STRATEGIC STUDIES QUARTERLY

Liberating Cyber Offense

James E. McGhee

Abstract

Offensive cyber operations are increasingly an important part of our national defense and provide commanders with unique capabilities to thwart enemy attacks. Conducting cyber operations, however, is not as simple as pushing a button on a keyboard. Challenges involving cyber operations frustrate operators and commanders alike. Four specific problem areas exist, but certain recommended changes can assist operators and commanders to more efficiently conduct cyber operations.

✳ ✳ ✳ ✳ ✳

The Department of Homeland Security (DHS) runs a national clearinghouse of cyber-threat information known as the US Computer Emergency Readiness Team (US-CERT). Part of its job is to track cyber incidents, which could include unauthorized attempts to access a network, distributed-denial-of-service (DDoS) attacks, or other nefarious behavior. According to data from a 2013 review, US-CERT received almost 12,000 cyber incident reports in 2007. By 2009 that number had more than doubled—and it quadrupled by 2012.[1] According to the Pentagon's Cybersecurity Culture and Compliance Initiative memo, between September 2014 and June 2015, Department of Defense (DOD) networks experienced 30 million known malicious cyber intrusions. That translates to 3 million attacks per month or 100,000 per day.[2] While these statistics are stunning, they are not news. Most articles discussing cyber incidents sound the klaxon regarding US ability to prevent a cyber Pearl Harbor but do not discuss the difficulty of executing cyber operations. Other articles that discuss cyber operations talk about cyber attack as any garden-variety cyber operation, even those that are not actual attacks. Such articles conflate incidents below the use-of-force threshold

James E. McGhee is currently the legal advisor for Special Operations Command North. He graduated from the University of Pittsburgh School of Law in 2000 and served eight years as an Army JAG officer before becoming the Assistant US Attorney in Tucson, Arizona. McGhee previously served as operational law attorney for the Twenty-Fourth Air Force.

with actual use-of-force operations considered an armed attack. Their authors believe every cyber incident is a cyber attack and say things such as, "We're dropping cyber bombs."[3] Those articles also presume cyber operations are easy to do, perhaps too easy. The authors seem to gloss over the "how to," making it appear as if the DOD can simply "launch" a cyber capability whenever it chooses. The current reality is that offensive cyber operations are difficult; adding to the problem are unnecessary restrictions, limitations, and ambiguity. The United States can reach a point where conducting offensive cyber operations becomes easy and quick, but only if there are fewer restrictions and constraints. This article presents some of the challenges that create hardships in offensive cyber operations and offers recommendations to liberate the cyber offense.

Several questionable restrictions regarding offensive cyber operations decrease effectiveness and efficacy of cyber capabilities. First, offensive cyber operations require high-level (presidential or secretary of defense in most cases) approval authority before they can be used. This is true even in emergency defensive situations when existing, approved defenses against cyber threats will not suffice. Even so, such an emergency response still requires multiagency coordination to make such a determination in the first place. Second, it is generally impractical to use offensive cyber operations because, contrary to the speed at which they are carried out, planning these operations generally takes more time than planning conventional, kinetic operations. Third, even though we mistakenly conflate cyber operations with kinetic operations and place more restrictions on cyber offense, clearly cyber has different effects. We also use different cyber definitions throughout the government to describe the same things. These terms are ambiguous and lead to misunderstandings about the efficacy of cyber offense. Finally, confusion remains regarding who is actually in charge of the response in the event of a cyber "attack" against the United States.

Despite each of these issues, cyber offensive operations can be liberated and become quite useful with certain changes and recommendations.

High-Level Approvals

In accordance with the 2015 DOD Cyber Strategy, the DOD has three primary cyber missions. First, the DOD must defend its own networks, systems, and information. Second, the DOD must be prepared to defend the United States and its interests against cyber attacks of significant consequence. To this end, "if directed by the president or the secretary of defense, the US military may conduct cyber operations to counter an imminent or on-going attack against the US homeland or US interests in cyberspace." Third, if directed by the president or the secretary of defense, the DOD must be able to provide integrated cyber capabilities to support military operations and contingency plans.[4]

The approval authority for any cyber operation that goes outside of a DOD network is very high. Corresponding approval authorities for kinetic operations is much lower. For instance, if a joint force commander wanted to disrupt the power in a large area, he could attack a power plant being used by the enemy in several ways, such as sending in a team to sabotage it, calling in an airstrike, firing a missile, or asking for a cyber operation. The first three courses of action are quick and relatively easy. The commander can likely take those actions at his or her level. The cyber operation, however, can only be used if an execute order (EXORD) authorized cyber operations, that particular power plant was already on a cyber targeting list, the cyber operators already performed appropriate operational preparation of the environment (OPE) on the power plant's network, and interagency and possibly international deconfliction had taken place.

Absent an EXORD authorizing offensive cyber operations, agencies must request specific use of cyber capabilities through the review and approval process for cyber operations (RAPCO).[5] RAPCO applies to cyberspace operations requiring presidential or secretary of defense approval for deployment and initial or ongoing employment. This process takes time, and, due to the interagency nature, it often gets bogged down—ultimately resulting in the request being overcome by events or bypassed in lieu of kinetic operations. While kinetic operations also require an EXORD, additional authorizations are much easier and faster to obtain, as are delegations of authority, if need be.

Offensive cyber operations are difficult even with an EXORD or RAPCO approval. They still require OPE time, coordination, and deconfliction, and there is no guarantee the deconfliction will go smoothly. One of the partners can object, shuttering the whole process. Additionally, planners run into an attribution problem. Perhaps we can discern that the cyber intrusion is emanating from country X, but that does not tell us whether country X is behind the act or whether it is a criminal or rogue element. Perhaps the best one can hope for is to sever the command and control to stop the event.

Long Planning Times

Preparing and using offensive cyber operations is not a static process. The careful planning required can be lengthy and detailed in nature. Even if an EXORD and valid rules of engagement exist, authorizing cyber operations, target approval, and deconfliction must still be accomplished, which takes more time than conventional kinetic operations. For instance, some examples of preparatory cyber operations may include "reconnaissance (e.g., mapping a network), seizure of supporting positions (e.g., securing access to key network systems or nodes), and pre-emplacement of capabilities or weapons (e.g., implanting cyber access tools or malicious code)."[6] While we may have some number of cyber capabilities "on the shelf," their operational use requires much more than simply loading them and sending them on their way. Our operators must first know and understand the target network, node, router, server, and switch before using any cyber capability against them. However, to conduct such preparatory work still requires operators being told to do so in the first place.

Cyber planners must also consider collateral second- and third-order effects, outlining not only what the capability will do against the target but also what may happen further down the chain, to comply with the principle of distinction. However, the cyber-targeting analysis is different for the principle of proportionality.[7] In assessing incidental injury or damage, remote harms and lesser forms of harm—such as mere inconveniences or temporary losses—need not be considered in applying the proportionality rule. In the case of a power plant supporting civilian infrastructure, this can mean outlining effects against unintended targets, including hospitals, religious sites, orphanages, or other places that might be on a restricted or no-strike target list. This can require weeks or months of accessing, probing, and mapping. While some OPE is also required for kinetic weapons, the time frame for such conventional targeting is reduced to hours or days and in some circumstances mere minutes. Static targets, targeted via kinetic strikes, normally do not change. Once on a targeting list, they are likely to stay on the list. The same is not necessarily true for cyber targets. Networks, servers, routers, and so forth change all the time; they are updated and patched to keep up with security threats—and sometimes are simply turned off. Moreover, their use can change, too, from strictly military to civilian, resulting in heightened potential for collateral damage. This requires constant OPE to make any required changes to the offensive cyber operation. It is somewhat ironic, then, that offensive cyber operations, which move at the speed of light, require such long prep times and lead some commanders to balk at using cyber operations.

Restrictive Cyber Rules

Equating offensive cyber operations with kinetic operations, in theory, should make use easier. On the one hand, we tend to treat them the same and apply the same rules to their use, but on the other hand, we treat cyber differently, making it harder to actually use it. If they are truly the same and the same rules apply, then why the vast differences in their actual use? This is especially true if we accept that cyber operations are merely one tool among many, including kinetic tools, which a commander may legally use against valid targets. To be sure, "cyber operations, many military experts and scholars have said, will likely be used as a tool in conjunction with larger, more conventional military efforts in future conflicts."[8] Moreover, using cyber operations in lieu of kinetic options is likely cleaner and more apt to comply with the laws of war (LOW), which should in fact call for greater use. The DOD *LOW Manual* states

> In some cases, cyber operations that result in non-kinetic or reversible effects can offer options that help minimize unnecessary harm to civilians. In this regard, cyber capabilities may in some circumstances be preferable, as a matter of policy, to kinetic weapons because their effects may be reversible, and they may hold the potential to accomplish military goals without any destructive kinetic effect at all.[9]

Using the previous example, if the commander decides to blow up the power plant via a kinetic operation, it is likely completely destroyed. If he chooses the cyber option, it can merely be turned off or taken off-line without any physical damage or destruction. Additionally, the offensive cyber option may likely be reversible, which makes it much easier to turn the power back on. This is an important consideration, because if previous experiences are any indication, the United States will likely end up replacing the damaged infrastructure and correcting any resulting damage from second- and third-order effects. A cyber operation actually allows a joint force commander more control to limit effects.

While some of the same old rules may apply equally to both cyber operations and kinetic operations, it is not true that they apply in the same ways. In 2012 Harold Koh, legal advisor to the Department of State, gave a speech at the US Cyber Command (USCYBERCOM) Inter-Agency Legal Conference wherein he ostensibly declared US policy regarding cyber operations and international law. His speech has since become the standard for US cyber operations policy, and much of what he presented has largely been codified in the recently released *LOW Manual*. In that speech, he answered 10 questions regarding cyber operations and international law. Koh said that "cyber activities will sometimes constitute a use of force under Article 2(4) of the UN Charter and customary international law." He then gave several examples, including cyber activities that proximately result in death, injury, or significant destruction, such as operations triggering a nuclear plant meltdown, opening a dam above a populated area causing destruction, and disabling air traffic control, resulting in airplane crashes. In other words, "If the physical consequences of a cyber attack work the kind of physical damage that dropping a bomb or firing a missile would, that cyber attack should equally be considered a use of force." Koh also reaffirmed the proposition that the United States would, "when warranted, respond to hostile acts in cyberspace as we would to any other threat to our country."[10]

Koh also asserted that "there is no legal requirement that the response to a cyber armed attack take the form of a cyber action, as long as the response meets the requirements of necessity and proportionality."[11] For instance, "Operations that target an adversary's cyberspace capabilities, but are not achieved in or through cyberspace, would not be considered cyber operations."[12] These include bombing a network hub or jamming wireless communications.[13] In other words, it is more efficient and quicker to just drop a bomb on the adversary's network hub or other target than to disable or disrupt it via a cyber operation. Koh acknowledged, "There are other types of cyber actions that do not have a clear kinetic parallel, which raise profound questions about exactly what we mean by 'force.'"[14] Nonetheless, we continue to equate offensive cyber operations with kinetic operations and have yet to engage in a robust discussion of what we mean by *force* regarding those cyber actions that do not have those clear kinetic parallels. Even cyber actions that do have clear kinetic parallels still have much greater restrictions than kinetic actions. It is also somewhat ironic that a kinetic operation and a cyber operation may result in the exact same overall effect—lack of power, for instance—but the kinetic strike, which causes clear damage, destruction, and probably even death (not just to the enemy but collateral as well), has fewer restrictions than the cyber operation. The result of these added restrictions is that we are essentially forcing a law-of-armed-conflict (LOAC) analysis on cyber operations, falling well below the use-of-force/armed-attack threshold, when none is needed. This forces planners and operators to seek unnecessary authorizations and to consider unnecessary factors.

Ambiguous Definitions and Misunderstandings

Ambiguous definitions that lead to a lack of understanding of cyber utility exacerbate the disconnect between offensive cyber operations and kinetic operations. Within the DOD we have a common set of definitions regarding cyber operations, which are found in Joint Publication (JP) 3-12, *Cyberspace Operations*. We do not necessarily understand what those definitions mean, because they are not well defined. Outside of the DOD there is another set of definitions, which are contained in Presidential Policy Directive 20 (PPD 20). Those definitions, too, are not well defined or easily understood. While the definitions are similar, they differ enough to cause confusion between the DOD and interagency elements. Nonetheless, the DOD must comply with the requirements in PPD 20, which creates problems when trying to define cyber operations using DOD terms and definitions.

Moreover, none of these definitions are helpful in determining what a cyber use of force or cyber armed attack is under the United Nations Charter and the LOW. To date, there is no international consensus defining either a cyber use of force or cyber armed attack. While some attempts have been made—for example, the Schmitt Analysis and the *Tallinn Manual*—they have not been accepted throughout the international community. The United States has provided several examples of what it would consider a cyber use of force or armed attack, but those examples equate cyber effects to kinetic effects. This adds to the mistrust of cyber operations from a misunderstanding of what they can and cannot do. There seems to be a generalized fear that if we use a cyber operation to take down a server, it is more serious than if we had bombed the same server—that somehow the offended nation will be more upset. Both are a violation of state sovereignty, but a bomb is clearly open and hostile, while a cyber operation is stealthier. This lack of understanding and the very nature of cyber operations give one pause. Most nations would agree that if the physical consequences of a cyber attack produce the same kind of physical damage as dropping a bomb or firing a missile, that attack should be equally considered a use of force. However, we use terms such as "significant consequences" and "disrupt, deny, degrade, negate, impair, and destroy" to describe a cyber attack worthy of a response even without physical consequences.

We are not only concerned strictly about government systems, such as the DOD or the DHS, but also about critical infrastructure. *Critical infrastructure* is defined as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on national security, economic security, public health and safety, or any combination of these matters."[15] Much of this critical infrastructure is privately owned, adding to the confusion about how to handle any such cyber threats. Some examples include common supervisory control and data acquisition (SCADA) systems, including manufacturing, power generation, and water treatment. Other examples of critical infrastructure include the financial industry. It does not include Target, Home Depot, or Sony. We know our adversaries have probed SCADA systems, but what, exactly, are significant consequences? What, exactly, does it mean to disrupt or negate these systems? Even if such systems are disrupted or negated, does that then equate to a cyber use of force/armed attack?

The cyber event that targeted Sony was clearly not a cyber attack. It was, at best, a cybercrime perpetrated by a nation. (Despite what Hollywood elites think to the contrary, Hollywood is not part of the critical infrastructure either.) Likewise, the cyber event that targeted the Office of Personnel Management (OPM) was not a cyber attack. OPM was simply a legitimate target of cyber espionage, which is not prohibited under international law. Did either event result in significant consequences or disruption, degradation, or impairment? One can arguably answer "yes" to both, but how about actual physical consequences such as loss of life, incapacity, or destruction? Then the answer is clearly "no." However, that merely begs some questions: When do the "significant consequences" have to manifest? How extensive must the disruption, degradation, or impairment be, and for how long? It is puzzling that the terms *disrupt*, *degrade*, *negate*, and *impair* are coupled with *destroy*. The first four terms imply some temporary and perhaps even reversible effects, while *destroy* leaves little doubt of permanent effects. Trying to determine exactly what a significant consequence is or whether something has been degraded or disrupted is nothing more than an exercise in futility absent physical damage, personal injury, or death, which typically will not arise as a result of a cyber operation. As an example of how complicated and confusing this made-up lexicon can be, *degrade* is more granularly defined as "to deny access (a function of amount) to, or operation of, a target to a level represented as a percentage of capacity." Likewise, *disrupt* is further defined as "to completely but temporarily deny (a function of time) access to, or operation of, a target for a period represented as a function of time."[16] Thus, we define the terms using other terms in the overall definition.

Clear cultural and language barriers also affect cyber operations. When Col William Hartman, commander of the Army's first offensive cyber operations brigade, joined the 25th Infantry Division for an exercise, the commanding general told Hartman that his "cyber operators talked in unintelligible 'dolphin speak.'"[17] Others acknowledge that "cyber is too important to leave to the cyber geeks. 'This is a commander's business, ultimately. He's the one responsible for integrating all these capabilities.'"[18] However, to integrate fully requires more than merely participating in exercises. "Cyber experts must start educating commanders on the art of the possible so they can drive requirements. There aren't enough requirements out there, because people don't know what to ask for and they don't believe they'll ever get to use it."[19] Without a coherent lexicon, common across the DOD, the intelligence community, and the legal profession, cyber language often means nothing to the commanders who make decisions. If they do not understand what cyber operations are or what they are capable of doing, they certainly will not ask for them—thus, the lack of requirements.

While some cyber operations may have the capacity to cause damage and destruction similar to kinetic strikes, the vast majority cannot reach that level. That is not what cyber operations are about. They are not designed to attack people but rather networks, network architecture, components, and equipment—generally resulting in an inability to communicate on time or correctly. Shutting down a power plant via a cyber operation is clearly not the same as dropping a bomb on the power plant. One is clearly a use of force/armed attack, while the other may not be.[20] Unfortunately, far too many people have a basic misunderstanding about cyber operations. One recent example of this appears in a *Nextgov* article, "Pentagon Contractors Developing Lethal Cyber Weapons," in which the writer, Aliya Sternstein, asserts, "Under a forthcoming nearly half-billion-dollar military contract, computer code capable of killing adversaries is expected to be developed and deployed if necessary."[21] She continues, "Digital arms designed to kill are sanctioned under Pentagon Doctrine [referring to the DOD *LOW Manual*]. . . . The manual lays out three sample actions the Pentagon deems uses of force in cyberspace: 'trigger a nuclear plant meltdown; open a dam above a populated area, causing destruction; or disable air traffic control services, resulting in airplane crashes.'"[22] Sternstein totally misses the point, making it appear as if the United States is currently designing cyber capabilities that would have these intended effects. However, those who know and understand cyber operations and the LOW recognize the three examples as clear violations of the LOW—namely, specifically attacking civilian populations. Instead, what the *LOW Manual* suggests is that if any of those actions happened inside the United States, the government would clearly consider them a use of force/armed attack against the United States under the UN Charter and respond accordingly. There is a distinct difference in contracting for offensive cyber capabilities that we can use against an adversary (that is, their networks, command and control, communications, and so forth) and contracting for offensive cyber capabilities that can actually directly kill our adversaries. While second- and third-order effects of cyber operations may harm people, it is hard to fathom a realistic scenario wherein a cyber operation directly kills anyone.

The misunderstandings regarding cyber operations permeate the highest levels of US decision making, not only military commanders but also top civilian political leaders. Robert Work, deputy secretary of defense, recently stated, in response to activity against ISIS [the Islamic State in Iraq and Syria], "We are dropping cyber bombs. We have never done that before."[23] However, as a recent *Defense One* article states,

> Cyber options are adjunct powers, utilized in conjunction with other more traditional forms of coercion. Analogizing cyber operations as a kinetic weapon renders us cognitive misers, cheating our way through a difficult test. It is better to see cyber operations for what they are: changing lines in spreadsheets, intercepting email, jamming communication, and deception. We ought to be

> careful when talking about cyber bombs because if we really think we are dropping cyber bombs, then these "bombs" are all landing with a resounding thud.[24]

Others, however, appear more sensitive about the topic. In a recent interview in Colorado Springs in which she was asked about Work's "cyber bombs" comment, National Security Advisor Susan Rice said, "It should not be taken out of proportion; it is not the only tool."[25] Some of Work's colleagues admitted to wincing when he said it, because lawyers for the government have worked diligently to narrowly limit cyber attacks to highly precise operations with as little collateral damage as possible.[26]

Who's in Charge?

A recent Government Accountability Office (GAO) report states that the Pentagon does "not clearly define its roles and responsibilities for cyber incidents."[27] There is confusion regarding who would be the supported command and have primary responsibility for supporting civil authorities. US Northern Command's (USNORTHCOM) defense support of civil authorities (DSCA) response concept plan states that USNORTHCOM would be the supporting command for a DSCA mission that may include cyber-domain incidents and activities. Other guidance directs that US Cyber Command (USCYBERCOM) would be responsible. Another problem is that key DSCA guidance documents do not identify the role of the dual-status commander, the commander who has authority over federal military and National Guard forces.[28] Some believe the DHS would have the lead, along with the Federal Bureau of Investigation and other agencies. Then there is also the newly created National Mission Forces, which are charged with defending the nation against "cyber attacks of significant consequence."[29]

It seems clear that, regardless who actually gets the initial approval, USCYBERCOM should be the supported command, simply because it has the capacity and capabilities to handle such incidents whereas USNORTHCOM and the DHS may not. To be sure, it is generally assumed that USNORTHCOM or the DHS would likely call upon USCYBERCOM for help. In recent comments, RADM Dwight Shepherd, director of cyberspace operations for USNORTHCOM and North American Aerospace Defense Command (NORAD), said, "From a cyber standpoint, we would have to coordinate with DHS because DHS or FEMA [Federal Emergency Management Agency] may be the leading federal agencies and we'd have to coordinate obviously with the states that are affected."[30] But Shepherd conceded that USNORTHCOM is not best suited for the cyber component in national incidents. "I can tell you from a NORAD/NORTHCOM perspective we're really good at hurricanes [and] tornados but we're not capable, truthfully, to tackle a cyber event. So we, in my mind, would be supporting of CYBERCOM or JFHQ-DoDIN [joint forces headquarters-Department of Defense information network] along with coordinating with DHS or FEMA or the states." He said, "The real cyber expertise comes from CYBERCOM and the JFHQ-DoDIN."[31]

Liberating Cyber Offense

Offensive cyber operations seem to scare people who are unfamiliar with their conduct (and even some who are familiar with them). A general fear is that some super cyber weapon will be released and "escape" into the wild, taking down the entire Internet or inadvertently taking down the financial sector or SCADA systems. However, if one looks at Stuxnet as a real-world example of a cyber operation, it is clear that it is possible to specifically design a cyber capability with the LOW in mind. While it did spread throughout the world, it only affected what it was specifically designed to affect—Iranian nuclear components—thus complying with the principles of distinction and proportionality. Another general fear is that using offensive cyber operations will eventually lead to a cyber arms race and possibly a tit-for-tat escalation leading to all-out war. While this is a legitimate concern, it is overblown. An offensive cyber operation is usually a one-off, meaning that once used it probably cannot be used again, because the adversary has seen it, is aware of it, and quite likely knows how to mitigate the vulnerability or the effects. This is also known as *fragility*, that is, "the possibility that once used an adversary may be able to devise defenses that will render a cyber tool ineffective in the future."[32] As a result, escalation is limited because it takes so much time to not only develop such high-level cyber capabilities but also to conduct appropriate OPE to employ them. The idea that any cyber capability may be a one-off also leads commanders to hold onto them until absolutely needed, often ultimately rendering them useless through passage of time. Nonetheless, while the DOD struggles to get its cyber game in order, others are already doing so. Gen Keith Alexander, US Army, retired, discussing cyber operations at a recent Association of the United States Army conference, stated, "It's like the recon/counter-recon fight. It's not the only fight: it's the first fight. If we win that, we'll still be in the second fight. What we can't afford to do is have our nation crippled in the cyber fight so it's fighting blind in the clashes that follow. In fact, China's already put out a strategy like that."[33] China, however, is not the only country to worry about. Maj Gen Stephen Fogarty, head of the Army's newly created Cyber Center at Fort Gordon, Georgia, believes Russia is also better at the cyber game. In an interview, he stated, "Russian activities in Ukraine . . . really are a case study in the potential for [what Army doctrine calls] CEMA, cyber-electromagnetic activities. It's not just cyber, it's not just electronic warfare, it's not just intelligence, but it's really effective integration of all these capabilities with kinetic measures [that is, bullets and bombs, drones and tanks] to actually create the effect that their commanders want to achieve."[34] The interviewer concludes, "That Russian-style integration of cyber/electronic warfare, drones, and old-fashioned high explosive is frankly impressive. It's also something US troops don't want to be on the receiving end of, ever. The only way to ensure we aren't is to get better at integrating cyber into traditional operations ourselves."[35]

Integrating offensive cyber operations into traditional operations requires commanders understanding what cyber can provide. It requires commanders comprehending the timing and tempo of cyber operations, particularly OPE. Other nations, such as Russia, China, and Iran, clearly do not restrict their cyber operators as does the United States. In fact, they partner with nongovernment hackers to broaden their reach and also to be able to assert plausible deniability and mask their identity. Adm Michael Rogers, former commander of USCYBERCOM and former director of the National Security Agency (NSA), warned that "nation states with advanced cyber warfare capabilities are taking steps to mask their cyber attacks by cooperating with nongovernmental hackers."[36] James Lewis, a cyber expert at the Center for Strategic and International Studies, agrees that "the Russians are so good we don't usually see them. The FSB [Russian Federal Security Service] hackers do classic political espionage, and it's a tribute to their success that they got into State, DOD and White House networks last year. The frightening thing about those incidents is that it may have been practice events for new teams. They really are [our] peers in cyberspace."[37] Russian capabilities may equal ours, and they are obviously using them. Their operators are enabled, while the United States lags behind, always on the defense, reacting instead of being proactive. The DOD is currently building a cyber force of 6,200, while Russia and China have tens of thousands doing the same kind of work. While the DOD struggles to find and retain cyber operators, other nations seem resilient.

Highlighting the complex and confusing nature of cyber operations, Admiral Rogers said, "It literally probably took us two years to generate an internal consensus as to who was going to do what. . . . We've moved beyond a discussion of who ought to do what to OK, now we have clearly identified who has what responsibilities. Now let's roll up our sleeves and focus on how we're going to make this work."[38] We can make this work only if we remove the barriers that make offensive cyber operations too difficult.

First, the United States needs to reduce the approval authorities for offensive cyber operations to those commanders who are employing them, just as we do for kinetic operations. Offensive cyber operations are tools, just like kinetic options, that a commander may choose to use. To make this easier, perhaps the president or secretary of defense should preapprove a list of certain cyber capabilities to be used at the discretion of lower-level commanders and also expand the countries and areas in which they may be used. Those that fall outside of preapproved actions would still require approval, but we can speed up the request process. The United States should reconsider streamlining the RAPCO process to reduce the number of individuals involved, especially when many lack a comprehensive understanding of cyberspace. This will greatly speed up cyber operations, making them much more useful to commanders when needed. Cyberspace operations cannot continue to be held hostage to a slow, cumbersome, interagency process within which any agency that does not understand cyberspace operations can stop an operation supporting a joint force commander.

Despite the good work the NSA does, it sometimes forgets it is a DOD support agency and, as a result, does not like to collaborate and share with others, especially those who may disrupt their intelligence gathering or even appear to do so. The intelligence gain/loss is a concern, but it should not stop or hinder cyber operations. To be sure,

> Initial demands from the White House regarding cyber operations against ISIS, generated some resistance. The NSA has spent years penetrating foreign networks, placing thousands of implants in them. Those implants can also be used to manipulate data or to shut down a network. That frequently leads to a battle between the NSA civilians—who know that to make use of an implant is to

> blow its cover—and the military operators who want to strike back. NSA officials complained that once the implants were used to attack, the Islamic State militants would stop the use of a communication channel and perhaps start one that was harder to find, penetrate or de-encrypt.[39]

The nation must allow better sharing of data between agencies regarding access and mapping data of adversary networks. This would drastically reduce the time it takes to conduct OPE. We also need to educate combatant commanders and their planners about cyber operations so they understand the timeframes of cyber. It is relatively quick and easy for a joint force commander or other commanders to call for a kinetic strike, but not so for cyber. Without OPE, which takes some amount of time, cyber operations will not achieve the intended effects. Cyber operations cannot be on-call, on-demand, or on stand-by without appropriate OPE times taken into account. Cyber operations must be baked into the overall operation and planning with a clear understanding of the preparatory times required. If done correctly, offensive cyber operations can operate faster than kinetic operations either as stand-alone or preparatory to kinetic follow-on operations.

The DOD needs to pinpoint clear differences between cyber operations and kinetic operations where clear differences exist. This will avoid the clumsy and confusing misunderstanding that results with conflating them. We cannot simply treat them the same since the effects of each are different and affect different targets. The same rules can apply, but we cannot continue to apply them the same way for both cyber and kinetic operations. Most, if not all, of what the United States does in cyber falls well below the use of force/armed attack threshold, while kinetic operations are all but certain to be use of force/armed attack. Nonetheless, we continue to talk in terms of use of force and armed attack when dealing with cyber operations. It will be the rare cyber operation that actually crosses this threshold. Instead of worrying about when a cyber operation will cross that line, we should instead focus on the vast majority that do not and find ways to discuss and use them accordingly without having to engage in a LOAC analysis.

We need to delineate between true offensive cyber operations, OPE, and cyber surveillance and reconnaissance (SR) and those cyber capabilities that fall below the use of force/armed attack. Even those cyber operations that qualify as truly offensive cyber may not meet the international law definition of use of force/armed attack. We need a vigorous dialogue regarding OPE and the authorities and approvals for conducting OPE and, more recently, cyber SR. These are not true offensive cyber operations. They are access tools and mapping tools. The DOD must have a robust discussion regarding countermeasures taken in response to cyber incidents. Countermeasures are generally considered "part of the subject of reprisals not associated with armed conflict."[40] In other words, they are used against actions that fall below use of force/armed attack and are themselves below that threshold—namely, exactly what most of our adversaries are engaged in.

We must consolidate working cyber operations definitions that come from the cyber operators, cyber commanders, and their cyber lawyers, those who truly know and understand cyber operations. There are profound differences among cybercrime, cyber espionage, and cyber attack. Likewise, there are profound differences between cyber tools, cyber capabilities, and cyber weapons. It is imperative that organizations understand these differences before having a serious discussion. The type or kind of cyber intrusion dictates who responds and how. Calling everything a cyber attack does a disservice to everyone. Having a standard set of commonsense and coherent definitions allows us to more easily explain to those who are not familiar with cyber operations exactly what cyber operations can accomplish.

Finally, we need to issue or update guidance that clarifies DOD roles and responsibilities to support civil authorities in a domestic cyber incident, in accordance with the recommendations of the GAO. It is imperative in an emergency situation that we have clear guidance on who is in control and that we work through the issues in an exercise environment prior to real-world events forcing us to fumble through.

If we fail to take these actions, alternative avenues will be pursued and leave offensive cyber operations behind. In fact, this is already happening as frustrated commanders rely on relatively simple and quick kinetic solutions. Agencies are also using different authorities to accomplish the same results without having to battle the same restrictions. If faced with a choice—destroy it now via a kinetic strike or wait some days, weeks, or perhaps even months for a cyber operation to potentially achieve the same effects—it seems clear which choice commanders will make. It does not have to be this way. If the proposals discussed above are implemented, offensive cyber operations can actually begin to move at the speed of light and benefit the commanders who most need them. SSQ

Notes

[1] Brian Fung, "How Many Cyberattacks Hit The United States Last Year," *Nextgov*, 8 March 2013, http://www.nextgov.com/cybersecurity/2013/03/how-many-cyberattacks-hit-united-states-last-year/61775/.

[2] Department of Defense Cybersecurity Culture and Compliance Initiative memorandum, 30 September 2015.

[3] David Sanger, "US Cyberattacks Target ISIS in a New Line of Combat," *New York Times*, 24 April 2016, http://www.nytimes.com/2016/04/25/us/politics/us-directs-cyberweapons-at-isis-for-first-time.html.

[4] Department of Defense, *DOD Cyber Strategy*, April 2015, http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf. The purpose of this document is to guide the development of the DOD's cyber forces and strengthen our cyber defense and cyber deterrence posture.

[5] Chairman of the Joint Chiefs of Staff Manual (CJCSM) 3139.01, *Review and Approval Process*, 22 October 2013, 3–4.

[6] Office of General Counsel, Department of Defense, *Department of Defense Law of War (LOW) Manual*, June 2015, 16.1.2.1, http://www.dod.mil/dodgc/images/law_war_manual15.pdf.

[7] Ibid., 16.5.1.1.

[8] Mark Pomerleau, "Cyber Operations Come Out of the Shadows," *Cyber Defense* (web site), 5 May 2016, https://defensesystems.com/articles/2016/05/05/us-cyber-war-isis.aspx.

[9] *LOW Manual*, 16.5.3.1.

[10] Harold Hongju Koh, legal advisor, US Department of State (address, USCYBERCOM Inter-Agency Legal Conference, Fort Meade, MD, 18 September 2012).

[11] Ibid.

[12] *LOW Manual*, 16.1.2.2.

[13] Ibid., 16.1.2.2.

[14] Koh, USCYBERCOM Inter-Agency Legal Conference.

[15] Title 42, United States Code, Section 5 195c(e).

[16] Joint Publication 3-12, *Cyberspace Operations*, 5 February 2013, 11-6.

[17] Sydney J. Freedberg Jr., "Army Fights Culture Gap between Cyber and Ops: 'Dolphin Speak,'" *Breaking Defense*, 10 November 2015, http://breakingdefense.com/2015/11/army-fights-culture-gap-between-cyber-ops-dolphin-speak/.

[18] Ibid.

[19] Ibid.

[20] For the purposes of this paper, I have combined use of force and armed attack, because the United States does not acknowledge a distinction between the two.

[21] Aliya Sternstein, "Pentagon Contractors Developing Lethal Cyber Weapons," *Nextgov*, 4 November 2015, http://www.nextgov.com/cybersecurity/2015/11/lethal-virtual-weapons-real/123417/.

[22] Ibid.

[23] Sanger, "US Cyberattacks Target ISIS."

[24] Brandon Valeriano, Heather Roff, and Sean Lawson, "Stop Saying We're Dropping 'Cyber Bombs' on ISIS," *Defense One*, 24 May 2016, http://www.defenseone.com/ideas/2016/05/stop-saying-were-dropping-cyber-bombs-isis/128581/?oref=d-river.

[25] Ibid.

[26] Ibid.

[27] US Government Accountability Office, Report to Congressional Committees*, Civil Support*: *DOD Needs to Clarify Its Roles and Responsibilities for Defense Support of Civil Authorities during Cyber Incidents*, GAO-16-332 (Washington, DC: Government Accountability Office, April 2016), http://purl.fdlp.gov/GPO/gpo68065.

[28] Ibid.

[29] DOD Cyber Strategy, 2015.

[30] Mark Pomerleau, "DOD Says It's Prepared to Support Civilian Response to a Cyber attack," *Defense Systems* (web site), 25 April 2016, https://defensesystems.com/articles/2016/04/25/dod-support-response-to-domestic-cyber-attack.aspx.

[31] Ibid.

[32] *LOW Manual*, 16.5.3.1.

[33] Freedberg, "Army Fights Culture Gap."

[34] Quoted in ibid.

[35] Ibid.

[36] Bill Gertz, "China Continuing Cyber Attacks on U.S. Networks," *Washington Free Beacon*, 18 March 2016, http://freebeacon.com/national-security/china-continuing-cyber-attacks-on-u-s-networks/.

[37] Ibid.

[38] Andrew Tilghman, "Cyber Force Grows, along with Retention Concerns," *Military Times*, 16 March 2015, http://www.militarytimes.com/story/military/careers/2015/03/14/cyber-growing/70210162/.

[39] Sanger, "US Cyberattacks Target ISIS."

[40] *LOW Manual*, 18.18.1.1.

Disclaimer

The views and opinions expressed or implied in SSQ are those of the authors and are not officially sanctioned by any agency or department of the US government. We encourage you to send comments to: strategicstudiesquarterly@us.af.mil.