STRATEGIC STUDIES QUARTERLY

Overcoming the Cyber Weapons Paradox

Maj Timothy M. Goines, USAF

Abstract

To increase the effectiveness of its cyber deterrence policy, a US Department of Defense official recently called for "loud" cyber weapons: cyber weapons that could be easily discovered and traced to the United States. These weapons, if employed, could offer unique advantages for US deterrence policy. However, the prospect of employing cyber weapons creates a paradox between overt factors of deterrence and the covert nature of offensive cyber operations—and the paradox of cyber weapons themselves. The current processes in place for using cyber weapons are not adequate to ensure such employment avoids the cyber-weapons paradox. A better process is to use interagency coordination that provides for a whole-of-government approach. The results of this evaluation demonstrate that, by using an interagency coordination process, the United States will be better positioned to employ an effective cyber deterrence policy.

✳ ✳ ✳ ✳ ✳

With thousands of malicious cyber acts occurring daily, the United States appears to be rather unsuccessful at deterring bad actors from attempting to infiltrate its networks and do damage.[1] For example, the Department of Defense (DOD) reported in 2008 that it was probed hundreds of thousands of times each day, and the problem has only grown.[2] One reason for the lack of success stems in part from the covert nature of cyber operations.[3] Under current policy, US cyber operations are highly classified; operations may be conducted in response to cyber acts, but the operations and the specific actor are obscured. Recently,

Maj Timothy M. Goines serves as an assistant professor of law, at the US Air Force Academy, Colorado Springs, Colorado. He is a judge advocate and has earned a master of arts degree from the Air Command and Staff College in 2017 as well as a master of laws degree from the University of Nebraska in 2016.

however, the commander of US Cyber Command (USCYBERCOM) stated the command is looking for attributable or "loud" cyber weapons that can be used by the DOD and definitively traced to the US military. As proposed, when using these new cyber weapons, the United States would not obscure the operation or actor from being discovered by the victim and attributed to the United States. It would broadcast US use of cyber weapons, making them easily discoverable. The logic is that by using loud cyber weapons, the United States gains a deterrent advantage. First, it allows the United States to signal its intent to defend specified domestic assets and its willingness to engage in aggressive cyber operations against an adversary.[4] Second, it informs the cyber adversary of US cyber capabilities—something that is suspected but not known. Finally, it increases the credibility of the US deterrence program by demonstrating that the United States is capable and committed to responding to malicious cyber acts. Upon consideration, this appears to be a rather simple and effective solution to the current problems with US cyber deterrence policy. Making cyber weapon use easily discoverable and allowing actors to trace the use back to the United States will open a line of communication, albeit rather indirect. Nevertheless, this line of communication allows the United States to indicate which targets it is willing to defend as well as its capabilities, its commitment, and the credibility of its future threats. In other words, this solution meets the requirements of deterrence, allowing the United States to communicate its system of rules and signal its commitment and credibility in the cyber environment.

However, two US government communities concurrently conduct cyber operations: the intelligence community and the DOD. These two communities have complementary capabilities, resources, and staff but often conflict with each other because of exclusive planning, unknown vulnerabilities or exploits, uncoordinated timing, and detrimental targeting. As the DOD starts to employ loud cyber weapons, these operations could render future missions ineffective or substantially degraded. While some overt offensive cyber use adds to deterrence, at the same time it creates a sort of cyber weapons paradox between overt cyber deterrence and covert cyber usefulness because any overt use can render the weapon useless. The paradox also exists because of the nature of cyber weapons themselves.

In addressing the paradox, this article explores the following question: How can the United States most effectively employ offensive cyber weapons to achieve maximum deterrent effect without foreclosing the US ability to conduct covert offensive cyber operations? The article begins by defining deterrence and discussing the essential factors for effective cyber deterrence. Next it analyzes the paradox that emerges within current offensive cyber processes and the existence of a paradox within cyber weapons themselves. Following this, the article proposes overcoming the cyber weapons paradox through interagency working groups that focus on prioritizing cyber weapons.

Unfortunately, the employment of these weapons raises a slew of other concerns. First, there are policy concerns. For example, what are the potential consequences of using these weapons? If employed against certain actors, what are their likely responses? Does responding to these actions result in the escalation of conflict? If so, is that advisable? What would the threshold be for potential responses? Is the United States willing to accept these potential responses? By revealing its hand, the United States exposes itself to scrutiny from the international community and potential cyber responses from the actor. Given the significant policy considerations, this article cannot adequately address and resolve them all. Instead, it assesses the more practical concerns associated with employing attributable cyber weapons—specifically, the paradox that results from loud versus covert and used versus useless cyber weapons.

Essentials of Cyber Deterrence

A thorough history and analysis of deterrence theory is provided by deterrence scholars Alexander L. George and Richard Smoke.[5] They have noted that deterrence theory traces its roots back to Thucydides and the Peloponnesian War, but its most significant employment was far later, during the Cold War between the United States and the Soviet Union. As both parties attempted to avoid a nuclear war during this period, many theorists studied deterrence theory in its various forms: strategic (thermonuclear), limited, and "sublimited" deterrence.[6] From these studies, deterrence theory across all forms was reduced to a goal of affecting the decision-making calculus in the mind of the actor: "In its simplest form, deterrence is merely a contingent threat: 'If you do x I shall do y to you.' If the opponent expects the costs of y to be greater than the benefits of x, he will refrain from doing [x]; he is deterred."[7]

While the practice of deterrence is rarely this simple, the heart of the theory is logically sound. If the potential costs of a particular action outweigh the potential benefits of that action, the actor should rationally choose not to pursue that action. More accurately, if the actors believe the deterring state will defend itself and the actors believe the costs of such a response will exceed the benefits of their proposed action, they will not conduct the action.[8] Thus, the goal of any viable deterrence policy should be to raise the credibility of the potential response. From this, we can extract important requirements of a successful deterrence policy.

Rules, Signals, Commitment, and Credibility

The deterring state must develop a clear policy that contemplates qualifying actions (such as threshold questions), qualifying targets, qualifying actors, and the corresponding responses, which this article will term a *system of rules*.[9] By developing these rules, the deterring state fully forms its intent to protect certain aspects of the nation (such as national infrastructure, institutions, and territory) and develops the corresponding responses to any of these threats. Nuclear deterrence is a prime example, whereby the United States declared that any launch of a nuclear weapon by an adversary would result in a retaliatory strike.

After a system of rules is created, the rules must be communicated to the actor to be deterred; if that actor does not know about the potential consequences, the actor is not likely to change his actions.[10] This is commonly completed through *signaling*, where the deterring state declares its intent and the consequent actions.[11] For example, in conventional operations, if states want to deter an adversary from invading their territory, they can "signal" their intent to resist an invasion by amassing troops along the border. Similarly, if states want to demonstrate their global reach, they may send naval squadrons to a particular area.

Next, the deterring states must be *committed* to carrying out their prescribed consequences.[12] If deterring states are or appear unable or unwilling to employ their system of rules, they would do little to impact the decision calculus of the other actor. With nuclear deterrence example, if the United States were unwilling to resort to nuclear war, adversaries would not be affected by the threat of a strike. Similarly, if the United States were incapable of launching a retaliatory strike (due to monetary or deployment constraints), the adversary would not likely be deterred. Thus, this requirement has two components: the state must

have the will to employ the system of rules, and it must also have the "acquisition and deployment of capacities to back up the intent."[13]

Finally, the deterrence policy, as a whole, must be *credible*.[14] This requirement is related to both the commitment by the deterring states and the capability of the deterring states to carry out the actions within their system of rules. For example, if the response threat were (or appeared to be) outlandish or unreasonable, an adversary would likely not believe the potential threat and likely not be deterred.

It is important to note that the general goal is to deter, but this is by no means an all-or-nothing theory; in other words, deterrence theory considers that it may succeed at times and it may fail at times.[15] This especially applies in the cyber environment, where deterrence of every malicious cyber act is an unrealistic goal. Although this might seem to be a drawback with deterrence strategy, it is not exclusive to deterrence—after all, military operations can and do fail, as do other political attempts. Thus the goal of any deterrence policy should be to designate actions we want to deter and then coordinate operations to maximize our ability to deter those acts.

From general deterrence theory, the United States has formulated its deterrence policy. The most recent version was articulated in the 2006 publication *Deterrence Ops, Joint Operating Concept, Version 2.0.*[16] More recently, in 2015, the *DOD Cyber Strategy* was issued, which also addresses deterrence (specifically, cyber deterrence) and reinforces the concepts in *Deterrence Ops*.[17]

The stated goal of the DOD deterrence policy is "to decisively influence the adversary's decision-making calculus in order to prevent hostile actions against US vital interests."[18] As such, an adversary's decision-making calculus consists of weighing three factors: (1) the benefits of a course of action, (2) the costs of a course of action, and (3) the implications of restraint.[19] Deterrence operations, therefore, seek to affect adversary decision-making calculus by providing the basic framework for all deterrence operations to build upon, including cyber deterrence.

Denying Benefits

The first way to deter an adversary is by denying the benefits of a course of action. In the cyber domain, the primary method through which a state denies benefits is through a robust and effective cybersecurity system, reducing the number of vulnerabilities within its network and

preventing infiltration and exploitation. This method of denying benefits is a purely defensive operation.[20] As a result, this article will not discuss denying benefits in great detail since its primary focus is offensive cyber operations, which are more appropriately categorized under cost imposition and encouraging adversary restraint.

Imposing Costs

The second way to deter an adversary is to credibly threaten to impose costs as a consequence of an aggressive cyber act. Examples of cost imposition range from criminal prosecution to offensive cyber operations to conventional military operations.[21] It is worth highlighting the distinction between cost imposition and the threat of cost imposition. In essence, once costs have to be imposed, the act has occurred and deterrence has failed. Therefore, the goal of a deterrence strategy should be to effectively threaten cost imposition such that an actor chooses not to engage in the act in the first place. DOD policy reflects this logic, stating one of its goals is "to declare or display effective *response* capabilities to deter an adversary from initiating an attack" (emphasis in original).[22]

Implications of Restraint

The third and final way to deter an adversary—to encourage restraint—is accomplished primarily through voluntary agreements to restrain, such as multilateral and bilateral agreements in the form of arms control treaties or conventions. For example, in September 2015, the United States and China agreed to stop all economic espionage in cyberspace against one another.[23] While this effort has been somewhat successful, most efforts have been rather unsuccessful at achieving adversary restraint.[24] Fortunately, a state looking to deter actors can also encourage restraint through general deterrence, demonstrating its ability to deny benefits (through defensive operations) and impose costs (through offensive operations) by interacting with other countries. Upon seeing the capability of the deterring state, an adversary is more likely to see a greater benefit and less cost in *not* attempting a cyber act against the deterring state.

Underlying this DOD deterrence policy is the concept (borrowed from deterrence theory) that the decision to act is made by individuals based on their perception of these factors, given their values and perceived probabilities of alternate outcomes.[25] So the DOD's policy recognizes

that deterrence is not a one-size-fits-all approach; to be effective, it must be tailored to specific adversaries within their specific contexts.[26] For example, knowing why an actor carried out a cyber act offers insight into its decision-making calculus (motive and what it stands to lose or gain from an act) and can help in creating an effective deterrence strategy, whether criminal prosecution or responding with offensive cyber operations is more appropriate.[27]

The Paradox of Cyber Processes

As with most things relating to cyber operations, the current US government process used to approve offensive cyber operations is classified. While the unclassified instruction Joint Publication (JP) 3-12, *Cyberspace Operations*, does provide general information on the employment of offensive cyber operations, it fails to provide much, if any, description of the current process for employment and approval.[28] JP 3-12 discusses the employment of offensive cyber operations, where it highlights valid concerns including transregional effects, conflict probability, and foreign policy implications.[29] Unfortunately, it does not specify how to account for these concerns within an established process. Instead, it appears to endorse an ad hoc approach, requiring initiation, planning, coordinating, deconflicting, and executing each operation, one at a time. This requires any offensive cyber operation to start from ground zero instead of being able to use an established process.

Beyond that, there is very little description of the approval process for offensive cyber operations. The lone reference to any approval process simply states that approval for offensive cyber operations requires "national level approval."[30] What can reasonably be assumed is that "national level approval" requires authority beyond the hierarchy of any one US agency (the DOD, the National Security Agency [NSA], the Department of Justice [DOJ], the Department of Homeland Security [DHS]). This would likely put the approval level at the National Security Council (NSC), the president, or vice president.

Although more information is likely contained within classified documents, there is no evidence that it extends beyond an ad hoc nature and the approval authority is at the "national level." For example, there is no evidence of an established interagency process within the NSC or outside of it. In fact, JP 3-12 is a DOD-specific instruction and only applies to DOD operations. Furthermore, given the covert nature of

cyber operations and the historical desire to keep operations classified, having a process that crosses multiple agencies, especially when it comes to the employment of offensive cyber operations, is not likely to exist.

Therefore, given the limited access to classified information, it is a reasonable assumption that the current process to approve and employ offensive cyber operations begins solely within the DOD, funneled through the secretary of defense, and approved by someone at the national level.[31] When evaluated under the specific factors outlined earlier, there are a number of concerns with this process.

Limited Visibility of Other Operations

With national-level approval, the current process allows offensive cyber operations to be a smaller piece in the larger deterrence policy. Unfortunately, the responsibility to assess the effectiveness of every operation falls on the DOD chain of command and the national level approval authority, without the assistance of knowledgeable outside organizations, experts, and technicians. This is a significant stress on the process, since the responsibility of maximizing each offensive operation's deterrent effect is left to one authority.

Second (and related to the first concern since it originates solely within the DOD community), the particular vulnerability and exploit are not vetted through each organization for past use, current use, or potential future use. It is highly unlikely that the single national-level approval authority would know each vulnerability and exploit previously, currently, and intended to be employed by all the disparate agencies with cyber capabilities. Furthermore, it is even more unlikely that the national-level authority would have a system in place to consult with these organizations, consolidate the vulnerabilities and exploits in a unified database, and set rules and priorities for their employment. The likely consequence is that, unless the authority is informed of other operations, he or she is likely to approve an offensive cyber operation that could conflict with current or future operations.

No Whole-of-Government Approach

The current process also does not use a whole-of-government approach. There are a number of agencies that either possess or could easily possess offensive cyber capabilities, for instance USCYBERCOM, the NSA, the DOJ, and the Central Intelligence Agency. Each has access

to certain vulnerabilities and exploits, and each has a mission they are attempting to accomplish. Currently, these agencies do not work in concert. Instead, they are segregated from one another to ensure the secrecy of their operations. These disparate missions likely contribute to the paradox.

Moreover, cyber threats come from various types of individuals, including state actors, state-sponsored actors, organized criminal groups, individual hackers, and extremist groups with radical ideologies. Each of these actors can and must be deterred in different ways, through different mechanisms. Achieving deterrence is not exclusive to offensive cyber operations. Rather, a cyber operation is just one of many possible alternatives for a deterring state; other options include criminal prosecution, sanctions, public condemnation, and conventional military operations. Each of these alternatives can be effective at deterring future actors, depending on the circumstances.

As noted above, offensive cyber operations originate solely within the DOD and its chain of command. They are only elevated beyond the DOD when they are seeking approval to conduct the specific cyber operation on the specific target. Not only does this result in a lack of vetting the specific cyber vulnerabilities and exploits with other cyber-capable agencies, but it also does not consider other response options from other agencies. It is conceivable that an offensive cyber operation could be used where prosecution of a conventional military operation would have a greater deterrent effect.

From a practical perspective, it is not likely that the DOD self-initiates the process for employing an offensive cyber operation in response to a cyber act. Rather, it is more likely that the national-level authority requests a proposed offensive cyber operation when weighing all the response options. Unfortunately, much like the vetting process, this puts a significant strain on the approval authority to determine which action is likely to be the most effective, especially considering the various political factors. This is aggravated by the ad hoc nature of the current process.

Slow Decision Timelines

Under the current process, when a cyber response is desired, an offensive cyber operation is planned, reviewed, and elevated throughout the DOD. This process likely includes reviews for viability, legality, conflict escalation, and policy concerns. It is then sent forward to the national-

level authority for consideration. This process, like any process requiring multiple reviews within multiple layers of bureaucracy, takes time. Also, because each offensive cyber operation must start from ground zero, unfamiliarity with the process can produce unnecessary delays. As a result, the ad hoc nature of the current process can produce slow operation timelines, leaving more time for the adversary to find and patch vulnerabilities.

Stress on Decision Maker

With the designation of the national-level authority for the approval of offensive cyber operations, there appears to be a single authority deciding which vulnerabilities and exploits to employ for which purpose. As noted with the previous factors, the current process puts a tremendous amount of strain on the decision maker. This is due to the lack of a vetting process, the lack of a whole-of-government approach, and the ad hoc nature of the current approval process. As a result, even though a final authority is designated, the process does not have the intended effect of creating a cooperative environment and avoiding the potential for multiple agencies employing the same cyber weapon for two different purposes.

For these reasons, the current processes for offensive cyber operations are not adequate to ensure their employment is conducted to avoid the paradox and mission conflict. This situation creates problems for the use of loud cyber weapons—which are paradoxical themselves.

The Paradox of Cyber Weapons

Before discussing the paradox inherent in cyber weapons, it is important to first consider some of the unique aspects of cyber weapons that undergird the paradox.

Perishability and Obsolescence

Cyber weapons (both attributable and covert) are perishable and rendered obsolete over time. A cyber operation is composed of two parts, a vulnerability and an exploit. A vulnerability is a "weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source."[32] The

prototypical example of a vulnerability is a zero-day vulnerability, which is a hole in the software that is unknown to the author.[33]

The upside with vulnerabilities is that the operator of the system is unaware of them, providing another actor the ability to access their system. The downside is that, once the vulnerabilities are discovered, they are often fixed by the vendor, manufacturer, or owner quickly. For example, Microsoft has historically released security patches to fix holes in its Windows Operating System (OS) on the second Tuesday of each month.[34] So, a vulnerability has a window from the time it is known to a potential actor to when it is discovered and fixed by the operator. Using the Windows OS schedule as an example, a vulnerability could be fixed in as little as 30 days after its discovery; the time could be longer or shorter depending on a number of factors (the nature of the vulnerability, how prevalent it is, and so forth). The greatest factor in determining a vulnerability's lifetime is discovery. The longer it can remain undiscovered, the longer an actor can exploit it.

Vulnerabilities are discovered through self-initiated examinations, through notices from government or cybersecurity organizations (such as the United States Computer Emergency Readiness Team or the Symantec Corporation), or in response to an exploit. Thus vulnerabilities suffer from perishability (fixed once discovered through its use with an exploit) and obsolescence (fixed once discovered by self-initiated examinations or discovery by other organizations).[35]

Exploits are "operations [or] intelligence collection capabilities conducted . . . to gather data from target or adversary information systems or networks."[36] Essentially, the exploit is the code, worm, virus, or Trojan horse that is inserted via the vulnerability to do damage, collect information, or complete another operation. Perhaps the most famous example of this is the Stuxnet worm, which was inserted into the Iranian nuclear material enrichment facility and caused many of the centrifuges to spin out of control.[37]

Similarly to vulnerabilities, exploits also suffer from perishability and obsolescence; once they are used, the operator can develop a patch that can render the exploit ineffective (although this is less effective than patching the vulnerability). For example, once Stuxnet was discovered, the author of the targeted devices' OS developed a patch that rendered the code useless.[38] Additionally, certain exploits can be rendered ineffective if they are sophisticated, only becoming active once specific condi-

tions exist. For example, Stuxnet depended on the specific conditions to exist (a certain version of the OS, a certain type of logic controller, and a certain type of centrifuge).[39] This was a positive thing, since it limited the impact it would have on other computers if it propagated outside of the nuclear facility. However, the negative of this was that, if any of these conditions changed, Stuxnet would have been rendered useless.

Reusability and Forensic Data

Another attribute of an exploit that can lead to problems is that, once discovered, exploits can be replicated and forensically studied. Once the "code" is out in the world, nothing can be done to erase or destroy it. This leads to two potential problems. First, any discovered exploit could be studied, modified, and then used again, potentially against the creator. For example, Stuxnet was a very sophisticated exploit with thousands of lines of code.[40] Once discovered, Stuxnet was widely distributed throughout the internet, allowing many to study its tactics and its ability to avoid detection.[41] It has since been replicated hundreds of times, possibly serving as the foundation for many new cyber weapons.[42] Granted, many of these variants would likely be ineffective given the widespread knowledge of Stuxnet's code, but many devices may remain vulnerable to its methods. In any event, cyber operators must be cognizant of the reusability of cyber exploits before employing certain code within an attributed cyber weapon.

Second, any discovered exploit can be studied and compared to other exploits for similarities in methods and organization. This may lead to the conclusion that two exploits came from the same organization. For example, Stuxnet was studied extensively by many organizations around the world. Within the code, information was discovered that allegedly tied Stuxnet to certain countries, although no one has officially confirmed these suspicions.[43]

This particular attribute of cyber weapons can be disastrous for cyber operations—each discovered cyber weapon gives the target forensic evidence that can expose other (more covert) operations. Consequently, any misuse of these vulnerabilities and exploits could result in either the DOD or intelligence community (IC) compromising the effectiveness of the other. For example, if the DOD deployed a cyber weapon that exploited a vulnerability that the IC was using for intelligence gathering, the vulnerability could be fixed quickly by the target, and the IC's operation

would be degraded. Similarly, if the IC developed an exploit and it was discovered, the target could adapt its system to be immune from future exploits of this nature. In another scenario, the DOD could develop an exploit and deploy it, and once discovered, it could bear similarities to other covert operations by the IC. This could link the two operations and expose covert operations to the international community.

As the DOD starts to employ attributable cyber weapons, it is easy to imagine how its operations could conflict with those of the intelligence community, rendering one or both of the missions ineffective. Fortunately, it does not appear that this paradox as played out has resulted in any disastrous effects thus far. However, as loud cyber weapons are employed more frequently, the potential for these operations to conflict increases. Thus, the United States should anticipate the potential problems and be proactive in overcoming the paradox.

Perishability and obsolescence make deployment of cyber weapons unlike that of other weapons in the US arsenal. Once a vulnerability or exploit is used, future use is foreclosed; however, waiting too long to use a vulnerability or exploit provides the target time and opportunity to discover the flaws, also resulting in the foreclosure of its future use. Thus, offensive cyber operations must strike a balance between waiting for the best opportunity to employ a particular weapon and not waiting too long such that the exploit or vulnerability is rendered obsolete.[44]

The problem this paradox poses is made more significant by the fact that the number of vulnerabilities and exploits are somewhat limited. While these are theoretically unlimited (a computer system is manmade, so it will likely never be without a flaw, and there are always creative ways to code an exploit), the discovery of vulnerabilities and development of exploits is increasingly expensive. Accordingly, available vulnerabilities and exploits must be closely guarded and cautiously used.

The large majority of cyber operations conducted by the United States are classified. Therefore, the following discussion is limited to the unclassified information available. As detailed below, however, this does not detract from the conclusions. Instead, the covert nature of US cyber operations hits on a major problem for cyber deterrence: the inability to communicate the deterrence policy. This inability prevents the United States from communicating its system of rules, signaling, and commitment—all necessary for effective deterrence.

Lack of a Clear System of Rules

While current US deterrence policy does specifically identify certain protected targets, it leaves ample ambiguity surrounding potentially protected targets.[45] While this may appear to allow leeway as technology changes and the protected targets shift, it works both ways. The potential actors are unclear as to what targets will generate a response and what targets will not. What qualifies as the "DOD network" and "DOD data"? Since the majority of DOD traffic flows over civilian networks, where does the United States draw the line between the civilian network and the DOD network?[46]

Perhaps in an effort to clear up some of this confusion, in July 2016, President Obama approved a Presidential Policy Directive (PPD), which directly addressed the federal government's classification and response to cyber acts.[47] Along with this PPD, the president also released a Cyber Incident Severity Schema (CISS), which identified "targets" and sought to establish a framework through which the severity of cyber incidents would be classified.[48] Identified targets include critical infrastructure, national security, public health, civil liberties, and the lives of US persons. Unfortunately, the CISS did little to clear up the confusion. What qualifies as an act targeting US national security, critical infrastructure, or civil liberties? If it is unclear to those who execute the PPD, it is definitely unclear to potential foreign actors who lack familiarity with US culture and internal operations.

While in certain categories of deterrence ambiguity can be a benefit, this is not necessarily the case in cyber operations. For example, in nuclear deterrence, being unclear as to what targets would provoke a retaliatory strike has been beneficial. A nuclear strike is on the highest end of the escalation ladder, so the prospective response is extreme. A potential adversary would not want to chance a debilitating retaliatory strike to see whether the United States would respond. Instead, the adversary would avoid any action that may provoke a response. In cyber operations, this relationship is reversed: cyber operations are on the lower end of the escalation ladder, so a prospective response would also be low. Given this scenario, adversaries are more willing to "poke and prod" US networks to determine what they can do and what provokes a US response; the worst response is still very low on the escalation ladder. Thus, ambiguity in what would provoke a response ostensibly serves to tempt adversaries to probe US networks and see where the United States will draw the line.

The more clearly the United States defines what will generate a response and draw the line proactively, the less likely an adversary will be tempted to test the waters. Until the United States develops a comprehensive system of rules, the confusion that results only reduces the effectiveness of the current deterrence policy.

Also, the current DOD policy completely ignores civilian targets and civilian infrastructure. The CISS attempts to include some civilian aspects, but they are framed in vague generalizations. While the reluctance to incorporate specific civilian targets under the umbrella of already overworked DOD cyber operators is understandable, their exclusion is noteworthy. If anything, the absence of specific civilian targets creates confusion over what targets would generate a response and what targets would not.

Inability to Signal

Signaling is the method by which deterring states communicate their intent to defend certain targets or areas.[49] In conventional operations, the United States communicates its intent to defend a particular target and expresses a commitment to the defense with a show of force, lending credibility to the threat. However, with the covert nature of cyber operations, the United States is unable to signal potential actors. Consequently, the United States does not effectively communicate which targets it is committed to defend and the credibility of its potential response is not confirmed, at least not in any meaningful way. Furthermore, even if adversaries suspect certain capabilities and assume that a target is one that the United States will defend, they do not know what actions will result in a US response.

Unacknowledged Responses

Moreover, the covert nature of operations prevents effective communication after an offensive cyber act. Even if the United States responds with an effective cyber operation, the target of the response may not discover the response and, if discovered, may never know that the United States was the responsible party. This is another area where cyber deterrence contrasts significantly with nuclear deterrence. In nuclear deterrence, not only would a response be easily recognizable (e.g., a launched missile), but the source of the response would also be easily identifiable.

However, in cyber operations, there is considerable ambiguity, and the ambiguity actually hurts the effectiveness of deterrence. Many adversaries may suspect the United States could and would respond, but they may not be able to confirm the response or the source. This can be a lost opportunity, where an adversary is left with the perception that he "got away with it." That perception can render a deterrence policy wholly ineffective.

To be fair, there are certainly scenarios where the United States may prefer ambiguity or to mask the source of the operation. For example, US operators may desire to monitor the actor's activities for intelligence-gathering purposes or to prevent confirmation of the source of the response. However, it must be acknowledged that these types of operations have little to no deterrent effect; if an actor does not know of the monitoring or the source of the response, it is very unlikely to impact his decision-making calculus—the primary goal of deterrence.

Another side effect of this ambiguity is that it puts too much power into the hands of potential adversaries. As an adversary "pokes and prods" US networks and as the United States seemingly ignores those actions, the adversary continues to push the boundary. If the United States has not clearly articulated its system of rules (and communicated them), this can actually allow the adversary to define the threshold for a response. In other words, until the United States draws a line in the sand, the adversary is empowered to do so—to the detriment of US interests.

Overcoming the Cyber Weapons Paradox

Overcoming the cyber weapons paradox means balancing a number of factors relating to cyber operations and national security. Any process or system employed to overcome the paradox must be empowered to work within the existing national deterrence framework in two ways. First, it will necessarily be a smaller piece of a larger deterrence policy that meets the characteristics of deterrence: rules, signals, commitment, and credibility. Obviously, as framed here, the paradox specifically addresses offensive cyber operations with the advent of attribution, which is a narrow issue in relation to a national deterrence policy. While this article does not specifically address the larger deterrence policy, it recognizes the need that any proposed solution must work within it. Determining when to employ one of the many different options should be the main responsibility of the larger deterrence policy, which high-

lights the need for a whole-of-government approach in that component as well. But, more specifically for the purposes of this article, any process or system must funnel its work product into the larger deterrence policy to inform it of the potential offensive cyber responses available for each situation. Additionally, there must be a final authority to make the decision on what response to employ in every scenario. This decision maker is critical for offensive cyber weapons, where it is important to have a single authority deciding which weapons to employ for which purpose. Channeling this decision to a single authority creates a cooperative environment and avoids the potential for multiple agencies employing the same cyber weapon for two different purposes.

Second, the process or system must be given the necessary authority and scope to manage offensive cyber operations in a manner that maximizes their effectiveness. This authority must include the authority over US government organizations that possess cyber capabilities or authorities (IC, DOD, DOJ, DOS, and DHS). In other words, the process or system must have the authority to gather the various vulnerabilities and exploits across all relevant organizations and set the rules for their employment, by which these organizations must abide. This authority should be distinguished from the decision maker having the power to authorize the employment of an offensive cyber weapon, which is not a prerequisite for overcoming the paradox. Rather, the process or system is only required to consult with US government organizations regarding offensive cyber weapons, consolidate these weapons in a unified database, and set binding rules and priorities for their employment. Without this authority, the prioritization serves as guidance, which can seemingly be ignored and produce the very paradox it is meant to prevent. The process must also recognize time is a significant factor in cyber operations where some vulnerabilities only last 30 days. Therefore, overcoming the paradox requires a process or system that accounts for time, using a streamlined process that minimizes the time from discovery of the vulnerability or exploit to its employment.

Proposed Interagency Working Groups

The approach to overcome the paradox requires establishing two interagency working groups.[50] The first will be the cyber interagency working group (CIWG) comprising the government agencies with cyber capabilities. Membership of the group would include all government agencies

with cyber capabilities, both offensive and defensive; this membership will ensure all past, present, and future operations are considered. This interagency working group will have the mission to consolidate all the known vulnerabilities and exploits into a unified list and set rules and priorities for their employment. It will also have the authority to require compliance with the rules and priorities they determine.

Given the disparate nature of the missions of the organizations in the CIWG, a lead agency should be appointed to ensure that progress is made at a sufficient rate. USCYBERCOM is currently delegated responsibility for planning and conducting cyber operations for the DOD.[51] Due to the significant role it plays in US cyber operations, the lead agency for the CIWG should be USCYBERCOM.

It should be noted that private technical (tech) companies are not included as members of the CIWG. While having private tech companies participate in the consolidation and prioritization process would appear to be an advantage due to their technical capabilities, their participation would create a conflict of interest. Private companies aspire to create software that is secure from potential penetration by hackers and other governments. In addition, they currently sell their software worldwide, to allies and adversaries. By disclosing the known vulnerabilities in their software and the potential exploits to these civilian tech companies, we would create a potential conflict of interest, whereby these companies would be tempted, if not obligated by their shareholders, to find and fix the vulnerabilities as soon as possible.

The concern was recently highlighted by the president of Microsoft, Brad Smith, who declared that civilian tech companies should proclaim their neutrality in the cyberspace battlefield.[52] A neutral party would clearly not endeavor to assist any government in finding vulnerabilities and developing exploits. Furthermore, as Smith added, private tech companies must be committed to "100% defense and zero percent offense."[53] Therefore, it appears that at least some tech companies recognize this conflict of interest and do not wish to participate in planning or executing offensive operations.

To ensure the effectiveness of larger deterrence policy, the second interagency working group will be the deterrence interagency working group (DIWG). This deterrence working group will serve as a component of the NSC, be responsible for assembling the various agencies that can impose costs on cyber adversaries, and advise the NSC on the courses

of action that maximize the deterrent effect. The CIWG would be subordinate to the DIWG. A representative from the cyber working group would participate in discussions of cyber policy and serve as the subject-matter expert within the DIWG.

The placement of the sub-working group under the DIWG may appear to limit its deconfliction responsibilities and usefulness to deterrence purposes only; however, loud cyber weapons have utility outside of deterrence effects. Therefore, while the sub-working group is placed under the DIWG, it will provide deconfliction services for all cyber operations, including covert cyber operations. Given that the majority of loud cyber operations will be for deterrence purposes, the placement under the DIWG provides the most logical supervisory structure.

Once again, given the disparate nature of the missions of DIWG members, a lead agency should be appointed. The DHS is an executive agency with the mission to "ensure a homeland that is safe, secure, and resilient against terrorism and other hazards."[54] This mission specifically includes preventing terrorism, enhancing security, and securing cyberspace.[55] Considering the effects that cyber acts have on the United States and its citizens, the lead agency for this larger working group should be DHS. However, the final authority for any action taken would be the NSC.

Practically, the process would begin with the sub-working group, which would be a standing committee, meeting regularly to discuss, consolidate, and prioritize cyber vulnerabilities and exploits. As individual vulnerabilities and exploits are employed, perish, or are rendered obsolete, the list would be updated to account for the changes. Given the nature of cyber operations, this would likely be a continuous process. In the event an act occurred, the proposed DIWG would determine what response would provide the maximum deterrent effect, consulting the representative of the cyber sub-working group for potential options. If the best course of action is a cyber response, the representative from the cyber sub-working group would reference the current list of priorities and designate a vulnerability and exploit for employment. When evaluated under the specific criteria outlined above, these working groups offer a number of benefits for overcoming the cyber weapons paradox.

Benefits of the Integrated Working Groups

With the DIWG serving as an advisor to the NSC, it would be empowered to advise on the response that would result in the greatest

deterrence effect. As a component of the DIWG, the sub-working group on cyber operations would similarly be empowered. It would have the necessary authority and scope to manage offensive cyber operations in a manner to maximize their effectiveness. Part of this empowerment would come from the sub-working group's position within the NSC and the authority given by the president; the other part would come from the fact that all the cyber-capable agencies would be members and part of the prioritization process. So, not only would the agencies be required to follow the prioritization scheme, but they would also be shareholders of the process.

The DIWG and the sub-working group on cyber would both be made up of agencies that have parts to play in the larger deterrence policy and cyber capabilities. These agencies include the DOD, DOJ, DOS, NSA, and DHS—all agencies that can offer the NSC response options. For the DIWG, these agencies can work together; sort through the various options, consequences, and policy limitations; and select the most appropriate response option to maximize deterrence. This process helps provide comprehensive advice to the NSC and ensures all options are appropriately considered.

A similar construct would exist for the sub-working group on cyber. It would be made up of similar agencies, but the membership would largely be the technical experts within these agencies. By working together to prioritize the various cyber vulnerabilities and exploits, the working group ensures that each vulnerability or exploit is used discriminately, ensuring that loud operations do not conflict with current or future operations or expose covert options. In addition, the prioritization ensures that each cyber vulnerability and exploit is used in the most effective way.

As proposed, the CIWG will be a standing committee, meeting regularly to consolidate, prioritize, re-prioritize, develop, and designate cyber weapons for employment. Given the membership and the organization of the sub-working group, this proposal appears to add a layer (or layers) of bureaucracy, which can potentially lead to delay. However, as proposed, this sub-group employs two mechanisms to avoid delay. First, it appoints a lead agency, USCYBERCOM, to consolidate and prioritize the process. This gives the NSC and the larger DIWG a designated agency to assign duties and define timelines, ensuring the process is accomplished in a timely manner.

Second, instead of an ad hoc arrangement, the CIWG meets well before a cyber act occurs and continually prioritizes available cyber responses. Once a malicious cyber act occurs, the prioritized list allows the DIWG to review and select a cyber response in a timely manner. This greatly reduces the likelihood that a vulnerability or exploit will be kept past the window of usability. Also, by speeding up the timeline between approval and execution, the US signals "this action and others like it will not be tolerated."

The final authority for the employment of all cyber weapons would be the NSC. Positioning the DIWG as a component of the NSC and utilizing a whole-of-government approach alleviates some of significant strain on the final authority to account for the numerous variables within foreign relations. Instead of relying on the final authority to consider the numerous factors at play, this process allows the final authority to consult with the DIWG, consider the guidance, and make the final call.

Drawbacks and Limitations

While the interagency process provides for an improved practice, certain drawbacks exist. For example, anytime a number of different agencies with disparate missions and unique cultures attempt to work together, the likelihood of disagreement is high, which can introduce deadlock and delay. Additionally, there will be an initial period when the member agencies adjust to the procedure and the proposed hierarchy. However, the goal of the proposed process is not to design cyber operations by committee; rather, the goal is to foster a collaborative environment for all agencies to have a voice in the selection and employment of offensive cyber operations. Unfortunately, this requires the various agencies to buy in to the process and cede some of their power and independence. Therefore, the proposed process may suffer from an initial lack of cooperation and collaboration.

Another limitation with the proposed interagency process is that it exposes US cyber operations to more vulnerabilities—specifically, human vulnerabilities. Those who have access to the system with certain privileges or those who know of US cyber operations are vulnerable to exploitation. For example, a malicious cyber actor can access information on a particular person, which can be used as threats or other tactics to gain intelligence about potential cyber operations. Under the current

process, the covert nature of cyber operations reduces the number of people with access, thereby reducing the number of human vulnerabilities.

Another limitation is the vulnerabilities equities process (VEP), a classified procedure by which the US government determines when to publicly disclose discovered software and hardware vulnerabilities.[56] Some of the documents detailing the process were made public in 2010 in response to a Freedom of Information Act lawsuit.[57] In short, the VEP has existed within the US government, in some form, since 2008; it also went through a "reinvigoration" in 2014, when the administration made some changes to the process. The goal of the VEP is to identify vulnerabilities and then determine whether to share them with the US public for their security or to retain the vulnerability for offensive use. Unfortunately, the VEP has been a source of frustration for both civil liberty groups arguing that the US government should disclose all known vulnerabilities and government agencies arguing that the VEP serves to frustrate cyber operations.

The interagency process proposed in this article is not a substitute for the VEP. Instead, the interagency working group would work in concert with the VEP. In this regard, the proposed interagency process differs from the VEP in two significant ways. First, the VEP focuses on the disclosure or retention of vulnerabilities. On the contrary, the interagency working group does not consider the disclosure of vulnerabilities but rather the most effective use of vulnerabilities (regardless of the decision of the VEP) and exploits. Additionally, the VEP's goal is the privacy of the US public and the security of its devices and network, whereas the proposed interagency working group is focused on criminals and US adversaries.

It is possible that employment of loud cyber weapons can and will result in disclosure of vulnerabilities. Therefore, it is critical that the CIWG work with the VEP to ensure the exploited vulnerability has been quietly and properly disclosed prior to its employment—particularly for critical infrastructure and the defense industrial base.

Finally, the main criticism of the VEP has been the tension between the strategic disadvantages of disclosure and the risks to security and privacy due to retention. That same tension does not exist within the interagency process. While the CIWG must consider the strategic disadvantages of disclosure, it would be less concerned with security and privacy; any vulnerability will be shared prior to employment.

Conclusion

This article touches on but does not discuss at length the various other concerns raised by loud offensive cyber weapons. Opportunities exist for further research in this area on questions such as: What are the potential consequences? What are their likely responses? What is the threshold for potential responses? Is the United States willing to accept these potential responses? These concerns are significant and would benefit from more consideration. In addition, although the proposed solution discusses a framework for developing and selecting offensive cyber operations, it does not discuss the specific methods and means to consider when implementing this framework; further research is needed regarding specific cyber adversaries and how best to deter them. For example, what are the best cyber techniques to deter terrorist organizations, cyber armies, and cyber criminals? How do these techniques differ from state actors? Regardless, the proposal here represents a viable solution to the cyber weapons paradox. In short, this process ensures the United States can employ offensive cyber weapons to most effectively achieve maximum deterrent effect without foreclosing the US ability to conduct clandestine offensive cyber operations. SSQ

Notes

1. Commission on Cybersecurity for the 44th Presidency, *Securing Cyberspace for the 44th Presidency* (Washington, DC: Center for Strategic and International Studies, 2008), 11–13.
2. Ibid.
3. For the purposes of this article, a cyber operation is considered to have two necessary pieces: a "vulnerability," which is a flaw in the target system's security, and an "exploit," which is the software (or code) that uses a vulnerability. Both vulnerabilities and exploits are perishable and rendered obsolete over time. Perishability defines the characteristic of a cyber weapon when it is no longer effective after being used due to the identification and subsequent elimination of the vulnerability or exploit. Obsolescence refers to a cyber weapon becoming ineffective because time has afforded the opportunity to identify (and subsequently eliminate) the vulnerability. These two characteristics of cyber weapons are unique among the US arsenal since any *discovered* use of a cyber weapon can foreclose the ability to use it again.
4. Alexander L. George and Richard Smoke, *Deterrence in American Foreign Policy: Theory and Practice* (New York: Columbia University Press, 1974), 60.
5. Ibid.
6. Ibid., 1.
7. Ibid., 48.
8. Ibid., 60.
9. Ibid.

10. Ibid.
11. Ibid.
12. Ibid.
13. Ibid., 64.
14. Ibid., 60.
15. Ibid., 93.
16. Department of Defense (DOD), *Deterrence Ops Joint Operating Concept, Version 2.0* (Washington, DC: Office of the Secretary of Defense, December 2006), http://www.dtic.mil/doctrine/concepts/joint_concepts/joc_deterrence.pdf.
17. DOD, *Department of Defense Cyber Strategy* (Washington, DC: Office of the Secretary of Defense, April 2015).
18. DOD, *Deterrence Ops*, 5.
19. Ibid. Presented another way, an adversary may consider the relative benefits and costs of action versus restraint.
20. While other methods for denying benefits are available outside of the cyber domain (i.e., refusing to relent to an adversary's demands), they are not the primary focus of this article.
21. Matthew J. Sklerov, "Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses against States Who Neglect Their Duty to Prevent," *Military Law Review* 201 (Fall 2009): 1–85, https://www.jagcnet.army.mil/DOCLIBS/MILITARYLAWREVIEW.NSF/20a66345129fe3d885256e5b00571830/d471dd1e07eb949d85257672004463bc?OpenDocument.
22. DOD, *Cyber Strategy*, 11.
23. Ellen Nakashima and Steven Mufson, "The U.S. and China Agree not to Conduct Economic Espionage in Cyberspace," *Washington Post*, 25 September 2015, https://www.washingtonpost.com/world/national-security/the-us-and-china-agree-not-to-conduct-economic-espionage-in-cyberspace/2015/09/25/1c03f4b8-63a2-11e5-8e9e-dce8a2a2a679_story.html?utm_term=.a31d532717a5.
24. Joseph Menn and Jim Finkle, "Chinese Economic Cyber-Espionage Plummets in U.S.: Experts," Reuters, 21 June 2016, https://www.reuters.com/article/us-cyber-spying-china/chinese-economic-cyber-espionage-plummets-in-u-s-experts-idUSKCN0Z700D; and Michael A. Vatis, *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy* (Washington, DC: The National Academies Press, 2010), 207–24, https://www.nap.edu/read/12997/chapter/14.
25. DOD, *Deterrence Ops*, 11.
26. Ibid., 44.
27. Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND, 2009), 75.
28. Joint Publication (JP) 3-12(R), *Cyberspace Operations* (Washington, DC: Joint Chiefs of Staff, 5 February 2013), http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf.
29. Ibid., II-7.
30. Ibid., II-7–8.
31. While other agencies may have cyber capabilities, only the DOD, as the military cyber force, would have the role of employing offensive cyber operations.
32. Committee on National Security Systems Instruction (CNSSI) 4009, "Committee on National Security Systems Glossary," 6 April 2015, 131, https://www.cnss.gov/CNSS/openDoc.cfm?LlSjfKedpJ/cVMi+7zozig==.
33. PC Tools, "What Is a Zero-Day Vulnerability?" PC Tools by Symantec, accessed 17 February 2017, http://www.pctools.com/security-news/zero-day-vulnerability/.

34. Microsoft Security Tech Center, "Microsoft Security Bulletins," Microsoft.com, accessed 17 February 2017, https://technet.microsoft.com/en-us/security/bulletins.aspx.

35. Christopher A. Bartos, "Cyber Weapons Are Not Created Equal," *Proceedings* 142 (June 2016), https://www.usni.org/magazines/proceedings/2016-06/cyber-weapons-are-not-created-equal.

36. CNSSI 4009, "Glossary," 25.

37. Kim Zetter, "An Unprecedented Look at Stuxnet, the World's First Digital Weapon," *Wired*, 3 November 2014, https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.

38. Ibid.

39. Ibid.

40. Ibid.

41. Ibid.

42. Ibid.

43. Ibid.

44. Robert Axelrod and Rumen Iliev, "Timing of Cyber Conflict," *Proceedings of the National Academy of Sciences of the United States of America* 111, no. 4 (January 2014): 1298–1303, http://doi.org/f5q64n.

45. DOD, *Cyber Strategy*.

46. Eric Talbot Jensen, "Cyber Deterrence," *Emory International Law Review* 26, no. 2 (2012): 773–824, http://law.emory.edu/eilr/_documents/volumes/26/2/symposium/jensen.pdf.

47. The White House, *Fact Sheet: Presidential Policy Directive on United States Cyber Incident Coordination* (Washington, DC: Office of the Press Secretary, 26 July 2016), https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident.

48. Ibid.

49. George and Smoke, *Deterrence in American Foreign Policy*, 60.

50. It should be noted that this proposal is not without a precedent. In 2015, the DOD established the Joint Interagency Combined Space Operations Center (JICSpOC), which assembles representatives from the DOD, the intelligence community, and other agencies in the national security space enterprise. The JICSpOC serves as an example for implementation of the interagency process. *See* "New Joint Interagency Combined Space Operations Center to Be Established," news release, DOD, 11 September 2015, https://www.defense.gov/News/News-Releases/News-Release-View/Article/616969/new-joint-interagency-combined-space-operations-center-to-be-established/. Also see Colin Clark, "JICSPOC Morphs to 'National Space Defense Center'; What It Means," *Breaking Defense*, 4 April 2017, http://breakingdefense.com/2017/04/jicspoc-morphs-to-national-space-defense-center-what-it-means/.

51. United States Strategic Command (USSTRATCOM), accessed 17 February 2017, http://www.stratcom.mil/Media/Factsheets/Factsheet-View/Article/960492/us-cyber-command-uscybercom/; and "About," USSTRATCOM, accessed 17 February 2017, http://www.stratcom.mil/About/.

52. Elizabeth Weise, "Microsoft Calls for 'Digital Geneva Convention,'" *USA Today*, 14 February 2017, http://www.usatoday.com/story/tech/news/2017/02/14/microsoft-brad-smith-digital-geneva-convention/97883896/.

53. Ibid.

54. Department of Homeland Security (DHS), "Our Mission," DHS, accessed 17 February 2017, https://www.dhs.gov/our-mission.

55. Ibid.

56. Dave Altel and Matt Talt, "Everything You Know about the Vulnerability Equities Process Is Wrong," *Lawfare*, 18 August 2016, https://www.lawfareblog.com/everything-you-know-about-vulnerability-equities-process-wrong.

57. Ibid.

Disclaimer