**NAVAL WAR COLLEGE**
**Newport, R.I.**

# Integrated Offensive Cyber Operations to the Operational Commander for Efficacy and Deterrence

**A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Maritime Advanced Warfighting School.**

**The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.**

**15 MAY 2020**

# REPORT DOCUMENTATION PAGE

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



| 1. REPORT DATE *(DD-MM-YYYY)* | 2. REPORT TYPE | 3. DATES COVERED *(From - To)* |
|---|---|---|
| 27-04-2020 | FINAL | |

**4. TITLE AND SUBTITLE**

Integrated Offensive Cyber Operations to the Operational Commander for Efficacy and Deterrence

**5a. CONTRACT NUMBER**

**5b. GRANT NUMBER**

**5c. PROGRAM ELEMENT NUMBER**

**6. AUTHOR(S)**

LCDR Rachel Katz Barnett

Paper Advisor (if Any): Robert Gardner

**5d. PROJECT NUMBER**

**5e. TASK NUMBER**

**5f. WORK UNIT NUMBER**

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

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

**8. PERFORMING ORGANIZATION REPORT**

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

**10. SPONSOR/MONITOR'S ACRONYM(S)**

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

**12. DISTRIBUTION / AVAILABILITY STATEMENT**

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. 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**

Integrated Offensive Cyber Operations to the Operational Commander for Efficacy and Deterrence

Delegating the authority for offensive cyber operation (OCO) to the operational commander will increase cyber fires efficacy. OCO as cyber fires can be executed at all levels of war but are particularly effective at the operational level. Like other type of fires, OCO are more effective when they are integrated into other military operations at the operational level of war. Finally, operational OCO would contribute to conventional deterrence by demonstrating US capabilities and resolve. While there are risks associated with the increased public knowledge of US operational OCO abilities, the delegation of appropriate authorities will strengthen US the operational posture.

**15. SUBJECT TERMS**

OCO, Offensive Cyber, Operational Level of War

| 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 | | | 19b. TELEPHONE NUMBER *(include area code)* |
| UNCLASSIFIED | UNCLASSIFIED | UNCLASSIFIED | | 17 | 401-841-3556 |

**Contents**

**Abstract**

*Integrated Offensive Cyber Operations to the Operational Commander for Efficacy and Deterrence*

Delegating the authority for cyber fires to the operational commander will increase offensive cyber operation (OCO) efficacy. Similar to the advances in aviation that led to the modern use of airstrikes, the evolution of cyber capabilities has given commanders additional options to use against their enemies. First, OCO as cyber fires can be executed at all levels of war but are particularly effective at the operational level. In addition, like other types of fires, OCO are more effective when they are integrated into other military operations at the operational level of war. Finally, operational-level OCO would contribute to conventional deterrence by demonstrating US capabilities and resolve. While there are risks associated with the increased public knowledge of US operational OCO abilities, the delegation of appropriate authorities will strengthen US the operational posture.

## INTRODUCTION

To specify the terms associated with cyberspace, *JP 3-12 Cyberspace Operations* outlines three categories for military cyber operations: offensive cyber operations (OCO), defensive cyber operations (DCO), and Department of Defense information network (DODIN).[1] The objective or desired outcome determines the category for the operation.[2] The US military has chosen to treat OCO as another type of fires, despite objections that cyber operations are not sufficiently violent to qualify as an act of force and that the cyber domain is an artificial construct.[1] Indeed, 2018 saw a shift in the US Cyber Command (CYBERCOM) approach to the problem of cyberspace dominance.[3] Rather than taking a solely defensive role, CYBERCOM announced as a persistence force it would go on the offensive, "continuously engaging our adversaries."[4] The US tacitly announced that it would engage in OCO.

*JP 3-12* defines these OCO as "cyber operation missions intended to project power in and through foreign cyberspace through actions taken in support of CCDR or national objectives."[5] A more useful definition comes from the description of cyberspace attack, which can be OCO or some types of DCO: "actions taken in cyberspace that create noticeable denial effects (i.e., degradation, disruption, or destruction) in cyberspace or manipulation that leads to denial that appears in a physical domain, and is considered a form of fires."[6] Simply put, OCO damage information and equipment. This damage breaks down further: cyber operators can deny (degrade, disrupt, and destroy targets) or manipulate systems and objects connected to information them.[7] Just as conventional weapons vary in their degrees of damage by explosive

[1] See Thomas Rid, "Cyber War Will Not Take Place," *Journal of Strategic Studies* 35, no. 1 (2012): 5-32 and McGuffin, Chris and Paul Mitchell, "On Domains: Cyber and the Practice of Warfare," *International Journal* 69, no. 3 (09, 2014): 394-412. This was reaction to the "Cyber Pearl Harbor" that Gen Alexander foretold in Alexander, Keith, Memorandum for Record, Subject: United States Cyber Command (USCYBERCOM) Commander's Strategic Assessment for Operating in Cyberspace – Preventing a Pearl Harbor Environment.

power, caliber, or warhead size, cyber effects offer the military commander a wide range of fires to further US interests.

Delegating the authority for these cyber fires to the operational commander will increase OCO efficacy. Similar to the advances in aviation that led to the modern use of airstrikes, the evolution of cyber capabilities has given commanders additional options to use against their enemies. First, OCO as cyber fires can be executed at all levels of war but are particularly effective at the operational level. In addition, like other types of fires, OCO are more effective when they are integrated into other military operations at the operational level of war.[2] Finally, operational-level OCO would contribute to conventional deterrence by demonstrating US capabilities and resolve. While there are risks associated with the increased public knowledge of US operational OCO abilities, the delegation of appropriate authorities will strengthen US the operational posture.

## EVOLUTION OF CYBERSPACE

The US approach to the cyber domain is evolving from serving only an intelligence function to including operational fires and protection. The evolution of aviation serves as an example. The French military used the precursors to aircraft, the first balloons, in combat to collect intelligence on the opposing Austrian positions in 1794.[8] As technology and innovation advanced, aviation assets became another method of applying fires to the enemy. In WWI, there were advances in the planes themselves (range, altitude, enemy planes that presented themselves as targets) and in the weapons that gave them more firepower. These advances precipitated

[2] DOD defines cyberspace as "a global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers." U. S. Office of the Chairman of the Joint Chiefs of Staff. *Cyberspace Operations*, *Joint Publication (JP) 3-12*, GL-4.

changes in how leaders viewed the new technology. Once airborne machine guns successfully brought down other aircraft, aviation served a protection function (fighters accompanying bombers).[9]

Similarly, cyber operations have evolved from their meager beginnings. Just as aviation's civilian origins involved transporting human beings from one place to another, cyber operations trace their lineage back to the movement of information. This movement of information facilitated the command and control (C2) function of military operations and thus presented an opportunity for intelligence collection. Creative cyber operators (both inside and outside the military) have advanced the state of the art to include weapons in the form of bits of code. Those bits cause harm not just to the computers themselves and the data they house, but also the physical objects that those computer systems direct. Just as aerial guns and bombs expanded the 20th century battlefield, so cyber operators are expanding that of the 21st century. The US has taken far-reaching measures to address the protection operational function in cyberspace but needs to approach OCO the same way it would other types of fires. As each evolution of military thought has shown, no technology yet has negated the need for all military services to cooperate on the battlefield.[10] The US approach needs to evolve further to incorporate OCO with air, sea, and land power at the operational level of warfare.

## ANOTHER TYPE OF FIRES

OCO resembles other types of fires in its ability to target at multiple levels of war. The Department of Defense Cyber Strategy highlights the need for scalable cyber capabilities.[11] Commanders thus can aim OCO at operational, tactical, and strategic targets. OCO use as operational fires would have "a decisive impact of the course and outcome of a campaign or

major operation."[12] However, most known US OCO has been at the strategic level due to the sensitivity with which the US has treated the developing domain.

The Soviet oil pipeline explosion in 1981 was the first significant demonstration of how destructive OCO can be when they control systems in the physical world. According to Thomas C. Reed, who served as Secretary of the United States Air Force and Director of the National Reconnaissance Office, the US inserted malicious code into the operating system, or supervisory control and data acquisition (SCADA) system, for the trans-Siberian pipeline. This eventually resulted in an explosion equivalent to a three-kiloton device, causing intelligence officials to look for indications of a Soviet nuclear bomb. [13] The oil infrastructure was an attractive strategic target from the US perspective: energy revenue was a large portion of the Soviet economy.[14]

The incident that dramatically drew public attention to the cyber domain in the twenty-first century, the Stuxnet attack on centrifuges in Natanz set back Iranian plans for a nuclear bomb.[15] The attack aimed at a political objective, though the target was inside a research and development facility with applications for military technology. Because the damage of the attack took years to occur, the Iranians wasted time and resources trying to figure out why the equipment was failing.[16] The delay in Iran's obtaining a nuclear bomb that resulted had strategic implications for the region, especially for nearby US allies. Using OCO to slow Iran's nuclear program, similar to Israel's air strikes on nuclear sites in Syria or Iraq, is an example of using cyber to achieve a political and military strategic objective.[17]

US Joint Task Force Ares executed another strategic OCO against Islamic State in Iraq, Syria, and the Levant (ISIL) in 2016. Declassified documents obtained in 2020 by a George Washington University Freedom of Information Act request reveal that two of Operation Glowing Symphony's (OGS) objectives were "disrupt and counter ISIL's use of social media"

and "disrupt ISIL's sponsored media."[18] Similar to surgical strikes, OGS destroyed ISIL databases and disrupted accounts of terrorists who led the ISIL "public relations" and recruiting.[19] Rather than focusing on the tactical cells or intelligence collection that defined early cyber operations against terrorist in Iraq, this operation executed non-lethal fires to disrupt ISIL communications at the strategic level.[20] ISIL's ability to spread their message has been one of their strengths throughout their existence. Cutting off all ISIL social media until terrorist operatives were able to reset their accounts and access back-up data achieved a strategic objective against a US enemy.

In addition to these strategic examples of OCO, examples of tactical OCO abound. On the ground, OCO could hypothetically target enemy digital communication networks to prevent coordinated attacks on friendly forces conducting a noncombatant evacuation.[21] Air warriors dream of "neutralizing the enemy's integrated air defense systems" with "a few key strokes" rather than bombs to allow for US aircraft to pass into enemy airspace.[22] In the maritime domain, Norwegian cyber experts suggest that hacking an individual ship's autopilot via Automatic Identification System (a tracking and identification system ships use to prevent collisions at sea) could even lead to its veering off course and grounding.[23]

Though each of these effects could lead to tactical success, using OCO at the operational level of war could shape the environment for US operations. For example, the fantastic explosion triggered by the US tampering with the Soviet pipeline attack could have, instead, damaged a local fuel facility for a Soviet fleet concentration area. Such a target would have had operational implications for the ships that depended on the facility. Targeting such a facility would have required detailed intelligence on the network of pipelines and SCADA systems controls; collection to this degree of refinement was likely impossible at the time. As another example,

just as the US used air power to destroy the Iraqi critical infrastructure in the Gulf War, operational OCO could shut oil and power facilities down in preparation for a US invasion in a future conflict.[24] Some other suggestions follow below:

- divert enemy logistic support away from the current theater
- exploit a software vulnerability in enemy aircraft to facilitate a force-wide grounding of enemy platform
- target enemy C2 nodes at the operational level to prevent the enemy leadership from making timely decisions
- inject false information to contribute to an operational deception
- corrupt enemy payroll functions to sow discord among troops

Each of these OCO would "enhance the chances for a successful outcome of a campaign of major operation."[25] Operational commanders can affect the battlespace through OCO and further friendly operational objectives.

## CYBER AS ANOTHER AVENUE OF APPROACH AT THE OPERATIONAL LEVEL

Just as the shift from attrition to maneuver increased the importance of the operational level of war, shifting from an attrition mentality to a maneuver mentality in cyber will result in a more creative use of OCO to reach an operational desired end state.[26] OCO offer many advantages for fires at the operational level if commanders think of OCO as creating another avenue of approach to reach military objectives.[27] Similar to the opportunity for aviation to bomb some targets during WWII, the cyber domain has opened an opportunity to deal the enemy damage (though some targets are more vulnerable than others to such an assault). OCO elements offer a flexible, scalable tool for operational commanders to resolve low-level conflicts. OCO can also help shape a larger-scale conflict with operational fires. Finally, operational

commanders are better positioned than strategic commanders to most efficiently employ limited cyber assets for operational objectives.

Offensive cyber operations give the military commander additional options below the level of conventional armed attack, especially if organized into a cyber campaign.[28] Such an option is especially useful as grey zone conflict increases. Chinese military actions hover at the edges of armed conflict, and information drives everything the Chinese military does.[29] While this paper does not thoroughly describe the threat to US interests in the cyber domain, China is already using cyber to shape the battlespace of future conflicts.[30] By not acting offensively, the US is ceding ground. Creating operations on the low level of cyber "force" can enable operational commanders to increase the cost and confusion for the US's adversaries beyond unconnected tactical pinpricks. An OCO that dimmed the lights for a People's Liberation Army (PLA) cyber unit that is stealing US industrial secrets would be tactical.[3] A more operational effort would be to "allow" the PLA unit to steal a file that corrupted their whole network and disrupted the unit's industrial espionage efforts for weeks.

OCO efforts need to contribute to the operational goal rather than just chipping away at isolated tactical gains. In the US Army's *Cyber Defense Review,* Dr. David Goie gives the following example of OCO elements tailored to operational objectives: "a cyber maneuver may involve degrading enemy network operations, plans, C2, (lines of communication, or similar) which would retard the enemy's operational tempo, which, in turn, retards initiative."[31] If the strategy is sound, wars are won at the operational level.[32] Especially in the opening moves of a conflict, OCO can shape the environment, looking to the next phase of the operations rather than reacting to the current situation. Reminiscent of US submarine attacks on Japanese shipping that

[3] As satisfying as this might sound, it could also tip the unit off to US knowledge of its activities and location and the fact that US OCO actors had access to the local power grid.

decimated Japan's logistical capacity during WW2, the US could, for instance, utilize OCO in a cumulative way to whittle down an adversary's communications connections to the global commons.[33] Individual cyber effects often are overlooked because they appear to be small upon discovery.[34] Either way, the efforts must stem from the operational level of war rather than being thrown in as an afterthought.[35]

Because operational commanders work at the operational level of war, they are best able to integrate OCO into that level of operations. The timing for OCO, just one element of its integration with conventional efforts, is crucial to maximize its effect when other domains are in play; in addition to the benefit of surprise, an OCO must follow the creation of a vulnerability or risk losing access.[36] Dr. Goie argues that cyber "is an iterative effort and must be continually synchronized with the joint force and other related elements both during the planning process and execution phase."[37] Operational commanders are also best able to allocate limited cyber resources (intelligence gathering, skilled cyber operators) to meet their operational objectives since they are constructing the operational design. If such a design requires OCO but authorities for OCO reside only at the strategic level, that commander will have to put forth extra effort to integrate OCO since the request must go to the strategic commanders for approval. OCO will be less integrated at the operational level of war than it would be if authority resides with operational commanders.

## OCO ENHANCES CONVENTIONAL DETERRENCE

Increased operational OCO can enhance conventional deterrence because it displays a US integrated cyber fires capability at the operational level and signals US willingness to use that cyber capability. Such deterrence differs from deterring enemy cyberattacks on US interests. A state-of-the-art DCO stance (including some efforts that resemble OCO in DCO Response

Actions[4]) attempts to make US networks difficult for enemies to breach and falls in the "denial" method of deterrence. Capable displays of OCO, however, project a US ability and willingness to inflict "punishment" on adversaries that incur its ire from hostile actions, cyber or otherwise.[38]

Since modern deterrence theory originated during the Cold War, US policy officials initially applied rationales to cyber deterrence that were similar to those used for nuclear attacks. Indeed, since cyberattacks could threaten a state's ability to launch nuclear weapons by targeting command and control nodes similarities exist.[5] Such an OCO target could lead to an extreme escalation of a conflict.[39]A separate concern has been that a hostile state actor would launch a cyberattack against the US homeland (including civilian critical infrastructure) if the US choses to take offensive actions in cyberspace. The opposite then also became the standard thinking: if the US refrained from OCO, its adversaries would do the same. However, to assume that if the US refrains from OCO its enemies will do the same is to commit the cognitive error of mirror imaging (or worse, wishful thinking) and to ignore an important military tool.[6]

Public displays of OCO would build the perception of US military as a strong offensive cyber player. Continued activities of Chinese and Russian hackers give the impression that the US is losing the cyber arms race.[40] In 2012, CYBERCOM commander General Keith Alexander warned that the US was headed for a Cyber Pearl Harbor if it failed to act to improve its cyber capabilities.[41] The US cyber posture has dramatically improved since then, and the increased OCO that delegating authority to the operational commander would achieve will send a clear

---

[4] DCO operations are made up of Internal Defensive Measures and Response Actions. See *JP 3-12*, II-4.

[5] David C. Gompert & Martin Libicki (2019) "Cyber War and Nuclear Peace," *Survival*, 61:4, 45-62, DOI: 10.1080/00396338.2019.1637122. The US recognizes cyber threats to its own nuclear command and control systems. See Office of the Secretary of Defense, *Nuclear Posture Review* February 2018, 57. https://media.defense.gov/2018/Feb/02/2001872886/-1/-1/1/2018-NUCLEAR-POSTURE-REVIEWFINAL-REPORT.PDF

[6] That is not how US commanders look at torpedoes or anti-ship cruise missiles. For more on cognitive errors, see Dr. Charles King, *How to Think*. Accessed from faculty.georgetown.edu/kingch/ HowtoThink.htm. Georgetown University, School of Foreign Service and Department of Government, 1999.

message that the US has a robust offensive cyber capability. This would require a shift in the US's approach to publicizing its successes since OCO "are often hidden due to the highly classified nature before and after they have occurred."[42] A robust cyber capability is increasingly becoming part of a modern military force and must be visible to have deterrent value.[43]

Another contrast to nuclear deterrence is that using OCO increases its importance as a deterrent. The deterrence value of nuclear weapons relies on the threat of their use.[7] Commander of CYBERCOM General Paul Nakasone contrasts the two: "Unlike the nuclear realm, where our strategic advantage or power comes from possessing a capability or weapons system, in cyberspace it's the use of cyber capabilities that is strategically consequential."[44] OCO is more versatile and often reversible.[45] If the US is willing to deploy a small-scale cyberattack in response to a small action by an enemy, it implies that a larger offense could lead to a larger cyber response. OCO can even fall below the threshold of armed conflict, making them a potentially subtle tool to respond to adversary grey zone conflicts.

If US cyber forces do not act when they find a vulnerability in an adversary, they may lose the opportunity. The late US Navy Captain Wayne P. Hughes exhorts war fighters to "attack effectively first."[46] For cyber targets, since OCO weapons require tailoring and access may be fleeting, the maxim should be to attack when possible.[8] Cyber vulnerabilities are often bounded in time since once they are discovered by an adversary, they are no longer exploitable.[47] General Nakasone estimates that US cyber tools have a shelf life of less than six months.[48] OCO opportunities are often fleeting and can be lost when enemy actions to secure their networks deny US cyber actors the access they previously enjoyed. Thus, enemy system maintenance

[7] Schelling, Thomas C., 1921-2016 and Harvard University. Center for International Affairs. *Arms and Influence*. New Haven: Yale University Press, 1966;1967; 24. Civilians can easily be the targets of either type of attack.

[8] Assuming, of course, that rules of engagement and other principles of the Law of Armed Conflict are amenable.

constantly depletes the US OCO arsenal regardless of whether commanders choose to utilize these weapons. A silo full of expired cyber weapons does not make a credible deterrent.

## ALTERNATIVE VIEWS

Some would say that delegating cyber fire authority to the operational commanders will lead to excess use, revealing US cyber capabilities and decreasing their impact when needed for combat against peer or near-peer powers. Many worry that operational commanders will not adequately protect US OCO capabilities' secrets. Additional use of OCO could reveal US tools and then lead to adversaries or even criminal elements obtaining the US tools. OCO could even lead to an unintended escalation of hostilities and destroy critical intelligence tools.

Operational commanders' employing OCO could compromise cyber advantages the US holds. Once a specific cyberattack has launched, it is almost impossible to use it again the exact same way. The targeted network operators will become aware of the vulnerability that the attack exploited and will address the vulnerability. If US OCOs bring adversary attention to their own vulnerabilities, US cyber operators will lose opportunities, and enemy network operators will improve their proficiency in securing their networks.[49] US senior leaders have been reticent to employ OCO use cyber for fear that using it in low-level conflict or peacetime means that the specific tool will not be available for a larger-scale conflict.

An even worse consequence to US OCO actions becoming known is that their revelation could lead to adversaries or even criminal elements obtaining US cyber tools. Malicious code is easy to copy, proliferating and mutating from hacker to hacker.[50] Specialized tools cost US cyber organizations time and money to build. Injudicious use could compromise US tools and result in enemies of the US turning such tools on the very country that US cyber experts designed them to protect. Alternatively, malicious actors could use tools that resemble those that US cyber actors

use in an attempt to portray their own malicious actions as coming from the US, which could further damage US interests by discrediting US cyber organizations.

Because OCO technology continues to evolve and may have unintended consequences, the danger of unintended escalation looms. Also, ambiguity exists in the cyber domain since intentions of US cyber activities may not be clear to its adversaries.[51] While an enemy may respond to US OCO (or even cyber espionage) with a cyber action of its own, the severity of the enemy attack may be based on their perceived severity of the US OCO rather than the actual (or intended) severity.[52] If an adversary misjudges the severity or intent of a US attack, or if US cyber actors err in calibrating their attack to achieve the intended damage, the chance of a drastic but unintended escalation increases.

Intelligence gathered from cyber vulnerability may be more beneficial than the cyber fire effect exploiting that same vulnerability. Stemming from OCO's origin within the US intelligence community, intelligence officials have been reticent to condone increased OCO.[53] For instance, OCO against enemy communications networks can destroy or compromise intelligence tools that provide valuable intelligence from US adversaries.[54] Additionally, multiple OCOs from different organizations could target the same network for different operations. Cyberspace is more complicated than other "spaces" since cyber networks have a logical geography as well and a physical one.[55] Even if intelligence gathering tools are not disrupted by a conflicting OCO, an OCO may tip off an adversary to a vulnerability that intelligence tools or other friendly OCO actors were leveraging. Once the adversary addresses the vulnerability, intelligence collectors will have to find another vulnerability to exploit, requiring additional time and resources.[56] The additional cost in time and resources may not be worth the gain the OCO achieved.

## CONCLUSION AND RECOMMENDATIONS

Specific delegation of appropriate authority along with coordination and deconfliction will protect the US competitive OCO advantage while still projecting power in the cyber domain. CYBERCOM can give specific guidance on what the operational cyber forces can and cannot do, basing these decisions on rules of engagement (ROE), collateral damage assessments, the type of OCO "weapon" employed, and consultations to evaluate the intelligence gain/loss potential of each target. Joint Targeting Coordination Boards should vet potential OCO targets, similar to other targets for kinetic strikes.

Because some OCO are destructive enough to equal the "use of force," ROE play a role in determining what an operational commander can attack.[57] Indeed, General Alexander as CYBERCOM commander lamented the lack of cyber ROE.[58] Clear ROE guidance in advance, including preplanned responses where appropriate, will give operational commanders flexibility to meet their missions and avoid "creating unintended consequences outside of the immediate cyber domain."[59]

Collateral damage assessments provide another tool for determining what OCO operational commanders can execute. As OCO tools reach completion, cyber operators must also provide commanders with an honest assessment on how much damage they could cause. This should include a "confidence level" in that assessment: for example, a high confidence assessment would mean that the developers judge that the tool will almost certainly perform as intended without unintended effects. Release authority for OCO tools that lack such confidence should be held at a higher level.

The sophistication of an OCP tool should also determine whom holds release authority. CYBERCOM spends time and resources on exquisite OCO weapons, which should be reserved

for "cyber hardened" or other sensitive targets.[9] However, not all OCO tools are this advanced. Simpler tools can achieve objectives, especially if "the target of the attack is not the system itself but confidence in that system and any other system the adversary depends on."[60] Even adding decoys of information adds to the complexity and cost for an enemy.[61] Delegation of selected OCO tools to the operational level will increase the US's operational reach for OCO while still protecting its investments in cyber research and development.

Finally, deconfliction must occur across multiple OCO actors and with intelligence collectors. Just as US submarines and aircraft manage their water and airspace, cyberspace management can prevent interference. Thus operational commanders must ensure their OCO actors coordinate across the US cyber community and that their actions will not prevent other OCO or intelligence gathering. Also, intelligence collections in cyberspace should maintain a restricted target list to prevent friendly OCO from destroying assets. The OSG After Action Report revealed that "CYBERCOM established a standard operating procedure for operational deconfliction," with inputs from both multiagency and multinational partners.[62] When needed, JP 3-12 provides for an Intelligence Gains/Loss assessment "to weigh the risks of conducting the CO versus achieving the desired objective via other methods."[63]

In summary, OCO present a complex tool for the operational commander, but one that bestows a wide range of options with many benefits. The DOD *Cyber Strategy* pledges to "accept and manage operational and programmatic risk in a deliberate manner that moves from a

[9] As commander of US Strategic Command in 2007, General James Cartwright, USMC, expressed concern regarding the balance between expensive, "exquisite" tools and more economic, less advanced technology. (See "REP. ELLEN O. TAUSCHER HOLDS A HEARING ON THE U.S. STRATEGIC COMMAND." *Political Transcript Wire,* Mar 12, 2007.) He reiterated this concern as vice chairman of the Joint Chiefs in 2008; See Philpott, Tom. "Military must Choose Better, Smarter Weapons." *Montgomery Advertiser,* Nov 23, 2008. https://login.usnwc.idm.oclc.org/login?qurl=https%3A%2F%2Fsearch.proquest.com%2Fdocview%2F412926378%3Faccoun

'zero defect' culture to one that fosters agility and innovation because success in this domain requires the Department to innovate faster than the US's strategic competitors."[64] To fulfill this pledge, educating and empowering operational commanders to take those risks in authorizing OCO will make the best use of US cyber abilities. Comprehending the risks of OCO will allow senior leaders to make better risk decisions for OCO.[65] While the US may accept risk in delegating OCO authority to operational commanders, the rewards in increased effectiveness and deterrence are worth potential losses.

Notes:

[1] U. S. Office of the Chairman of the Joint Chiefs of Staff. *Cyberspace Operations*, *Joint Publication (JP) 3-12*, II-2.
[2] Ibid, II-2.
[3] Nakasone, Paul M. "A Cyber Force for Persistent Operations." *Joint Force Quarterly* no. 92 (2019): 10.
[4] *Achieve and Maintain Cyberspace Superiority: Command Vision for U.S. Cyber Command* (Washington, DC: U.S. Cyber Command, March 2018). 5. https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010.
[5] *JP 3-12*, xi.
[6] Ibid, GL-4.
[7] Ibid, II-7.
[8] David Brown, 1938, Kenneth Macksey, and Christopher F. Shores. *The Guinness History of Air Warfare*. Enfield [England]: Guinness Superlatives Ltd, 1976, 2.
[9] Ibid, 12.
[10] Vego, Milan. *Joint Operational Warfare: Theory and Practice.* Newport, RI: Naval War College, reprint 2009, XI-56.
[11] U.S. Department of Defense, *2018 Department of Defense Cyber Strategy* (Washington, DC: Department of Defense, 2018), 4.
[12] Vego, *Joint Operational Warfare*, VIII-59-60.
[13] Thomas C. Reed. *At the Abyss, an Insider's History of the Cold War.* New York, NY. Ballantine Books. 2004, 268, quoted in Richard M. Crowell, "War in the Information Age: A Primer for Information Operations and Cyberspace Operations in 21st Century Warfare," Newport, RI: U.S. Naval War College, January 2016. (NWC 2021D), 1-2.
[14] Ibid.
[15] Sanger, David E. *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age*. First ed. New York: Crown Publishers, an imprint of the Crown Publishing Group, 2018, 21.
[16] Ibid, 21, 24.
[17] Ibid, 28.
[18] USCYBERCOM, Operation Glowing Symphony Assessment Framework Briefing Version 1.1, November 14 2016, slide 3, obtained by Freedom of Information Act request by National Security Archive, George Washington University. January 21 2020. https://nsarchive.gwu.edu/briefing-book/cyber-vault/2020-01-21/uscybercom-after-action-assessments-operation-glowing-symphony.
[19] *How the U.S. Cracked into One of the most Secretive Terrorist Organizations*. Washington, D.C.: NPR, 2019. https://login.usnwc.idm.oclc.org/login?qurl=https%3A%2F%2Fsearch.proquest.com%2Fdocview%2F2297846253%3Faccou.
[20] Harris, Shane, *@WAR: The Rise of the Military-Internet Complex,* Boston: Houghton Mifflin Harcourt, 2014, 8.
[21] Brewster, William M. and Gerald W. Jr Kearney. "Integrating Cyber Fires into MAGTF Operations." *Marine Corps Gazette* 99, no. 7 (2015): 16.
[22] Jason M. Gargan, "The Joint Force Air Component Commander and the Integration of Offensive Cyberspace Effects." *Air & Space Power Journal* 30, no. 1 (2016). 86.

[23] Odd Sveinung Hareide, Øyvind Jøsok, Mass Soldal Lund, Runar Ostnes, and Kirsi Helkala. "Enhancing Navigator Competence by Demonstrating Maritime Cyber Security." *Journal of Navigation* 71, no. 5 (2018): 1034-1035.
[24] Vego, *Joint Operational Warfare*, VIII-66.
[25] Ibid, VIII-68.
[26] David Gioe. "Can the Warfare Concept of Maneuver be Usefully Applied in Cyber Operations?" *Cyber Defense Review*, January 14, 2016, https://cyberdefensereview.army.mil/CDR-Content/Articles/Article-View/Article/1136059/can-the-warfare-concept-of-maneuver-be-usefully-applied-in-cyber-operations/
[27] Kenton G. Fasana (2018) Another Manifestation of Cyber Conflict: Attaining Military Objectives through Cyber Avenues of Approach, *Defence Studies*, 18:2, 167. DOI: 10.1080/14702436.2018.1462661.
[28] Richard J. Harknett & Max Smeets (2020): Cyber campaigns and strategic outcomes, *Journal of Strategic Studies*, 7, DOI: 10.1080/01402390.2020.1732354.
[29] Peng Guangqian and Yao Youzhi, ed. *The Science of Military Strategy* (Beijing: People's Republic of China: Military Science Publishing House, 2005), 475-476 quoted in Crowell, Richard M. "War in the Information Age: A Primer for Information Operations and Cyberspace Operations in 21st Century Warfare," Newport, RI: U.S. Naval War College, January 2016. (NWC 2021D), 27.
[30] General Keith B. Alexander, March 23, 2012, Memorandum for Record, United States Cyber Command, United States Cyber Command (USCYBERCOM) Commander's Strategic Assessment for Operating in Cyberspace – Preventing a Pearl Harbor Environment, 2. See also, Commander, U.S. Pacific Command, "U.S. Pacific Command Posture" 14 February 2018, House Armed Services Committee, 17.
[31] Gioe, "Can the Warfare Concept of Maneuver."
[32] Vego, *Joint Operational Warfare*, XIV-16.
[33] Harknett & Smeets, "Cyber campaigns and strategic outcomes," 8. See, J. C. Wylie, Jr., "Reflections On The War In The Pacific", U.S. Naval Institute *Proceedings*, vol. 78, no. 4 (April 1952), pp. 351-361 for a discussion on cumulative operations.
[34] Harknett & Smeets, "Cyber campaigns and strategic outcomes," 12.
[35] Gioe, "Can the Warfare Concept of Maneuver."
[36] *JP 3-12*, IV-20.
[37] Gioe, "Can the Warfare Concept of Maneuver."
[38] See Glenn H Snyder, *Deterrence by Denial and Punishment* (Center of international studies, Princeton University, 1959).
[39] Gompert & Libicki, "Cyber War and Nuclear Peace," 45-62.
[40] Sanger, *The Perfect Weapon*, xxii. (My own review of cyber literature shows the term "cyber arms race" increased circulation after Stuxnet in 2012.)
[41] Alexander, "Preventing a Pearl Harbor Environment," 1. Subsequent press reporting indicates Secretary of Defense Leon Panetta began using the term later that year.
[42] Reith, Mark. "Brandishing our Air, Space, and Cyber Swords: Recommendations for Deterrence and Beyond." *Air & Space Power Journal* 31, no. 4 (2017): 105.
[43] Sanger, *The Perfect Weapon*, xxi.
[44] "An Interview with Paul M. Nakasone." *Joint Force Quarterly: JFQ* no. 92 (First, 2019): 4. https://search-proquest-com.usnwc.idm.oclc.org/docview/2176619413?accountid=322.

[45] *JP 3-12*, IV-3.
[46] Wayne P. Hughes Jr. and Robert P. Girrier, *Fleet Tactics and Naval Operations.* 3rd. ed. Annapolis, MD., Naval Institute Press, 2018, 29-30.
[47] Max Smeets (2018) A Matter of Time: On the Transitory Nature of Cyberweapons, *Journal of Strategic Studies*, 41:1-2, 10-11, DOI: 10.1080/01402390.2017.1288107
[48] "An Interview with Paul M. Nakasone," 8.
[49] Burk, Rosemary A. and Jan Kallberg. "Bring on the Cyber Attacks – the Increased Predatory Power of the Restrained Red Queen in a Nation-State Cyber Conflict." *The Cyber Defense Review* 1, no. 2 (2016): 61.
[50] Whiting, Nicola. "Cyberspace Triggers a New Kind of Arms Race." *Signal* 72, no. 6 (02, 2018): 39.
[51] Brown, Gary. "Spying and Fighting in Cyberspace: What is which?" *Journal of National Security Law & Policy* 8, no. 3 (2016): 7.
**[52]** Brandon Valeriano, "Managing Escalation Under Layered Cyber Deterrence, " *Cyber Solarium Commission,* April 1, 2020, https://www.lawfareblog.com/managing-escalation-under-layered-cyber-deterrence
[53] Sanger, *The Perfect Weapon*, 248.
[54] *JP 3-12*, II-11
[55] Phillips, Jennifer Leigh. "Tactical Maneuver in the Cyber Domain: Dominating the Enemy." *JFQ: Joint Force Quarterly*, no. 93 (2019 2nd Quarter 2019): 17. http://search.ebscohost.com.usnwc.idm.oclc.org/login.aspx?direct=true&db=mth&AN=136571929&site=ehost-live.
[56] Reith, "Brandishing our Air, Space, and Cyber Swords," 107-108.
[57] DOD Law of War Manual, Chapter XVI – Cyber Operations in the DOD Law of War Manual, June 2015 (Updated December 2016), 16.3.1 https://dod.defense.gov/Portals/1/Documents/pubs/DoD%20Law%20of%20War%20Manual%20-%20June%202015%20Updated%20Dec%202016.pdf?ver=2016-12-13-172036-190
[58] Gen Keith B. Alexander, and Jamil N. Jaffer, "Ensuring US Dominance in Cyberspace in a World of Significant Peer and Near-Peer Competition," *Georgetown Journal of International Affairs* 19, no. 1 (2018): 54. Alexander cites himself: Alexander, Keith, "Cyber Warfare Today," 3 ; The White House, "Press Briefing on the Attribution of the WannaCry Malware Attack to North Korea," last modified December 17, 2017, https://docs.house.gov/meetings/AS/AS00/20180411/108077/HHRG-115-AS00-Wstate-AlexanderK-20180411.pdf.
[59] Phillips, "Tactical Maneuver in the Cyber Domain," 17.
[60] Libicki, Martin C. "The Broad Effects of Brandishing Cyberattack Capabilities." In *Brandishing Cyberattack Capabilities*, 9. RAND Corporation, 2013. Accessed April 24, 2020. www.jstor.org/stable/10.7249/j.ctt5hht3r.7.
[61] Reith, "Brandishing our Air, Space, and Cyber Swords," 108.
[62] USCYBERCOM, Operation Glowing Symphony J3 AAR Observations, November 22 2016, slides 2-3, obtained by Freedom of Information Act request by National Security Archive, George Washington University. January 21 2020. https://nsarchive.gwu.edu/briefing-book/cyber-vault/2020-01-21/uscybercom-after-action-assessments-operation-glowing-symphony.
[63] JP-3-12, IV-7.

[64] U.S. Department of Defense, *2018 Department of Defense Cyber Strategy* (Washington, DC: Department of Defense, 2018), 4.
[65] Phillips, "Tactical Maneuver in the Cyber Domain," 18.

## BIBLIOGRAPHY


Gen Alexander, Keith B. “Cyber Warfare Today,” 3; The White House, “Press Briefing on the Attribution of the WannaCry Malware Attack to North Korea,” last modified December 17, 2017, https://docs.house.gov/meetings/AS/AS00/20180411/108077/HHRG-115-AS00-Wstate-AlexanderK-20180411.pdf.

___, March 23, 2012. Memorandum for Record. United States Cyber Command. United States Cyber Command (USCYBERCOM) Commander’s Strategic Assessment for Operating in Cyberspace – Preventing a Pearl Harbor Environment.

Gen Alexander, Keith B. and Jaffer, Jamil N. "Ensuring US Dominance in Cyberspace in a World of Significant Peer and Near-Peer Competition," *Georgetown Journal of International Affairs* 19, no. 1 (2018): 51-66.

Burk, Rosemary A. and Jan Kallberg. "Bring on the Cyber Attacks – the Increased Predatory Power of the Restrained Red Queen in a Nation-State Cyber Conflict." *The Cyber Defense Review* 1, no. 2 (2016): 61-71.

Brewster, William M. and Gerald W. Jr Kearney. "Integrating Cyber Fires into MAGTF Operations." *Marine Corps Gazette* 99, no. 7 (2015): 16-18.

Brown, David, 1938, Kenneth Macksey, and Christopher F. Shores. *The Guinness History of Air Warfare*. Enfield [England]: Guinness Superlatives Ltd, 1976, 2.

Brown, Gary. "Spying and Fighting in Cyberspace: What is which?" *Journal of National Security Law & Policy* 8, no. 3 (2016): 1-22. https://search.proquest.com/docview/1831706360?accountid=322.

Commander, U.S. Pacific Command, “U.S. Pacific Command Posture” 14 February 2018, House Armed Services Committee

Clarke, Richard A. 1951 and Robert K. Knake. *Cyber War: The Next Threat to National Security and what to do about it*. First ed. New York: Ecco, 2010.

Crowell, Richard M. “War in the Information Age: A Primer for Information Operations and Cyberspace Operations in 21st Century Warfare.” Newport, RI: U.S. Naval War College, January 2016. (NWC 2021D)

Department of Defense *Law of War Manual*, Chapter XVI – Cyber Operations in the DOD Law of War Manual, June 2015 (Updated December 2016), 16.3.1 https://dod.defense.gov/Portals/1/Documents/pubs/DoD%20Law%20of%20War%20Manual%20-%20June%202015%20Updated%20Dec%202016.pdf?ver=2016-12-13-172036-190

Fasana, Kenton G. (2018) Another Manifestation of Cyber Conflict: Attaining Military Objectives through Cyber Avenues of Approach. *Defence Studies*, 18:2, 167-187. DOI: 10.1080/14702436.2018.1462661.

Gargan, Jason M. "The Joint Force Air Component Commander and the Integration of Offensive Cyberspace Effects." *Air & Space Power Journal* 30, no. 1 (2016). 86-93.

Gioe, David. "Can the Warfare Concept of Maneuver be Usefully Applied in Cyber Operations?" *Cyber Defense Review*, January 14, 2016. https://cyberdefensereview.army.mil/CDR-Content/Articles/Article-View/Article/1136059/can-the-warfare-concept-of-maneuver-be-usefully-applied-in-cyber-operations/

Gompert, David C. and Libicki, Martin (2019) "Cyber War and Nuclear Peace," *Survival*, 61:4, 45-62, DOI: 10.1080/00396338.2019.1637122.

Hareide, Odd Sveinung, Øyvind Jøsok, Mass Soldal Lund, Runar Ostnes, and Kirsi Helkala. "Enhancing Navigator Competence by Demonstrating Maritime Cyber Security." *Journal of Navigation* 71, no. 5 (2018): 1025-1039.

Harknett, Richard J. and Smeets, Max (2020): Cyber campaigns and strategic outcomes, *Journal of Strategic Studies*, DOI: 10.1080/01402390.2020.1732354.

Harris, Shane. *@WAR*: The Rise of the Military-Internet Complex. Boston: Houghton Mifflin Harcourt, 2014.

"How the U.S. Cracked into One of the most Secretive Terrorist Organizations." Washington, D.C.: NPR, 2019. https://login.usnwc.idm.oclc.org/login?qurl=https%3A%2F%2Fsearch.proquest.com%2Fdocview%2F2297846253%3Faccou

Hughes, Wayne P. Jr. and Girrier, Robert P. *Fleet Tactics and Naval Operations*. 3rd. ed. Annapolis, MD., Naval Institute Press, 2018.

"An Interview with Paul M. Nakasone." *Joint Force Quarterly: JFQ* no. 92 (First, 2019): 4-9. https://search-proquest-com.usnwc.idm.oclc.org/docview/2176619413?accountid=322.

Dr. King, Charles. *How to Think*. Accessed from faculty.georgetown.edu/kingch/HowtoThink.htm. Georgetown University, School of Foreign Service and Department of Government, 1999.

Lewis, James A. "Multilateral Agreements To Constrain Cyberconflict." *Arms Control Today* 40, no. 5 (2010): 14-19. Accessed April 24, 2020. www.jstor.org/stable/23628809.

Libicki, Martin C. "The Broad Effects of Brandishing Cyberattack Capabilities." *In Brandishing Cyberattack Capabilities*, 5-18. RAND Corporation, 2013. Accessed April 24, 2020. www.jstor.org/stable/10.7249/j.ctt5hht3r.7.

McGuffin, Chris and Mitchell, Paul. "On Domains: Cyber and the Practice of Warfare." *International Journal* 69, no. 3 (2014): 394-412.

Nakasone, Paul M. "A Cyber Force for Persistent Operations." *Joint Force Quarterly* no. 92 (2019): 10-22.

Peng Guangqian and Yao Youzhi, ed. *The Science of Military Strategy* (Beijing: People's Republic of China: Military Science Publishing House, 2005) quoted in Crowell, Richard M. "War in the Information Age: A Primer for Information Operations and Cyberspace Operations in 21st Century Warfare," Newport, RI: U.S. Naval War College, January 2016. (NWC 2021D).

Phillips, Jennifer Leigh. "Tactical Maneuver in the Cyber Domain: Dominating the Enemy." *JFQ: Joint Force Quarterly*, no. 93 (2019 2nd Quarter 2019): 14–20. http://search.ebscohost.com.usnwc.idm.oclc.org/login.aspx?direct=true&db=mth&AN=136571929&site=ehost-live.

Philpott, Tom. "Military must Choose Better, Smarter Weapons." Montgomery Advertiser, Nov 23, 2008. https://login.usnwc.idm.oclc.org/login?qurl=https%3A%2F%2Fsearch.proquest.com%2Fdocview%2F412926378%3Faccoun

Reed, Thomas C. *At the Abyss, an Insider's History of the Cold War*. New York, NY. Ballantine Books. 2004, 268, quoted in Crowell, Richard M. "War in the Information Age: A Primer for Information Operations and Cyberspace Operations in 21st Century Warfare," Newport, RI: U.S. Naval War College, January 2016. (NWC 2021D).

Reith, Mark. "Brandishing our Air, Space, and Cyber Swords: Recommendations for Deterrence and Beyond." *Air & Space Power Journal* 31, no. 4 (2017): 103-114.

"REP. ELLEN O. TAUSCHER HOLDS A HEARING ON THE U.S. STRATEGIC COMMAND." Political Transcript Wire, Mar 12, 2007.)

Rid, Thomas. "Cyber War Will Not Take Place." *Journal of Strategic Studies* 35, no. 1 (2012): 5-32.

Sanger, David E. *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age*. First ed. New York: Crown Publishers, an imprint of the Crown Publishing Group, 2018.

Schelling, Thomas C., 1921-2016 and Harvard University. Center for International Affairs. *Arms and Influence.* New Haven: Yale University Press, 1966.

Singer, P. W. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. New York;Oxford;: Oxford University Press, 2014.

Smeets Max. (2018) A Matter of Time: On the Transitory Nature of Cyberweapons. *Journal of Strategic Studies*. 41:1-2, 6-32. DOI: 10.1080/01402390.2017.1288107

Snyder, Glenn H, *Deterrence by Denial and Punishment*. Center of international studies, Princeton University, 1959.

U.S. Army War College. *Strategic Cyberspace Operations Guide*. Carlisle, PA: Center for Strategic Leadership, November 30, 2018.

U.S. Cyber Command. *Achieve and Maintain Cyberspace Superiority: Command Vision for U.S. Cyber Command.* Washington, DC: U.S. Cyber Command, March 2018. https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010

---. Operation Glowing Symphony Assessment Framework Briefing Version 1.1, November 14 2016. obtained by Freedom of Information Act request by National Security Archive, George Washington University. January 21 2020. https://nsarchive.gwu.edu/briefing-book/cyber-vault/2020-01-21/uscybercom-after-action-assessments-operation-glowing-symphony.

---. Operation Glowing Symphony J3 AAR Observations. November 22 2016. obtained by Freedom of Information Act request by National Security Archive, George Washington University. January 21 2020. https://nsarchive.gwu.edu/briefing-book/cyber-vault/2020-01-21/uscybercom-after-action-assessments-operation-glowing-symphony

U.S. Department of Defense, *2018 Department of Defense Cyber Strategy*, Washington, DC: Department of Defense, 2018.

U. S. Office of the Chairman of the Joint Chiefs of Staff. *Cyberspace Operations, Joint Publication (JP) 3-12*. Washington, DC: CJCS, 8 June 2018

U.S. Office of the Secretary of Defense, *Nuclear Posture Review* February 2018, 57. https://media.defense.gov/2018/Feb/02/2001872886/-1/-1/1/2018-NUCLEAR-POSTURE-REVIEWFINAL-REPORT.PDF

Valeriano, Brandon. "Managing Escalation Under Layered Cyber Deterrence." *Cyber Solarium Commission*. April 1, 2020. https://www.lawfareblog.com/managing-escalation-under-layered-cyber-deterrence.

Vego, Milan. *Joint Operational Warfare: Theory and Practice.* Newport, RI: Naval War College, reprint 2009.

Whiting, Nicola. "Cyberspace Triggers a New Kind of Arms Race." *Signal* 72, no. 6 (02, 2018): 38-40.

Wylie, J. C., Jr. "Reflections On The War In The Pacific". *U.S. Naval Institute Proceedings*, vol. 78, no. 4 (April 1952). pp. 351-361