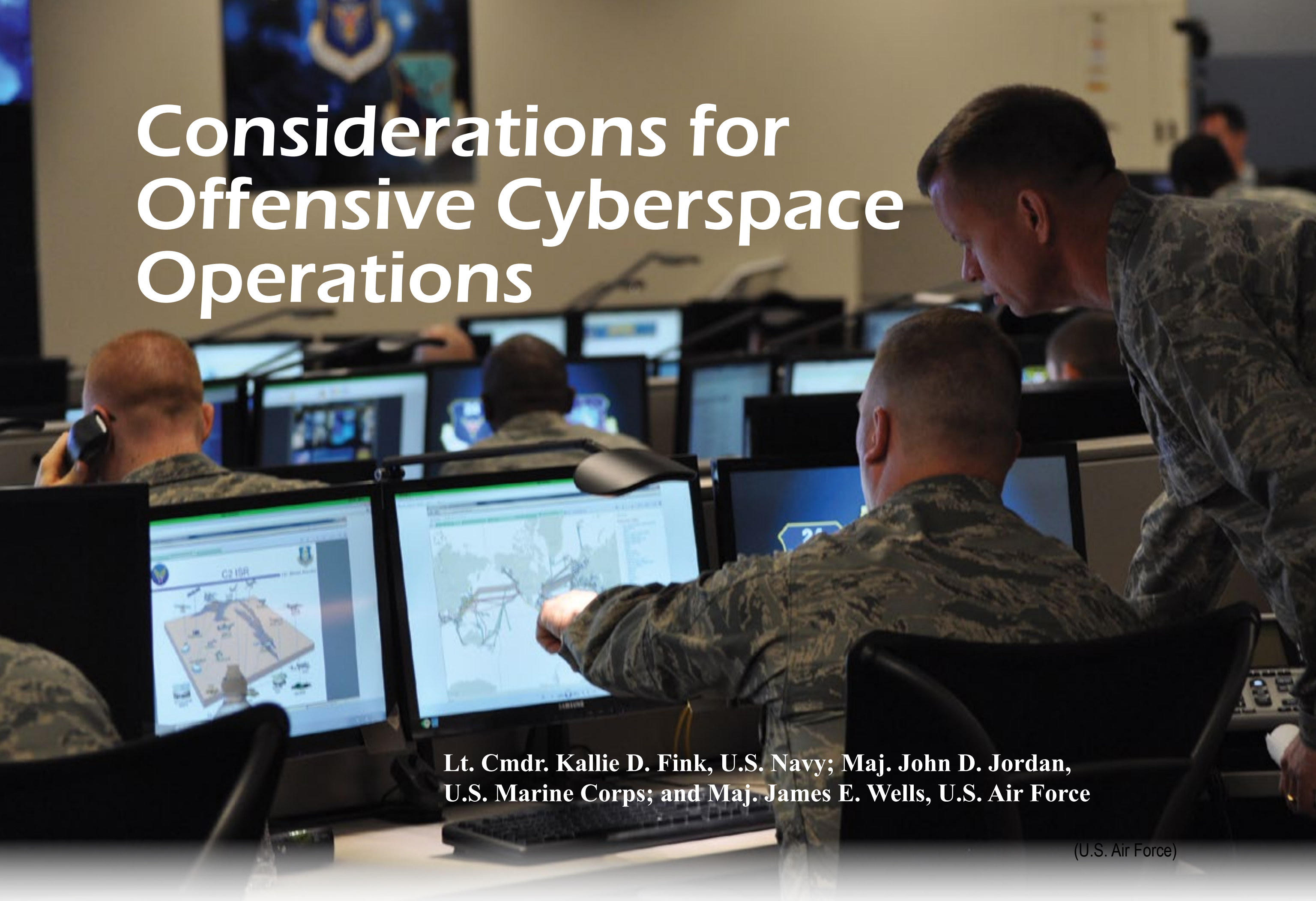
# Considerations for Offensive Cyberspace Operations



Lt. Cmdr. Kallie D. Fink, U.S. Navy; Maj. John D. Jordan, U.S. Marine Corps; and Maj. James E. Wells, U.S. Air Force

(U.S. Air Force)

OFFENSIVE CYBERSPACE OPERATIONS (OCO) have become ubiquitous over the last decade, and their inclusion in deliberate planning is increasing. However, much of this inclusion is *pro forma*, as OCO are in many ways inscrutable to those who are not familiar with them. Moreover, the joint targeting cycle does not take into account the distinct characteristics of OCO. Improvements to the institutional perception of OCO and the integration of OCO into the joint targeting cycle would enable joint task force (JTF) commanders to make the most of this potent capability during deliberate planning.

*Lt. Cmdr. Kallie D. Fink, U.S. Navy, is an information warfare officer assigned to Navy Information Operations Command Maryland. She holds a B.A. in German from the University of Minnesota and an M.S. in strategic intelligence from the National Intelligence University. Lt. Cmdr. Fink previously served as the deputy executive assistant to the Deputy Chief of Naval Operations for Information Dominance (N2/N6).*

*Maj. John D. Jordan, U.S. Marine Corps, is assigned to the Joint Staff J-7, Joint Force Development, as an operations research analyst working on cyberspace projects. He holds a B.S. in aerospace engineering from the University of Virginia and an M.S. in operations research from the Naval Post Graduate School. Major Jordan is a CH-46E pilot, and his previous assignments include flying casualty evacuation missions in Iraq, humanitarian assistance missions throughout United States Pacific Command, and service as a forward air controller in Afghanistan.*

*Maj. James E. Wells, U.S. Air Force, is assigned to the National Geospatial-Intelligence Agency as the chief of joint requirements programs. He holds a BFA in visual communications and an M.A. in human relations from the University of Oklahoma. Maj. Wells previously served as the chief of 3d Wing exercises and plans at Joint Base Elmendorf-Richardson, Alaska.*

However, two main problems hinder effective inclusion of OCO in deliberate operational planning. The first problem is that planning staffs have misconceptions about OCO capabilities and limitations within an operational environment. Moreover, staffs are uncomfortable with the highly classified and technically complex aspects of the cyberspace domain because they do not understand them. The second problem is that OCO do not fit neatly into the joint targeting cycle and require much extra work and time to incorporate into deliberate planning.

## Misconceptions About and Challenges to the Operational Employment of OCO

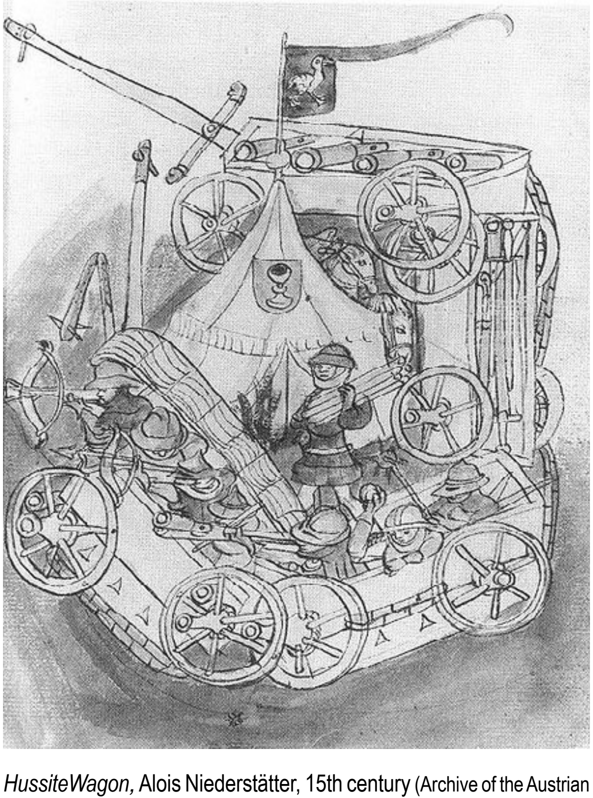
Among the many common misconceptions about OCO, two are particularly significant. The first misconception is that OCO are nonlethal enablers that play a marginal role in operations. The second is that since details of OCO are either inscrutable due to their technical complexity or inaccessible due to their classification, they are not worth the trouble of trying to employ at an operational level.

**The "it's just computers" misconception.** A common perception among planners is that OCO are nonlethal means of attacking an opponent's networks, with little physical effect. However, over the last decade OCO have become more than just a nonlethal enabler like electronic warfare. The nature and potential of OCO have not changed significantly, but our understanding of them has.

A revolutionary weapon system typically starts out as an asymmetric weapon that can, under favorable conditions, be used to counter traditional forms of military power. A historical example is the use of gunpowder weapons in the hands of the Hussites, a band of 15th-century religious dissenters who used primitive firearms to defeat armored knights.[1] In the 21st century, offensive cyberspace capabilities can give state and nonstate actors a new asymmetric weapon to use against traditional seats of power.

An event in Estonia in 2007 is considered by some to represent the first offensive cyberspace attack against a nation. It began after the Estonian government removed a World War II Soviet war memorial commemorating a Russian victory over the Nazis.[2] The Estonian government suspected Russia of coordinating subsequent retaliatory cyber strikes at Estonia's digital infrastructure, government command and control (C2), financial institutions, and media networks.[3] The massive attacks shut down government agencies' emails, published false documents, and severely limited Internet access. The digital bombardment lasted two weeks and forced a major bank, Hansabank, to shut down online services for more than an hour; its losses eventually were estimated around $1 million.[4] The denial and disruption of government, media, and financial networks caused confusion and chaos without physical damage or destruction. The attack did great economic damage to Estonia. Coordinating a defensive response was very difficult because the attack was so widely dispersed—no single Estonian authority was responsible for defense of so many different cyberspace assets.[5]

**How new asymmetric weapons become integrated into a standard military arsenal.** After military forces have used a new asymmetric weapon successfully, they sometimes adopt it as a complement to the traditional military arsenal. For



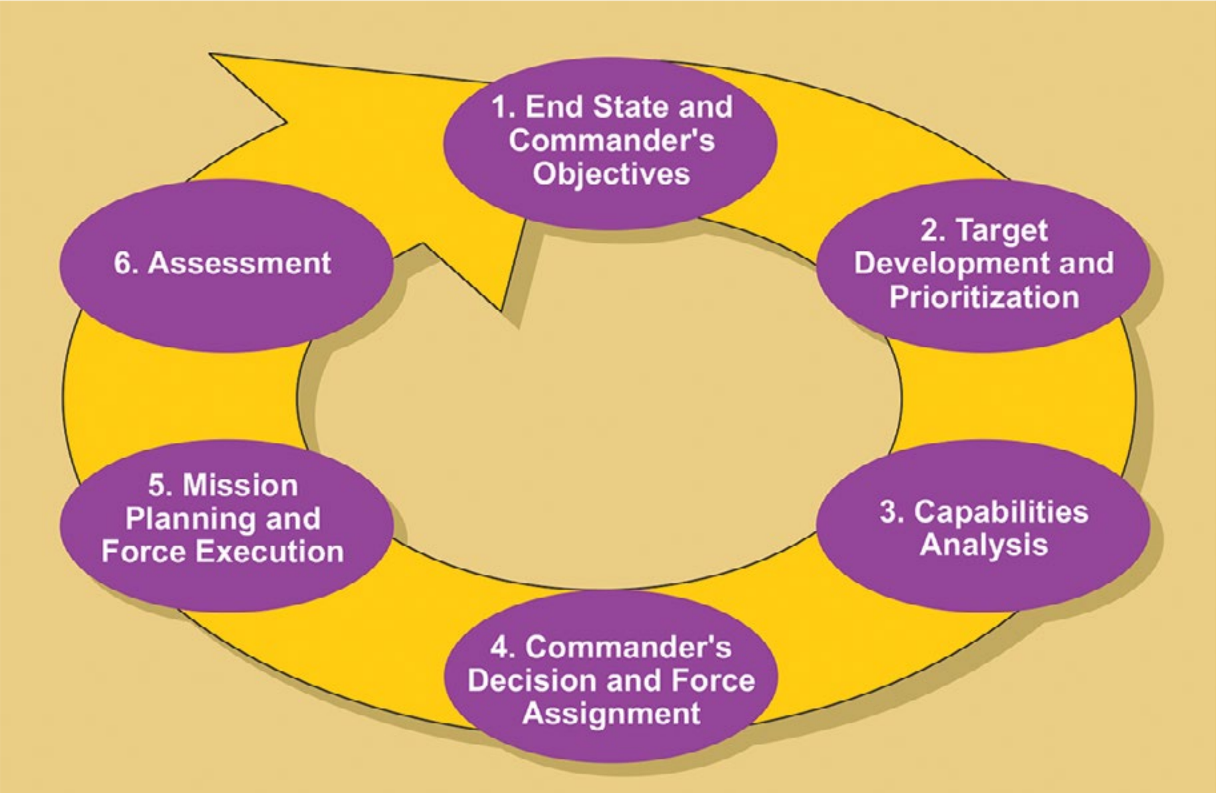
*HussiteWagon,* Alois Niederstätter, 15th century (Archive of the Austrian National Library) example, by the 16th century, armies had combined muskets with pikes and armored knights. During the 2008 Russian-Georgian War, some speculated that Russian forces integrated OCO with traditional operations to enhance their overall operational effectiveness. The Russians evidently conducted numerous cyberspace attacks that rendered Georgia's governmental and media networks inoperable.[6] These attacks severely disrupted Georgian military C2. They were synchronized with the Russian troops' crossing of the Georgian border.[7] Cyber expert Eli Jellenc stated this event represented "the birth of true, operational cyber warfare," as it appeared to be the first coordinated usage of cyber and conventional attacks on a nation state.[8]

A complementary weapon eventually can evolve into a primary weapon. For example, the musket equipped with a socket bayonet replaced the pike by the early 18th century as the universal infantry arm. In 2010, a computer worm known as Stuxnet evidently was used as a primary offensive weapon to create tangible operational effects. Stuxnet, while of unknown origin, was a "fire and forget" program, considered the world's first "cyber missile."[9] The program apparently was deployed to sabotage Iran's nuclear fuel-refining centrifuges, which could be used to develop weapons-grade uranium, by altering the electrical current.[10] According to German researcher Ralph Langner, the attack may have been intended to destroy the centrifuge rotor by vibration—which could cause the centrifuge to explode—or simply to degrade the output over time (by slowing down and speeding up the motor).[11] Stuxnet—although delivered through what is perceived as a nonphysical and nonlethal domain—achieved decidedly physical effects by damaging Iranian nuclear facilities.

The examples from Iran and Georgia show how OCO have produced effects ranging from nonphysical harassment and information operations through physical damage to key infrastructure. Without forces or weapons having direct physical contact, OCO can create nonphysical and physical operational effects. They can shut down air defense systems and C2 nodes, open or close a dam's floodgates, and destroy or damage industrial machines such as nuclear centrifuges.[12] Offensive cyberspace capabilities, like standard lethal and tangible weapons, can be arrows in a JTF commander's quiver. They can enable a commander to address a range of targets efficiently, on their own or in conjunction with other weapons.

**The "I don't understand it" or "I can't get to it" misconception**. Cyberspace capabilities, particularly OCO, tend to be shrouded in secrecy. OCO are highly classified because the nature of these operations could divulge strategic and operational intentions if they are revealed. If a hostile power learned about even one OCO target under development, that power could learn much about U.S. cyberspace capabilities and a combatant command's operations. If certain enemies learned that an operation plan featuring them as a target involved a cyberspace attack on an infrastructure node, they could use U.S. military doctrine to develop some understanding of the plan. Further, if technical data were compromised, an

An Iranian technician works at the Uranium Conversion Facility just outside the city of Isfahan 255 miles south of Tehran, Iran, 3 February 2007. (AP Photo/Vahid Salemi)


1. End State and Commander's Objectives
2. Target Development and Prioritization
3. Capabilities Analysis
4. Commander's Decision and Force Assignment
5. Mission Planning and Force Execution
6. Assessment

**Joint Targeting Cycle**

opponent could use the data to design and build a cyber weapon to attack U.S. or allied interests.

In addition to the challenges of secrecy, the technical aspects of cyberspace operations are difficult to grasp for those without technical training. This is especially so in comparison to traditional weapon systems. Cyberspace is not like the traditional physical domains where we can touch and see all the parts. Rather, cyberspace is primarily a virtual realm that can be manipulated to achieve real-world effects in the air, land, maritime, and space domains. Putting a bomb on target is easier to visualize than launching a multihost cyber attack that will penetrate a network and eventually weaken or destroy a critical system.[13]

**Marginalization by inaccessibility.** Whether the issue is difficulty in understanding, getting access to, or employing technically complex cyberspace capabilities—inaccessibility can marginalize OCO more than any opponent's defenses. Unfortunately, inaccessibility can make operational planners apathetic about employing OCO. They may regard "cyberspace operations" as a buzzword the boss wants to pay lip service to rather than a set of weapons and tactics that deliver tangible benefits. At best, OCO can become marginalized—employed on the fringes of operations as they are not understood, not accessible, not easy to employ, and not trusted.

**The joint targeting cycle.** In addition to the common misconceptions and inaccessibility issues surrounding OCO, certain challenges are inherent to fitting OCO into the joint targeting cycle (see figure).[14] Two phases of the joint targeting cycle—target development and prioritization, and capabilities analysis—have the most significant upstream effect on planning the operational employment of OCO.

United States Cyber Command (USCYBERCOM) coordinates the desired cyberspace effects against a target, based on the priorities of the combatant commander or JTF commander. During contingency planning, the capabilities analysis phase seeks to match apportioned assets and ordnance with the target and effect desired. Once a target is selected to be serviced by traditional means, it is periodically reviewed during the plan review cycle. No further resources are expended on maintaining access to the target until the plan is executed. By contrast, designating a target to be engaged with OCO starts the immediate allocation and expenditure of additional resources. Maintaining and developing a target requires a significant amount of time. During Operation Odyssey Dawn in 2011, U.S. officials debated the use of OCO against Libya but decided against it for several reasons—mainly because of time. Analysts at the *New York Times* reported that "in reality it takes significant digital snooping to identify potential entry points and susceptible nodes in a linked network of communications systems, radars and missiles like that operated by the Libyan government, and then to write and insert the proper poisonous codes."[15]

**How the joint targeting cycle applies to OCO.** The first step to engage a target with OCO is to gain access to it. Without physical or electronic access to the target, it is impossible to proceed with OCO. A system linked to the Internet is, in general, more accessible, though getting into its targeted portions may be challenging due to its own network security environment. A closed system, such as the Iranian nuclear program, would require insider access to gain firsthand knowledge of the computing environment in the target facility.[16] Once forces gain access to a target system, they need to maintain it as long as they might wish to strike the target. Network upgrades or system changes made in the regular maintenance of the target could make it difficult to maintain or regain access. The risk from gaining access to a system is that an adversary might detect the hacking well before the attack. The adversary would discover which systems were being targeted. Moreover, discovery would assuredly result in access being lost—and the possibility of the adversary studying the attack to understand U.S. cyberspace operations and develop better defenses or even counterattacks.

Once access is gained, the next step is to learn the unique internal attributes of the targeted system. Cyber attackers may need to acquire the software being targeted so they can determine its nature and vulnerabilities. For commercially available systems, this is relatively easy to do—a copy can be purchased. For rare systems or those whose development and use are limited to a given country or region, forces might need to obtain insider knowledge of the network environment (as may have occurred with Stuxnet).[17] Depending on the system to be attacked, the code might be commented in a language other than English. For whatever reason, if USCYBERCOM is unable to gain technical insight into the targeted software, then OCO cannot proceed; coordinating the proper effect is impossible. The JTF commander must consider these attributes of OCO when setting target priorities during deliberate planning.

Once USCYBERCOM has coordinated a means for continuous access and learned the targeted system, they must then coordinate acquisition or development of the weapon with which to attack it. Some weapons designed to attack common operating systems such as Windows are commercially available. However, systems produced and used only in certain countries typically require forces to develop weapons from scratch. This becomes a software acquisition project, in both the technical and legal sense. For purposes of defense acquisition, software development projects are more complex than physical engineering projects.[18] Developing a cyber weapon is a complex challenge for this reason and many others. Once a weapon has been developed, the attackers must constantly maintain access to and monitor the target. They must ensure routine system maintenance does not nullify their labors until the weapon is employed, or until the target is removed from the joint integrated prioritized target list (JIPTL).

**OCO force assignment challenges.** All of these actions require a significant amount of time, perhaps months, before anything besides a rudimentary attack can be launched with a presumption of success. Furthermore, depending on the target and its accessibility, a weapon may need to navigate through several networks to its intended target. According to cyber forensics analysts, Stuxnet may have infected its target environment through a removable device inserted by a willing or unwitting third party or insider.[19] Stuxnet would have needed numerous developers working up to six months to infect target computers in the Iranian nuclear program's closed network.

Currently, USCYBERCOM coordinates all OCO, with the concurrence of the appropriate combatant command. This further complicates the challenge of matching targets to weapons. Not only must a combatant command request USCYBERCOM to attack a target, but also each target in the command's JIPTL competes for resources against targets in the JIPTLs of other commands. USCYBERCOM sorts through all of these lists, assigning a global priority to individual targets and allocating scarce resources to them. Even if USCYBERCOM considers a target high priority, the command may not have the resources needed to service it. USCYBERCOM needs to inform combatant commands and JTFs of its ability to service targets on their JIPTLs.

**Onerous legal reviews.** Stewart A. Baker, former Department of Homeland Security assistant secretary for Policy and Technology, suggests that U.S. legal interpretation of the Hague Conventions reduces the operational utility of OCO.[20] He writes that "lawyers across the government have raised so many show-stopping legal questions about cyberwar that they've left our military unable to fight, or even plan for, a war in cyberspace."[21]

Part of this legal complexity stems from the nature of OCO. As noted above, any but the most rudimentary cyberspace attack on an enemy requires the acquisition, development, or modification of software to engender the effects that a JTF commander desires. This brings Department of Defense Directive (DODD) 5000.01, *The Defense Acquisition System*, into the process. DODD 5000.01 requires that "the acquisition or procurement of DOD weapons and weapon systems shall be consistent with all applicable domestic law and treaties and international agreements."[22] In regard to Air Force operations, Air Force Instruction 51-402 states that the office of the Judge Advocate General of the Air Force will conduct legal reviews of any new cyberspace capabilities (including weapons) or any contemplated modification of a cyberspace capability to ensure legality under the Law of Armed Conflict (LOAC), domestic law, and international law.[23] A traditional attack on a target with missiles and bombs only has to pass through legal scrutiny during target development and prioritization since the weapons being employed have long since passed their assessment (per DODD 5000.01) during acquisition. By contrast, since cyberspace weapons are unique for almost every target, Air Force OCO require two legal reviews: one during target validation and the second during the acquisition process. This puts conducting OCO at the mercy of the most restrictive reading of the LOAC by two separate legal teams.

This constraint, and the general ambiguity of how the LOAC applies to cyberspace operations, has created what Stewart Baker interprets as "a cyberwar strategy that simply omitted any plan for conducting offensive operations. Apparently, they're still waiting for all these lawyers to agree on what kind of offensive operations the military is allowed to mount."[24]

*Cyberspace, including OCO awareness, should be part of every officer's basic accession curriculum.*

## Solutions

**Clarifying the perception of OCO.** Education is the key to changing how we think, plan for, and employ OCO. Cyberspace, including OCO awareness, should be part of every officer's basic accession curriculum. Joint professional military education (JPME) level I should include foundational cyberspace operations and doctrine for all officers. Intermediate and senior officers should study and integrate operational and strategic cyberspace operations into joint planning through JPME II. In addition, capstone courses should include instruction in the capabilities and limitations of OCO. The goal of this education should not be to turn officers into cyber specialists, but to give them the same basic awareness of this domain that officers who are in supporting or combat arms fields have of how those in the other fields conduct their profession.

Not unlike the intricacies of sophisticated conventional weapon systems, the details of OCO should remain classified. This is an attribute of cyberspace operations that must be taken into account when targeting: knowledge of the specific processes by which cyber effects are achieved should be limited to those with a need to know. The inaccessibility of offensive cyberspace capabilities—to anyone not working directly on developing and executing them—contributes a level of operational security that will support the capability over time. Additionally, maintaining a level of inaccessibility surrounding the offensive cyberspace capabilities affords the option to mask operational intent. Most joint planners do not possess the knowledge or security clearance to know how to build a Tomahawk cruise missile from scratch; nor should joint planners have the access to dissect an offensive cyberspace capability.

An example of this paradox is the espionage virus Flame, discovered in 2012 and thought to have circulated on the Internet approximately four years before detection.[25] According to Debra Van Opstal, Flame "exploited the Windows operating system to capture audio, screenshots, keyboard activity, and network traffic information from infected computers."[26] Whoever decided to employ Flame likely did not understand the intricacies of its inner workings, but they did understand the desired effect. Flame is just one example of an offensive cyberspace tool that is difficult to detect, but its complex nature offers a unique perspective into the level of detail required to produce a pervasive cyber effect. The challenge for the combatant command and JTF staffs is accepting and operating in this borderless environment, which may involve hitting the "I believe" button when vetting desired, prioritized effects through USCYBERCOM.

**Improvements to the joint targeting cycle.** To better utilize OCO capabilities, joint targeting coordination boards (JTCBs) must change how they assemble their JIPTLs; they must coordinate cyber target nomination with USCYBERCOM. This will enable the JTCBs to enhance OCO utilization, while fully integrating cyberspace capabilities with the traditional land, air, and sea power.

**Iterative capabilities analysis.** Each JTCB should have a cyberspace representative assigned to it. The representative should be coequal with the joint force air, land, and maritime component command representatives. The cyberspace representative should provide a cyberspace target nomination list to the JTCB. When the JTCB begins to synthesize the target nomination lists into the draft JIPTL, the cyberspace representative can coordinate the draft JIPTL with USCYBERCOM. With this information, USCYBERCOM can inform the JTCB as to which targets are considered susceptible to OCO, enabling the board to better shape the JIPTL. In addition, this practice will allow USCYBERCOM to look for possible synergies with work it is already undertaking for other plans. This information sharing will shape the design of the JIPTL and enable the JTCB to integrate OCO into its design.

To get the best results from OCO, the JTCB also needs to ensure that targets for OCO are enduring. The JTCB needs to focus on the effects needed rather than how the effects are generated. Enduring targets are necessary because they allow USCYBERCOM to most efficiently coordinate resources and avoid chasing fleeting targets. An enduring target should be one that will persist through multiple plan review cycles. This gives USCYBERCOM enough time to develop the weapons needed to engage it successfully. Moreover, a focus on effects will enable USCYBERCOM to propose alternate courses of action to the JTCB. This will allow the JTCB to maintain focus on the big picture rather than the details of OCO. The cyberspace representative to the JTCB should be more than capable of deconflicting and coordinating OCO with the rest of the JIPTL.

**Coordination of global OCO assignment.** Each JTCB must remain flexible regarding its JIPTL, as USCYBERCOM's requirement to provide global support means that resources may shift. Whether for priority changes or other reasons, not every target on every JIPTL will be serviced. USCYBERCOM must inform each JTCB of the status of its targets, especially when priorities change, as this may have a significant effect on a command's JIPTL. Each JTCB must prepare itself for this possibility by developing branch JIPTLs that reflect the lack of access to a cyberspace target. This again requires the JIPTL to be continuously reviewed and updated instead of sitting on the shelf until the next operation plan review. The direct link afforded by the cyberspace representative makes this less onerous, but it will require the JTCB to conduct extra research and planning to meet the commander's desired end state. The temptation remains, of course, to ignore or marginalize cyberspace capabilities because using them would cause frustration and extra work. The JTCB must weigh the potential payoff of OCO with the extra workload this may inflict during deliberate planning. However, successful integration of OCO can enable a JTF to expand its reach beyond what traditional fires assets would allow, and to husband those assets for more suitable targets.

**Consolidated legal review.** The legal challenges facing a JTCB seem daunting, but the board can address them in a way that satisfies the combatant commander's requirements. While the details of rules of engagement and target legitimacy reside in the realm of law, it is, especially with new technologies, a subjective field. The use of two distinct legal processes—in the target development and prioritization process described in Joint Publication 3-60 and the acquisitions process described in DODD 5000.01—to approve the development and employment of a cyber weapon is redundant and overuses scarce legal resources.

Instead, USCYBERCOM should conduct both legal reviews. The legal review during target development and prioritization should be skipped for cyberspace targets. USCYBERCOM should conduct an initial and final LOAC review while coordinating with the JTCB during the cyber weapon development. Moreover, since cyber weapons are custom crafted to engage a specific target, the legal team can conduct the legal reviews mandated by DODD 5000.01 as well as target validation. USCYBERCOM, in coordination with the cyberspace representative, should have the technical expertise to review and assist in the weapon development. This will enhance the effectiveness of OCO development and employment. Furthermore, since the legal review team is not part of the combatant command, there is less opportunity for "group think" or command influence to warp the process.

## Conclusion

OCO offer potent tools for a combatant command or JTF commander. However, our own internal friction—manifested as misunderstanding, inaccessibility, and slowly evolving processes—has not allowed us to take full advantage of these capabilities. None of the solutions described above are particularly costly, nor do they involve purchasing equipment or adding to the force structure. Rather, they focus on developing our people and processes so they are more prepared to engage an adversary in all domains. While implementing these solutions would be a long-term effort, delaying implementation only would enable the problem to fester, effectively denying use of OCO to joint force commanders. ***MR***

NOTES

[1] Saul David, *The Illustrated Encyclopedia of Warfare: From Ancient Egypt to Iraq* (London: DK Publishing, 2012), 95.

[2] Sascha-Dominik Bachmann, "Hybrid Threats, Cyber Warfare and NATO's Comprehensive Approach for Countering 21st Century Threats—Mapping the New Frontier of Global Risk and Security Management," *Amicus Curiae* 88 (January 2012).

[3] Mark Landler and John Markoff, "After Computer Siege in Estonia, War Fears Turn to Cyberspace," *New York Times* (29 May 2007).

[4] Ibid.

[5] Joshua Davis, "Hackers Take Down the Most Wired Country in Europe," *Wired.com* (21 August 2007), <http://www.wired.com/politics/security/magazine/15-09/ff_estonia?currentPage=all>.

[6] James P. Farwell and Rafal Rohozinski, "Stuxnet and the Future of Cyber War," *Survival: Global Politics and Strategy* 53, no. 1 (January 2011): 23-40.

[7] Stephen W. Korns and Joshua E. Kastenburg, "Georgia's Cyber Left Hook," *Parameters* 38, no. 4 (Winter 2008-2009).

[8] Eli Jellenc, quoted in Iain Thomson, "Georgia Gets Allies in Russian Cyberwar," *Vnunet.com* (12 August 2008), <http://www.v3.co.uk/v3-uk/news/1997915/georgia-allies-russian-cyberwar>; see also John Markoff, "Before the Gunfire, Cyberattacks," *New York Times* (12 August 2008), <http://www.nytimes.com/2008/08/13/technology/13cyber.html?_r=0>.

[9] Mark Clayton, "How Stuxnet Cyber Weapon Targeted Iran Nuclear Plant," *The Christian Science Monitor* (16 November 2010): 4.

[10] Farwell and Rohozinski, *23-40.*

[11] Ralph Langner, as reported in Clayton, 4.

[12] Stephenie Gosnell Handler, "The New Cyber Face of Battle: Developing a Legal Approach to Accommodate Emerging Trends in Warfare," *Stanford Journal of International Law* 48, no. 1 (Winter 2012): 209.

[13] Anoop Singal and Ximming Ou, *Security Risk Analysis of Enterprise Networks Using Probabilistic Attack Graphs* (Gaithersburg, MD: NIST Interagency Report 7788, National Institute for Standards and Technology, U.S. Department of Commerce, August 2011).

[14] Joint Publication 3-60, *Joint Targeting* (Washington, DC: U.S. Government Printing Office [GPO], 31 January 2013), Figure II-2.

[15] Eric Schmitt and Thom Shanker, "U.S. Debated Cyberwarfare in Attack Plan on Libya," *New York Times* (17 October 2011). <http://www.nytimes.com/2011/10/18/world/africa/cyber-warfare-against-libya-was-debated-by-us.html?_r=0>.

[16] Nicolas Falliere, Liam Murchu, and Eric Chien, W32.Stuxnet Dossier (Cupertino: Symantec Corporation, 2011), <http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf>.

[17] Ibid.

[18] Rene G. Rendon and Keith F. Snider, Management of Defense Acquisition Projects (Reston, VA: American Institute of Aeronautics and Astronautics, 2008), 66.

[19] Falliere, Murchu, and Chien, 3.

[20] Stewart A. Baker and Charles Dunlap Jr., "What Is the Role of Lawyers in Cyberwarfare?" ABA Journal (1 May 2012). <http://www.abajournal.com/magazine/article/what_is_the_role_of_lawyers_in_cyberwarfare>.

[21] Ibid.

[22] Department of Defense Directive 5000.01, The Defense Acquisition System (Washington, DC: GPO, 12 May 2003), 7.

[23] U.S. Air Force, Air Force Instruction 51-402: Legal Reviews of Weapons and Cyber Capabilities (Washington, DC: GPO, 27 July 2011), 2.

[24] Baker and Dunlap Jr.

[25] Debra Van Opstal, "'Aha' Findings from the Workshop on Securing the Smart Grid: Best Practices in Supply Chain Security, Integrity, and Resilience," Center for Critical Infrastructure Protection and Homeland Security 11, no. 2 (August 2012).

[26] Ibid.