfare operations. Lastly, as each COCOM's mission and objectives have expanded, IW capabilities and planning continue to be disaggregated across multiple J-codes and supporting commands. By examining this current state of information warfare, it becomes clear that COCOMs require an Information Warfare Component Commander.

Defining Information Warfare through the Lens of Warfighting

The purpose of this paper is not an attempt to implicitly define (or redefine) information warfare (IW) but to provide a framework from which a Joint Force Commander can apply IW capabilities and resources to achieve objectives. In the context of this paper, IW does not include supporting information capabilities that are not used as the "tool" to achieve a commander's operational objective. For example, the definition of IW does not include intelligence. Intelligence is well defined in joint publications as an operational function that supports other warfighting objectives. In other words, intelligence alone cannot achieve objectives. Similarly, information technology management, which supports the IT infrastructure necessary to communicate, is not IW. However, both intelligence and IT play a crucial role in enabling operational fires, movement and maneuver (M2), command and control (C2), and other operational functions defined in joint doctrine[3].

It is helpful to compare the current state of IW to the early days of the aircraft. Military strategists and thinkers in the early twentieth century saw the potential of the aircraft. Still, it wasn't until after much experimentation, technological development, and

[3] Joint Publication 3 (JP-3), "Joint Operations", With Change 1, 2018, III-4.

practice in war that doctrine and organizational concepts were implemented to support the deployment of airpower. In a similar fashion to the early days of the aircraft, IW is in a state of change. At the same time, IW is not an entirely new concept. In this sense, current IW operations have more in common with aircraft at the end of World War II in that: technological developments and practice have laid the foundations to inform structure, execution, and future investments. IW as a discipline has been used in the wars in Afghanistan, Iraq, and elsewhere. China, Russia, and many others, including non-state actors, heavily utilize IW capabilities in war and across the conflict continuum[4]. Comparably, as the aviation organizational structure evolved into the modern Joint Force Air Component Commander (JFACC) as aircraft transitioned from biplanes to single-engine, and then again from jet-powered to modern fifth-generation low-observable, the organizational structure to employ joint IW capabilities needs to modernize to include a component commander.

IW, therefore, are those capabilities that are leveraged to achieve the commander's objectives. For example, on one end of the conflict continuum, a COCOM could stand up a JTF for the sole purpose of controlling the information environment. In this example, a notional state actor continually conducts unsafe flight interactions with US reconnaissance aircraft. The IW component commander, under the Joint Force Commander (JFC), would have operational control (OPCON) and/or tactical control (TACON) of resources across service components with the objective of shaping the IE around unsafe interactions. In another example, a notional state actor utilizes a network-linked integrated air defense system (IADS) which must be neutralized to achieve a land-based objective. The IW

[4] Joint Publication 1 (JP-1), "Doctrine for the Armed Forces of the United States", with Change 1, 2017. JP-1 describes the "conflict continuum" as the range of military operations (RMO) spanning from peace to war. Different than the "phases of war", the idea of the conflict continuum encompasses competition between war and during war.

component commander, under the JFC, would have OPCON and/or TACON of the resources needed to execute a combined attack utilizing offensive cyber, IO, and EW to neutralize the IADS. Both examples require the support of intelligence and IT but, in contrast, are executed to achieve an operational objective. Finally, shifting away from some traditional IW definitions, IW capabilities are not limited to effects in the information domain. Instead, creating effects against objectives using IW domain-based capabilities.

How, then, should information warfare be defined for the COCOM? Many have attempted to define what this term means explicitly. Civilian and military professionals alike have written books and research papers intending to define the term IW. IW is not easily defined, which speaks to its very nature of ambiguity in execution. This ambiguity in execution creates further confusion when a bureaucratic organization (such as the United States Department of Defense) attempts to develop policy and structure to support "information warfare" or related terms such as "information operations." Further arguments for this analysis are driven by using the congressional research service (CRS) concept of IW: "A strategy for the use and management of information to pursue a competitive advantage, including both offensive and defensive operations."[5] Competitive advantage infers utilizing IW capabilities against specific objectives. Defining IW in this way baselines the examination of a COCOM organizational construct to best employ IW capabilities.

Strategic Competition includes Information Warfare: Russia and China and Evolving Doctrine to Fight and Win in the Information Environment

[5] Theohary, 2021.
Author Note: The referenced document states that the US Government has no official definition of Information Warfare, and that the quoted statement is the typical concept of Information Warfare.

In recent years, the principal strategic competitors of the US: China and Russia, are rethinking and reshaping their military doctrines to utilize the information environment more effectively in pursuit of national objectives. It is dangerous to use "tit for tat" or "mirror imaging" to inform advancements in military strategy; however, COCOMs are not well postured to identify, counter, or seize the initiative against existing and future IW threats. Sun Tzu asserts that: "If you know the enemy and know yourself, you need not fear the result of a hundred battles."[6] By building an IW force for the future, COCOMs can seize the initiative in the information environment and deny the adversary freedom of action in the same.

In 2013, General Valery Gerasimov, Russia's senior military leader (equivalent to the US's Chairman of the Joint Chiefs of Staff), published an article titled: "The Value of Science is in Foresight." The key element within his paper was the strategic bridging between political and military efforts to achieve political aims.[7] While this idea is not alien to military planning and, in fact, is widely accepted according to Carl von Clausewitz's infamous assertion that "war is only policy by other means,"[8] Gerasimov re-imagined it as a form of hybrid warfare now referred to as the "Gerasimov Doctrine." In his model, information is the bridging mechanism used to shape the strategic environment and encompasses all components of Russian society. Everyone has a part to play: from the President to the military; to bankers and business people. In this fashion, the Gerasimov

[6] Sun Tzu, "The Art of War", Translated into English by Lionel Giles in 1910, *Project Gutenberg*, 2005, Chapter 2, paragraph 18, https://www.gutenberg.org/files/17405/17405-h/17405-h.htm#chap03 .
[7] Molly K. McKew, "Gerasimov Doctrine", *Politico*, September/October 2017.
[8] Carl von Clausewitz, "On War", *Project Gutenberg, 2006,* Book VIII, Chapter VI, 1874. https://www.gutenberg.org/files/1946/1946-h/1946-h.htm .

Doctrine uses information as the tool to "win." In this way, information becomes the main effort of national policy and potentially avoids head-to-head conflict.

In practice, Russia used significant IW efforts to shape the environment before and during conflicts in Georgia in 2008,[9] Crimea and the Donbas region of Ukraine in 2014,[10] and the current (2022) invasion of Ukraine. In both the 2008 and 2014 conflicts, Russia conducted significant IW operations in cyber and IO to create an operational environment that supported its operational objectives. Their military actions were very successful and largely uncontested due to the contribution of IW operations. As the 2022 Ukraine invasion progresses, it is apparent that Russia was not as successful in using IW shaping fires. While not enough data exists to holistically analyze their use of IW, it is clear that IW is part of their operational plan.

Additionally, China has adopted similar hybrid warfare models wherein the Chinese are focusing their efforts on Sun Tzu's idea of "winning without fighting."[11;12] In this way, China seeks to shape the information environment to support incremental steps to achieve its objectives while preventing escalatory actions that would lead to kinetic war. Such was the case as China incrementally developed multiple military installations across the South China Sea. Using the "9 Dash Line" and non-escalatory press statements about their purpose, China built several bases capable of monitoring and perhaps closing one of the most important commercial waterways in the world. PRC Colonel's Qiao Liang and Wang Xiangsui wrote in "Unrestricted Warfare" in 1999: "The new concept of weapons will cause ordinary people

[9] Keir Giles, "Handbook of Russian Information Warfare", NATO Defense College, Research Division, 2016. 35.
[10] Ibid, 49.
[11] Eric Jacobson, "Sino-Russian Convergence in the Military Domain", Center for Strategic and International Studies, Issue 15, March 22, 2018.
[12] Victor R. Morris, "Grading Gerasimov: Evaluating Russian Nonlinear War Through Modern Chinese Doctrine", *Small Wars Journal*, September 17, 2015.

and military men alike to be greatly astonished at the fact that commonplace things that are close to them can also become weapons with which to engage at war."[13] Liang and Xiangsui pair the changes in technology, specifically tied to information, with the emergence of a "new" form of warfare.

Both EUCOM and INDOPACOM, as the primary COCOMs responsible for Russia and China, respectively, were caught in reaction to Russia's aggression and Chinese expansion. Concerning Georgia and Crimea, the pace of employment of IW to deter Russian aggression was too slow to be effective. If EUCOM had an IW component commander, the response would likely have been executed earlier with objective-based effects and may have deterred Russia's actions. Similarly, as China began its South China Sea expansion, INDOPACOM would have benefitted from an IW component commander's expertise and execution of IW capability to deter China and persuade partner nations to seize the initiative and prevent unlawful expansion. However, due to disaggregated and unsynchronized IW capabilities, neither COCOM could effectively seize the information initiative.

Writing on the Wall: DoD Services and Allies are Developing IW Capabilities, and the Joint Force Needs to Seize the Information Initiative in Unity

Across the DoD, the Army, Airforce, Marines, Space Force, Navy (and Coast Guard as a sister service in the Department of Homeland Security) continue to man, train, and equip (MT&E) forces to conduct IW. Furthermore, key US allies and partners are experimenting with organizational structures to address changes in IW employment. Service components, allies, and coalition partners recognize the need for IW modernization. The information age

[13] Qiao Liang and Wang Xiangsui, "Unrestricted Warfare", Albatross Publishers, Naples, Italy, 2020. 17. "Unrestricted Warfare" speaks to the changes in technology which are creating a "new" form of warfare and a "change in the state of military affairs".

and warfare in the information age have created complex strategic, operational, and tactical problems that COCOMs must address to effectively integrate and lead joint and coalition IW forces.

The US Navy developed and implemented the "Information Warfare Dominance Community" (IDWC, now Information Warfare Community, or IWC) in 2009 as the first service component to try and provide a structure for the execution of IW tasks. When the Navy combined its Intelligence Community, Cryptologic Community, Information Professionals, and Meteorological Communities as the IDWC, each community had unique capabilities. In addition, the Navy established Naval Information Forces (NAVIFOR) to execute type commander (TYCOM) responsibilities for the information domain, like Naval Air Forces (NAVAIRFOR) and Naval Sea Forces (NAVSEAFOR) do for the air and sea domains. Furthermore, in 2013, the Navy released the "US Navy Information Dominance Roadmap, 2013-2018", which outlined three operating concepts which continue to drive Navy IW operations, and are listed below[14]:

- Battlespace Awareness
- Assured Command and Control
- Integrated Fires

In perhaps typical Navy fashion – the Navy created a command-and-control (C2) structure to MT&E an operational force, created left and right lateral limits, and began executing "Information Warfare." At the same time, the term itself was still undefined. This is by no means derogatory to the Navy. Instead, the operating concepts found in the roadmap continue

[14] RAML William E. Leigher, "US Navy Information Dominance Roadmap 2013-2028", 2013.

to drive organizational and operational successes within the Navy while continuing to define and redefine precisely what IW means for Naval Forces.

Similarly, each branch of the DoD is changing to modernize its IW force. The US Army Cyber Command (ARCYBER), for example, changed its mission statement in 2019 to read: [ARCYBER] "integrates and conducts full-spectrum cyberspace operations, electronic warfare, and information operations, ensuring freedom of action for friendly forces in and through the cyber domain and the information environment, while denying the same to our adversaries."[15] The US Air Force followed suit and organized the Sixteenth Air Force/Air Forces Cyber, which encompasses all Air Force Cyber, Intelligence Surveillance and Reconnaissance (ISR), EW, and weather capabilities into one IW command.[16] Additionally, the USMC established the "Marine Corps Information Operations Center" in order to "establish Operating in the Information Environment (OIE) as a valued and critical element of combined arms."[17] Finally, as previously stated, the Navy established the IWC community in 2009. Each service clearly understands the complexity of the IE and the necessity to modernize its force to win tomorrow's fight.

Not only is the US military changing its way of thinking about IW, but allies and partners are establishing IW branches. Australia, for example, created the "Information Warfare Division" under their "Joint Capabilities Group."[18] Multiple countries, including Japan, Canada, and Germany, have begun to organize forces that conduct IW into a single

[15] Conrad Crane, "The United States Needs an Information Warfare Command: A Historical Example", *War on the Rocks*, June 14, 2019.
[16] Mark Pomerleau, "Air Force Information Warfare Command Reaches Critical Milestone", *C4ISRNET,* July 15, 2020.
[17] USMC MCIOC Official Website, https://www.hqmc.marines.mil/Agencies/Deputy-Commandant-for-Information/MCIOC/,Accessed February 2022.
[18] Official Australian Department of Defense Website, https://defence.gov.au/JCG/iwd.asp, Accessed March, 2022.

cadre or have publicly recognized the need for more focus on IW capabilities in defense spending.[19;20;21] Leveraging allies and partners is one of the most important capabilities that a COCOM has at its disposal. Utilizing the IW component commander model can bridge IW capabilities across joint, allied, and coalition forces.

Within each step of technological development comes the need to orient the force towards specific objectives. While each COCOM is responsible for its geographic area, the service components develop and maintain the capabilities needed to meet COCOM objectives. In this way, COCOM requirements documented through the Joint Integrated Priority List (JIPL) are typically the bridging mechanism to develop service-led programs and capabilities. Using this development-funding model, each COCOM can support technological development requirements, which can be leveraged in the joint fight.

Service-led efforts have resulted in significant capability development to maneuver and control the IE. However, the disaggregation and lack of an IW commander at the COCOM level has resulted in capabilities being developed in stovepipes without unity of effort. For example, in the USMC's new concept of Expeditionary Advanced Basing Operations (EABO), the USMC has included "low-signature" as one of the primary tenets of EABO.[22] However, successful EABO relies on the joint force for sustainment, M2, and fires coordination. While the USMC is funding and designing low-signature EABO capabilities that are USMC specific, the joint force is not coordinating the IW capabilities required across

[19] Masaya Kako, "Cyber- and Electronic Warfare at Core of Japan's Defense Policy", *NikkeiAsia*, 2018.
[20] Guest Post (Blog), "Germany Develops Offensive Cyber Capabilities Without a Coherent Strategy of What to do with Them", *Council on Foreign Relations*, from Net Politics and Digital and Cyberspace Policy Program, 2018
[21] Mark G. Hazen, et al., "Characteristics of Information Warfare: The Battle for the Narrative", Defense Research and Development Canada (DRDC-RDDC-2017-P136), 2017.
[22] USMC EABO Official Website, https://www.marines.mil/News/News-Display/Article/2708120/expeditionary-advanced-base-operations-eabo/ , Accessed March 2022.

the force to support EABO. An IW component commander at the COCOM-level would be able to orient the COCOM commander to the task and purpose of a service-led IW requirement, and coordinate funding and resource requirements within the JIPL for the joint IW force in support of the commander's objectives for EABO.

Milan Vego, a noted Naval War College professor and academic expert in operational art, noted that "information overload" was experienced in Kosovo in 1999, Afghanistan beginning in 2001, and Iraq in 2003.[23] The point that Vego is making is that more information is not always an advantage. Vego claims that information, when not adequately processed, can lead to "information overload."[24] Based on the author's experience, military commands across the DoD are learning in stride how to manage vast amounts of information to create usable decision space for commanders across all levels of war; and across the width and breadth of the conflict continuum. In order for COCOMs to keep pace with the growth of IW, establishing an IW component commander is a method that will unify requirements and technology development against COCOM objectives.

Shaping the Fight: Disaggregation Undermines Joint Force Employment

The current INDOPACOM staff model, similar across all COCOMs, disaggregates IW capability across multiple J-codes. For example, the J39 is typically responsible for IO and EW coordination and planning. However, the J39 is not responsible for cyber operations. Instead, US Cyber Command (USCC) established Joint Force Headquarters Cyber, a Navy Fleet Cyber Command responsibility, to execute cyber operations for INDOPACOM.[25] Furthermore, the protection of COCOM information infrastructure is spread between cyber

[23] Dr. Milan Vego, "Joint Operational Warfare: Theory and Practice", US Naval War College, 2009. III-67.
[24] Ibid. III-65.
[25] Mark Pomerleau, "As threats increase, combatant commands want more cyber support and integration", *FEDSCOOP*, March 2, 2022.

elements, the J2, and the J6. SAP and STO capabilities are coordinated in the J2, J3, and J39. More importantly, each service component executes IW differently, and no service component has total responsibility within the information domain. Instead, each service component, as well as Special Operations Command (SOCOM) and USCC (as functional components), have responsibility for niche IW capabilities that are not centrally commanded and controlled.

In Large Scale Exercise 2021 (LSE), ADM Mike Gilday, the Chief of Naval Operations, stated: "By maneuvering across all domains, we will create operational dilemmas, exploit uncertainty and overwhelm our adversaries."[26] While the exercise details are classified, it is likely that the IW domain was heavily stressed. However, as with many exercises, (and based on the author's experience), it is also certain that some decision points and events were "white carded." Meaning that: a capability exists (or is expected to exist at a later time) that will meet a particular objective, and the exercise simply allowed the event or decision to proceed based on the assumption that the capability would work. Two often white-carded capabilities are IW capabilities (specifically cyber and IO) and logistics. In a globe-spanning exercise like LSE, synchronizing IW component commanders across multiple COCOMs would support the introduction of IW capability realism within the exercise to prevent unrealistic white-cards in the scenario. As with any move in a wargame, the IW capabilities brought to bear will either be sufficient or present opportunities for improvement. In this way, the joint IW force will be challenged to improve both technology and interoperability.

[26] Caitlin Kenney, "Globe-Spanning Wargame Puts New Naval Concepts to the Test", *Defense One*, August 10, 2021.

A 1999 RAND Corporation study on IW states: "The continuing challenge for military planners is to place these new information technologies and capabilities into a logical construct with ties to current and past military thought and operations."[27] Since RAND first published this report over twenty years ago, COCOMs have done little to maximize the use of IW capabilities at their level. JP-1 outlines each COCOM's authority to establish Joint Task Forces (JTFs) as necessary in response to theater events.[28] Typical components within a JTF are JFACC (Joint Force Air Component Command), JFMCC (Joint Force Maritime Component Command), JFLCC (Joint Force Land Component Command), and JFSOCC (Joint Force Special Operations Component Command). While each situation is different and requires different levels of action from each component, the functional component commander idea is based on bringing service capabilities under a joint commander to meet objectives in a particular domain. Since the 1999 RAND stud, this structure has not evolved to maximize service-level IW capabilities to meet COCOM objectives.

As each service develops IW capabilities and organizational structures to meet growing IW requirements, the COCOM organizational structure has not kept pace with modernization. Based on the changing nature of military operations and the need to control the information environment across the entirety of the conflict continuum, one possible solution to the problem is to create a "Joint Force Information Warfare Component Commander" or "JFIWCC" (pronounced "Jiff-Wick"). This functional commander would

[27] Edward Harshberger and David Ochmanek, *Chapter Six: Information Warfare: New Opportunities for U.S. Military Forces*, From: "Strategic Appraisal: The Changing Role of Information Warfare", ed. Zalmay M. Khalilzad and John P. White, 1999. 163.
[28] JP-1, 2017.

exist alongside the other component commanders; and, just like the JFACC or JFSOCC, would command joint resources in their domain against JFC (or COCOM) objectives.

The disaggregation of IW capabilities across multiple J-Codes and other functional component entities has resulted in the ineffective planning, coordination, and execution of IW capabilities. This lack of coherence and consistency can be corrected at the COCOM level by having a commander responsible for actions in the Information Warfare Domain. The JFIWCC will serve to focus on service-component IW development and deliver synchronized effects-based capabilities against COCOM objectives. Additionally, the JFIWCC will be able to plan and execute IW operations across the conflict continuum allowing the COCOM to seize the information initiative.

Staffing For Success: Method for Expanding the COCOM Staff to Synchronize Information Warfare

Even though the JFIWCC model is one method to synchronize IW capabilities, it is not the only option available to the COCOM. Another possibility would be to expand the COCOM J-Staff to centralize IW capabilities under a new J-code.

By implementing a new J-code, "J10" perhaps, a COCOM could bring together IW capabilities described earlier, such as cyber offense and defense, EW, IO, and STO. In this model, the J10 would be responsible for coordinating IW efforts across the joint force. This would undoubtedly benefit the synchronization of efforts as well as support the service-component capability development within the JIPL. Additionally, the J10 would become the focal point for any IW planning efforts within the J3 and the J5. By implementing the J10, a COCOM staff can help define and synchronize IW across the joint force.

The J10 model, however, lacks several key components that the joint IW force requires to modernize. First, without "command" authority, the J10 would not have OPCON and/or TACON of joint and allied capability to leverage them against objectives. While the J10 would surely improve IW synchronization, it would not have the authority of execution. The JFIWCC, on the other hand, would have that authority. Second, since COCOM inception following the Goldwater-Nichols Act, COCOM staffs have continued to expand in both personnel and property. Further expansion of the J-staff would require additional manpower and space, and in a zero-sum fiscal environment, it would be difficult for a COCOM to implement. The JFIWCC, however, is a task-oriented model in which the JFC directs a subordinate commander, such as MARFORPAC, or PACFLT (in the case of INDOPACOM), to assume the duties as JFIWCC. In this way, the JFIWCC has both OPCON and/or TACON of capabilities and represents them across the joint force for the JFC.

Finally, while the "J10" model may be useful for coordination and synchronization, it doesn't address the root of the problem: effects-based execution using IW-domain-based capabilities. The JFIWCC model, on the other hand, can both synchronize IW efforts across services and execute operations to meet JFC's objectives.

Conclusions: Leading from the Front: The Joint Force Information Warfare Component Command

All branches of the DoD and many allied and coalition partners recognize the efficacy of utilizing IW capabilities to gain and maintain an advantage over adversaries. Where IW differs from the traditional domains (air, sea, ground) is that conflict in the information environment exists across the breadth and scope of the conflict continuum. Even those

actions taken in the traditional domains in peacetime are often done for an information-based effect. Freedom of navigation patrols challenge unlawful claims of territorial control, strategic bomber flights in contested airspace send the message that the US will come to the aid of its allies, ground exercises like COBRA GOLD send the message that the US values its allies and partners. In each of these cases, a JFIWCC will ensure that COCOMs have unity of effort to meet their information objectives.

Beyond joint and coalition forces, the strategic competitors described in the current national defense strategy[29] already use significant IW capabilities, often without ethical or internationally accepted legal considerations, to wage an ongoing war to control the information domain. Russia, China, and Iran, along with terror groups such as ISIS, Al-Shabaab, and others, continue to undermine the global international world order using all methods of IW. To counter these malign actors across the conflict continuum, a JFIWCC will ensure COCOM, service, and allied IW capabilities are executed in unity to dominate the information environment. It is time to modernize the COCOM structure and implement a JFIWCC to execute IW and control the information domain.

According to JP-1, "A JFC can establish functional component commands to conduct operations." Furthermore, it states, "Functional component commands are appropriate when forces from two or more Military Departments must operate within the same mission area or physical domain, or there is a need to accomplish a distinct aspect of the assigned mission."[30] Additionally, JP1 describes situations such as how Marine Air-Ground Task Force (MAGTF) aircraft might be assigned to a JFACC for tasking. Each service component utilizes IW

[29] James Mattis, "Summary of the 2018 National Defense Strategy of The United States of America", US Department of Defense, 2018.
[30] JP-1, 2017. IV-4.

capabilities and is therefore operating in the same mission area and domain. From this perspective, the JFC has the authority required to establish a JFIWCC to meet its objectives. By focusing requirements, and unifying service IW capabilities, the JFIWCC will enable the unity of action and unity of purpose across the joint IW force.

One method of imagining the JFIWCC is to look at the component command through the lens of Joint Functions (or Operational Functions). According to Joint Publication 3 (JP 3), joint functions are broken into seven basic groups: Command and Control (C2), Information, Intelligence, Fires, Movement and Maneuver (M2), Protection, and Sustainment.[31] Each component commander under the JFC is responsible in either a supporting or supported role for each joint function. While operational planning doesn't typically call out each function explicitly, each component commander utilizes the joint functions process to assess their purpose and task against a JFC objective.

The JFIWCC, just like any other component command, would require OPCON and/or TACON authority over the employment of capabilities and people. In the previous example, without a JFIWCC, the COCOM J39 would typically be responsible as a coordinator across the joint force but lacks the authority to command those resources. Similarly, a Cyber Team commander has OPCON of their resources but is not unified in action with other IW actions. According to JP-1, functional component commanders typically have OPCON of forces with the same service as the component commander and TACON of forces from other services.[32] However, due to the lack of COCOM-level OPCON and/or TACON of IW forces, the joint force often operates independently along service lines to plan IW, resulting in ineffective execution. Ultimately, at the operational level of war, bridging IW resources under a

[31] JP-3, 2018. III-4.
[32] JP-1, 2017. IV-4.

JFIWCC will strengthen the joint force and give the JFC the ability to better leverage IW capabilities across the conflict continuum. How better to bring the full might of IW capabilities to bear across all facets of the conflict continuum than by utilizing an IW component commander, the JFIWCC, to lead IW capabilities across the joint and coalition force.

BIBLIOGRAPHY

Clausewitz, Carl von. "On War". *Project Gutenberg, 2006.* Book VIII, Chapter VI. 1874. https://www.gutenberg.org/files/1946/1946-h/1946-h.htm

Crane, Conrad. "The United States Needs an Information Warfare Command: A Historical Example". *War on the Rocks*. June 14, 2019.

Giles, Keir. "Handbook of Russian Information Warfare". NATO Defense College, Research Division. 2016.

Harshberger, Edward and David Ochmanek. *Chapter Six: Information Warfare: New Opportunities for US Military Forces*. From: "Strategic Appraisal: The Changing Role of Information Warfare". edited by Zalmay M. Khalilzad and John P. White. 1999.

Hazen, Mark G., and Anthony Isenor, Francine Desharnais, Tania Randall. "Characteristics of Information Warfare: The Battle for the Narrative". Defense Research and Development Canada (DRDC-RDDC-2017-P136). 2017.

Jacobson, Eric. "Sino-Russian Convergence in the Military Domain". Center for Strategic and International Studies. Issue 15. March 22, 2018.

Joint Publication 1 (JP-1). "Doctrine for the Armed Forces of the United States". With Change 1. 2017.

Joint Publication 3 (JP-3). "Joint Operations". With Change 1. 2018.

Kako, Masaya. "Cyber- and Electronic Warfare at Core of Japan's Defense Policy". *NikkeiAsia*. 2018.

Kenney, Caitlin. "Globe-Spanning Wargame Puts New Naval Concepts to the Test". *Defense One*. August 10, 2021.

Liang, Qiao and Wang Xiangsui. "Unrestricted Warfare". Albatross Publishers. Naples, Italy. 2020.

Leigher, RAML William E. "US Navy Information Dominance Roadmap 2013-2028". 2013.

James Mattis. "Summary of the 2018 National Defense Strategy of The United States of America". US Department of Defense. 2018.

McKew. Molly K. "Gerasimov Doctrine". *Politico*. September/October 2017.

Morris, Victor R. "Grading Gerasimov: Evaluating Russian Nonlinear War Through Modern Chinese Doctrine". *Small Wars Journal*. September 17, 2015.

Official Australian Department of Defense Website. https://defence.gov.au/JCG/iwd.asp. Accessed March, 2022.

Pomerantsev, Peter. “Russia and the Menace of Unreality: How Vladimir Putin is revolutionizing information warfare”. *The Atlantic*. September 9, 2014.

Pomerleau, Mark. “Air Force Information Warfare Command Reaches Critical Milestone”. *C4ISRNET.* July 15, 2020.

Pomerleau, Mark. “As threats increase, combatant commands want more cyber support and integration”. *FEDSCOOP*. March 2, 2022.

Theohary, Catherine A. Specialist in National Security Policy. “Defense Primer: Information Operations”. Cyber and Information Operations. Congressional Research Service. Updated December 1, 2021.

Tzu, Sun. “The Art of War”. Translated into English by Lionel Giles in 1910. *Project Gutenberg*, 2005. https://www.gutenberg.org/files/17405/17405-h/17405-h.htm#chap03

Guest Post (Non-Attributed). “Germany Develops Offensive Cyber Capabilities Without a Coherent Strategy of What to do with Them”. *Council on Foreign Relations*. From Net Politics and Digital and Cyberspace Policy Program, 2018.

USMC EABO Official Website. https://www.marines.mil/News/News-Display/Article/2708120/expeditionary-advanced-base-operations-eabo/. Accessed March 2022.

USMC MCIOC Official Website. https://www.hqmc.marines.mil/Agencies/Deputy-Commandant-for-Information/MCIOC/. Accessed February 2022.

Vego, Dr. Milan. “Joint Operational Warfare: Theory and Practice”. US Naval War College. 2009.