“The Joint Officer in the Next War Better Know His Cyber, and Good!”

Methods to Integrating Cyberspace Operations Into Joint Planning

Word Count: 3,460

A paper submitted to the Faculty of the United States Naval War College Newport, RI in partial satisfaction of the requirements of the Department of Joint Military Operations.

DISTRIBUTION A. Approved for public release: distribution unlimited. The contents of this paper reflect the author’s own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

REPORT DOCUMENTATION PAGE	*Form Approved* *OMB No. 0704-0188*

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. **PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.**

1. REPORT DATE *(DD-MM-YYYY)* 14-05-2020	**2. REPORT TYPE** FINAL	**3. DATES COVERED** *(From - To)* N/A

4. TITLE AND SUBTITLE "The Joint Officer in the Next War Better Know His Cyber…and Good!" Methods to Integrating Cyberspace Operations Into Joint Planning	**5a. CONTRACT NUMBER** N/A
	5b. GRANT NUMBER N/A
	5c. PROGRAM ELEMENT NUMBER N/A
6. AUTHOR(S) Major Mary Hossier, USAF	**5d. PROJECT NUMBER** N/A
	5e. TASK NUMBER N/A
	5f. WORK UNIT NUMBER N/A
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Writing & Teaching Excellence Center 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) N/A	**10. SPONSOR/MONITOR'S ACRONYM(S)** N/A
	11. SPONSOR/MONITOR'S REPORT NUMBER(S) N/A

12. DISTRIBUTION / AVAILABILITY STATEMENT
Distribution Statement A: Approved for public release; Distribution is unlimited.

13. SUPPLEMENTARY NOTES A paper submitted to the faculty of the NWC in partial satisfaction of the requirements of the curriculum. 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

Cyberspace operations are redefining national security, the character of warfare, and the struggle for power in the global environment. Yet, Joint Force Commanders continue to place emphasis on kinetic warfare, and often assume a passive posture in integrating cyberspace operations into the joint planning process. In order to achieve the optimal balance between the domains and apply operational art for the creation of the formidable combined force, Joint Force Commanders must integrate cyberspace operations into their understanding of combined arms to employ it effectively. While most Joint Force Commanders would hardly claim that cyberspace operations are not significant, many approach cyberspace operations in a way that indicates otherwise. This is because Joint Force Commanders lack a fundamental common understanding about the cyberspace domain that is directly fueled by a lack of integration in cyberspace doctrine and theory, a lack of cyberspace operations integration into the core curriculum of professional military education, and in the cultural values that drive the development and selection of current and future Joint Force Commanders. Addressing the lack of cyberspace integration into these three critical areas will posture current and future Joint Force Commanders to employ cyberspace operations effectively as part of combined arms to triumph against U.S. adversaries.

15. SUBJECT TERMS (Key words)
Joint warfare, cyberspace operations, joint force commanders, non-kinetic effects, kinetic effects, education, wargaming, doctrine, theory, policy, development

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON** Director, Writing Center
a. REPORT UNCLASSIFIED	**b. ABSTRACT** UNCLASSIFIED	**c. THIS PAGE** UNCLASSIFIED	N/A	21	**19b. TELEPHONE NUMBER** *(include area code)* 401-841-6499

Contents

Abstract

Cyberspace operations are redefining national security, the character of warfare, and the struggle for power in the global environment. Yet, Joint Force Commanders continue to place emphasis on kinetic warfare to the detriment of cyberspace operations, and often assume a passive posture in integrating cyberspace operations into the joint planning process. In order to achieve the optimal balance between the domains and apply operational art for the creation of a formidable combined force, Joint Force Commanders must integrate cyberspace operations into their understanding of combined arms to employ it effectively. While most Joint Force Commanders would hardly claim that cyberspace operations are insignificant, many approach cyberspace operations in a way that indicates otherwise. This is because Joint Force Commanders lack a fundamental common understanding about the cyberspace domain that is directly fueled by a lack of integration in cyberspace doctrine and theory, a lack of cyberspace operations integration into the core curriculum of professional military education, and in the cultural values that drive the development and selection of current and future Joint Force Commanders. Addressing the lack of cyberspace integration into these three critical areas will posture current and future Joint Force Commanders to employ cyberspace operations effectively as part of combined arms to triumph against U.S. adversaries.

INTRODUCTION

During World War II, Admiral William Halsey's leadership in the Pacific demonstrated a masterful application of operational art with the employment of naval aviation. He integrated aircraft carriers not merely as a substitution for battleships, but for the "creation of a modern, combined-arms fleet, one that included submarines and land-based aviation," that was lauded for its innovation.[1] Ten years earlier, Halsey earned his flying wings at the age of 52. This experience shaped his understanding of naval aviation throughout his career and had an enormous impact on the conduct of war in the Pacific theater in World War II. He considered airpower to be integral to the future of the Navy and commented, "The naval officer in the next war had better know his aviation, and good!"[2] His understanding of aviation, along with his developmental assignments in the Navy, and wargaming at the Naval War College, enabled him to create a formidable combined force, transforming carriers from their previous use as a 'hit-and-run' weapon to an elevated role for shielding amphibious forces and carrier battle.[3]

Halsey's example holds many lessons for the challenges the modern force is facing concerning cyberspace operations (CO). In 1944, many naval leaders were preparing for fleet-on-fleet decisive conflicts. Informed by his experience, Halsey saw beyond the paradigm impeding his contemporaries to employ naval aviation effectively in the use of combined arms. General Paul Nakasone, Commander, USCYBERCOM, said, "The environment we operate in today is truly one of great power competition, and in these competitions, the locus of the struggle for power has shifted towards cyberspace."[4] Yet modern Joint Force Commanders (JFC)

[1] Thomas Hone, "Replacing Battleships with Aircraft Carriers in the Pacific in World War II," *Naval War College Review* Vol. 66, Number 1, Article 6: 17, Winter, 2016.
[2] Walter Borneman, *The Admirals: Nimitz, Halsey, Leahy, and King – The Five-Star Admirals Who Won the War at Sea* (New York, NY: Little, Brown and Company, 2012) 157.
[3] Thomas Hone, "Replacing Battleships with Aircraft Carriers in the Pacific in World War II," *Naval War College Review* Vol. 66, Number 1, Article 6: 17, Winter, 2016.
[4] Paul Nakasone, "Gen. Nakasone Lays Out Vision for '5th Chapter' of US Cyber Command," *Meritalk*, September 7, 2018, https://www.meritalk.com/articles/nakasone-cyber-command-vision/.

continue to place emphasis on kinetic warfare to the detriment of CO.[5] In order to achieve the optimal balance between the domains and apply operational art for the creation of a formidable combined force as Halsey did, JFCs must integrate CO into their understanding of combined arms to employ it effectively.

This may seem counterintuitive, as one would be hard-pressed to find a JFC who would claim that CO is insignificant, yet many JFCs approach CO in a way that indicates otherwise. USCYBERCOM leadership shared they often reach out to JFCs to explain what CO can offer, because JFCs do not automatically consider CO in their joint planning.[6] This is because JFCs lack a "shared cyberspace knowledge and an agreed operational approach to link cyberspace missions and actions and place them in the larger context of joint operations."[7] Halsey proved that experience with a domain directly impacts JFCs ability to employ it effectively in the larger context of joint operations. JFCs are not integrating CO fully into joint planning because of a lack of integration in cyberspace doctrinal and theoretical framework, professional military education (PME), and the development of current and future JFCs.

Cyberspace Background

Before considering cyberspace integration, it is important to provide context. Colonel (Retired) Michael Harasimowicz, former commander, 688th Cyberspace Wing, claimed the joint force, "doesn't know if cyberspace is a valuable part of our culture or if it's a sideshow."[8] Yet, CO is indispensible to joint warfighting as "it is impossible to fully employ today's joint force *without* leveraging cyberspace."[9] Admittedly, cyberspace considerations are new to joint

[5] Timothy Noah, "Birth of a Washington Word—When Warfare gets 'Kinetic,'" *Slate*, November 20, 2002. https://slate.com/news-and-politics/2002/11/kinetic-warfare.html; Kinetic Warfare: warfare waged in the physical domains of air, land, sea, and space, and frequently implies lethal warfare.

[6] Trey Herr. "Cyber Operations in Context: A Look at Joint Task Force ARES," *Atlantic Council,* September 16, 2019, https://www.atlanticcouncil.org/event/cyber-operations-in-context-a-look-at-joint-task-force-ares/.

[7] Sean Kern, "Expanding Combat Power Through Military Cyber Power Theory," *Joint Forces Quarterly* 79, 4th Quarter (2015), 89. https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-79/jfq-79_88-95_Kern.pdf.

[8] Michael C. Harasimowicz, interview with the author, April 22 2020.

[9] Kern, *Expanding Combat Power*, 89.

warfighting. In 2011, Department of Defense (DoD) designated cyberspace an operational domain noting that CO is *redefining* national security. Stability in cyberspace can to lead to freedom of action in the physical domains by possessing superiority over machines independent of their owners or by limiting adversary decision-making and command and control (C2).[10] CO is also vital to the collection, analysis, and utilization of intelligence and deterrence operations.[11]

While significant, cyberspace is challenging to understand. It is a man-made operating space to exchange and exploit information, but has natural elements with physical characteristics stemming from electromagnetic forces.[12] Cyberspace is also a uniquely global domain where effects are not limited to a geographical region, creating complications with command authorities and levels of decision-making. Additionally, cyberspace conflict can occur at the speed of computation, which requires JFCs' time and space considerations to be more dynamic and complex.[13] Due to the complexities, thinking about cyberspace among the joint force has been uneven. Even the term 'cyberspace' is misleading, when cyberspace consists of thousands of networks and 'cyberspaces' comprised of government and commercial infrastructure.[14] It is considered a non-kinetic domain, yet exists in the physical world in the form of machines, cables, and infrastructure. Experts caution that calling cyberspace a domain implies an inaccurate homogeneous nature, and viewing it as *merely* another warfighting domain obscures the distinctions it has from the kinetic domains of air, land, sea, and space.[15] Yet cyberspace shares similarities with the kinetic domains, which require mental agility to recognize when to employ

[10] Richard Crowell, "Some Principles of Cyber Warfare Using Corbett to Understand War in the Early Twenty–First Century," *King's College London—The Corbett Centre for Maritime Policy Studies*, January 2017, 5.
[11] Kern, *Expanding Combat Power*, 89.
[12] Adam Morgan and Steve Stone, "Command and Control for Cyberspace Operations—A Call for Research," *Military Cyber Affairs,* Vol 4: Issue 1, Article 4. 2019, 8.
https://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1051&context=mca
[13] Morgan and Stone, *Command and Control for Cyberspace Operations*, 8.
[14] Kern, *Expanding Combat Power*, 89.
[15] Alexander Klimburg, *The Darkening Web: The War for Cyberspace*. (New York: Penguin Books, 2018),138.

and deviate from traditional warfighting concepts. Like Halsey learning a new combat system at 52, JFCs will need similar mental flexibility to employ CO for maximum combat power.

Cyberspace Framework Lacks Cohesion

The doctrinal and theoretical framework for CO must be cohesive in order for JFCs and planners to think about CO in common terms. Harasimowicz lamented that the "lack of precision in our language has haunted cyber leaders. You can create a lack of expertise and make problems worse by being imprecise."[16] The foundation of precision in language and thinking about CO is rooted in doctrine and theory, which enable a common understanding of what a domain is, how the joint force can employ it, and facilitates a standard operating language.[17] The problem for JFCs is that joint doctrine is incoherent and the CO theory is nonexistent.

Doctrinal Inconsistencies

The doctrinal framework for CO across the joint force does not approach CO in an integrated way. Some doctrine is quite thorough in integrating CO, like cyberspace operations and multi-domain operations doctrine, while others, like C2 and joint fire support doctrine, exhibit inconsistencies that contribute to a misunderstanding of how to employ CO.[18]

Defense leaders recognize traditional C2 doctrine has substantial limitations when applied to cyberspace, namely speed and agility, but have not yet updated it to address these challenges.[19] C2 doctrine is critical because there is "a near total-reliance on cyberspace" to communicate, exercise C2, and move information to decision-makers across all levels of war.[20] The DoD owns more than 15,000 networks interconnected by commercial infrastructure, which

[16] Michael C. Harasimowicz, interview with the author, April 22 2020.

[17] Milan Vego, *Joint Operational Warfare: Theory and Practice,* (Newport, RI, USNWC Press, 2007) XII-3. Vego defines Doctrine as: fundamental principles, organizational tenets, and methods of force employment intended to guide the planning, preparation and execution of one's forces to accomplish given military objectives.

[18] Mark Hofer, "The C2 of Cyberspace is a Mess!" *U.S. Naval Institute Proceedings,* August 2019, https://www.usni.org/magazines/proceedings/2019/august/c2-cyberspace-mess

[19] Morgan and Stone, *Command and Control for Cyberspace Operations*, 2.

[20] Richard Crowell, "War in the Information Age: A Primer for Information Operations and Cyberspace Operations in 21st Century Warfare – Land, Maritime, Air, Space, and Cyberspace Domains, " *The United States Naval War College—Joint Military Operations Department*, 5th Edition, January 2019, 42.

means JFCs often lack exclusive control of all key cyber terrain and must understand and incorporate these limitations into their joint planning process.[21] Speed and agility considerations for C2 doctrine are vital for JFCs because cyberspace has unique flexibility of terrain and a lack of object permanence, resulting in defending content and activity and not specific terrain.[22] Experts from the Army Cyber Institute stated, "Our C2 doctrine does not envision an environment where objects can appear, disappear, reappear, and change at computational speed."[23] Fully integrated C2 doctrine would influence joint planning considerations in recognition that cyberspace defense may be as agile as offense. It is more concerned with protecting content and function versus defending a particular piece of land, sea, or airspace.[24]

Integrating CO is absolutely critical because, if it is not done correctly, it can create confusion as evidenced by joint fire support doctrine.[25] While integrating CO into joint doctrine helps put CO into a standard joint lexicon, experts argue this particular instance of integration did not effectively allow for CO mission growth and attempted to apply it to instances that were not applicable. This stems from an oversimplification of the effectiveness Joint Task Force-ARES's (JTF-ARES) operations had in combining CO with kinetic warfare. [26] Established to counter ISIS cyberspace activity, JTF-ARES executed offensive CO to disable and degrade ISIS cyberspace efforts. While many aspects are still classified, one known operation included using CO means to disable ISIS command posts one by one, forcing ISIS to reveal other command posts in Iraq and Syria. Once revealed, joint forces launched ground attacks and disabled these

[21] Kern, *Expanding Combat Power*, 89.

[22] Morgan and Stone, *Command and Control for Cyberspace Operations*, 8.

[23] Jan Kallberg and Thomas Cook, "Unfitness of Traditional Military Thinking in Cyber." *IEEEAccess*, Volume 5 (2017). 8126-8130. https://cyberdefense.com/wp-content/uploads/2018/09/Unfitnesstraditionalthinking.pdf

[24] David Fahrenkrug, "Countering the Offensive Advantage in Cyberspace: an Integrated Defensive Strategy," *The United States Naval War College—Joint Military Operations Department*, 4th International Conference on Cyber Conflict, 2012, 199.

[25] Paul Ducheine and Jelle van Haaster, "Fighting Power, Targeting and Cyber Operations," *NATO Cooperative Cyber Defence Centre of Excellence,* 2014, https://ccdcoe.org/uploads/2018/10/d2r1s9_ducheinehaaster.pdf.

[26] Michael Martelle, "Cyber-Attacks and Fire Support: Documents Illustrate Historic Trend in Integration of Military Technology," *Unredacted,* February 28, 2019. https://unredacted.com/2019/02/28/cyber-attacks-and-fire-support-documents-illustrate-historic-trend-in-integration-of-military-technology/

operating posts.[27] While JTF-ARES proves how effective CO can be in contributing to the achievement of kinetic ends, the full impact of CO goes far beyond kinetic effects.[28]

One case that disputes the joint fire support framework was USCYBERCOM's operation to counter Russian election interference in the 2018-midterm elections. USCYBERCOM acted unilaterally in cyberspace to monitor individual operators and disable networks of the Internet Research Agency.[29] Experts contend this is a notable example of where the joint fire support framework ceased to be useful in executing autonomous CO.[30] While integrating CO into doctrine cohesively is crucial for a shared understanding, doing so in a way that does not account for nuance and complexities perpetuates misunderstanding.

Needed Cyberspace Theory

Beyond doctrine, theory for CO does not exist. Military cyber power theory would aid decision-makers with a common understanding of how to employ CO to achieve military objectives and political ends.[31] Viewing operations through this lens is vital for the Joint Force Cyber Component Commander to provide the best military advice to JFCs, and for JFCs and planners to consider, plan for, and generate expanded combat power.[32] A cohesive theory of cyberspace should address the intertwining of human and cyberspace activity, how cyberspace facilitates achieving objectives, and how CO contributes to the pursuit of victory.[33] Based on clear doctrine and theory of CO, the DoD could generate precise and tailored cyberspace policy.

[27] Shannon Vavra, "U.S. cyber-offensive against ISIS continues, and eyes are now on Afghanistan, general says." *CyberScoop*. September 17, 2019. https://www.cyberscoop.com/isis-jtf-ares-cyber-offensive-afghanistan/

[28] Applegate, Scott. "The Dawn of Kinetic Cyber." *Center for Secure Information Systems—George Mason University.* 2013. https://ccdcoe.org/uploads/2018/10/10_d2r1s4_applegate.pdf

[29] Martelle, *Cyber-Attacks and Fire Support*.

[30] Martelle, *Cyber-Attacks and Fire Support*.

[31] Crowell, *Some Principles of Cyber Warfare*, 2.

[32] Kern, *Expanding Combat Power*, 89.

[33] Crowell, *Some Principles of Cyber Warfare*, 2.

As graduated cyber commanders noted, a critical lesson from their tenure was the need for DoD policies to alleviate issues like C2 complications that adversely impacted CO employment.[34]

Military cyber theory would also classify CO among the levels of war, which has been a chronic issue plaguing CO in joint operations. Historically, decision-makers at the national and department levels viewed CO as a matter of national policy, which stemmed from the sensitivities concerning the potential unintended global effects of CO.[35] The result was a resistance to embrace the operational and tactical implications for CO, and centralizing decision-making at the highest levels of command. Some centralization stemmed from senior leaders' risk aversion due and limited understanding of CO.[36] There has been some progress in this area with new release authorities recently being delegated to USCYBERCOM.[37] However, experts contend more authority should be at the operational and, potentially, tactical level.[38] Issues of delegation with global impact potential are highly complex, but, at a minimum, this debate highlights the need for cohesive cyber theory to ensure CO authorities are delegated to the correct level for joint warfighting success. Additionally, theory and doctrine should be continuously modified to address the changing character of war and address gaps in current military thinking.

Integrate Cyberspace into Professional Military Education

Shortcomings with the doctrinal and theoretical framework for CO would be less significant if JFCs had an educational background that equipped them to engage in cyberspace. The Chairman of the Joint Chiefs of Staff (CJCS) designated "Globally Integrated Operations in the Information Environment" to be part of Joint PME curriculum, yet most institutions spend

[34] Jason Healey and Karl Grindal. "Lessons from the First Cyber Commanders." *Atlantic Council.* March 14, 2012. https://www.atlanticcouncil.org/blogs/new-atlanticist/lessons-from-the-first-cyber-commanders/

[35] Crowell, *War in the Information Age*, 42.

[36] Williams, *The Joint Force Commander's Guide to Cyberspace Operations*.

[37] Mark Pomerleau, "New authorities mean lots of new missions at Cyber Command," *Fifth Domain,* May 8, 2019, https://www.fifthdomain.com/dod/cybercom/2019/05/08/new-authorities-mean-lots-of-new-missions-at-cyber-command/

[38] Williams, *The Joint Force Commander's Guide to Cyberspace Operations*.

only days on the subject.[39] In addition to the required framework, the joint force requires *much* more exposure to the cyberspace domain throughout their careers to promote familiarity and fluency. Lieutenant General John Shanahan, Director of the Joint Artificial Intelligence Center, contends that adequate exposure entails, "the right combination of education and training, experimentation, wargames, and exposure to modeling and simulation…[and] how to apply theory to real-world use cases."[40] PME is where current and future JFCs and planners establish and deepen their understanding of each domain, learn the interrelationships between them, and gain hands-on experience with the domains when possible.

Fundamentals of Cyberspace

PME *must* have an expanded emphasis on the employment of CO as a warfighting domain. Meeting the intent of CJCS guidance requires more time allocated to the study of CO and diversity in teaching methods. Harasimowicz argued, "If we want to say we value multi-domain warfare, there's a responsibility to learn about each of those domains beyond a superficial level." PME is an ideal time to learn the fundamentals of cyberspace, contextualize CO by bridging from similar kinetic domains, and recognize the human element in cyberspace.

PME can help bridge the technical gap by building from familiar domains. Many JFCs and planners often view CO as "too technical," but multiple experts highlight the similarities it bears to the maritime domain.[41] Sir Julian Corbett wrote, "The normal position is not a commanded sea, but an uncommanded sea."[42] Richard Crowell highlights the parallel to the maritime domain, as cyberspace, like the sea, is vast and virtually impossible to "command" in

[39] JPME Chairman's Special Areas of Emphasis (SAE) for Academic Years 20 and 21, *Joint Chiefs of Staff,* https://www.jcs.mil/Portals/36/Documents/Doctrine/education/jpme_sae_2020_2021.pdf

[40] John N.T. Shanahan, e-mail to author, April 19, 2020.

[41] Crowell, *Some Principles of Cyber Warfare*, 6-7; Brandon Valeriano Brandon and Benjamin Jensen, "The Myth of Cyber Offense: The Case for Restraint," *CATO Institute,* January 15, 2019, https://www.cato.org/publications/policy-analysis/myth-cyber-offense-case-restraint

[42] Julian Corbett, *Some Principles of Maritime Strategy*, (New York: AMS Press, 1972), 91.

the traditional sense.[43] The struggle within the cyber and maritime domains is to attain some modicum of control concerning access and use of the domain, which Corbett describes as the "object" of warfare.[44] JFCs achieve a semblance of control in both domains through balancing the operational factors of time, space, and force, and sequencing warfighting functions as required.[45] While the character of warfare in cyberspace may have distinct time, space, and force considerations, the governing principles are highly applicable.

The human interface with technology is imbedded in PME and building onto this foundation is necessary to understand the relationship between humans and machines and contextualize the significance of cyber warfare in future conflicts. States and non-state actors will defend and use content, connectivity, and understanding to achieve operational objectives and strategic ends.[46] Armed with this understanding, future JFCs will be able to integrate CO innovatively and gain a critical competitive advantage. The human element of CO is significant because it involves people, their habits, and the way they operate.[47] In the fight against ISIS, one cyberspace operator recalled learning the adversary, their habits, account names, passwords, applications on their phones, and which e-mails they open.[48] Cyberspace operators at USCYBERCOM closely resembled highly trained snipers, studying targets to know precisely the ideal time to exploit their target when they received the command "fire!"[49] The human-factors elements were as integral to the operation as traditional CO functions like writing lines of code.[50]

[43] Crowell, *Some Principles of Cyber Warfare*, 6-7.
[44] Fahrenkrug, *Countering the Offensive Advantage in Cyberspace*, 199.
[45] Crowell, *War in the Information Age*, 37.
[46] Crowell, *Some Principles of Cyber Warfare*, 4
[47] Tim Huening, “The Importance of Human Factors for Joint Cyber Planning,” *Small Wars Journal,* Accessed March 21, 2020, https://smallwarsjournal.com/jrnl/art/the-importance-of-human-factors-for-joint-cyber-planning
[48] Dina Temple-Raston, “How the U.S. Hacked ISIS,” *National Public Radio,* September 26, 2019, https://www.npr.org/2019/09/26/763545811/how-the-u-s-hacked-isis.
[49] Temple-Raston, *How the U.S. Hacked ISIS*.
[50] Temple-Raston, *How the U.S. Hacked ISIS*.

As joint leaders deepen their understanding of the cyberspace domain, they will be able to employ cyber forces differently than, but as effectively as, air, land, sea, and space forces.[51]

Integrated Curriculum, Integrated Thinking

Thinking about CO in an integrated manner is difficult when PME does not integrate CO fully into its curriculum. Using the Naval War College as an example, the weeklong Future Warfighting Symposium was beneficial for increasing exposure to future warfighting domains. However, the separate construct perpetuates viewing CO as a "sideshow," when it should be integrated into the core curriculum. Some might agree CO should be integrated, but argue it is difficult to determine what to remove from the current curriculum. Future JFCs and planners will employ CO in areas of international relations, strategy, and operations and the curriculum should prioritize material that highlights the cyberspace elements in these areas.

International relations courses already focus on contemporary issues. Selecting readings that highlight the impact of CO and non-kinetic warfare in the increasingly politicized warfighting environment will be of ultimate value to future joint leaders making political, diplomatic, and economic considerations. Additionally, CO will only continue to increase in diplomatic and political significance as the example of USCYBERCOM's operations to prevent Russian election interference indicates. For strategy courses, JTF-ARES' operations against ISIS highlight the interrelationship of CO and kinetic operations, and are a significant lesson learned from the 'wars' in the Middle East. CO is also an ideal consideration for strategy courses that include understanding the arc of technology in warfare throughout history and its evolving employment. Humans historically misunderstood new domains as they were introduced. In 1932, Stanley Baldwin argued that the, "bomber will always get through," demonstrating a gross

[51] Crowell, *War in the Information Age*, 42.

miscalculation of air warfare in World War II.[52] Airpower is analogous to cyberspace because it required JFCs and planners to alter their thinking about the character of war to account for unique capabilities airpower brought to the joint fight.[53] Finally, joint planning courses should prioritize material integrating CO employment into sessions focused on combined arms, C2, multi-domain operations, tabletop exercises, and wargaming.

Wargaming

Wargaming, modeling, and simulation provide hands-on experience to aid joint leaders toward an intuitive understanding of the domain. Harasimowicz exposed General John Hyten, then Commander of Air Force Space Command, to a simple cyberspace wargaming session that mirrored the game "capture the flag" and included finding and patching vulnerabilities as well as identifying and exploiting adversary vulnerabilities. After the four-hour period, the cyberspace wing commander was able to have more advanced conversations with the general about CO. Structured, simple, and introductory wargaming is crucial because, "it gives a feeling of what it means to exist in the domain."[54] Joint planning courses already include wargaming as part of their curriculum, and even a few hours would provide future JFCs and planners an intuitive experience to understand the cyberspace domain in a new way.[55]

Joint Leader Development

A proper framework and cyberspace experience are of limited benefit to JFCs if their efforts to integrate CO into joint planning are inhibited by senior leadership who do not understand the cyberspace domain. Many senior leaders have risen to the top by proving their ability to direct joint operations in the air, land, sea, and space domains, and often rely on past

[52] Kern, *Expanding Combat Power*, 89.

[53] Brett Williams, "The Joint Force Commander's Guide to Cyberspace Operations," *Joint Force Quarterly* 73, April 1, 2014, https://ndupress.ndu.edu/Media/News/Article/577499/the-joint-force-commanders-guide-to-cyberspace-operations/

[54] Michael C. Harasimowicz, interview with the author, April 22 2020.

[55] Michael C. Harasimowicz, interview with the author, April 22 2020.

expertise versus developing new capabilities. The result has been relegating CO to a secondary domain and a lag in operationalizing it for combat power. Major General Brett Williams, Director of Operations for the Joint Staff, argued, "there is too much at stake for our senior leaders not to understand CO in the same way they understand operations in the other domains."[56] Senior leaders drive which assignments the force values, hinder or accelerate CO integration, and set the stage for the optimal blend of experience for future joint leadership.

Assignments

Assignments, and longer exposure, are highly beneficial to building experience with new technology to empower innovative combined arms employment. As Halsey's example shows, JFCs and planners are directly influenced by their experiences in assignments. However, service culture drives which assignments rising leaders see as desirable, and senior leadership influences service culture by rewarding, hiring, and promoting officers with desired experience. [57] Senior leaders valuing CO is crucial for rising leaders to gain vital career CO experience, and antiquated thinking deters future JFCs from needed experience by driving their efforts elsewhere.

Accelerate Cyberspace Integration

There is a cost to traditional thinking. The Air Force considered nominating leaders from space and cyberspace domains to be the Chief of Staff of the Air Force (CSAF) but ultimately nominated leaders from the air domain due to concerns about deviating from conventional wisdom too fast too soon. Harasimowicz shared a major challenge to retaining cyberspace talent and executing CO was the CSAF's view that CO was a strategic issue. This thinking hamstrung the unit's CO efforts and made clear to cyberspace operators (and the Air Force) that CO was

[56] Williams, *The Joint Force Commander's Guide to Cyberspace Operations*.

[57] Jason Bender, "The Cyberspace Operations Planner: Challenges to Education and Understanding of Offensive Cyberspace Operations," *Small Wars Journal,* https://smallwarsjournal.com/jrnl/art/the-cyberspace-operations-planner.

"someone else's job."[58] Leaders who lack the necessary experience to value emerging domains complicate the perceived value and intellectual investment these domains deserve.

In contrast, the rise of cyberspace leaders to some senior joint positions has had positive effects. Like Halsey, many officers serving in senior cyberspace roles hail from other functional communities and had a steep learning curve to be successful in these roles. Regardless, those with cyberspace experience lobbied their services tirelessly for reorganization like 16th Air Force, which consolidated non-kinetic functions and removed stovepipes. These leaders championed CO as a supporting role to combatant commanders and not merely independent functions, but even they admit their development is not a template to follow for the future.[59]

Set the Stage

It is unwise to assume the tremendous, yet incomplete, progress made with CO will continue without experienced CO professionals in command of joint organizations.[60] As with Halsey's example, the joint force needs leaders who understand the cyberspace domain and drive it toward the necessary measures to employ it effectively. These leaders will ensure the joint force maintains its competitive edge for success in future conflicts.[61] If General Nakasone is correct in stating the struggle for power is shifting toward CO, it is time for the joint force to think seriously about developing and selecting Combatant Commanders, Service Chiefs, and JFCs who have extensive CO experience as future warfighting success will depend on it.

[58] Michael C. Harasimowicz, interview with the author, April 22, 2020.

[59] John N.T. Shanahan, e-mail to author, April 19, 2020; Pomerleau, *Here's what Combatant Commanders Want From Cyber Teams*.

[60] Thomas Spoehr, and James Di Pane, "Elevating Cyber Command: An Overdue Step Towards Enhancing Military Cyber Operations," *The Heritage Foundation,* October 1, 2018. https://www.heritage.org/cybersecurity/commentary/elevating-cyber-command-overdue-step-towards-enhancing-military-cyber.

[61] Mark Pomerleau, "Here's what Combatant Commanders Want From Cyber Teams," *Fifth Domain,* November 19, 2018, https://www.fifthdomain.com/dod/cybercom/2018/11/19/heres-what-combatant-commanders-want-from-cyber-teams/.

Conclusion

Cyberspace has enormous significance for current and future national defense operations, and JFCs struggle to fully integrate CO because of its complexity, unique characteristics, and difficulty in transitioning their thinking toward this new kind of warfare. While these challenges are substantial, steps toward solving these challenges include making the CO doctrinal and theoretical framework cohesive; integrating CO into PME through curriculum adjustments and wargaming; and, developing senior leaders who understand and will advocate for the significance of CO and organize the force for its effective employment. Much like Halsey, these measures will better equip future JFCs to employ CO effectively as part of combined arms to triumph against U.S. adversaries.

Bibliography

Applegate, Scott. "The Dawn of Kinetic Cyber." *Center for Secure Information Systems—George Mason University.* 2013. https://ccdcoe.org/uploads/2018/10/10_d2r1s4_applegate.pdf.

Bender, Jason. "The Cyberspace Operations Planner: Challenges to Education and Understanding of Offensive Cyberspace Operations." *Small Wars Journal.* https://smallwarsjournal.com/jrnl/art/the-cyberspace-operations-planner.

Borneman, Walter R. *The Admirals: Nimitz, Halsey, Leahy and King – The Five-Star Admirals Who Won the War at Sea*. (New York: Little, Brown and Company, 2012).

Cohen, Rachel. "Joint Staff Wargames Explore Who's in Charge of Non-Kinetic Attacks." *Air Force Magazine.* October 24, 2019. https://www.airforcemag.com/joint-staff-wargames-explore-whos-in-charge-of-non-kinetic-attacks/.

Corbett, Julian S. *Some Principles of Maritime Strategy*. (New York: AMS Press, 1972).

Crowell, Richard. "Some Principles of Cyber Warfare Using Corbett to Understand War in the Early Twenty–First Century." *King's College London—The Corbett Centre for Maritime Policy Studies*. January 2017.

"War in the Information Age: A Primer for Information Operations and Cyberspace Operations in 21st Century Warfare – Land, Maritime, Air, Space, and Cyberspace Domains." *The United States Naval War College—Joint Military Operations Department*. 5th Edition, January 2019.

Ducheine, Paul and van Haaster, Jelle. "Fighting Power, Targeting and Cyber Operations." *NATO Cooperative Cyber Defence Centre of Excellence.* 2014. https://ccdcoe.org/uploads/2018/10/d2r1s9_ducheinehaaster.pdf.

Fahrenkrug, David. "Countering the Offensive Advantage in Cyberspace: an Integrated Defensive Strategy." *The United States Naval War College—Joint Military Operations Department*. 4th International Conference on Cyber Conflict. 2012.

Grzegorzewski, Mark. "Why U.S. Officials are revealing more about Cyber Ops." *Defense One.* January 10, 2020. https://cdn.defenseone.com/a/defenseone/interstitial.html?v=9.15.0&rf=https%3A%2F%2Fwww.defenseone.com%2Fideas%2F2020%2F01%2Fwhy-us-officials-are-revealing-more-about-cyber-ops%2F162341%2F.

Herr, Trey. "Cyber Operations in Context: A Look at Joint Task Force ARES." *Atlantic Council.* September 16, 2019. https://www.atlanticcouncil.org/event/cyber-operations-in-context-a-look-at-joint-task-force-ares/.

Healey, Jason and Grindal, Karl. “Lessons from the First Cyber Commanders.” *Atlantic Council.* March 14, 2012. https://www.atlanticcouncil.org/blogs/new-atlanticist/lessons-from-the-first-cyber-commanders/.

Hofer, Mark G. “The C2 of Cyberspace is a Mess!” *U.S. Naval Institute Proceedings* 145, no. 8. *(*August 2019). https://www.usni.org/magazines/proceedings/2019/august/c2-cyberspace-mess.

Hone, Thomas. “Replacing Battleships with Aircraft Carriers in the Pacific in World War II.” *Naval War College Review.* Volume 66: no. 6 (Winter 2016). https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1318&context=nwc-review.

Huening, Tim. “The Importance of Human Factors for Joint Cyber Planning.” *Small Wars Journal.* Accessed March 21, 2020. https://smallwarsjournal.com/jrnl/art/the-importance-of-human-factors-for-joint-cyber-planning.

House Committee on Armed Services, *Subcommittee on Intelligence, Emerging Threats and Capabilities: Statement of General Paul M. Nakasone, Commander, U.S. Cyber Command,* 116th Congress, March 13, 2019. https://armedservices.house.gov/_cache/files/e/d/ed0549b9-c479-4ae0-943d-66cf8fd933c1/AEDF855100875FF9DBB6F5E7472F6E36.nakasone-cybercom-hasc-posture-statement-final-3-13-19.pdf (accessed March 21, 2020).

Joint Publication 3-12. “Cyberspace Operations.” *Joint Chiefs of Staff.* June 8, 2018. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf.

Joint Publication 3-09. “Joint Fire Support.” *Joint Chiefs of Staff.* April 10, 2019. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_09.pdf.

Kallberg, Jan & Cook, Thomas. “Unfitness of Traditional Military Thinking in Cyber.” *IEEEAccess*, Volume 5 (2017). 8126-8130. https://cyberdefense.com/wp-content/uploads/2018/09/Unfitnesstraditionalthinking.pdf

Kern, Sean C.G. “Expanding Combat Power Through Military Cyber Power Theory.” *Joint Forces Quarterly* 79, 4th Quarter (2015). https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-79/jfq-79_88-95_Kern.pdf.

Klimburg, Alexander. *The Darkening Web: The War for Cyberspace*. (New York: Penguin Books, 2018).

Kramer, Franklin, Starr, Stuart H, and Wentz, Larry, Eds., *Cyberpower & National Security* (Washington: Potomac Books, 2009).

Martelle, Michael. “Joint Task Force ARES and Operation GLOWING SYMPHONY: Cyber Command’s Internet War Against ISIL.” *National Security Archive*. August 13, 2018. https://nsarchive.gwu.edu/briefing-book/cyber-vault/2018-08-13/joint-task-force-ares-operation-glowing-symphony-cyber-commands-internet-war-against-isil.

"Cyber-Attacks and Fire Support: Documents Illustrate Historic Trend in Integration of Military Technology." *Unredacted.* February 28, 2019. https://unredacted.com/2019/02/28/cyber-attacks-and-fire-support-documents-illustrate-historic-trend-in-integration-of-military-technology/.

Morgan, Adam and Stone, Steve. "Command and Control for Cyberspace Operations—A Call for Research." *Military Cyber Affairs.* Volume 4: no. 4. 2019. https://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1051&context=mca.

Parker, Thomas and Parker, Warren. "Cyber Warfare Doctrine Already Exists." *U.S. Naval Institute.* Volume 145, no. 2. February 2019. https://www.usni.org/magazines/proceedings/2019/february/cyber-warfare-doctrine-already-exists

Pomerleau, Mark. "Here's what Combatant Commanders Want From Cyber Teams." *Fifth Domain.* November 19, 2018. https://www.fifthdomain.com/dod/cybercom/2018/11/19/heres-what-combatant-commanders-want-from-cyber-teams/.

"New authorities mean lots of new missions at Cyber Command. " *Fifth Domain.* May 8, 2019. https://www.fifthdomain.com/dod/cybercom/2019/05/08/new-authorities-mean-lots-of-new-missions-at-cyber-command/

Nakasone, Paul. "Gen. Nakasone Lays Out Vision for '5th Chapter' of US Cyber Command." *Meritalk*. September 7, 2018. https://www.meritalk.com/articles/nakasone-cyber-command-vision/.

Noah, Timothy. "Birth of a Washington Word—When Warfare gets 'Kinetic.'" *Slate*. November 20, 2002. https://slate.com/news-and-politics/2002/11/kinetic-warfare.html

Spoehr, Thomas and Di Pane, James. "Elevating Cyber Command: An Overdue Step Towards Enhancing Military Cyber Operations." *The Heritage Foundation.* October 1, 2018. https://www.heritage.org/cybersecurity/commentary/elevating-cyber-command-overdue-step-towards-enhancing-military-cyber.

Temple-Raston, Dina. "How the U.S. Hacked ISIS." *National Public Radio.* September 26, 2019. https://www.npr.org/2019/09/26/763545811/how-the-u-s-hacked-isis.

Valeriano, Brandon and Jensen, Benjamin. "The Myth of Cyber Offense: The Case for Restraint." *CATO Institute.* January 15, 2019. https://www.cato.org/publications/policy-analysis/myth-cyber-offense-case-restraint

Vavra, Shannon. "U.S. cyber-offensive against ISIS continues, and eyes are now on Afghanistan, general says." *CyberScoop*. September 17, 2019. https://www.cyberscoop.com/isis-jtf-ares-cyber-offensive-afghanistan/.

Williams, Brett. “The Joint Force Commander’s Guide to Cyberspace Operations.” *Joint Force Quarterly*, 73. April 1, 2014. https://ndupress.ndu.edu/Media/News/Article/577499/the-joint-force-commanders-guide-to-cyberspace-operations/