STRATEGIC STUDIES QUARTERLY

Deterring Malicious Behavior in Cyberspace

Scott Jasper

Abstract

Recent incidents reveal cyberattacks are being employed and honed in a systematic, coordinated fashion to achieve the objectives of malicious actors. Deterrence of the wide array of actors in cyberspace is difficult, since deterrence has to work in the mind of the attacker. Each attacker will weigh the effort of the attack against the expected benefit under their own criteria or rationality. This article analyzes whether the contemporary and complementary deterrence strategies of retaliation, denial, and entanglement are sufficient to deter malicious cyber actors or if the alternative of active cyberdefense is necessary and viable.

✳ ✳ ✳ ✳ ✳

Hackers, criminals, terrorists, foreign powers, and virtual states, a collection of actors working in concert online to influence world affairs, continue to probe and penetrate cyberspace.[1] Many of these actors seek our state secrets, trade secrets, technology, and ideas or aim to strike our critical infrastructure and to harm our economy.[2] Recent incidents reveal cyberattacks are being employed and honed in a systematic, coordinated fashion in an attempt to achieve competitors' objectives. In his first major television interview, the director of the Federal Bureau of Investigation, James Cook, said China has hacked every big US company looking for useful information; however, the cases investigated by the US Senate related to Chinese hackers breaking into computer networks of private transportation companies working for the US military

Scott Jasper, CAPT, USN, retired, is a lecturer at the Center for Civil-Military Relations and the National Security Affairs Department at the Naval Postgraduate School, specializing in defense capability development and cybersecurity. He is the editor of *Conflict and Cooperation in the Global Commons*, *Securing Freedom in the Global Commons*, and *Transforming Defense Capabilities: New Approaches for International Security*, and is a PhD candidate at the University of Reading, UK.

point more to preparing the digital battlefield for a potential conflict.[3] The Islamic State terrorist organization appears eager to enter into digital jihad, boasting of plans to establish a "cyber caliphate" from which to mount catastrophic hacking and virus attacks on the United States and the West.[4] Although their aspirations or objectives vary, the wide array of malicious actors in cyberspace has one thing in common: an expanding choice of cyberattack vectors to enact cyber aggression. Each attacker will weigh the effort of the attack against the expected benefit under their own criteria or rationality.

Given the ubiquitous nature of these threats, can malicious cyber actors be deterred? The aim of deterrence is to create disincentives for hostile action and normally involves two components: deterrence by punishment (the threat of retaliation) and deterrence by denial (the ability to prevent benefit). Some notable scholars have suggested a complementary third component: deterrence by entanglement (mutual interests) that encourages responsible behavior of actors based on economic and political relationships.[5] However, are contemporary and complementary deterrence strategies of retaliation, denial, and entanglement sufficient to dissuade and deter malicious cyber actors, or is an alternative required?

Deterrence of the wide array of actors in cyberspace is difficult, since deterrence has to work in the mind of the attacker. The point of deterrence is to add another consideration to the attacker's calculus.[6] Deterrence instills a belief that a credible threat of unacceptable counteraction exists, that a contemplated action cannot succeed, or that the cost of action outweighs the perceived benefits. Complicated issues, like attribution, legality, liability, privacy, trust, and verification hamper conventional strategies and beg for an alternative ability to influence malicious behavior. The controversial concept of active cyberdefense (proactive actions), which relies on forensic intelligence and automated countermeasures, offers such an alternative and could limit exposure to threats.

Before considering each of the four strategies mentioned above, it is instructive to first consider aspects of cyberattack vectors along with current threat-actor strategies. The complexity and severity of acts of cyber aggression indicate that implementation of any strategy will require cooperation among all stakeholders in industry, government, and defense spheres. A proven method for national cooperation is the comprehensive approach used in international stabilization and reconstruction operations as witnessed through the North Atlantic Treaty Organization (NATO).

Attack Vectors and Actor Strategies

A cyberattack vector is a specific method or technique to access equipment, computers, or systems to deliver a hostile payload for a malicious outcome. These vectors range from social engineering attacks, Internet Protocol (IP) address spoofing, web malware attacks, Bluetooth eavesdropping, and other malicious code delivery means by physical manifestation (like thumb drives).[7] Cyberattack vectors have grown in number, complexity, and sophistication. Their expansive propagation enables unbridled acts of cyber aggression, like theft or exploitation of data, disruption or denial of access or service, and destructive action—including corruption, manipulation, and damage or the alteration of data. The technical properties of cyberattack vectors that prevent attribution allow actors to operate with near anonymity and impunity.

Criminal exploitation, military or industrial espionage, nationalist hacker protests, and infrastructure infiltration or sabotage are prominent in competitor operations and campaigns. A diverse array of cyberattack vectors are used to threaten the security of industrial, commercial, governmental, and military systems and devices. Not only has the volume of malicious code, known as malware, increased to 31 million new strains in 2013, but also the means of delivery have expanded to take advantage of human and technological weaknesses and modern-day platforms. The most sensational and publicized attack vectors are various types of intrusions by groups of attackers categorized as an advanced persistent threat (APT) and assaults by distributed denial of service (DDoS) methods. APT hacking is designed to covertly penetrate networks and systems to steal or alter information, manipulate data, or cause damage. A DDoS assault disrupts web site availability by overwhelming network equipment with volumetric attacks or consuming resources with application-centric attacks.[8]

The buying or renting of malicious code viruses, exploits of code vulnerabilities, botnets, and command-and-control servers provide an array of tools and services for motivated threat actors and states. The state-criminal nexus is evident, as cyber intruders who commit crimes and espionage use similar methods, for instance Remote Access Trojan tools that capture and extract information, including Poison Ivy, Ghost, and PlugX.[9] For those actors willing to pay, professional hackers are for hire, including the Hidden Lynx group, which operates from China. Hidden Lynx professionals obtain specific information that could be used to gain competitive advantages at both corporate and nation-state levels.[10] They have been involved in several high-profile campaigns, including Operation Aurora—the obscure APT intrusions on Google and more than 30 other companies disclosed in 2010.[11]

A medium-sized Chinese APT group (about 50 members) ran the NetTraveler cyberespionage campaign. This malware infected more than 350 victims in 40 countries from 2005 through 2013.[12] The group stole more than 22 gigabytes of data found on 30 command-and-control servers.[13] The domains of interest they sought were space exploration, nanotechnology, energy production, nuclear power, lasers, medicine, and communications.[14] However, not all cyberespionage campaigns for hire originate from China. An Indian APT group, possibly a commercial security firm that has targeted entities and industries mainly in Pakistan since September 2010, runs Operation Hangover. Oddly rudimentary, the group uses publicly available tools and basic obfuscation methods while exploiting only known and fixed vulnerabilities.[15]

In late 2012, then Secretary of Defense Leon Panetta warned that the attacks on energy companies in the Persian Gulf and on banks in the United States mark a significant escalation of the cyber threat and renewed concerns over still more destructive scenarios.[16] Whether or not these incidents are representative of catastrophic results is debatable, since Saudi Aramco production systems were not breached and the longest interruption of the US banks was merely hours. However, preparations for conflict indicate we may already be in Phase Zero ("Shape") of cyberwarfare campaigns as postulated in the notional six-phase model of joint and multinational operations described in US joint doctrine.[17] The head of US Cyber Command (USCYBERCOM) stated in Congressional testimony that China was responsible for the APT intrusion into RSA SecurID systems.[18] Moreover, in February 2013, the long-suspected role of the Chinese People's Liberation Army (PLA) in systematic cyber espionage and data theft was confirmed by a US security firm that exposed APT1, believed to be a military unit under the PLA General Staff Department.[19] The Pentagon made further allegations against China in its 2013 annual report, alluding to the use of "computer network exploitation capability to support intelligence collection against the U.S. diplomatic, economic, and defense industrial base sectors."[20] This sort of state-sponsored espionage threatens military operations and readiness.[21]

The cost to the United States in intellectual property (product plans, research results, and customer lists) and confidential business information (trade secrets, exploration data, and negotiation strategies) theft amounts to billions of dollars annually.[22] In May 2014 the Department of Justice indicted five members of the Chinese military on charges of computer fraud, damaging a computer, aggravated identify theft, and economic espionage.[23] The conspirators, working for Unit 61398 in the vicinity of Shanghai, stole trade secrets useful to Chinese companies, including state-owned enterprises. For example, they hacked into SolarWorld computers to steal files about production capabilities and cost structure while the Oregon-based company was an active litigant in trade cases against Chinese solar manufacturers that had dumped products into US markets at prices below fair value.

The term cybered conflict could be an appropriate moniker to frame the complexity and ambiguity of struggle involving cyberspace, including hybrid warfare and insurgent campaigns.[24] Cybered conflict characterizes "old and new forms of conflict born of, enabled through, or dramatically altered by cyberspace."[25] For instance, cyberattacks occurred on both sides over the weekend of Crimea's vote to secede from Ukraine and join Russia in March 2014. Beginning Saturday evening, NATO's main public web site, which carried a statement by the secretary general over the illegitimacy of the vote, worked intermittently. A hacker group called Cyber Berkut said the attack was carried out by "patriotic" Ukrainians angry over NATO interference; of note, *Berkut* refers to the feared riot squads of ousted pro-Russian Ukrainian president Victor Yanukovich.[26] On Sunday, a wave of 42 DDoS attacks hit Ukrainian government sites. The Monday after the vote, 132 separate DDoS blasts, most likely by OpRussia and Russian Cyber Command hackers who opposed annexation, slammed Russian sites.[27] Political conflicts have also spawned cyberattacks against Western news organizations, evidenced by the Syrian Electronic Army, a group of pro-regime hackers, compromising external web sites and social media accounts of the *New York Times*, the *Associated Press*, *CNN*, the *Huffington Post*, and *Forbes* to gain publicity for the embattled Syrian regime.[28]

Complementary Deterrence Strategies

Deterrence seeks to shape another's perception of costs and benefits. Deterrence requires national resolve to commit resources, enhance cooperation, or use force when necessary. In July 2013 the US chairman of the Joint Chiefs of Staff, Gen Martin E. Dempsey, US Army, posited that national mission teams could counter threat actors' activities but recognized the need to work with other nations to set norms of responsible behavior in cyberspace, while improving information sharing and cyber standards.[29] In the Senate hearing to consider the nomination for the new commander of USCYBERCOM, Senator James Inhofe fittingly summarized the central problem in stating that "the lack of a cyber-deterrence policy . . . [has] left us more vulnerable to continued cyber aggression." When asked "how do we prevent that," the nominee, Vice ADM Michael S. Rogers, responded, "We're generating capability, we're generating capacity. . . . But in the end I believe we've got to get some idea of deterrence within the cyber arena."[30] The concept of deterrence is still hotly debated in the cyber community, because, for instance, traditional nuclear deterrence relies on an adversary having knowledge of the destruction that will result from transgressions, which is not possible in cyber because the secrecy of weapons is necessary to preserve their effectiveness.[31]

Deterrence stems from an adversary's belief that a threat of retaliation exists, that the intended action cannot succeed, or that the costs outweigh the benefits of acting. [32] The strategic debate during the Cold War over how best to deter nuclear attack normally was divided into deterrence by punishment (threat of retaliation) and deterrence by denial (limitation of damage).[33] Since today US policy would not condone the punishment of another country, a more appropriate view of this form of deterrence would simply be retaliation. With the strategic and economic interdependence that has resulted from contemporary globalization, one might also add deterrence by entanglement (mutual interests).[34]

For deterrence to be effective, it must be based on capability (possessing the means to influence behavior), credibility (instilling believability that counteractions may actually be deployed), and communication (sending the right message to the desired audience). The achievement of these conditions for effectiveness is extremely difficult. State capabilities to influence the behavior of threat actors in cyberspace are constrained by these actors' abilities to operate undiscovered for great lengths of time; even if actors are convinced counteractions may be deployed, their rationality cannot be assumed. Additionally, the audience of actors conducting cyber aggression is vast and varied in motivations and intentions. No singularly sufficient answer exists to deter different types of groups using varied means of cyber aggression.

Identifying the need to "integrate newer behavioral approaches outside a rational state based actor construct," the Assistant Chief of Staff for US Strategic Deterrence and Nuclear Integration, Maj Gen William A. Chambers, USAF, encourages moving beyond reliance solely on "imposition of costs to integrate denial of benefits and other methods for encouraging restraint."[35] To make this move beyond Cold War-vestiges the focus must be on linking cyberdeterrence to desired effects, regardless of the actor being deterred.[36] The strategy of deterrence by entanglement can encourage responsible state behavior—to refrain from the conduct, endorsement, or allowance of malicious cyberactivity within a nation's territory—through cooperation based on mutual interests. However, for the wider array of threat actors, a different paradigm or concept must be considered to achieve deterrence's central premise—altering an adversary's behavior. The concept of active cyberdefense that entails tenets of deterrence is another method for encouraging adversaries' restraint. Automated, active cyberdefense-technologies can interdict, isolate, or remove threat vectors, denying benefit and engaging, deceiving, or stopping adversaries while imposing costs—regardless of the source.

US Department of Defense (DOD) cyberspace policy maintains effective deterrence is partly founded upon ensuring the capability to respond to hostile acts with a proportional and justified response.[37] This form of deterrence by retaliation is complicated by the difficulty in monitoring cyberspace, in identifying intrusions, and in locating the source with a high degree of confidence and in a timely manner. For example, advanced persistent threats conceal detection of attacker identities and allow plausible deniability. If definitive attribution can be obtained, the military could act within its prescribed authority in self-defense against an armed attack-equivalent in cyberspace. The cyberspace policy also recognizes effective deterrence in cyberspace is founded upon both the security and resilience of networks and systems. This strategy for deterrence discourages adversaries through the denial of benefit of their attack. In this context, security infers reducing risk by defensive cyber measures, and resilience means the ability to withstand and recover from disruptions or attacks. Defensive measures emphasize the continual deployment of solutions to protect multiple threat points, including network, endpoint, web, and e-mail, from cyberattack vectors.

Pursuit of deterrence by entanglement through mutual interests has potential to reduce miscalculation and escalation. This strategy assumes potential adversaries are stakeholders in cyberspace, so embedded in the network they would not attack in peacetime or crisis. The deterrent effect is restraint based on the cost associated with attacks in cyberspace, in particular the loss of access for one's own purposes. Deterrence by entanglement involves encouraging others to accept a stake in the integrity of cyberspace through formal or informal rules or norms. The challenge in agreeing upon defined and achievable rules or norms that pertain to and are accepted by all state actors in the cyber realm lends credence to exploration of other options for achieving the effects of deterrence.

The DOD defines active cyberdefense as the synchronized, real-time capability to discover, detect, analyze, and mitigate threats and vulnerabilities.[38] This definition implies the limitation of damage and elucidates the threat of retaliation—both elements of deterrence. Active cyberdefense is widely understood to include offensive actions in cyberspace taken for defensive purposes, with the limited goal of mitigating an immediate hostile act.[39] Federal or international laws and legislation govern any action beyond internal networks. Today "it's illegal to chase bad guys up the wire, even if you have the capability to do so—it's illegal to shoot back."[40]

Deterrent Responses to Malicious Behavior

Analyzing the sufficiency of deterrent responses—retaliation, denial, entanglement, or active defense—to influence malicious behavior by threat actors in cyberspace requires answering the following questions:

- Can threats of proportionate response realistically achieve deterrence by retaliation?
- Are defensive measures adequate to achieve deterrence by denial?
- Will cooperative measures restrain behavior through deterrence by entanglement?
- Is the concept of active cyberdefense technically and legally viable?

Feasible answers to these four questions are found in the following inspection of initiatives, issues, and constraints.

Deterrence by retaliation imposes costs for hostile acts in cyberspace. Retaliation is based on a nation's right to use all necessary means to defend itself, its allies and partners, and its interests in cyberspace. As appropriate and consistent with applicable international law, the means for a proportional and justified response includes diplomatic, informational, military, and economic measures.[41] Military response options may include using cyber- and/or kinetic capabilities. Under some circumstances, hostile acts in cyberspace could constitute an armed attack within the meaning of Article 51 of the United Nations (UN) Charter. Established principles would apply in the context of an armed attack (*jus ad bellum*). First, the right of self-defense applies against an imminent or actual armed attack whether the attacker is a state or nonstate actor. Second, the use of force in self-defense must be limited to what is necessary and proportionate to address an imminent or actual use of force. Third, states are required to take measures to ensure their territories are not used for purposes of armed activities against other states. Existing rules and principles of the international law of armed conflict address the use of cybertools in the context of armed conflict (*jus in bello*).

Regarding the question of whether or not a cyber operation constitutes an armed attack, the *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Rule 13) offers, that, it depends on the scale and effects.[42] Cyber operations that result in death or injury of individuals or destruction or damage of objects could rise to the level of an armed attack.[43] Although the Stuxnet computer worm caused physical damage, the International Group of Experts that developed the *Tallinn Manual* was divided on whether the damage constituted an armed attack. Future cyberattacks could be structured to transmit data or subtly modify, degrade, or corrupt data in a malicious but not immediately apparent manner.[44] NATO's Policy on Cyber Defense reiterates that any collective defense response is subject to political decisions by the North Atlantic Council.[45] This ambiguity gives an adversary good reason to use cyber as a method of attack against critical infrastructure.[46]

The imposition of costs in deterrence by retaliation is intended to reduce an adversary's willingness or ability to initiate or continue an offensive. While some argue the fundamental interconnectedness of networks means the effects of responsive cyber operations cannot be limited, others claim that contained operations are possible even within broadly connected systems.[47] However, deliberate, inadvertent, or accidental escalation could trigger a chain reaction that raises the level of conflict beyond that contemplated by any party to the conflict.[48] In the United States, only the president can approve a cyber operation likely to result in significant consequences—a tough decision due to the inability to predict collateral damage and the uncertainty over political effect.[49] Equally, the threat of massive cyber retaliation would probably encourage actors to seek low levels of malicious behavior that fall below the threshold that would trigger such retaliation.[50] In many cases, target countries may be constrained to seek justice rather than retribution. In court, target states can press for access to individuals or to information and use refusal to cooperate as a justification for retaliation. However, until retaliation does ensue, there is no punishment—hence, no deterrence.[51] Meaning the threat alone of proportionate responses will not realistically achieve deterrence by retaliation.

Deterrence by denial of benefit denies an adversary's objectives by increasing the security and resilience of networks and systems. Traditional passive reactive methods, like antivirus software and blacklists, have grown ineffective as the volume and complexity of threats increase.[52] A defense-in-depth approach emphasizes the continual deployment of reactive solutions to protect multiple threat points, including network, endpoint, web, and e-mail security.[53] The spectrum of cybersecurity tools and techniques ranges from next-generation firewalls, application whitelisting, intrusion prevention systems and sandboxes to access control, data encryption, patch management, and data loss prevention. Layering multiple technologies combined with best practice endpoint management can decrease the risk of customized malware payloads, because each layer blocks a different aspect of multipronged cyberattacks. For example, at the delivery phase, device control can block infected Universal Serial Bus (USB) devices. At the exploitation phase, patch and configuration management can eliminate known vulnerabilities. At the installation phase, application control can prevent unapproved executables.[54] Cybersecurity frameworks suggest technical measures that can monitor networks and systems, detect attack attempts, identify compromised machines, and interrupt infiltration. The Council on Cyber Security's Critical Security Controls offers a prioritized program for computer security based on the combined knowledge of actual attacks and effective defenses.[55] These controls cover a range of best practices, including vulnerability assessment, malware defenses, and access control. The controls identify commercial tools to detect, track, control, prevent, and correct weaknesses or misuse at threat points. The top three drivers for adopting these controls are increasing visibility of attacks, improving response, and reducing risk.[56] When the Congress failed to enact the necessary legislation, Pres. Barack Obama signed an executive order for the development of a Cybersecurity Framework that incorporates voluntary consensus standards and industry best practices. The inaugural Cybersecurity Framework is built around the core functions of identify, protect, detect, respond, and recover.[57] The Critical Security Controls are part of the Framework's informative references that illustrate methods to accomplish activities under these functions.

To facilitate cybersecurity information sharing, as called for in the executive order, the National Cybersecurity and Communications Integration Center (NCCIC) works with the private sector and government and international partners. The NCCIC strives to establish shared situational awareness of harmful activity, events, or incidents to improve the ability of partners to protect themselves. The NCCIC integrates analysis and data into a series of actionable and shareable information products. In addition, the NCCIC engages with information-sharing and analysis centers (ISAC) to protect portions of critical information technology with which they interact, operate, manage, or own. For example, during the 2012 series of DDoS assaults on US major banks, the NCCIC collaborated with the Financial Services ISAC to provide technical data and assistance to financial institutions. Data included DDoS-related IP addresses and supporting contextual information, which was also provided to over 120 international partners.[58]

Agencies and companies acknowledge the need to share more data about threats across enterprise boundaries but are worried about liability and risk. Commercial offerings, like Internet Identity's Active Trust platform, let contributors retain ownership of data and control dissemination.[59] However, only cybersecurity legislation can enable the private sector to share real-time cyber threat activity detected on its networks without fear of violating civil liberties and rights to privacy of citizens.[60] Thus, by design, participation in sharing arrangements and adoption of industry best practices for securing cyberspace remains voluntary for the private sector that largely owns the nation's critical infrastructure.[61]

Private sector awareness of threats, vulnerabilities, and consequences is questionable, when external parties reveal 85 percent of cyberespionage breaches months after intrusion.[62] Defensive measures are not adequate to achieve deterrence by denial, as security has not kept pace with the threat; more dynamic, active defenses are necessary. It is not a matter of if a company will be breached, but when. While the defense is not catatonic, it is not certain the offense will get continually better either, particularly when defense defines what the offense can do.[63]

Deterrence by entanglement encourages responsible behavior, while restraining malicious behavior through cooperation based on common interests. To some extent, nations share political, economic, commercial, and strategic dependency in cyberspace—as well as some degree of vulnerability. According to the UN secretary general, "While all Nations appreciate the enormous benefits of ICTs [information and communication technologies], there is also broad recognition that misuse poses risks to international peace and security."[64] The secretary general's report, authored by the Group of Governmental Experts, identifies that the development and spread of sophisticated tools and techniques increases the risk of mistaken attribution and unintended escalation. States have repeatedly affirmed the need for cooperative action against threats resulting from this malicious use. States must lead these efforts, but effective cooperation would benefit from participation by the private sector and civil society in a comprehensive approach. An array of actions is required to promote a peaceful, secure, and open information and communications technology environment.[65]

One action to strengthen deterrence by entanglement could be the implementation of formal binding agreements. Arms control aims to establish legal regimes that make conflict less likely. The objective of such regimes is to reduce the existence of, or restrict the use of, certain weapons. However, imposing limitations on the development and proliferation of cyberweapons is difficult, because their properties are incompatible with the rationale for arms-control treaties.[66] The lack of universal consensus on what even constitutes a cyberweapon complicates verification of compliance. Most of the technology relied on in an offensive capacity is inherently dual-use, like vulnerability assessment tools, and software can be minimally repurposed for malicious action.[67] Control of cyberweapon development, spread, and use is practically impossible. Cyberweapons require no controlled materials, identifiable manufacturing facilities, or restricted skills.[68] Open-source software that could be used as a cyberweapon is widely available for free or for purchase, i.e., the Blackhole exploit kit.[69] Alternative devices and systems are continually being compromised and turned into cyberweapon platforms. Additionally, the creator or source of the weapon is not often the user, i.e., in hacktivist campaigns cybertools with instructions are provided to patriotic or ideological hackers supporting a cause.

Absent practical and acceptable treaties, cooperative measures could enhance international peace, stability, and security. Internationally acceptable norms, rules, and principles of responsible behavior by states could encourage order in the domain. These measures start with the premise that international law—in particular the Charter of the United Nations—is applicable to cyberspace. The Seoul Conference on Cyberspace resulted in a "Framework for and Commitment to Open and Secure Cyberspace" that offers guidelines for governments and organizations on coping with cybercrime and cyberwar.[70] These guidelines include verbatim recommendations by the UN Group of Government Experts for states to meet their international obligations regarding wrongful acts attributed to them, to refrain from using proxies to commit wrongful acts, and to ensure their territories are not used by nonstate actors for unlawful acts.

Regional or bilateral dialogue can establish voluntary confidence-building measures to promote trust and assurance, like those agreed upon by the United States and Russia for sharing of threat indicators.[71] Other practical measures to increase predictability and reduce misperception include exchange of views on national policies, like a recent briefing by the DOD given to Chinese officials regarding Pentagon doctrine for defending against cyberattacks.[72] Finally, capacity-building assistance might be necessary for states to fulfill their responsibilities for cyberspace. Efforts for assistance range from developing technical skill and sharing best practices to strengthening national legal frameworks. Overall, cooperative measures—international norms, confidence-building measures, and capacity-building assistance—are well-suited mechanisms for deterrence by entanglement. These mechanisms can address potential threats, vulnerabilities, and risks, but a clash of self-interests might thwart cooperation that restrains malicious behavior. For example, Beijing suspended a US-Sino working group on cyber-related issues after the indictment of the Unit 61398 members, citing "we should encourage organizations and individuals whose rights have been infringed to stand up and sue Washington."[73]

Active cyberdefense is defined as the "proactive detection, analysis and mitigation of network security breaches in real-time combined with the use of aggressive countermeasures deployed outside the victim network."[74] These tasks imply defensive measures and proportionate responses that shape an adversary's perception of benefits and costs—the essence of deterrence. In military terms, the tasks are very similar to defensive cyberspace operations described by the director of operations at USCYBERCOM as "passive and active cyberspace defense activities that allow us to outmaneuver an adversary."[75] Defensive cyberspace operations provide the ability to discover, detect, analyze, and mitigate threats with malicious capability and intent to affect key cyber terrain. Subcategories of these operations are internal defensive measures (IDM), actions taken internally, and response actions (RA) taken outside the information environment. Tasks for IDM are hunting on friendly terrain for threats and directing appropriate internal responses, whereas RA are about going after the shooter outside friendly network space to stop the attack.

For the private sector, active cyberdefense entails working with cybersecurity solution providers to identify and interdict cyber intrusions.[76] Once packets are determined to be malware, defensive actions can be taken, including diverting packets to a holding area or other actions aimed at the attacker. The broad spectrum of actions available include using honeypots, beaconing, sinkholing, and deceiving, which raise adversary costs and risks through interference, delay, obstruction, or trickery.[77] Even limited action would contribute to assurance (detection of intrusions) and attribution (identification of actors). Many public debates center on aggressive response aspects of active cyberdefense, like hack back, for which existing legal constraints would have to be adapted to allow use of these tactics.[78]

A more practical description of active cyberdefense is a range of proactive actions that engage the adversary before and during a cyber incident. Examples would be using a honeypot to see which documents the adversary chooses to exfiltrate, remotely tracking stolen documents by passive watermarks on files, or allowing the adversary to steal documents that contain false or misleading information.[79] Legal issues confront employing actions outside of the victim's network, like taking control of remote computers to stop attacks or launching denial of service attacks against attacking machines. The primary law in the United States that applies to these more aggressive techniques is the Computer Fraud and Abuse Act (CFAA), codified as Title 18, Section 1030. A defendant can violate the CFAA by accessing a "protected computer" without authorization or by exceeding authorized access.[80]

One could argue US common law admits certain rights of self-defense and of defense of property in preventing the commission of a crime against an individual or a corporation. Applying the latter for hostile cyberattacks, the range of allowable actions is roughly comparable to the range for *nonlethal* self-defense. While individuals are not permitted to engage in revenge or retaliation for a crime, they are—in some instances—entitled to take otherwise-prohibited actions for the purpose of preventing or averting an imminent crime or addressing one that is in progress. However, in most cases, challenges in quickly obtaining definitive attribution preclude exercising this right.[81] Therefore, under current law, a private-sector actor may realistically only respond to hostile attacks within its own networks and systems organizational boundaries. Only one active defense capability, HawkEye G, exists internal to the network today. It uses automated countermeasures to remove cyber threats before they can compromise intellectual property or cause process disruption.[82] Until legally viable for vendors to provide solutions outside the network, the concept is technically limited to denial of benefit.

A Comprehensive Approach

The US Joint Staff recognizes the government and the private sector must plan and coordinate their activities to prepare for cyber threats. However, the staff also realizes that achieving unity of effort to meet national security goals is always problematic due to challenges in information sharing, competing priorities, and uncoordinated activities. Success in preparation and response to cyberattacks is dependent upon unity of effort enabled by collaboration and coordination among partners.[83] The US *Cyberspace Policy Review* also delineates the need for a comprehensive framework to facilitate coordinated responses by government, the private sector, and allies to a significant cyber threat or incident. The review maintains that "addressing network security issues requires a public-private partnership as well as international cooperation and norms."[84] Deterrence, as an element of cybersecurity policy, provides a strategic response that is underpinned by this partnership and cooperation. The challenge is to align the efforts of all involved parties for a common purpose. NATO has used the concept of a comprehensive approach to align parties in NATO operations by capitalizing on shared interests, complementary opportunities, and mutual procedures. The comprehensive approach is based on "principles and collaborative processes that enhance the likelihood of favorable and enduring outcomes within a particular situation."[85] NATO proclaims "the need to promote a comprehensive approach applies not only to operations, but more broadly to many of NATO's efforts to deal with 21st century security challenges, such as . . . protecting against cyber attacks."[86]

Although NATO experiences offer a starting point to design a comprehensive approach for operations in a particular domain of interest (cyberdeterrence), the methodology must be modified and translated for different operational conditions, structural characteristics, and prominent partners, including commercial actors. The Comprehensive National Cybersecurity Initiative aims to build an approach to cyberdefense strategy that deters interference and attack in cyberspace. The White House provides a shining example of embracing a comprehensive approach for cyberdeterrence by suggesting public- and private-sector partnerships for cyberdefense of critical infrastructure sectors.[87] Within this context of a comprehensive approach, a partnership would be defined as close cooperation between parties having common interests in achieving a shared vision.

Given cooperative interaction can potentially facilitate the common interests of organizations, the comprehensive approach aims for congruence of purpose—not unity of command.[88] However, the approach needs to recognize and overcome a clash of self-interests—where one party strives to maintain economic or military advantage—that might prevent cooperation in deterring cyber aggression. For instance, the private sector is reluctant to share cyber threat data with the government, because it does not believe the latter can protect the confidentiality of a company that has been attacked, which may devalue stocks or compromise proprietary information to the advantage of competitors.[89] A state might not agree to cooperative action if binding rules constrain its preferred method of competition in cyberspace. Critical to gaining consensus for the comprehensive approach is the multilateral characteristic of diffuse reciprocity, whereby parties recognize their self-interests will be satisfied over the long term. Examination of models and precedents in other functions or domains, like the emerging International Code of Conduct for Outer Space Activities, could identify principles, measures, and mechanisms that not only foster trust and cooperation but also facilitate openness and transparency.[90]

In reality, many cyber incidents today are merely easily-corrected annoyances—causing irritation, inconvenience, and perhaps delay.[91] Even the vaulted Stuxnet worm that resulted in the replacement of about 1,000 IR-1 centrifuges at the Iranian nuclear facility in Natanz, only exposed vulnerabilities in Iranian enrichment facilities that ultimately improved centrifuge performance.[92] Whether cyber means are capable of inflicting real persistent harm on the fighting power of an enemy is doubtful.[93] Likewise, the analytical basis for cyber alarmism is dubious, despite public policy makers ranting repeatedly about wake-up calls following cybersecurity incidents.[94] However, bolstering that stream of concern, the US Director of National Intelligence has testified, "We assess that the likelihood of a destructive attack that deletes information or renders systems inoperable will increase as malware and attack tradecraft proliferate."[95] Admiral Rogers believes China, along with one or two other countries, already has cyber capabilities that could shut down the electric grid in parts of the United States.[96] A comprehensive approach has produced interaction among diverse organizations, leading to a more effective overall effort in operations.[97] For cyberspace, the framework could enable the implementation of complementary deterrence strategies or an alternative that achieves similar desired effects.

Conclusion

The US chairman of the Joint Chiefs of Staff claims "disruptive and destructive cyber attacks are becoming a part of conflict," and "civilian infrastructure and business are targeted first."[98] In response, the *Quadrennial Defense Review* reiterates that deterrence of these sorts of cyber threats requires a multistakeholder coalition that enables "the lawful application of the authorities, responsibilities, and capabilities resident across the U.S. Government, industry, and international allies and partners."[99] This mandate effectively endorses the use of a comprehensive approach to influence malicious behavior in cyberspace. The challenge remains in the number and type of malicious actors with various motivations and the assortment of cyberattack vectors at their disposal. When asked whether the cyber intrusions on JP Morgan Chase, and at least four other banks, were coming from entities associated with the Russian government, US Secretary of the Treasury Jack Lew replied, "We have a lot of concerns about the sources of attacks because there are many different sources."[100]

The cyber breach at JP Morgan Chase Bank offers an illustrative case to examine the sufficiency of the suggested deterrence strategies or alternative. In June 2014, hackers used a phishing attack vector to compromise a bank employee's user name and password and enter a web-development server. With a variety of malware, the hackers eventually gained access to more than 100 servers that housed personal data, but not account information, for 76 million household accounts.[101] Many believe the attacks were a direct result of sanctions imposed by the United States against Russia. The lack of any apparent profit motive generates speculation that the hackers were sponsored by the Russian government. For this case, deterrence by retaliation, by at least military means, falters as the incident does not cross any threshold for an armed attack. For deterrence by denial, JP Morgan's chairman admits that even though the bank has fortified its defenses (with a $250 million annual digital security budget) the battle is "continual and likely never-ending."[102] For deterrence by entanglement, the question is, would the Russian government investigate if asked, especially if the attack was indeed conducted by a proxy group on their behalf. Additionally, for the active cyberdefense concept, while the initial authenticated entry would not have been blocked, the breach might have been detected earlier by capabilities that discover and interpret subtle behaviors in enterprise activity.

In not only the above suspected case of state-sponsored espionage but also in other disruptive or destructive forms of cyber aggression, each suggested deterrence strategy has limited merit in preventing threat-actor action. The promise of active cyberdefense is in autonomous countermeasures that act without regard to the identity of the malicious threat actors or their motivations—only that their malware is isolated or eradicated. Although active defense can close the time between discovery and compromise, many organizations are reluctant to adopt machine-enabled defensives for fear of algorithmic misfires with unexpected consequences. Despite preventive efforts, attacks continue and increase in sophistication. Malicious actors are using multiple-stage attacks, stretched out over months or using new infection vectors.[103]

The proliferation of threat vectors and actors will not allow pause for policy makers to get some idea of deterrence within the cyber arena. Deterrence convinces adversaries not to take malicious actions by means of decisive influence over their decision making. Decisive influence is achieved by threatening to impose costs or deny benefits while imposing restraint.[104] The solution to the dilemma is a mix of strategies and capabilities that influence the decision-making process of an actor, regardless if rational or not. Ways do exist to enhance the sufficiency of the suggested responses, including imposing real consequences (retaliation), employing reactive defenses (denial), sustaining diplomatic perseverance (entanglement), and considering legal adaptation (active defense). The suggested responses are at least a starting point to achieving an end state where the actor chooses not to act for fear of some combination of cost, failure, or consequences. SSQ

Notes

1. Kevin G. Coleman, "Virtual States in Cyberspace Increase in Size and Numbers," *DefenseSystems.com*, 15 November 2012, http://defensesystems.com/articles/2012/11/15/digital-conflict-virtual-states.aspx.

2. Robert Anderson Jr., *Cybersecurity, Terrorism, and Beyond: Addressing Evolving Threats to the Homeland; Testimony before the Committee on Homeland Security and Government Affairs, United States Senate*, 113th Cong., 2nd sess., 10 September 2014, http://www.hsgac.senate.gov/download/?id=36272b88-c26a-45d8-887e-814fc8c8eb04.

3. James Cook, "FBI Director: China Has Hacked Every Big US Company," *Business Insider*, 6 October 2014, http://www.businessinsider.com/fbi-director-china-has-hacked-every-big-us-company-2014-10; and Danny Yadron, "Chinese Hacked U.S. Military Contractors, Senate Panel Says Hackers Broke into Computer Networks 20 Times in a Year," *Wall Street Journal*, 18 September 2014, http://online.wsj.com/articles/chinese-hacked-u-s-military-contractors-senate-panel-says-1410968094.

4. Jamie Dettmer, "Digital Jihad: ISIS, Al Qaeda Seek a Cyber Caliphate to Launch Attacks on US," *FoxNews.com*, 14 September 2014, http://www.foxnews.com/world/2014/09/14/digital-jihad-isis-al-qaeda-seek-cyber-caliphate-to-launch-attacks-on-us/.

5. Schuyler Foerster, "Strategies of Deterrence," in *Conflict and Cooperation in the Global Commons: A Comprehensive Approach for International Security*, ed. Scott Jasper (Washington, DC: Georgetown University Press, 2012), 64.

6. Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND Corporation, 2009), 6–37, http://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf.

7. Kevin G. Coleman, *The Cyber Commander's eHandbook: The Strategies and Tactics of Digital Conflict*, version 4 (McMurrary, PA: Technolytics, 2013), 52–80.

8. Chris Pepper, ed., *Defending against Denial of Service Attacks* (Phoenix, AZ: Securosis, 31 October 2012), 1–24, https://securosis.com/assets/library/reports/Securosis_Defending-Against-DoS_FINAL.pdf.

9. Kelly Jackson Higgins, "Chinese Cyberespionage Tool Updated for Traditional Cybercrime," *Dark Reading*, 27 November 2012, http://www.darkreading.com/attacks-breaches/chinese-cyberespionage-tool-updated-for-traditional-cybercrime/d/d-id/1138733?.

10. Stephen Doherty, Jozsef Gegeny, Branko Spasojevic, and Jonell Baltazar, *Hidden Lynx—Professional Hackers for Hire*, version 1.0 (Mountain View, CA: Symantec, 17 September 2013), http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/hidden_lynx.pdf.

11. William Jackson, "How Google Attacks Changed the Security Game," *Government Computer News*, 1 September 2010, http://gcn.com/articles/2010/09/06/interview-george-kurtz-mcafee-google-attacks.aspx?m=1.

12. Kaspersky Lab's Global Research and Analysis Team, *The NetTraveler (aka Travnet)* (Moscow, Russia: Kaspersky Lab, 2013), 1–25, http://kasperskycontenthub.com/wp-content/uploads/sites/43/vlpdfs/kaspersky-the-net-traveler-part1-final.pdf.

13. Kelly Jackson Higgins, " 'NetTraveler' Cyberespionage Campaign Uncovered," *Dark Reading*, 4 June 2013, http://www.darkreading.com/attacks-breaches/nettraveler-cyberespionage-campaign-uncovered/d/d-id/1139884?.

14. Kaspersky Lab's Global Research and Analysis Team, "NetTraveler Is Running! Red Star APT Attacks Compromise High-Profile Victims," *Securelist*, 4 June 2013, http://securelist.com/blog/research/35936/nettraveler-is-running-red-star-apt-attacks-compromise-high-profile-victims/.

15. Kelly Jackson Higgins, "'Commercialized' Cyberespionage Attacks Out of India Targeting U.S., Pakistan, China, and Others," *Dark Reading*, 20 May 2013, http://www.darkreading.com/attacks-breaches/commercialized-cyberespionage-attacks-out-of-india-targeting-us-pakistan-china-and-others/d/d-id/1139791?.

16. Leon E. Panetta, "Defending the Nation from Cyber Attack" (speech, Business Executives for National Security, New York, 11 October 2012), http://www.defense.gov/Speeches/Speech.aspx?SpeechID=1728.

17. US Joint Publication 5-0, *Joint Operation Planning,* 11 August 2011, III-38–III-44.

18. Kelly Jackson Higgins, "China Hacked RSA, U.S. Official Says," *Dark Reading*, 29 March 2012, http://www.darkreading.com/attacks-breaches/china-hacked-rsa-us-official-says/d/d-id/1137409?.

19. Mandiant, *APT1: Exposing One of China's Cyber Espionage Units* (Alexandria, VA: Mandiant, 27 February 2013), http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

20. Office of the Secretary of Defense (OSD), *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China* (Washington, DC: DOD, May 2013), 36, http://www.defense.gov/pubs/2013_china_report_final.pdf.

21. Larry M. Wortzel, *Cyber Espionage and the Theft of US Intellectual Property and Technology; Testimony before the Committee on Energy and Commerce, US House of Representatives*, 113th Cong., 1st sess., 9 July 2013, http://docs.house.gov/meetings/IF/IF02/20130709/101104/HHRG-113-IF02-Wstate-WortzelL-20130709-U1.pdf.

22. James Lewis and Stewart Baker, *The Economic Impact of Cybercrime and Cyber Espionage* (Washington, DC: Center for Strategic and International Studies, July 2013), http://csis.org/files/publication/60396rpt_cybercrime-cost_0713_ph4_0.pdf.

23. *United States of America v. Wang Dong, Sun Kailiang, Wen Xinyu, Huang Zhenyu, Gu Chunhui*, in United States District Court for the Western District of Pennsylvania, indictment, Criminal No. 14-118, filed 1 May 2014, 1–48.

24. Chris Demchak, "Cybered Conflict, Cyber Power, and Security Resilience as Strategy," in *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, ed. Derek S. Reveron (Washington, DC: Georgetown University Press, 2012), 121–36.

25. Peter Dombrowski and Chris Demchak, "Cyber War, Cybered Conflict, and the Maritime Domain," *Naval War College Review* 67, no. 2 (Spring 2014), 3, https://www.usnwc.edu/getattachment/762be9d8-8bd1-4aaf-8e2f-c0d9574afec8/Cyber-War,-Cybered-Conflict,-and-the-Maritime-Doma.aspx.

26. Adrian Croft and Peter Apps, "NATO Websites Hit in Cyber Attack Linked to Crimea Tension," *Reuters*, 16 March 2014, http://www.reuters.com/article/2014/03/16/us-ukraine-nato-idUSBREA2E0T320140316.

27. Mark Clayton, "Massive Cyberattacks Slam Official Sites in Russia, Ukraine," *Christian Science Monitor*, 18 March 2014, http://www.csmonitor.com/World/Security-Watch/Cyber-Conflict-Monitor/2014/0318/Massive-cyberattacks-slam-official-sites-in-Russia-Ukraine; and Jeffrey Carr, "Rival Hackers Fighting Proxy War over Crimea," *CNN Opinion*, 25 March 2014, http://www.cnn.com/2014/03/25/opinion/crimea-cyber-war/.

28. Mandiant, *M Trends: Beyond the Breach* (Alexandria, VA: Mandiant, April 2014), 1–7, https://dl.mandiant.com/EE/library/WP_M-Trends2014_140409.pdf; and Patrick Tucker, "Syrian Electronic Army Threatens to Hack CENTCOM," *Defense One*, 3 March 2014, http://www.defenseone.com/technology/2014/03/syrian-electronic-army-threatens-hack-centcom/79777/.

29. Martin E. Dempsey, "Defending the Nation at Network Speed" (discussion, Brookings Institution, 27 June 2013), http://www.brookings.edu/events/2013/06/27-defense-cyber security-dempsey.

30. *Hearing to Consider the Nominations of: Gen Paul J. Selva, USAF, for Reappointment to the Grade of General and to be Commander, US Transportation Command; and VADM Michael S. Rogers, USN, to be Admiral and Director, National Security Agency/Chief, Central Security Services/Commander, US Cyber Command; Statements Before the Senate Committee on Armed Services*, US Senate, 113th Cong., 2nd sess., 11 March 2014, http://www.armed-services.senate.gov/imo/media/doc/14-16%20-%203-11-14.pdf.

31. Zachary Fryer-Biggs, "US Cyber Moves beyond Protection," *Defense News*, 16 March 2014, http://www.defensenews.com/article/20140316/DEFREG02/303170013/US-Cyber-Moves-Beyond-Protection.

32. Joint Publication 3-0, *Joint Operations*, 11 August 2011, V-10 and V-39.

33. Schuyler Foerster, "Theoretical Foundations: Deterrence in the Nuclear Age," in *American Defense Policy*, 6th ed., ed. Schuyler Foerster and Edward Wright (Baltimore, MD: Johns Hopkins University Press, 1990), 47–51.

34. Roger G. Harrison, Deron R. Jackson, and Collins G. Shackelford, "Space Deterrence: The Delicate Balance of Risk," *Space and Defense* 3, no. 1 (Summer 2009): 1–30.

35. William A. Chambers, "Foreword," in *Thinking about Deterrence: Enduring Questions in a Time of Rising Powers, Rogue Regimes, and Terrorism*, ed. Adam Lowther (Maxwell AFB, AL: Air University Press, 2014), xii.

36. Adam Lowther, "The Evolution of Deterrence," in *Thinking about Deterrence: Enduring Questions in a Time of Rising Powers, Rogue Regimes, and Terrorism*, ed. Adam Lowther (Maxwell AFB, AL: Air University Press, 2014), 3–4.

37. DOD, *Department of Defense Cyberspace Policy Report* (Washington, DC: DOD, November 2011), 7, http://www.defense.gov/home/features/2011/0411_cyberstrategy/docs/NDAA%20Section%20934%20Report_For%20webpage.pdf.

38. DOD, *Department of Defense Strategy for Operating in Cyberspace*, July 2011, 13, http://www.defense.gov/news/d20110714cyber.pdf.

39. Herbert S. Lin, "Defining Self-Defense for the Private Sector in Cyberspace," *World Politics Review*, 6 February 2013, 2, http://www.worldpoliticsreview.com/articles/12694/defining-self-defense-for-the-private-sector-in-cyberspace.

40. Patience Wait, "Cyberthreats Grow More Ominous: Former NSA Chief," *Information Week*, 11 October 2013, http://www.darkreading.com/risk-management/cyberthreats-grow-more-ominous-former-nsa-chief/d/d-id/1111912?.

41. Executive Office of the President, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* (Washington, DC: The White House, May 2011), 13–14, http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

42. Michael N. Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare* (New York: Cambridge University Press, May 2013), 54–61.

43. Michael N. Schmitt, "Attack as a Term of Art in International Law: The Cyber Operations Context," in *4th International Conference on Cyber Conflict*, ed. C. Czosseck, R. Ottis, and K. Ziolkowski (Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2012), 283–93.

44. Martin R. Stytz and Sheila B. Banks, "Toward Attaining Cyber Dominance," *Strategic Studies Quarterly* 8, no. 1 (Spring 2014), 60, http://www.au.af.mil/au/ssq/digital/pdf/spring_2014/stytz.pdf.

45. North Atlantic Treaty Organization (NATO), "Defending the Networks: The NATO Policy on Cyber Defence" (policy statement, NATO, Brussels, Belgium, 8 June 2011.

46. Vincent Joubert, "Five Years after Estonia's Cyber Attacks: Lessons Learned for NATO?" (research paper 76, NATO Defense College, Rome, Italy, 2012), 5, http://www.ndc.nato.int/news/current_news.php?icode=394.

47. Maren Leed, *Offensive Cyber Capabilities at the Operational Level* (Washington, DC: Center for Strategic & International Studies, September 2013), 2–3, http://csis.org/files/publication/130916_Leed_OffensiveCyberCapabilities_Web.pdf.

48. Herbert Lin, "Escalation Dynamics and Conflict Termination in Cyberspace," *Strategic Studies Quarterly* 6, no. 3 (Fall 2012), 52–55, http://www.au.af.mil/au/ssq/2012/fall/lin.pdf.

49. James Andrew Lewis, "Truly Damaging Cyberattacks Are Rare," *Washington Post*, 10 October 2013, http://www.washingtonpost.com/postlive/truly-damaging-cyberattacks-are-rare/2013/10/09/ae628656-2d00-11e3-b139-029811dbb57f_story.html.

50. Sean Lawson, "Putting the War in Cyberwar: Metaphor, Analogy, and Cybersecurity Discourse in the United States," *First Monday* 17, no. 7 (2 July 2012), http://firstmonday.org/ojs/index.php/fm/article/view/3848/3270.

51. Martin Libicki, "Pulling Punches in Cyberspace," in *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for US Policy* (Washington, DC: National Academies Press, 2010), 123–47.

52. Lumension, *Redefining Defense-in-Depth* (Scottsdale, AZ: Lumension, March 2014), 1–6, https://www.lumension.com/Media_Files/Documents/Marketing---Sales/Whitepapers/Redefining-Defense-in-Depth.aspx.

53. Ed Metcalf, *Counter Stealth Malware* (Santa Clara, CA: McAfee, 2013), 1–3, http://www.mcafee.com/us/resources/solution-briefs/sb-counter-stealth-malware.pdf.

54. Lumension, *Preventing Weaponized Malware Payloads in Advanced Persistent Threats* (Scottsdale, AZ: Lumension, February 2013), 1–4, https://www.lumension.com/Media_Files/Documents/Marketing---Sales/Whitepapers/Lumension_2013-Febl_wp_Preventing_Weaponized_Malwa.aspx.

55. Council on CyberSecurity, *Critical Controls for Effective Cyber Defense*, version 4.1 (Bethesda, MD: SANS [SysAdmin, Audit, Networking, and Security], Institute, March 2013), https://ccsfiles.blob.core.windows.net/web-site/file/81d5ad9c89d242a7a555658e604fdc43/Critical%20Controls%20v4.1.pdf.

56. John Pescatore and Tony Sager, *Critical Security Controls Survey: Moving from Awareness to Action*, SANS white paper (Bethesda, MD: SANS Institute, June 2013), https://www.sans.org/media/critical-security-controls/CSC_Survey_2013.pdf.

57. National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, version 1.0 (Washington, DC: NIST, 12 February 2014), http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf.

58. Roberta Stempfley and Lawrence Zelvin, *Facilitating Cyber Threat Information Sharing and Partnering with the Private Sector to Protect Critical Infrastructure: An Assessment of DHS Capabilities; Hearing before the House Committee on Homeland Security, US House of Representatives*, 113th Cong., 1st sess., 16 May 2013, http://www.gpo.gov/fdsys/pkg/CHRG-113hhrg85613/html/CHRG-113hhrg85613.htm.

59. William Jackson, "Social Platform for Sharing Cyberthreat Intell Goes Live," *Government Computer News*, 11 February 2014, 6, http://gcn.com/articles/2014/02/11/activetrust.aspx.

60. Keith B. Alexander, *Statement of Gen Keith B. Alexander Commander US Cyber Command before the House Committee on Armed Services Subcommittee on Intelligence, Emerging Threats and Capabilities, US House of Representatives*, 113th Cong., 2nd sess., 12 March 2014, http://docs.house.gov/meetings/AS/AS26/20140312/101883/HHRG-113-AS26-Wstate-AlexanderUSAK-20140312.pdf.

61. Department of Homeland Security (DHS), *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience* (Washington, DC: DHS, March 2013), 1–14, http://www.dhs.gov/sites/default/files/publications/NIPP%202013_Partnering%20for%20Critical%20Infrastructure%20Security%20and%20Resilience_508_0.pdf.

62. Verizon, *2014 Data Breach Investigations Report* (New York: Verizon, June 2014), 41, http://www.verizonenterprise.com/DBIR/2014/reports/rp_Verizon-DBIR-2014_en_xg.pdf.

63. Martin C. Libicki, "Why Cyber War Will Not and Should Not Have Its Grand Strategist," *Strategic Studies Quarterly* 8, no. 1 (Spring 2014): 23–39, http://www.au.af.mil/au/ssq/digital/pdf/spring_2014/Libicki.pdf.

64. UN General Assembly, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/68/98 (New York: UN, 24 June 2013), 4, http://www.un.org/ga/search/view_doc.asp?symbol=A/68/98.

65. Ibid., 6–8.

66. Louise Arimatsu, "A Treaty for Governing Cyber-Weapons," in *4th International Conference on Cyber Conflict*, ed. C. Czosseck, R. Ottis, and K. Ziolkowski (Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2012), 91–109, http://www.ccdcoe.org/publications/2012proceedings/2_3_Arimatsu_ATreatyForGoverningCyber-Weapons.pdf.

67. DOD, *Department of Defense Cyberspace Policy Report*, 8.

68. Kevin G. Coleman, “Aggression in Cyberspace,” in *Conflict and Cooperation in the Global Commons: A Comprehensive Approach for International Security*, ed. Scott Jasper (Washington, DC: Georgetown University Press, 2012), 109–16.

69. Aditya Balapure,“Cyber Weapon of Mass Destruction—The Blackhole Exploit Kit,” *INFOSEC Institute*, 2 May 2013, http://resources.infosecinstitute.com/cyber-weapon-of-mass-destruction-the-blackhole-exploit-kit/.

70. H. E. Yun Byung-se, Minister of Foreign Affairs, “Statement by the Conference Chair” (Seoul Conference on Cyberspace, Seoul, South Korea, 17–18 October 2013), http://www.mofat.go.kr/english/visa/images/res/StatementbytheConferenceChair.pdf.

71. Executive Office of the President, “Fact Sheet: US–Russian Cooperation on Information and Communications Technology Security” (fact sheet, Washington, DC, 17 June 2013), http://www.whitehouse.gov/the-press-office/2013/06/17/fact-sheet-us-russian-cooperation-information-and-communications-technol.

72. Ellen Nakashima, “Indictment of PLA Hackers Is Part of Broad U.S. Strategy to Curb Chinese Cyberspying,” *Washington Post*, 22 May 2014, http://www.washingtonpost.com/world/national-security/indictment-of-pla-hackers-is-part-of-broad-us-strategy-to-curb-chinese-cyberspying/2014/05/22/a66cf26a-e1b4-11e3-9743-bb9b59cde7b9_story.html.

73. Sui-Lee Wee, “In Cyber Spying Row, Chinese Media Call U.S. a ‘Mincing Rascal,’” *Reuters*, 21 May 2014, http://uk.reuters.com/article/2014/05/21/uk-cybercrime-usa-china-media-idUKKBN0E107K20140521.

74. Robert S. Dewar, “The Triptych of Cyber Security: A Classification of Active Cyber Defense,” in *Proceedings 6th International Conference on Cyber Conflict*, ed. P. Brangetto, M. Maybaum, and J. Stinissen (Tallinn, Estonia: CCD COE, June 2014), 7–21, http://www.ccdcoe.org/cycon/2014/proceedings/d1r1s9_dewar.pdf.

75. Brett T. Williams, “The Joint Force Commander’s Guide to Cyberspace Operations,” *Joint Forces Quarterly* 73, no. 2 (2014), 12–19, http://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-73/jfq-73_12-19_Williams.pdf.

76. James P. Farwell and Rafal Rohozinski, “The New Reality of Cyber War,” *Survival: Global Politics and Strategy* 54, no. 4 (August–September 2012), 110, https://www.iiss.org/en/publications/survival/sections/2012-23ab/survival--global-politics-and-strategy-august--september-2012-f9ce/54-4-09-farwell-and-rohozinski-6b6d.

77. Franklin D. Kramer and Melanie J. Teplinsky, “Cybersecurity and Tailored Deterrence” (issue brief, Atlantic Council, Washington, DC, December 2013), 6, http://www.atlanticcouncil.org/images/publications/Cybersecurity_and_Tailored_Deterrence.pdf.

78. Jeffery Carr, “Cyber Laws May Need Tweaking,” *SC Magazine*, 3 December 2012, http://www.scmagazine.com/cyber-laws-may-need-tweaking/article/268650/.

79. Irving Lachow, “Active Cyber Defense: A Framework for Policy Makers” (policy brief, Center for a New American Security, Washington, DC, February 2013), 1–10, http://www.cnas.org/files/documents/publications/CNAS_ActiveCyberDefense_Lachow_0.pdf.

80. 18 US Code § 1030—*Fraud and Related Activity in Connection with Computers*, http://www.gpo.gov/fdsys/pkg/USCODE-2010-title18/pdf/USCODE-2010-title18-partI-chap47-sec1030.pdf.

81. William A. Owens, Kenneth W. Dam, and Herbert S. Lin, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities* (Washington, DC: National Academies Press, 2012), 204–05.

82. Hexis Cyber Solutions, “HawkEye G: The Active Defense Grid” (fact sheet, Hexis Cyber Solutions, Hanover, MD, 2013), http://www.hexiscyber.com/products/hawkeye-g.

[83] US Joint Staff J-7, "Foreword," in *Unity of Effort Framework Solution Guide* (Suffolk, VA: DOD, 31 August 2014), http://www.dtic.mil/doctrine/doctrine/jwfc/uef_solution_guide.pdf.

[84] Executive Office of the President, *Cyberspace Policy Review, Assuring a Trusted and Resilient Information and Communication Infrastructure* (Washington, DC: White House, May 2009), i.

[85] Ministry of Defence, United Kingdom, "The Comprehensive Approach," Joint Discussion Note 4/05 (Shrivenham, UK: Joint Doctrine and Concepts Centre, 2006), 1-4–1-5, http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0CCAQFjAA&url=http%3A%2F%2Fwww.arrc.nato.int%2Fsystems%2Ffile_download.ashx%3Fpg%3D3313%26ver%3D1&ei=fYqtVL-IMYiyggTulYPoAw&usg=AFQjCNEF5Hllu9tO_UUFuwzRhg7aludNtg&sig2=wAbfdmhadcjpikYwAlz9fg&bvm=bv.83134100,d.eXY.

[86] NATO, "A Comprehensive Approach," 27 October 2010, http://www.nato.int/cps/en/SID-3F43C5C6-1F3BD449/natolive/topics_51633.htm?blnSublanguage=true&selectedLocale=uk&submit=select.

[87] Executive Office of the President, *The Comprehensive National Cybersecurity Initiative* (Washington, DC: White House, 5 March 2010), 5, http://www.whitehouse.gov/sites/default/files/cybersecurity.pdf.

[88] Michael Hallet and Oke Thorngren, "Attempting a Comprehensive Approach Definition and Its Implications for Reconceptualizing Capability Development," in *Capability Development in Support of Comprehensive Approaches: Transforming International Civil-Military Interactions*, ed. Derrick J. Neal and Linton Wells II (Washington, DC: National Defense University, December 2011), 36, http://mercury.ethz.ch/serviceengine/Files/ISN/142718/ipublicationdocument_singledocument/f6211158-d4b8-4e9b-ae68-c719f6e3a404/en/full+text.pdf.

[89] Larry Clinton, "Cyber Security Social Contract," in *Conflict and Cooperation in the Global Commons: A Comprehensive Approach for International Security*, ed. Scott Jasper (Washington, DC: Georgetown University Press, 2012), 185–98.

[90] European Union, "International Code of Conduct for Outer Space Activities," version 16 September 2013, 1–12.

[91] Brandon Valeriano and Ryan Maness, "The Fog of Cyberwar," *Foreign Affairs*, 21 November 2012, http://www.foreignaffairs.com/articles/138443/brandon-valeriano-and-ryan-maness/the-fog-of-cyberwar.

[92] Jennifer O'Mahony, "Stuxnet Worm 'Increased' Iran's Nuclear Potential," *Telegraph* (UK), 15 May 2013, http://www.telegraph.co.uk/technology/news/10058546/Stuxnet-worm-increased-Irans-nuclear-potential.html.

[93] Colin S. Gray, *Making Strategic Sense of Cyber Power: Why the Sky Is Not Falling* (Carlisle, PA: Strategic Studies Institute, US Army War College Press, April 2013), 43–54, http://www.strategicstudiesinstitute.army.mil/pdffiles/PUB1147.pdf.

[94] Bob Gourley, "Reference to Cyber Security 'Wake-Up Calls,'" *CTOvision.com* (web site), 30 November 2013, https://ctovision.com/2013/11/reference-cyber-security-wake-calls/.

[95] James R. Clapper, *Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community; House Permanent Select Committee on Intelligence, US House of Representa-*

tives, 113th Cong., 2nd sess., 4 February 2014, 1, http://www.dni.gov/index.php/newsroom/testimonies/203-congressional-testimonies-2014/1011-statement-for-the-record-worldwide-threat-assessment-of-the-us-intelligence-community-hpsci.

96. Catherine Herridge, "NSA Director: China Can Damage US Power Grid," *FoxNews.com*, 20 November 2014, http://www.foxnews.com/politics/2014/11/20/nsa-director-china-can-damage-us-power-grid/.

97. James G. Stavridis, "The Comprehensive Approach in Afghanistan," *PRISM* 2 no. 2 (March 2011): 65–76, http://cco.dodlive.mil/files/2014/02/Prism_65-76_Stavridis.pdf.

98. Martin E. Dempsey, "Defending the Nation at Network Speed."

99. DOD, *Quadrennial Defense Review 2014*, 15.

100. Alan Zibel, "Lew Cautions on Financial Threat from Lone Hackers," *Washington Wire* (blog) on *Wall Street Journal* (web site), 5 October 2014, http://blogs.wsj.com/washwire/2014/10/05/lew-cautions-of-financial-threat-from-lone-hackers/.

101. Hugh Son and Michael Riley, "JP Morgan Password Leads Hackers to 76 Million Households," *Bloomberg News*, 3 October 2014, http://www.bloomberg.com/news/2014-10-03/jpmorgan-password-said-to-lead-hackers-to-76-million-households.html.

102. Jessica Silver-Greenberg, Matthew Goldstein and Nicole Perlroth, "JPMorgan Chase Hack Affects 76 Million Households," *New York Times*, 2 October 2014, http://dealbook.nytimes.com/2014/10/02/jpmorgan-discovers-further-cyber-security-issues/?_r=0.

103. James Andrew Lewis, "Cyber Threat and Response: Combating Advanced Attacks and Cyber Espionage" (white paper, Center for Strategic and International Studies, Washington, DC, March 2014), 1–8, http://csis.org/files/publication/140313_FireEye_WhitePaper_Final.pdf. These tactics are seen in Dragonfly, an ongoing cyberespionage campaign targeting the energy sector that began with malware in phishing e-mails to executives, shifted to the compromise of energy-related web sites, and continued with infection of legitimate software packages available for download by equipment providers; and Keith B. Alexander, Emily Goldman, and Michael Warner, "Defending America in Cyberspace," *National Interest* (November/December 2013), 24. While it is uncertain how damaging coordinated cyber attacks could be if mounted on a national scale, the Dragonfly campaign achieved sabotage capabilities that could have caused disruption to energy supplies.

104. US Strategic Command, *Deterrence Operations Joint Operating Concept*, version 2.0 (Washington, DC: DOD, December 2006), 7–27, http://www.dtic.mil/doctrine/concepts/joint_concepts/joc_deterrence.pdf.

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.