Policy Analysis

CATO INSTITUTE

January 15, 2019 | Number 862

The Myth of the Cyber Offense

The Case for Restraint

By Brandon Valeriano and Benjamin Jensen

EXECUTIVE SUMMARY

Great-power competition in the 21st century increasingly involves the use of cyber operations between rival states. But do cyber operations achieve their stated objectives? What are the escalation risks? Under what conditions could increasingly frequent and sophisticated cyber operations result in inadvertent escalation and the use of military force? The answers to these questions should inform U.S. cybersecurity policy and strategy.

In the context of recent shifts in cybersecurity policy in the United States, this paper examines the character of cyber conflict through time. Data on cyber actions from 2000 to 2016 demonstrate evidence of a restrained domain with few aggressive attacks that seek a dramatic, decisive impact. Attacks do not beget attacks, nor do they deter them. But if few operations are effective in compelling the enemy and fewer still lead to responses in the domain, why would a policy of offensive operations to deter rival states be useful in cyberspace?

We demonstrate that, while cyber operations to date have not been escalatory or particularly effective in achieving decisive outcomes, recent policy changes and strategy pronouncements by the Trump administration increase the risk of escalation while doing nothing to make cyber operations more effective. These changes revolve around a dangerous myth: offense is an effective and easy way to stop rival states from hacking America. New policies for authorizing preemptive offensive cyber strategies risk crossing a threshold and changing the rules of the game.

Cyberspace to date has been a domain of political warfare and coercive diplomacy. An offensively postured cyber policy is dangerous, counterproductive, and undermines norms in cyberspace. Many have promoted the idea of a coming "Cyber Pearl Harbor," but instead the domain is littered with covert operations meant to manage escalation and deter future attacks. Cyber strategy and policy must start from an accurate understanding of the domain, not imagined realities.

Senior leaders throughout the federal government should consider a more prudent and restrained approach to cyber operations. We argue for a defensive posture consisting of limited cyber operations aimed at restraining rivals and avoiding escalation. At the same time, the United States should focus on protective measures to make U.S. systems less vulnerable and on sharing intelligence with allies and partners. A policy of restraint that maintains control over the weapons of cyber war is strategically wise.

Brandon Valeriano is the Donald Bren Chair of Armed Politics at Marine Corps University. Benjamin Jensen is an associate professor at the Marine Corps University and a scholar-in-residence at American University's School of International Service.

"Recent policy shifts create a new risk of inadvertent escalation."

INTRODUCTION

In the summer of 2017, the Trump administration faced a series of stark choices for compelling North Korea to abandon its ballistic missile tests and its nuclear program. Under the previous administration, the United States used cyber operations in an effort to degrade North Korean weapons development through targeting "command, control, telemetry and guidance systems, before or during a North Korean missile test launch."[1] These cyber operations failed to halt North Korean weapons development, but they demonstrated U.S. capability while avoiding escalation.

This approach was consistent with the Department of Defense 2015 Cyber Strategy, which called for developing "viable cyber options [that] . . . control conflict escalation and shape the conflict environment at all stages."[2] In developing these options against China and other powers, Tom Bossert, Trump's former homeland security adviser, reportedly argued for coordinating these covert signals with economic policy and "other elements of national power to prevent bad behavior online."[3] President Trump's response, according to journalist Bob Woodward: "you and your cyber . . . are going to get me in a war—with all your cyber shit."[4]

This episode illustrates the core questions regarding offensive cyber operations. In the 21st century, great powers wage a constant battle in the digital shadows by exploiting the connectivity of our world to undermine rivals. But do cyber operations actually achieve stated foreign policy objectives? Relatedly, what are the escalation risks? Under what conditions could increasingly frequent and sophisticated cyber operations result in inadvertent escalation? The answers to these questions should inform U.S. cybersecurity policy.

Cyber operations to date have not been escalatory or particularly effective in decisively achieving desired outcomes. Recent policy changes and strategy pronouncements by the Trump administration, however, could make escalation more likely while doing nothing to improve effectiveness. These changes are driven by a dangerous myth that offense is an effective and easy way to stop rival states from hacking America.

New policies for authorizing preemptive offensive cyber strategies risk crossing a threshold and changing the rules of the game. Cyberspace, to date, has been a domain of political warfare and coercive diplomacy, a world of spies developing long-term access and infrastructure for covert action, not soldiers planning limited-objective raids. Recent policy shifts appear to favor the soldier over the spy, thus creating a new risk of offensive cyber events triggering inadvertent escalation between great powers.

Senior leaders throughout the federal government should consider a more prudent and restrained approach to cyber operations. Building on Sir Julian Corbett's *Principles of Maritime Strategy*, one of the preeminent works in 20th century military theory, we argue for a defensive posture consisting of limited cyber operations aimed at restraining rivals and avoiding escalation.[5] This approach counsels stepping back from preemption and focusing on sharing intelligence and hardening targets (that is, updating systems to repair existing vulnerabilities). The United States should exercise restraint and avoid preemptive strikes against great powers in cyberspace.

MAJOR CYBER OPERATIONS, 2000–2016

- 89 (32.7%) disruption
- 148 (54.4%) espionage
- 35 (12.9%) degradation

Source: Dyadic Cyber Incidents Dataset version 1.5, maintained by the authors. See Ryan C. Maness, Brandon Valeriano, and Benjamin Jensen, "The Dyadic Cyber Incident and Dispute Dataset, Version 1.1," 2017.

CYBER COMMAND'S NEW, MORE AGGRESSIVE POLICY

In April 2018, United States Cyber Command released a new vision statement calling for "persistent action"[6] to maintain cyber superiority.[7] The document echoed other major studies portraying the United States as ceding the digital high ground to adversaries. For example, a 2018 Defense Science Board study claimed the "the United States has fallen behind its competitors in the cyber domain, both conceptually and operationally."[8] Similarly, the Cyber Command vision statement portrays other great powers as increasingly capable of deploying sophisticated cyber actions against the United States. Major competitors, according to the statement, are using cyber operations to alter the long-term balance of power, short of military force.[9] In using cyber operations to undermine American power, it claims these actors—especially strategic competitors such as Russia and China—are threatening not just the U.S. military but the entire global infrastructure and open exchange of information. In fact, according to General Paul M. Nakasone, commanding general of Cyber Command, "the environment we operate in today is truly one of great-power competition, and in these competitions, the locus of the struggle for power has shifted towards cyberspace."[10]

In response to these threats, Cyber Command contends that the United States needs a more aggressive strategy. Cyber Command envisions a new era of persistent action that retains cyber superiority for the United States. Drawing on military doctrine, the document defines cyberspace superiority as "the degree of dominance in cyberspace by one force that permits the secure, reliable conduct of operations by that force, and its related land, air, maritime, and space forces at a given time and place without prohibitive interference by an adversary." In this view, the United States must command the digital commons to ensure other nonmilitary actors can access and use the new domain. Doing so requires persistence, defined as "the continuous ability to anticipate the adversary's vulnerabilities, and formulate and execute cyberspace operations to contest adversary courses of action under determined conditions."[11]

This approach increasingly sees preemption as the only viable path to security. U.S. cyber operations will "influence the calculation of our adversaries, deter aggression, and clarify the distinction between acceptable and unacceptable behavior in cyberspace," and, as a result, "improve the security and stability of cyberspace."[12] Achieving this new stability through persistent action depends on "scaling to the magnitude of the threat, removing constraints on [U.S.] speed and agility, and maneuvering to counter adversaries and enhance national security."[13] In other words, the United States must go on the offense and preempt threats in the cyber domain as a means of ensuring stability.

Cyber Command emphasizes a constant state of competition beneath the threshold of armed conflict and underscores the need for faster responses to adversary attacks. This parallels broader policy developments in the Trump administration. First, persistent action is linked to the concept of "contact" in the 2018 National Defense Strategy.[14] The new defense strategy, along with the 2018 National Security Strategy, envisions constant competition between great powers as the norm in the 21st century.[15] Renewed great-power competition requires a global operating model comprised of four layers (contact, blunt, surge, and homeland) designed to help the United States "compete more effectively below the level of armed conflict; delay, degrade, or deny adversary aggression; surge war-winning forces and manage conflict escalation; and defend the U.S. homeland."[16] In this model, cyberspace becomes another domain in which the United States must achieve command of the commons to guarantee the larger international order.

Securing command of the commons in the face of increasing cyber operations by China and Russia requires a policy framework that accelerates cyber offense. Offensive cyber operations entail missions "intended to project

"Cyber Command contends that the United States needs a more aggressive strategy."

"What the cyber hegemon (the United States) does defines the character of cyber operations."

power in and through foreign cyberspace."[17] In August 2018, Trump granted the military the initiative to launch offensive cyber operations with what appears to be little interagency consultation or coordination.[18] Cyberspace became a domain for soldiers, not just networks of spies. The move represented a dramatic shift from the restraints on cyber operations imposed by the Obama administration.

Obama's Presidential Policy Directive 20 originally specified the conduct and content of cyberspace operations. Secretly issued in October 2012 after Congress failed to provide guidance for cyber operations, the directive authorized offensive cyber operations under certain conditions and only after careful interagency vetting.[19] All operations had to be consistent with American values and had to balance the effectiveness of operations with the risk to all targets, as determined by the president and the national security adviser.[20]

This policy framework required decisionmakers to ask whether more conventional operations would be better suited for the target as well as the extent to which the operation might compromise other espionage and cyber operations. It also sought to ensure cyber effects were nonlethal and limited in magnitude: a clear attempt to avoid escalation. Similarly, the guidelines portrayed cyberspace as dynamic and boundless, increasing the risk that operations spill over to affect partner countries or impact American citizens.

In moving to the new framework, the Trump administration appears to be changing the rules of the game in cyberspace. North Korea, Iran, Russia, and China have long been exploiting the digital connectivity of our world for covert operations to gain a position of advantage. They have exhibited less restraint or concern for the consequences of militarizing cyberspace than the United States. Yet, what the cyber hegemon (the United States) does defines the character of cyber operations much more than these secondary actors.[21] Despite increasingly sophisticated operations, between 2000 and 2016 cyberspace was a domain defined by political warfare and covert signaling to control escalation more than it was an arena of decisive action.[22] Taking a more offensive posture and preempting threats at their source, an action implied by the Cyber Command Vision Statement, has the potential to change the character of cyber operations, and through it, 21st century great-power competition.[23]

THE CHARACTER OF CYBER OPERATIONS, 2000–2016

Evaluating the policy debate about offensive cyber operations requires empirically describing prevailing patterns and trends associated with how rival states employ their capabilities. Just as it is perilous to describe all wars based on observations of crucial cases such as the First World War, it is similarly dangerous to assume that high-profile cases such as the Stuxnet operation, which degraded Iranian nuclear capabilities, accurately represent all cyber strategy. Rather, developing cyber policy options and supporting strategies should start with a clear understanding of how states use the digital domain to achieve a position of advantage in long-term competition.

Between 2000 and 2016, there have been 272 documented cyber operations between rival states.[24] These exchanges are best thought of as major operations involving a foreign policy impact. Each operation therefore might involve thousands, if not millions, of individual incidents as adversaries hijack computer networks to launch distributed denial of service attacks (DDoS) or use sustained spear-phishing campaigns to gain access to key systems. Like other forms of covert action, for every cyber operation we learn about, there are surely countless others we do not know about, as well as failed access attempts.

Using the Dyadic Cyber Incident Dataset, we can categorize these operations based on three major tactics: disruption, espionage, and degradation.[25] Cyber disruptions are low-cost, low-pain initiatives, such as DDoS attacks and website defacements, that harass a target to signal resolve and gain a temporary position of advantage.[26] Cyber espionage reflects efforts

to alter the balance of information in a way that enables coercion.[27] Cyber degradations are higher-cost, higher-pain-inducing efforts that seek to degrade or destroy some aspect of the target's cyberspace networks, operations, or functions.[28] As strategies for achieving a position of advantage, degradation attacks typically involve coercion or efforts to compel or deter an adversary.[29]

To date, cyber operations do not appear to produce concessions by themselves. Offense, whether disruption, espionage, or degradation, does not produce lasting results sufficient to change the behavior of a target state.[30] Only 11 operations (4 percent) appear to have produced even a temporary political concession, with the majority associated with sustained, multiyear counterespionage operations by U.S. operatives usually targeting China or Russia.[31] Furthermore, each of these operations involved not just cyber actions, but other instruments of national power, such as diplomatic negotiations, economic sanctions, and military threats.[32]

Under the Obama administration, these operations were calibrated to limit escalation risks and took place alongside a larger series of diplomatic maneuvers designed to manage great-power relationships. For example, the United States used an interagency response to Chinese hacking that included covert retaliation but also involved pursuing a 2015 agreement to limit cyber-enabled economic warfare.[33] In response to Russian actions, the United States pursed a mix of sanctions, diplomatic maneuvers, and cyber actions.

This strategy of combining active defense and coercive diplomacy, the use of positive and negative instruments of power to alter adversary behavior, was also on display in Buckshot Yankee, the code name given to the U.S. retaliation against a massive intrusion of Defense Department networks by Russia in 2008.[34] Notably, many in the cybersecurity community view such activities as defensive counterstrikes designed to raise the costs of future adversary incursions into U.S. networks, rather than viewing them as preemptive offensive actions.[35] Cyber operations rarely work in isolation, and when they do, they tend to involve very sophisticated capabilities that impose costs and risks on the attacker.[36] Because such attacks can degrade or even destroy the target's networks and operations in the short term, they can also undermine espionage operations that rely on gathering information over the long term. Degradation attacks therefore make up the minority (14.76 percent) of documented operations between rival states. The majority of cyber operations were limited disruptions and espionage.

It is thus not surprising that given the limited objectives of most cyber operations, to date rival states have tended to respond proportionally or not at all. Returning to the data, between 2000 and 2016, only 89 operations (32.72 percent) saw a retaliatory cyber response within one year. Of those, 54 (60.7 percent) were at a low-level response severity (e.g., website defacements, limited denial of service attacks, etc.). Table 1 in the appendix compares the severity scores for cyber operations between rival states between 2000 and 2016.[37] When rival states do retaliate, the responses tend to be proportional: that is, they tend to match the severity of the initial attack.[38]

Low-level responses beget low-level counterresponses as states constantly engage in a limited manner consistent with the ebbs and flows of what famed Cold War nuclear theorist Herman Kahn called "subcrisis maneuvering."[39] Rarely does a response include an increase in severity. Instead, we witness counterresponses of a similar or lower level than the original intrusion or a response outside the cyber domain (for example, economic sanctions or legal indictment of specific individuals). The engagement is persistent but managed, and often occurs beneath an escalatory threshold.[40] As seen in Table 2 in the appendix, this behavior appears to apply equally to each possible cyber strategy: disruption, espionage, and degradation. Espionage saw little retaliatory escalation, while disruption and degradation both exhibited more low-level responses.

Of the remaining 35 operations that prompted retaliation, 25 (71.4 percent) were related

"Cyber operations do not appear to produce concessions by themselves."

> "Rival states use cyber operations as a substitute for riskier military operations."

to U.S. active defense responses to repeated Russian and Chinese cyber operations. That is, the United States preferred to wait on adversary networks, develop intelligence, and retaliate with precise strikes designed to undermine specific threats. This strategy was not preemptive. Consistent with the idea of active defense, the strategy is best thought of as a counterattack that exploits rival network intrusions.

Cyber operations also offer a means of signaling future escalation risk as well as a cross-domain release valve for crises. Rival states use cyber operations as a substitute for riskier military operations. Consider the standoff between Russia and Turkey in 2016. After a Turkish F-16 shot down a Russian Su-24 Fencer, a wave of DDoS attacks hit Turkish state-owned banks and government websites.[41] Similarly, China is responding to U.S. tariffs and increased freedom of navigation operations—provocatively sailing U.S. warships in waters that China claims—with increased cyber activity targeting military networks.[42] Russia is using a broad-front cyber campaign in response to Western sanctions, infiltrating targets ranging from the anti-doping agencies and sports federations to Westinghouse, which builds nuclear power plants, and the Hague-based Organization for the Prohibition of Chemical Weapons.[43] Rather than escalate with conventional military operations, cyber operations offer rivals a way to respond to provocations without significantly increasing tensions in a crisis. Better to have a Russian DDoS attack temporarily shut down Turkish networks than for Russian long-range missiles to target Turkish military bases.

THE MYTH OF THE OFFENSE

Contrary to observed patterns of limited disruption and espionage, Cyber Command sees cyberspace as a domain fraught with increasing risk, where great powers such as China and Russia will undermine American power. The only solution, from this perspective, is to go on the offense. Yet, the benefits of an offensive posture, especially in cyberspace, are mostly illusory to date. Instead, the cyber domain tends to be optimized for defense and deception, not decisive offensive blows. Not only is offense likely the weaker form of competition in cyberspace, it also risks inadvertent escalation. The fear, suspicion, and misperception that characterize interstate rivalries exacerbate the risk of offensive action in cyberspace.

Cyber Command's 2018 persistent-action strategy aims to "expose adversaries' weaknesses, learn their intentions and capabilities, and counter attacks close to their origins."[44] Put in simple terms, the best defense is a good offense: get on adversary networks and stop cyber operations targeting the United States before they occur. Under this strategy, offensive cyber operations will also be preemptive in that they are designed to "contest dangerous adversary activity before it impairs [U.S.] national power."[45] To use another sports metaphor, come out swinging. Go on the offense first and establish escalation dominance (that is, demonstrating such superior capabilities over the target state that it can't afford to escalate in response).[46]

According to Cyber Command, preemptive strikes will "impose . . . strategic costs on our adversaries, compelling them to shift resources to defense and reduce attacks."[47] Whether through punishment, risk, or denial strategies, offensive actions theoretically alter the target's behavior by increasing the expected costs of targeting U.S. interests.[48] Offensive action, according to this thinking, deters future aggression by signaling resolve and establishing escalation dominance. Yet, there are well-established reasons to doubt that offensive options produce the intended results in cyberspace.

Defense and Deception

The rationale behind persistent action—that the best defense is a good offense—is deeply flawed. In fact, most military and strategic theory holds that the defense is the superior posture.[49] For example, Sun Tzu describes controlling an adversary to make their actions more predictable, and hence easy to undermine, by baiting them to attack strong points.[50]

The stronger form of war is a deception-driven defense: confusing an attacker so that they waste resources attacking strong points that appear weak. This parallels cybersecurity scholars Erik Gartzke and Jon Lindsay's claim that cyberspace is not offense dominant, but deception dominant.[51] Rather than persistent action and preemptive strikes on adversary networks, the United States needs persistent deception and defensive counterstrikes optimized to undermine adversary planning and capabilities.

Fear and the Security Dilemma

New policy options proposed by Cyber Command and the Trump administration risk exacerbating fear in other countries and creating a self-reinforcing spiral of tit-for-tat escalations that risk war even though each actor feels he is acting defensively—or, as it is called in the scholarly literature, a security dilemma.[52] As shown above, most cyber operations to date have not resulted in escalation. The cyber domain has been a world of spies collecting valuable information and engaging in limited disruptions that substitute for, as well as complement, more conventional options. Shifting to a policy of preemptive offensive cyber warfare risks provoking fear and overreaction in other states and possibly producing conflict spirals. Even limited-objective cyber offensive action defined as "defending forward" can be misinterpreted and lead to inadvertent escalation.[53] As the historian Cathal Nolan puts it, "intrusions into a state's strategically important networks pose serious risks and are therefore inherently threatening."[54]

More worryingly, with a more offensive posture, it will be increasingly difficult for states to differentiate between cyber espionage and more damaging degradation operations.[55] What the United States calls defending forward, China and Russia will call preemptive strikes. Worse still, this posture will likely lead great powers to assume all network intrusions, including espionage, are preparing the environment for follow-on offensive strikes. According to cybersecurity scholar Ben Buchanan, "in the [aggressor] state's own view, such moves are clearly defensive, merely ensuring that its military will have the strength and flexibility to meet whatever comes its way. Yet potential adversaries are unlikely to share this perspective."[56] The new strategy risks producing a "forever cyber war" prone to inadvertent escalation because it implies all cyber operations should be interpreted as escalatory by adversaries.[57]

The Myth of Decisive Cyber Victory

There is a tendency in the military profession, at least in the United States and Europe, to uphold the concept of decisive battle as central to the Western way of war.[58] Often, disruptive technologies—from strategic bombers in the mid-20th century to cyber operations in the 21st century—are seen as providing decisive offensive advantages in crises. In the interwar period between the world wars, airpower enthusiasts argued that bombers would reliably reach their targets, forcing political leaders to end hostilities or face the prospect of destroyed cities and economic collapse.[59]

Yet the search for decisive battle is often an elusive, if not dangerous, temptation for military planners and policymakers. In a comparative historical treatment of major 19th- and 20th-century battles, Nolan argues that "often, war results in something clouded, neither triumph nor defeat. It is an arena of grey outcomes, partial and ambiguous resolution of disputes and causes that led to the choice of force as an instrument of policy in the first place."[60] Decisive victories in any one battle are rare. Adversaries can refuse to fight.[61] They can even signal resolve through demonstrating their ability to endure pain.

Planning and Assessment Pathologies

The new policy framework for offensive cyber operations risks compounding common pathologies associated with strategic assessments and planning. [62] Removing interagency checks increases the risks that an operation will backfire on the attacker or compromise ongoing operations.

Misperception is pervasive in insulated decisionmaking processes for several

"The new strategy risks producing a 'forever cyber war' prone to inadvertent escalation."

> "The United States should develop a cyber posture that signals restraint."

reasons.[63] First, small groups unchecked by bureaucracy tend to produce narrow plans prone to escalation during crises.[64] Second, leaders often give guidance to planners during crises that reflects their political bias or personality traits rather than a rational assessment of threats and options.[65] Third, offensive bias in planning may have little to do with the actual threat and more to do with a cult of the offensive and the desire of officers to ensure their autonomy and resources.[66] Removing interagency checks therefore risks compounding fundamental attribution errors and other implicit biases. Cyber operations are too important to be left to the generals at Cyber Command alone.

An Alternative Approach: Cyber Defense-in-Being

Rather than going on the offensive, the United States should develop a cyber posture that signals restraint and builds an active defense network. This network should adopt key tenets of Julian Corbett's concept of a "fleet-in-being." For Corbett, writing in 1911, the operative strategic problem for the British Empire was securing global interests. Regional adversaries could overwhelm local defenses and achieve fait accompli victories, and the British could not be everywhere at once. They had to adopt a fleet-in-being, a distributed network of cruisers (mobility) and fortified ports (strong points) that increased the costs of adversary aggression, buying time for diplomacy and, should it fail, for mobilizing sufficient forces for a counterattack. This dispersed network signaled resolve and generated options by disputing who could command the seas. A fleet-in-being "endeavor[ed] by active defensive operations to prevent the enemy either securing or exercising control for the objects he has in view." This strategy thus advocated "avoiding decisive action by strategical or tactical activity, so as to keep our fleet-in-being till the situation develops in our favor."[67]

In cyber operations, the United States requires a global network organized around active defenses rather than offensive actions designed to preempt other great powers. This network requires intelligence sharing and target hardening with partners, including industry, to reduce adversaries' expected benefits of cyber operations. Just as new technologies enabled new theories of victory for Corbett, digital connectivity puts a premium on deception and active defense in cyberspace.

Active Defense

In military theory, active defense is "the employment of limited offensive action and counterattacks to deny a contested area or position to the enemy."[68] The term comes from Chinese strategic theory and calls for a defensive posture that "strik[es] only after the opponent has struck first."[69] In the cyber context, active defense utilizes deception to expose the attacker's espionage and offensive operations in order prepare counterattacks.[70] With respect to persistent engagement, defending forward risks undermining the ability to isolate adversary capabilities and, if need be, degrade them through targeted counterattacks designed to limit escalation risks.

Deception and defense produce a position of advantage.[71] A connected society is inherently vulnerable. New hardware and endless software updates produce new vulnerabilities at a continual, even if variable, rate. The only true security comes from making adversaries doubt the wisdom of attack.

One technique that can be used to this effect is to lure would-be attackers into network traps, undermining their confidence in their own intelligence and capabilities. For example, a honeypot is false data that adversaries find so alluring that they attempt to access it. This allows defenders to either identify adversary cyber espionage capabilities or deliver their own payloads to rival networks. Thus, through deception, active defense can change the expected benefits of offensive cyber operations and effectively deter adversaries. The opposition must worry that all of their cyber espionage operations might be revealed, or worse, used as vectors for a counterattack.

Hardening Targets

Target hardening is a concept that emerged in the early Cold War. Based on a 1954 study on the vulnerability of U.S. forces,[72] Albert Wohlstetter and Fred Hoffman advocated, among other things, that U.S. forces use passive measures (geographic dispersion, constantly airborne platforms, etc.) and active measures (hardened silos) to reduce vulnerability and ensure a "delicate balance of terror."[73]

In cyberspace, target hardening also involves active and passive measures.[74] In addition to active defense, active measures include investments in human capital and new technology that make it more difficult to access a network. These can range from employing "white hat" hackers, ethical computer hackers who penetrate systems in order to identify vulnerabilities, to updating cyber defensive systems regularly. Passive measures can range from education (e.g., the importance of updating software and avoiding suspicious messages and websites) to ensuring accounts have two-factor authentication—measures that minimize the number of easy attack vectors.

If the goal of the recently released National Cyber Strategy is cost-imposition—increasing the costs of enemy activity—the question is how best to alter a rival's cost-benefit calculation in cyberspace. The current strategy relies on offense: operating forward to thwart attacks preemptively. In theory, a rival is deterred by the expectation of punishment for accessing U.S. networks. Yet, an alternative approach would be to adopt a defensive form of cost imposition by targeting hardening and increasing the marginal cost of gaining access to the system. That is, if rivals want to gain access to a network they have to invest more resources and take advantage of more complex—and rare—vulnerabilities.

Cost imposition in defense starts with target hardening, and worryingly, the United States has neglected this important measure. As a recent Government Accountability Office report makes clear, the Department of Defense has not prioritized security in weapons systems and there are weaknesses throughout the entire infrastructure.[75] According to the study, "from 2012–2017, DOD testers routinely found mission-critical cyber vulnerabilities in nearly all weapon systems that were under development. Using relatively simple tools and techniques, tests were able to take control of these systems and largely operate undetected."[76] The Pentagon should address these deficiencies and increase the expected costs of gaining access to U.S.—and allied—networks.

In cyber operations, the more money adversaries must spend on accessing and exploiting a key network, such as the critical infrastructure of the financial system, the less money they have to spend on conducting other attacks. Coupled with active defense and the use of deception to undermine adversary confidence in their offensive and espionage efforts, target hardening changes the projected benefits of cyber operations. Defensive options, such as hardening targets and increasing societal resiliency, ensure the target is difficult to coerce. As Buchanan notes, "no cybersecurity approach is credible unless it begins with a discussion of the vital role of baseline defenses."[77] These defenses, consistent with the Department of Homeland Security strategy, start with "identifying the most critical systems and prioritizing protection around those systems."[78] Cyber strategy should prioritize hardening key targets while seeding the network with digital traps—active defenses—that undermine adversary offensive and espionage options.

Intelligence Sharing and Coordination

There are also benefits to sharing threat intelligence with industry and allies. The United States operates a global security network that connects not just treaty allies but businesses and civil society actors.[79] Any cyber strategy must embrace this fact as a source of strength, not a point of vulnerability. A greater number of actors identifying adversary cyber operations provides early warning indicators and reveals adversary capabilities.

To date, intelligence sharing associated with cyber operations has been prone to interagency debate and coordination challenges. There are

"Cyber strategy should prioritize hardening key targets while seeding the network with digital traps."

"Restraint can help shape norms in cyberspace and make escalation taboo."

organizational seams, such as the divide between the FBI and CIA before the September 11th terrorist attacks, that often limit intelligence sharing and create barriers to effective response within the federal government.[80] This dilemma is compounded with respect to alliance partners and industry. States and many other organizations tend to stovepipe information and undermine effective coordination based on security risks. Yet, closing off information in a network limits responsiveness.

Rather than limit information sharing, the United States should reengage processes such as the Obama administration's Vulnerabilities Equities Policy, which sought disclosures of newly discovered and unknown malware that might pose a global threat.[81] Sharing threat intelligence is central to not just interagency coordination, but working with partner states, businesses, and civil society. In order to strengthen the defense of the network through depth, the United States will need to assume risk in sharing information, and hence lose some offensive options. This includes working with nontraditional actors, such as the white hat hacker community, which conducts probes in order to help strengthen networks from adversary attacks.[82] It also implies sacrificing some espionage and offensive cyber options to ensure partners can patch their networks and update their defenses.

CONCLUSION

Cyber policy and strategy should favor restraint over offense in protecting the digital commons. In MIT political scientist Barry Posen's proposed grand strategy, restraint calls for fewer forward-deployed forces and less coordination with partners.[83] In a cybersecurity context, restraint implies preserving the digital commons for commercial and social interests, thus limiting military action to the greatest extent possible.

Restraint can also help shape norms in cyberspace and make escalation taboo.[84] To date, restraint has largely been the prevailing norm in this domain. Restraint has prevailed not so much as a prescribed foreign policy strategy, but because more aggressive tactics are ineffective, and states therefore use them sparingly.[85] Data on cyber actions from 2000 to 2016 suggest a restrained domain with few aggressive attacks that seek a dramatic impact. Attacks do not beget attacks, nor do they deter them. The policy discourse is inconsistent with these observations. If few operations are effective in manipulating the enemy and fewer still lead to responses in the domain, why would a policy of offensive operations be useful in cyberspace?

For a variety of reasons, including the ineffectiveness of cyber operations and the fear of weapons proliferation, a normative system of restraint has gradually emerged in cyberspace. A policy of restraint that maintains control over the weapons of cyber war is therefore appropriate and strategically wise. Loosening the rules of engagement in pursuit of a more offensive posture, as the Trump administration advocates, violates norms and can lead to disastrous consequences for the entire system.

Given the ambiguous nature of signals in cyberspace, it is difficult to be sure that an offensive operation will be correctly interpreted as a warning shot designed to get adversaries to back down. Platitudes like "the best defense is a good offense" are best left for sports, not international politics. The evidence suggests that in cyberspace, the best defense is actually a good defense.

APPENDIX

Table 1
Retaliation dynamics

			Response severity (within 1 year)†							
			No response	1	2	3	4	5	6	Total
Cyber incident severity	1.0	Count	7.0	0.0	0.0	1.0	1.0	0.0	0.0	9.0
		Expected count	6.1	0.1	1.0	0.7	1.0	0.1	0.0	9.0
		Std. residual	0.4	-0.3	-1.0	0.4	0.0	-0.4	-0.2	
	2.0	Count	59.0	0.0	18.0	8.0	6.0	4.0	0.0	95.0
		Expected count	64.3	0.7	10.5	7.3	10.5	1.4	0.3	95.0
		Std. residual	-0.7	-0.8	**2.3	0.2	-1.4	**2.2	-0.6	
	3.0	Count	79.0	1.0	4.0	8.0	9.0	0.0	0.0	101.0
		Expected count	68.3	0.7	11.1	7.8	11.1	1.5	0.4	101.0
		Std. residual	1.3	0.3	**-2.1	0.1	-0.6	-1.2	-0.6	
	4.0	Count	30.0	1.0	3.0	4.0	13.0	0.0	1.0	52.0
		Expected count	35.2	0.4	5.7	4.0	5.7	0.8	0.2	52.0
		Std. residual	-0.9	1.0	-1.1	0.0	**3.0	-0.9	1.8	
	5.0	Count	7.0	0.0	5.0	0.0	0.0	0.0	0.0	12.0
		Expected count	8.1	0.1	1.3	0.9	1.3	0.2	0.0	12.0
		Std. residual	-0.4	-0.3	**3.2	-1.0	-1.2	-0.4	-0.2	
	6.0	Count	2.0	0.0	0.0	0.0	1.0	0.0	0.0	3.0
		Expected count	2.0	0.0	0.3	0.2	0.3	0.0	0.0	3.0
		Std. residual	0.0	-0.1	-0.6	-0.5	1.2	-0.2	-0.1	
Total		Count	184.0	2.0	30.0	21.0	30.0	4.0	1.0	272.0
		Expected count	184.0	2.0	30.0	21.0	30.0	4.0	1.0	272.0

Source: Dyadic Cyber Incidents Dataset version 1.5, maintained by the authors. See Ryan C. Maness, Brandon Valeriano, and Benjamin Jensen, "The Dyadic Cyber Incident and Dispute Dataset, Version 1.1," 2017.

Notes: †There were no documented responses greater than 6. Scores of 7–10 imply national-level sustained damage and death.
**Denotes column results that are statistically significant (p > .05).

Table 2
Cyber objectives and retaliation severity

			Cyber response severity (within 1 year) Response severity (0–10)†							
			No response	1	2	3	4	5	6	Total
Cyber objective	Disruption	Count	59.0	0.0	16.0	7.0	5.0	2.0	0.0	89.0
		Expected count	60.2	0.7	9.8	6.9	9.8	1.3	0.3	89.0
		Percent within disrupt	66.3	0.0	18.0	7.9	5.6	2.2	0.0	100.0
		Percent within response	32.1	0.0	53.3	33.3	16.7	50.0	0.0	32.7
		Std. residual	-0.2	-0.8	**2.0	0.0	-1.5	0.6	-0.6	
	Espionage	Count	107.0	2.0	6.0	11.0	21.0	1.0	0.0	148.0
		Expected count	100.1	1.1	16.3	11.4	16.3	2.2	0.5	148.0
		Percent within espionage	72.3	1.4	4.1	7.4	14.2	0.7	0.0	100.0
		Percent within response	58.2	100.0	20.0	52.4	70.0	25.0	0.0	54.4
		Std. residual	0.7	0.9	**-2.6	-0.1	1.2	-0.8	-0.7	
	Degradation	Count	18.0	0.0	8.0	3.0	4.0	1.0	1.0	35.0
		Expected count	23.7	0.3	3.9	2.7	3.9	0.5	0.1	35.0
		Percent within degrade	51.4	0.0	22.9	8.6	11.4	2.9	2.9	100.0
		Percent within response	9.8	0.0	26.7	14.3	13.3	25.0	100.0	12.9
		Std. residual	-1.2	-0.5	**2.1	0.2	0.1	0.7	**2.4	
Total		Count	184.0	2.0	30.0	21.0	30.0	4.0	1.0	272.0
		Expected count	184.0	2.0	30.0	21.0	30.0	4.0	1.0	272.0
		Percent within objective	67.6	0.7	11.0	7.7	11.0	1.5	0.4	100.0
		Percent within response	100.0	100.0	100.0	100.0	100.0	100.0	100.0	100.0

Source: Dyadic Cyber Incidents Dataset version 1.5, maintained by the authors. See Ryan C. Maness, Brandon Valeriano, and Benjamin Jensen, "The Dyadic Cyber Incident and Dispute Dataset, Version 1.1," 2017.

Notes: †There were no documented responses greater than 6. Scores of 7–10 imply national-level sustained damage and death. **Denotes column results that are statistically significant (p > .05).

NOTES

1. Bob Woodward, *Fear: Trump in the White House* (New York: Simon and Schuster, 2018). See chap. 12 for details on the North Korea debate.

2. Department of Defense, *Department of Defense Cyber Strategy* (Washington: DoD, April 2015), https://nsarchive2.gwu.edu/dc.html?doc=2692133-Document-25.

3. Woodward, *Fear: Trump in the White House*, p. 340.

4. Woodward, *Fear: Trump in the White House*, pp. 339–40.

5. Julian S. Corbett, *Some Principles of Maritime Strategy*, ed. Eric Grove (Annapolis: U.S. Naval Institute, 1988).

6. While the name in the vision statement is persistent action, in subsequent testimony General Paul Nakasone introduced what appear to be three subordinate concepts: persistent engagement, persistent presence, and persistent innovation. See "Gen. Nakasone Lays Out Vision for '5th Chapter' of US Cyber Command," Meritalk, September 7, 2018, https://www.meritalk.com/articles/nakasone-cyber-command-vision/.

7. United States Cyber Command, "Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command," June 2018, https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010. For a critique, see Herb Lin and Max Smeets, "What Is Absent From the U.S. Cyber Command 'Vision'," Lawfare, May 3, 2018, https://www.lawfareblog.com/what-absent-us-cyber-command-vision.

8. Department of Defense Science Board, *Task Force on Cyber as a Strategic Capability Executive Summary*, (Washington: Department of Defense, 2018), p. 1.

9. Richard Harknett, "United States Cyber Command's New Vision: What it Entails and Why It Matters," Lawfare, March 23, 2018, https://www.lawfareblog.com/united-states-cyber-commands-new-vision-what-it-entails-and-why-it-matters.

10. "Gen. Nakasone Lays Out Vision for '5th Chapter' of US Cyber Command," Meritalk, September 7, 2018, https://www.meritalk.com/articles/nakasone-cyber-command-vision/.

11. United States Cyber Command, "Achieve and Maintain Cyberspace Superiority," p. 6. For the joint definition, see "Department of Defense Dictionary of Military and Associated Terms," Department of Defense, Joint Publication 1-02, (amended through June 2015), p. 6, https://www.hsdl.org/?abstract&did=750658.

12. United States Cyber Command, "Achieve and Maintain Cyberspace Superiority," p. 6.

13. United States Cyber Command, "Achieve and Maintain Cyberspace Superiority," p. 2.

14. Department of Defense, "Summary of 2018 National Defense Strategy of the United States of America," 2018, https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

15. Donald J. Trump, "National Security Strategy of the United States of America," Executive Office of the President, 2017.

16. Trump, "National Security Strategy of the United States of America," p. 7.

17. United States Military Joint Publication, "Cyberspace Operations," June 8, 2018, p. II-5.

18. Ellen Nakashima, "Trump Gives the Military More Latitude to Use Offensive Cyber Tools against Adversaries," *Washington Post*, August 16, 2018, https://www.washingtonpost.com/world/national-security/trump-gives-the-military-more-latitude-to-use-offensive-cyber-tools-against-adversaries/2018/08/16/75f7a100-a160-11e8-8e87-c869fe70a721_story.html?noredirect=on&utm_term=.0b6bb33d31c8.

19. Glenn Greenwald and Ewen MacAskill, "Obama Orders US to Draw Up Overseas Target List for Cyber-Attacks," *The Guardian*, June 7, 2013, https://www.theguardian.com/world/2013/jun/07/obama-china-targets-cyber-overseas.

20. "Presidential Policy Directive 20," Federation of American Scientists, https://fas.org/irp/offdocs/ppd/ppd-20.pdf.

21. Joshua Rovner and Tyler Moore, "Does the Internet Need a Hegemon?" *Journal of Global Security Studies* 2, no. 3 (July 2017): 184–203.

22. Benjamin Jensen, "The Cyber Character of Political Warfare," *Brown Journal of World Affairs* 24, no. 1 (Fall/Winter 2017–18): 159–71]; and Austin Carson and Keren Yarhi-Milo, "Covert Communication: The Intelligibility and Credibility of signaling in Secret,"

Security Studies 26, no. 1 (2017): 124–56.

23. United States Cyber Command, "Achieve and Maintain Cyberspace Superiority."

24. This data represents the Dyadic Cyber Incidents Dataset version 1.5, which is maintained by the authors. This is an update from version 1.1 that is not finalized but represents a significant extension and expansion of our case coverage. See Ryan C. Maness, Brandon Valeriano, and Benjamin Jensen, "The Dyadic Cyber Incident and Dispute Dataset, Version 1.1," 2017. A cyber operation implies multiple incidents (i.e., tactics, tools, and tool sets) linked to a state actor applied over time to achieve an objective effect against a target of political significance to a rival state. This definition implies that these tools may be part of larger intrusion set linked to an Advanced Persistent Threat (APT) or a standalone incident.

25. Brandon Valeriano, Benjamin Jensen, and Ryan C. Maness, *Cyber Strategy: The Evolving Character of Power and Coercion* (Oxford: Oxford University Press, 2018).

26. Examples of cyber disruptions include DDoS attacks or defacements of high-profile government webpages, or escalating risk by hacking in to financial services networks via Trojans, viruses, or worms that are simple to design, easy to employ, require limited resources, and have short-term goals.

27. These benefits may be long-term material components of military power, such as stealing the plans for the F-35, or they may involve short to midterm critical information such as the identities of covert operatives in conflict zones. Creating information asymmetries can increase the costs of resistance and increase the probability that a target can be coerced in the future.

28. These operations destabilize the target, highlighting critical vulnerabilities and pushing them onto a defensive footing that limits their ability to respond to a crisis. These operations tend to involve more sophisticated viruses, worms, and logic bombs.

29. Jon R. Lindsay and Erik Gartzke, "Coercion through Cyberspace: The Stability-Instability Paradox Revisited," in *The Power to Hurt: Coercion in Theory and in Practice*, ed. K. M. Greenhill and P. J. P. Krause (New York: Oxford University Press, 2017); Erica D. Borghard and Shawn W. Lonergan, "The Logic of Coercion in Cyberspace," *Security Studies* 26, no. 3 (2017): 452–81; and Joseph S. Nye Jr., "Deterrence and Dissuasion in Cyberspace," *International Security* 41, no. 3 (Winter 2016/2017): 44–71.

30. These findings are consistent with propositions advanced in Erik Gartzke, "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth," *International Security* 38, no. 2 (Fall 2013): 41–73.

31. These operations are also referred to as counter cyber espionage operations (CCNE).

32. For a detailed overview, see Valeriano, Jensen, and Maness, *Cyber Strategy*, chap. 10.

33. Kim Zetter, "US and China Reach Historic Agreement on Economic Espionage," *Wired*, September 25, 2015, https://www.wired.com/2015/09/us-china-reach-historic-agreement-economic-espionage/. On the response dynamics, see David Sanger, "US Decides to Retaliate against China's Hacking," *New York Times*, July 31, 2015, https://www.nytimes.com/2015/08/01/world/asia/us-decides-to-retaliate-against-chinas-hacking.html.

34. Ellen Nakashima, "Defense Officials Disclose Cyberattack," *Washington Post*, August 24, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/08/24/AR2010082406495.html.

35. William F. Lynn III, "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs* 89 (September 2010): 97.

36. This logic is consistent with arguments advanced by Valeriano, Jensen, and Maness in *Cyber Strategy: The Evolving Character of Power and Coercion*; and in Borghard and Lonegran, "The Logic of Coercion in Cyberspace."

37. The table illustrates the highest response by the targeted to state within one year of the initial response.

38. In game theory, proportional retaliation in competitive interactions is also referred to as "tit-for-tat." See Robert Axelrod, *The Evolution of Cooperation* (New York: Basic Books, 2006).

39. Herman Kahn, *On Escalation: Metaphors and Scenarios* (New York: Praeger Press, 1965), pp. 41–42.

40. If cyber operations were escalatory, one would expect that the majority see a retaliation by the targeted state in one year and that these responses would be at a higher level of severity. First, 184 (67.4%) do not see a cyber retaliation within one year. While there may have been responses in other domains using other instruments of power—horizontal escalation—cyber responses

occurred less frequently than expected. Second, even those responses tended to match or fall below the severity level of the initial cyber operation. For example, severity score 2 and 5 responses had more retaliations at level 2 and 5 than expected. Vertical escalation was rare in cyberspace.

41. Adam Meyers, "Cyber Skirmish: Russia v. Turkey," *Crowdstrike* (blog), April 13, 2016, https://www.crowdstrike.com/blog/cyber-skirmish-russia-v-turkey/.

42. Lily Hay Newman, "China Escalates Hacks against the US as Trade Tensions Rise," *Wired*, June 22, 2018, https://www.wired.com/story/china-hacks-against-united-states/.

43. Sara Lynch, Lisa Lambert, and Christopher Bing, "U.S. Indicts Russians in Hacking of Nuclear Company Westinghouse," Reuters, October 4, 2018, https://www.reuters.com/article/us-usa-russia-cyber/us-indicts-russians-in-hacking-of-nuclear-company-westinghouse-idUSKCN1ME1U6.

44. Lynch, Lambert, and Bing, "U.S. Indicts Russians."

45. Lynch, Lambert, and Bing, "U.S. Indicts Russians."

46. For an overview and critique of the concept of escalation dominance, see Michael Fitzsimmons, "The False Allure of Escalation Dominance," War on the Rocks, November 16, 2017, https://warontherocks.com/2017/11/false-allure-escalation-dominance/.

47. Fitzsimmons, "The False Allure of Escalation Dominance."

48. Robert Pape, *Bombing to Win: Airpower and Coercion* (Ithaca: Cornell University Press, 1996).

49. Clausewitz discusses the interaction in Carl von Clausewitz, *On War*, trans. Michael Howard and Peter Paret (Priceton: Princeton University Press, 1976), pp. 357–59.

50. Derek MC. Yuen, "Deciphering Sun Tzu," *Comparative Strategy* 27, no. 2 (2008): 110, 183–200.

51. Erik Gartzke and Jon R. Lindsay, "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace," *Security Studies* 24, no. 2 (2015): 316–48.

52. On the concept of fear and its relationship to the security dilemma, as well as other core concepts in international relations, see Shiping Tang, "Fear in International Politics: Two Positions," *International Studies Review* 10, no. 3 (September 2008): 451–71.

53. Robert Jervis, "Cooperation under the Security Dilemma," *World Politics* 30, no. 2 (1978): 167–214.

54. Cathal Nolan, *The Allure of Battle: A History of How Wars Are Won and Lost* (New York: Oxford University Press, 2017), p. 2.

55. This idea relates to the concept of distinguishability in offense-defense theory and whether or not a state can differentiate between offensive and defensive capabilities and attributes. See Jervis, "Cooperation under the Security Dilemma."

56. Ben Buchanan, *The Cybersecurity Dilemma* (London: Hurst Publishers, 2017), p. 4.

57. Jason Healey, "Triggering the New Forever War in Cyberspace," *Cipher Brief*, April 1, 2018, https://www.thecipherbrief.com/triggering-new-forever-war-cyberspace. On the concept of inadvertent escalation, see Barry Posen, *Inadvertent Escalation: Conventional War and Nuclear Risks* (Ithaca, NY: Cornell University Press, 1991); Jeffrey Legro, "Military Culture and Inadvertent Escalation in World War II," *International Security* 18, no. 4 (Spring 1994): 108–42; Caitlin Talmadge, "Would China Go Nuclear? Assessing the Risk of Chinese Nuclear Escalation in a Conventional War with the United States," *International Security* 41, no. 4 (Spring 2017): 50–92; and Hyun-Binn Cho, "Provocation, Crisis Escalation, and Inadvertent War," conference paper presented at APSA 2015, ISA 2016, and Harvard International Security Conference 2017.

58. Victor David Hanson locates the Western way of war in individualism as a cultural value and the quest for decisive battle, features whose origins he locates in the ancient Greek Hoplite infantry. See Victor David Hanson, *The Western Way of War: Infantry Battle in Classical Greece* (New York: Alfred Knopf, 1989); and Victor David Hanson, *Carnage and Culture: Landmark Battles in the Rise of Western Power* (New York: Doubleday, 2001).

59. Tami Davis Biddle, *Rhetoric and Reality in Air Warfare: The Evolution of British and American Ideas about Strategic Bombing, 1914–1945* (Princeton: Princeton University Press, 2009).

60. Cathal Nolan, *The Allure of Battle: A History of How Wars Are Won and Lost* (New York: Oxford University Press, 2017), p. 2.

61. Robert Kaplan, "The Art of Avoiding War," *The Atlantic*, June 15, 2015, https://www.theatlantic.com/magazine/archive/2015/06/

the-art-of-avoiding-war/392060/.

62. For an overview as it relates to planning and assessments, see Risa Brooks, *Shaping Strategy: The Civil-Military Politics of Strategic Assessment* (Princeton: Princeton University Press, 2008).

63. Robert Jervis, *Perception and Misperception in International Politics* (Princeton: Princeton University Press, 1978); and James M. Goldgeier and Philip E. Tetlock, "Psychology and International Relations Theory," *Annual Review of Political Science* 4, no. 1 (2001): 67–92.

64. Irving L. Janis, *Groupthink: Psychological Studies of Policy Decisions and Fiascoes* (Boston: Houghton Mifflin, 1982); and Dominic D. P. Johnson and Dominic Tierney, "The Rubicon Theory of War: How the Path to Conflict Reaches the Point of No Return," *International Security* 36, no. 1 (2011): 7–40.

65. Keren Yarhi-Milo, *Knowing the Adversary: Leaders, Intelligence Organizations, and Assessments of Intentions in International Relations* (Princeton: Princeton University Press, 2014).

66. Jack Snyder, "Civil-Military Relations and the Cult of the Offensive, 1914 and 1984," *International Security* 9, no. 1 (1984): 108–46.

67. Corbett, *Some Principles of Maritime Strategy*, p. 211.

68. "Department of Defense Dictionary of Military and Associated Terms."

69. M. Taylor Fravel, "The Evolution of China's Military Strategy: Comparing the 1987 and 1999 Editions of Zhanlue Xue," in *The Revolution in Doctrinal Affairs: Emerging Trends in the Operational Art of the Chinese People's Liberation Army* (Alexandria: Center for Naval Analyses, 2005), p. 87.

70. Josh Johnson, "Implementing Active Defense Systems on Private Networks," InfoSec Reading Room SANS Institute, 2013, https://www.sans.org/reading-room/whitepapers/detection/implementing-active-defense-systems-private-networks-34312.

71. K. E. Heckman, F. J. Stech, B. S. Schmoker, and R. K. Thomas, "Denial and Deception in Cyber Defense," *Computer* 48, no. 4 (2015): 36–44.

72. Albert Wohlstetter and Fred Hoffman, *Defending a Strategic Force after 1960* (Santa Monica: RAND Corporation, 1954).

73. Albert Wohlstetter, "The Delicate Balance of Terror: Condensed from Foreign Affairs," *Survival* 1, no. 1 (1959): 8–17.

74. For an overview of active and passive measures, see Dorothy Denning and Bradley Strawser, "Active Cyber Defense: Applying Air Defense to the Cyber Domain" in *Understanding Cyber Conflict: 14 Analogies*, ed. George Perkovich and Ariel Levite (Washington: Georgetown University Press, 2017).

75. United States Government Accountability Office (GAO), "Weapons Systems Cybersecurity: DOD Just Beginning to Grapple with Scale of Vulnerabilities," report to the Committee on Armed Services, U.S. Senate, October 2018, p. 11.

76. GAO, "Weapons Systems Cybersecurity," p. 21.

77. Buchanan, *The Cybersecurity Dilemma*, p. 158.

78. U.S. Department of Homeland Security, "Cybersecurity Strategy," May 15, 2018, p. 8.

79. Charles Cleveland, Benjamin Jensen, Arnel David, and Susan Bryant, *Military Strategy in the 21st Century: People, Connectivity, and Competition* (New York: Cambria Press, 2018).

80. Tarun Chaudhary, Jenna Jordan, Mike Salomone, and Phil Baxter, "Patchwork of Confusion: The Cybersecurity Coordination Problem," *Journal of Cybersecurity* (forthcoming).

81. The White House, "Vulnerabilities Equities Policy and Process for the United States Government," November 15, 2017, https://www.whitehouse.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF.

82. Nina Kollars, "Beyond the Cyber Leviathan: White Hats and US Cyber Defense," War on the Rocks, 2018, https://warontherocks.com/2018/09/beyond-the-cyber-leviathan-white-hats-and-u-s-cyber-defense/.

83. Barry Posen, *Restraint: A New Foundation for US Grand Strategy* (Ithaca: Cornell University Press, 2014).

84. Brandon Valeriano and Ryan C. Maness, *Cyber War versus Cyber Realities: Cyber Conflict in the International System* (Oxford: Oxford University Press, 2015).

85. Valeriano, Jensen, and Maness, *Cyber Strategy*.