

Cyber Operations as Imperfect Tools of Escalation

ERICA D. BORGHARD
SHAWN W. LONERGAN*

Abstract

There are important empirical reasons to suspect that the risks of cyber escalation may be exaggerated. If cyberspace is in fact an environment that generates severe escalation risks, why has cyber escalation not yet occurred? We posit that cyber escalation has not occurred because cyber operations are poor tools of escalation. In particular, we argue that this stems from key characteristics of offensive cyber capabilities that limit escalation through four mechanisms. First, retaliatory offensive cyber operations may not exist at the desired time of employment. Second, even under conditions where they may exist, their effects are uncertain and often relatively limited. Third, several attributes of offensive cyber operations generate important tradeoffs for decision-makers that may make them hesitant to employ capabilities in some circumstances. Finally, the alternative of cross-domain escalation—responding to a cyber incident with noncyber, kinetic instruments—is unlikely to be chosen except under rare circumstances, given the limited cost-generation potential of offensive cyber operations.

There is a widespread view among practitioners and scholars that cyberspace is defined by an inherent potential for dangerous escalation dynamics between rivals.¹ On the practitioner side, for example, senior US intelligence and military leaders expressed concerns about first-strike incentives leading to escalation in a 2017 joint statement to Congress, testifying that “adversaries equipped with [offensive cyber capabilities] could be prone to preemptive attack and rapid escalation in a future crisis, because both sides would

*The views of the authors are personal and do not reflect the policy or position of the Army Cyber Institute, United States Military Academy, 75th Innovation Command, Army Futures Command, Department of the Army, Department of Defense, or US government.

have an incentive to strike first.”² On the academic side, there is a palpable fear that cyberspace is an environment in which offense has advantages over defense and that this—coupled with factors such as problems of attribution, poor command and control, and the absence of meaningful thresholds or red lines—generates real risks of inadvertent escalation.³ Concerns about escalation grew even more passionate in the wake of the US Department of Defense’s release of its 2018 Cyber Strategy document, which articulates an operational concept of “defending forward” in which the DOD “disrupt[s] or halt[s] malicious cyber activity at its source.”⁴

However, there are important empirical reasons to suspect that the risks of cyber escalation may be exaggerated. Specifically, if cyberspace is in fact an environment that (perhaps even more so than others) generates severe escalation risks, why has cyber escalation not yet occurred? Most interactions between cyber rivals have been characterized by limited volleys that have not escalated beyond nuisance levels and have been largely contained below the use-of-force threshold.⁵ For example, in a survey of cyber incidents and responses between 2000 and 2014, Brandon Valeriano et al. find that “rivals tend to respond only to lower-level [cyber] incidents and the response tends to check the intrusion as opposed to seek escalation dominance. The majority of cyber escalation episodes are at a low severity threshold and are non-escalatory. These incidents are usually ‘tit-for-tat’ type responses within one step of the original incident.”⁶ Even in the two rare examples in which states employed kinetic force in response to adversary cyber operations—the US counter-ISIL drone campaign in 2015 and Israel’s airstrike against Hamas cyber operatives in 2019—the use of force was circumscribed and did not escalate the overall conflict (not to mention that force was used against nonstate adversaries with limited potential to meaningfully escalate in response to US or Israeli force).⁷

We posit that cyber escalation has not occurred because cyber operations are poor tools of escalation. In particular, we argue that this stems from key characteristics of offensive cyber capabilities that limit escalation through four mechanisms. First, retaliatory offensive cyber operations may not exist at the desired time of employment. Second, even under conditions where they may exist, their effects are uncertain and often relatively limited. Third, several attributes of offensive cyber operations generate important tradeoffs for decision-makers that may make them hesitant to employ capabilities in some circumstances. Finally, the alternative of cross-domain escalation—responding to a cyber incident with noncyber, kinetic instruments—is unlikely to be chosen except under rare circumstances, given the limited cost-generation potential of offensive

cyber operations. In this article, we define cyber escalation and then explore the implications of the technical features and requirements for offensive cyber operations. We also consider potential alternative or critical responses to each of these logics. Finally, we evaluate the implications for US policy making.

Defining Offensive Cyber Operations and Escalation

Escalation, broadly defined, involves some meaningful increase in the nature or intensity of a conflict. It occurs when at least one party to a conflict crosses what at least one party perceives to be a critical threshold.⁸ Escalation occurs “when at least one of the parties involved believes there has been a significant qualitative change in the conflict as a result of the new development.”⁹ A state could escalate through quantitatively ratcheting up the amount of pain it inflicts on its adversary using the same type of capabilities, or qualitatively through introducing a new type of capability (the latter is what Bernard Brodie dubbed a “firebreak”).¹⁰ Escalation could occur deliberately through moving up Herman Kahn’s famed “escalation ladder” to achieve victory in a crisis, or inadvertently through security dilemma dynamics, misperceptions, windows of opportunity and vulnerability, or bureaucratic processes and standard operating procedures.¹¹

Escalation could occur along analogous pathways in cyberspace. The cyber literature is predominantly concerned about conditions under which one state’s use of offensive cyber capabilities could unintentionally trigger an escalatory spiral with a rival.¹² This scenario could hypothetically occur if the target responds with more intense and costly cyber means (cyber escalation within the cyber domain) or through breaching the cyber-kinetic threshold (cross-domain escalation).

However, we anticipate that the use of offensive cyber capabilities is unlikely to trigger escalatory responses, both within cyberspace and across other domains. Our argument that offensive cyber operations are poor tools of escalation rests on what we identify as the technical foundations of cyber capabilities. Of course, technical factors alone are insufficient to completely account for state decision-making about courses of action in response to adversary cyber operations. A full assessment of the determinants of escalatory decision-making must consider a range of factors, such as the salience of interests at stake, a decision-maker’s approach to risk, and cognitive biases. However, we claim that the technical characteristics of offensive cyber capabilities play an important role in circumscribing the options available to states, generating tradeoffs that decision-makers must consider, and creating breathing room during crises that, taken together,

dampen potential pathways to escalation. More often than not, the potential use of cyber capabilities in an escalatory fashion is time intensive, unreliable and unpredictable, and limited in the magnitude and range of effects. Below, we propose general hypotheses for how what we identify as key characteristics of offensive cyber are linked to potential pathways to cyber or cross-domain escalation in response to adversary cyber operations. We intend for these hypotheses to serve as a useful springboard for further empirical research on the link between the technical features of cyber capabilities and their utilities for escalation. The hypotheses are summarized in table 1.

Table 1. Linking offensive cyber attributes with escalation pathways

Cyber Attributes	Escalation Pathways
Role of access, nonuniversal lethality, and temporal nature of access and capability development and maintenance	Lack of cyber escalation options at the desired time and implications for considering alternative courses of action
Nonphysical nature of offensive cyber capabilities and limits on cost generation	Limited costliness of effects
Role of secrecy, attribution, and espionage	Countervailing tradeoffs
Nonphysical nature of offensive cyber capabilities, nonuniversal lethality, and limits on cost generation	Lack of willingness for cross-domain escalation in response to cyber incident with limited relative costs

Technical Features and Requirements for Offensive Cyber

Key features of cyber operations—the role of access, nonuniversal lethality of offensive cyber capabilities, and the temporal nature of access and capability development and maintenance—may dramatically circumscribe the escalatory options available to states through cyber means during a time of crisis.

First, escalatory cyber response options may simply not be available to a state because it lacks access to an appropriate set of targets against which to deliver an escalatory response. This is because offensive cyber operations deliver effects against targets through exploiting a vulnerability to gain access (through an attack vector) to a target’s network or system and deliver a payload that is activated by communicating back with a host or triggered by a command order written into the code.¹³ Absent the right access to deploy a capability, the latter might as well not exist.¹⁴

While critical to the success of offensive operations, the initial penetration of a target network or system can be resource intensive and net unpredictable results, which is why the employment of cyber capabilities that rely on access to a targeted network require prior planning and resource allocation

and development. Indeed, according to Chris Inglis, the planning staff at US Cyber Command during the 2009–10 period assessed that “the first 90 percent of cyber reconnaissance (i.e., ISR), cyber defense, and cyberattack consisted of the common work of finding and fixing a target of interest in cyberspace.”¹⁵ Therefore, rather than occurring at lightning speed, cyber operations have crucial aspects that take time and significant resource investments, even if at the tactical level a line of code can indeed be executed at “network speed.”¹⁶

Considering means of access and types of targets reveal the various aspects of gaining access that limit potential cyber escalatory responses at a given time. Table 2, Mainstream means of gaining access, depicts various common access methods and evaluates them along a spectrum of cost, risk, and reliability.¹⁷ The broadest distinction between means of access is remote (e.g., using the Internet) versus close (e.g., gaining access through a human agent or supply chain interdiction). Most of the low-cost and low-risk means of gaining access to a target (such as through various social engineering mechanisms) are not readily applicable against more hardened (and therefore more strategically valuable) targets, such as the air-gapped networks common in critical infrastructure systems and some military and defense systems. Conversely, the most reliable type of access, physical access through a human intermediary on the ground, is also the riskiest and costliest.

The nature of the targeted network or system also shapes access requirements and consequent level of difficulty. For instance, gaining access to operational technology (OT) is typically more difficult than to information technology (IT), although this may be changing as IT and OT systems converge.¹⁸ OT networks tend to be closed (they do not touch the global Internet) and run unique protocols used to control highly specific processes and systems.¹⁹ Typically, these characteristics also mean that these networks require specific knowledge because the programs they run are customized to those systems and the networking protocols they employ may not be widely proliferated. Additionally, the simple fact of “gaining access” to a target network does not guarantee that an attacker has gained access at the requisite network layer from which to launch an offensive operation.²⁰ Thus, most access operations are followed by operations that enable persistence through access escalation prior to the employment of any cyber weapon. Finally, gaining access to a target via a hardware implant—the actual physical components of a computer (e.g., motherboard, USB and other flash memory devices, routers, etc.)—is appreciably costlier and more difficult than gaining access to software (all of the digital programs

Table 2. Mainstream means of gaining access

<i>Remote access</i>	<i>Cost</i>	<i>Risk</i>	<i>Reliability</i>	<i>Feasibility against target sets</i>
<i>Hacking:</i> Using a computer to gain unauthorized access to a system using a suite of tools.	Low to High	Low to Medium	Low to High	Can be resource intensive depending on the target.
<i>Phishing:</i> Mass and indiscriminate dissemination of e-mail containing malware.	Low	Low	Low	Not feasible against air-gapped networks.
<i>Spear phishing:</i> Tailored dissemination of e-mail containing malware.	Low	Low	Medium. More targeted than phishing so more reliable but depends on the sophistication of social engineering. Ability to deliver the effects also depends on controls within a network.	Not feasible against air-gapped networks.
<i>Whaling:</i> Similar to spear phishing but targets a high-profile individual.	Low to Medium	Low	Medium. Tends to be more reliable compared to spear phishing given the highly targeted nature of the operation; however, can be resource intensive as it requires increased social engineering and target development and is often against a hardened target.	Not feasible against air-gapped networks.
<i>Pharming:</i> Directing Internet users to a cloned, but bogus, website that prompts them to provide user credentials.	Low	Low	Low	Not feasible against air-gapped networks.
<i>Man in the middle:</i> A common hacking operation that can rely on remote or physical access to essentially eavesdrop on communication between two parties.	Low to High	Low to High	Low to High	Varies depending on remote or close access.

<i>Close access</i>	<i>Cost</i>	<i>Risk</i>	<i>Reliability</i>	<i>Feasibility against target sets</i>
<i>Supply chain interdiction:</i> Intercepting and compromising a software or hardware component of the targeted network prior to delivery.	Medium to High	Low to Medium	Low to Medium. Attacker has no guarantee of how infected systems will react in the targeted environment or even that they will be used.	May be one of the only viable means to gain access to a closed system, but requires extensive planning and intelligence collection.
<i>Physical access:</i> Emplacing an operator on the ground to physically gain access to the targeted system and infecting it via a software or hardware implant.	High	High	Medium to High. Varies depending on what capabilities the operator has for the operation. It may be difficult to engineer solutions for data exfiltration if required.	May be one of the only viable means to gain access to a closed system. Often requires a trained operator surreptitiously gaining access to a targeted system or finding a person with access to wittingly or unwittingly deliver the exploit.
<i>Wireless access:</i> Associating wirelessly, typically via Wi-Fi or Bluetooth, as a mean to inject a software capability or harvest credentials. Standoff distance can vary greatly depending on the frequency the attacker is exploiting and the power emitted by the transmitter.	Medium	Medium to High	Low to High. Varies depending on what capabilities the operator has for the operation.	Feasibility varies depending on the standoff distance necessary to deliver the exploit and the permissibility of the environment of the operation.

on a computer, from the operating system to applications such as Microsoft Word).²¹ Software vulnerabilities are relatively easier to detect and to patch, and manufacturers routinely disseminate information about known vulnerabilities and remediation protocols.²²

Second, in addition to being dependent on access, offensive cyber capabilities lack universal effectiveness. While nuclear or conventional munitions are target agnostic—in most cases, the same munition can be used to target an aircraft hangar, a massed enemy formation, a munitions factory, or a hospital—some cyber weapons must be tailored to a specific target set or type.²³ As Martin Libicki notes, “A piece of malware that brings one system down may have absolutely no effect on another. The difference between the two may be as simple as which patch version of a piece of software each system runs.”²⁴ The 2017 WannaCry ransomware attack that wreaked billions of dollars in damage and was attributed to North Korea’s Lazarus Group, for instance, targeted hundreds of thousands of computers around the world across a range of industries that were running an older version of Windows.²⁵ The widespread damage belies the highly specific and targeted nature of the malware—almost all of the affected systems were running a version of Windows 7; the same strain of malware had no effect on computers running more up-to-date operating systems. Moreover, asset owners of targets of strategic significance—such as critical infrastructure—typically employ highly customized software and specific hardware with tailored configurations that are unique to those systems and usually only intimately understood by the original developers and manufacturers. It has been reported, for example, that the malware employed in the Stuxnet cyberattacks against the Iranian nuclear program was tailored to target the specific model of Siemens programmable logic controllers (PLC) used at the Natanz enrichment facility.²⁶ Indeed, while Stuxnet was discovered in computers around the world, it delivered destructive effects only against the centrifuges in Natanz.²⁷ The non-substitutability of entire classes of offensive capabilities by definition increases the cost of developing an arsenal of offensive cyber capabilities.²⁸

Therefore, the time and resource requirements to gain access and develop specific offensive capabilities may render important escalatory response options infeasible or impractical at the desired time. Operational planning and execution must consider that a given capability may not be usable or even exist at a chosen time of employment.²⁹ As the above discussion illustrates, many of the target sets that would represent strategic (and therefore escalatory) targets, such as a state’s critical infrastructure or nuclear command and control, demand extensive planning,

pre-positioning, and capability development in advance of employing offensive capabilities. Therefore, the timing of a crisis plays a crucial role in decisions about cyber escalation responses. Specifically, the time required to develop access to hold strategic targets at risk means that, even if a state seeks to escalate against an adversary using cyber means, it may find itself limited by the accesses and capabilities it possesses at the moment a crisis occurs. Cyber response options may be limited to less decisive or more vulnerable target sets, rather than those that are more strategically significant.

Third, these limitations become even more salient when we consider how strategic interactions are likely to play out over time during repeated crisis interactions. Because the virtual domain is changeable in a way that the physical world is not, actions taken by defenders in the context of a crisis can radically and unpredictably alter an attacker's ability to deliver and sustain effects against a target over time.³⁰ Access and capabilities are neither guaranteed nor indefinite—they have a shelf life.³¹ Footholds into a target's network that were time intensive to develop can unexpectedly disappear as vulnerabilities in a network are patched. Exploits may have a short shelf life as revealing information about them enables targets to identify indicators of compromise (IOCs) and use these to prevent further damage from specific malware strains or quarantine malicious traffic using known malware signatures. An example of the latter is the US Cyber Command initiative, beginning in 2018, to share information about adversary malware by uploading samples to VirusTotal.³² Therefore, a target can “transition from vulnerability (to a particular attack) to invulnerability in, literally, minutes.”³³ Third-party disclosure about software vulnerabilities by governments or private actors can also unintentionally precipitate the loss of access as exposure about vulnerability information enables network defenders to take measures to remedy them.³⁴ For instance, the disclosures that began in 2016 by the group Shadow Brokers of purportedly pilfered US National Security Agency exploits and zero days ostensibly put US government accesses at risk.³⁵ Put simply, a vulnerability upon which an access relies may in theory be only one update or disclosure away from being patched.

Thus, in the context of an ongoing crisis interaction between an attacker and defender, the former's operational tempo is likely to be interrupted by the latter's behavior, forcing the attacker to devote additional time to find or acquire new vulnerabilities and exploits in the midst of an offensive operation or campaign. As Inglis notes, to succeed in an offensive cyber campaign that unfolds over time, attackers must be able to sustain “the efficacy of tools under varying conditions caused by the defender's response and the natural variability and dynamism of cyberspace.”³⁶ The ability to

build or acquire new accesses and capabilities “in real time” during a crisis is highly limited.³⁷ Indeed, General Paul Nakasone remarked in a January 2019 interview on the radical difference in shelf life between conventional and cyber capabilities:

Compare the air and cyberspace domains. Weapons like JDAMs [Joint Direct Attack Munitions] are an important armament for air operations. How long are those JDAMs good for? Perhaps 5, 10, or 15 years, sometimes longer given the adversary. When we buy a capability or tool for cyberspace . . . we rarely get a prolonged use we can measure in years. Our capabilities rarely last 6 months, let alone 6 years. This is a big difference in two important domains of future conflict.³⁸

Therefore, as a 2013 Defense Science Board report notes, “offensive cyber will always be a fragile capability” when pitted against network defenders who are “continuously improving network defensive tools and techniques.”³⁹

Each side can take defensive measures to blunt the impact and effectiveness of the other’s access and capabilities—particularly as information about them is revealed. Consequently, strategic accesses and capabilities are likely to become more vulnerable and less reliable over time, shrinking the set of cyber escalatory response options for all parties. This cycle is likely to generate temporal breaks in the pace of adversarial engagements in cyberspace, where states must regroup and develop or rebuild accesses and capabilities during an ongoing interaction. These pauses are likely to diffuse the pressure that typically accompanies—even defines—crisis situations, creating breathing space and, by extension, room for decision-makers to deliberate alternative courses of action, for domestic political tensions to cool down, for intent to be communicated to adversaries, and for de-escalation pathways to be determined.

A potential counter to this argument is that most states likely already appreciate the time and resources required to develop accesses and tools, as well as their fragility. Therefore, those with sufficient resources are incentivized to alleviate these concerns through investing heavily in developing the ability to gain pre-positioned accesses and a range of capabilities and platforms to be prepared for the onset of a potential future crisis. Evidence of this kind of behavior could be, for example, the discovery of Russian malware in US critical infrastructure reported in 2018.⁴⁰ While dormant access is almost certainly the case, states are likely to remain stymied by inadvertent or deliberate discovery of these efforts prior to a crisis. More importantly, even if pre-positioned accesses and capabilities are available in the opening moments of a crisis, the difficulties of maintaining

them during iterated volleys between adversaries are likely to persist and blunt the ability of a given party to continue escalation of cyber capabilities.

Limited Costliness of Offensive Cyber Effects

Even under circumstances in which a state may possess the right cyber response capabilities at the desired time, its response may not generate sufficient costs against the target to be perceived as escalatory.⁴¹ Fundamental limits on the cost-generation potential of offensive cyber operations stem from the fact that cyber capabilities lack the physical violence of conventional and nuclear ones. Cyber weapons target data; they disrupt, manipulate, degrade, or destroy data resident on networks and systems or in transit.⁴² Moreover, aside from those cyber capabilities that permanently destroy data and for which there are no backups to which a target can revert, cyber effects are temporary and often reversible.

The utility of military instruments of power for the purposes of coercion or brute force inheres in their abilities to inflict—or credibly threaten to inflict—significant damage and harm against a target state (its civilian population or its military forces) to achieve a political objective.⁴³ Cyber weapons could be (and have been) used to disrupt an adversary's networks and systems—overwhelming them such that they temporarily lose the ability to function or the target loses confidence in their reliability—or even to produce destructive effects by destroying data resident on these systems or, in rarer circumstances, producing effects in the physical realm.⁴⁴ While conducting multiple cyberattacks against a targeted state's critical national infrastructure, for example, could in theory generate significant economic and national security consequences, the temporal aspects of offensive cyber operations as described above limit the ability of even the most capable states to sustain persistent, high-cost effects against multiple strategic targets over time. There is simply no guarantee that a state can generate significant costs against a target in the context of an unfolding crisis. This reality starkly contrasts with the relative predictability and reliability of conventional effects. Indeed, the empirical record has largely validated this claim; “the vast majority of malicious cyber activity has taken place far below the threshold of armed conflict between states, and has not risen to the level that would trigger such a conflict.”⁴⁵ This is why, in Lin's parlance, “going cyber is pre-escalatory” and countervalue cyberattacks (those that target civilian, rather than military, assets) occur “all the time now and are at the BOTTOM of the escalation ladder” [emphasis in original].⁴⁶ Rather than their ability to wreak permanent, destructive

effects, cyber operations are often prized for their temporary and reversible nature.⁴⁷

One metric to assess the cost-generation potential of offensive cyber is in terms of loss of life. By this measure, cyber operations are unlikely to inflict significant harm. While theoretically possible that cyber operations could lead directly to a loss of life, no one has reportedly died to date as a direct result of a cyberattack despite over 30 years of recorded cyber operations.⁴⁸ Even in hypothetical catastrophic scenarios, the cost in terms of human casualties is minimal. For instance, common worst-case scenarios of cyberattacks revolve around the loss of power stemming from a cyberattack on an electric grid.⁴⁹ However, even in this instance, the conceivable damage from the loss of power over an extended period is far less than that which could be wreaked using basic, limited conventional capabilities. To draw a comparison, when Hurricane Sandy hit the United States' eastern seaboard in late October 2012, over 8.5 million people were left without power—with many going weeks and even months before it was brought back online.⁵⁰ Yet a US National Hurricane Center postmortem of Hurricane Sandy reported that of the 159 people in the United States killed either directly or indirectly, only “about 50 of these deaths were the result of extended power outages during cold weather, which led to deaths from hypothermia, falls in the dark by senior citizens, or carbon monoxide poisoning from improperly placed generators or cooking devices.”⁵¹ If a cyberattack took out power of a similar magnitude and duration of Hurricane Sandy, it is conceivable that an equivalent number of casualties would result. The 2015 synchronized cyberattacks against Ukrainian power companies, attributed to Russia, was the first known example of an offensive cyber operation targeting a state's power grid. Its cost was ultimately low—service was temporarily disrupted to 225,000 customers for several hours, and energy providers operated at a limited capacity for some time after service was restored.⁵² There were no reported casualties from this power outage. While any casualty resulting from a cyberattack would certainly be lamentable, even worst-case scenario figures are minor in comparison to the cost in human lives stemming from other, even limited, kinetic military operations.

It is also possible to measure the cost of offensive cyberattacks in treasure rather than blood. By this standard, the financial or economic costs of cyberattacks are significant. For example, the most devastating and expensive cyberattack to date—the 2017 NotPetya malware that inflicted widespread economic damage against multinational corporations—reportedly cost Maersk and FedEx \$300 million each, and the total cost of the Not-

Petya attacks is estimated to be \$10 billion.⁵³ Despite this, even the most financially costly cyberattacks have thus far failed to invoke “act of war” or “act of force” thresholds.⁵⁴ Targets have also demonstrated a consistent ability to recover even from destructive cyberattacks with relative speed. In two such cases attributed to North Korea—the 2013 South Korean banks’ attack and the 2014 Sony attack—“despite the destruction of files, all are still in business, and none spent more than an inconsequential amount of time recovering.”⁵⁵ This does not imply that the economic costs of cyber operations are unimportant or lack strategic consequence. However, particularly when they occur in the absence of physical violence, contextualizing the cost of offensive cyber operations raises doubts about their effects in comparison to other types of offensive military operations.

Therefore, even if a state has the capabilities at the time and chooses to respond to a cyberattack with what could be characterized as a potentially escalatory offensive cyber operation, the effects of the response may not be sufficiently high to sustain or provoke a continued escalatory spiral between the parties. One possible counterargument to this line of reasoning is that states may perceive the costs of offensive cyber operations differently from each other, and this divergence could generate escalation risks. This concern is not new to the escalation literature; Herman Kahn acknowledged that his concept of an escalation ladder likely reflects a Western approach to escalation, and that the Soviet Union may take a different approach to conceptualizing such a ladder.⁵⁶ Similarly, in cyberspace, differences in factors such as strategic and organizational culture, regime type, strategy and doctrine, and force employment may mean that what is perceived as a relatively low-cost cyber response by one state may be in fact cross a key threshold of the other. We acknowledge that this is a legitimate concern, but one that could be remedied through improving ongoing efforts between adversaries to establish confidence building measures (CBMs) to signal intent and reduce crisis instability.⁵⁷ One example is the 2013 bilateral agreement between the United States and Russia to use the Nuclear Risk Reduction Center (NRRC) to communicate about cyber incidents.⁵⁸

Countervailing Tradeoffs

Even under hypothetical circumstances in which a state possesses the ability to escalate using cyber means, three characteristics of offensive cyber operations may blunt its willingness to do so: operational requirements for secrecy, attribution difficulties, and the role of espionage.

First, while secrecy is sometimes hypothesized to aggravate rather than relieve tensions because it increases uncertainty, in a cyber context the

operational requirement for secrecy can give decision-makers pause when weighing tradeoffs. For example, the costs associated with conducting a noisy offensive cyber operation may jeopardize important intelligence assets (discussed below) or render obsolete capabilities that a state may want to hold in reserve for some future engagement where stakes or interests may be higher.

Secrecy is key for operational success. Revealing plans to gain accesses to a target and efforts to develop tools (particularly highly tailored ones) prior to or during the course of an operation permits defenders to take concrete steps to render the threat inert.⁵⁹ In particular, secrecy is essential to maintaining access once a vulnerability has been discovered and an exploit built for it, especially once an attacker has already gained a foothold in a network but has not yet completed execution of its mission. Attackers must keep their behavior secret from network defenders who are employing multiple layers of methods to uncover and defeat the intrusion at each stage of the attacker's operation. Employing host-based hiding techniques, for example, prevents defenders from detecting an attacker's presence.⁶⁰ Network defenders can employ intrusion-detection approaches to uncover adversaries attempting to gain access to a network, such as deploying perimeter sensors to detect activity at all ingress and egress points in a network. Sophisticated defenders will also collect and analyze data about anomalous behavior within a network perimeter after a hypothetical adversarial breach, such as identifying novel or remote executables.⁶¹ If the target uncovers the presence of an adversary on its networks and has information about the attack vector, it can marshal defenses and take measures to patch vulnerabilities, rendering moot the attacker's access (and therefore whatever effects might be delivered). This is why military and intelligence organizations, for instance, typically maintain secrecy about zero-day exploits and why markets for zero days on the Dark Web proliferate.⁶² Indeed, from a defensive perspective, cyber hunt teams exist because attacker obfuscation is so integral to offensive missions, particularly when attempting lateral movement or privilege escalation within a network. Secrecy is also critical to preserving the tool itself because exposing that information allows the target to develop defenses against it and may also reveal the attacking state's targeting strategy and broader set of capabilities.

Therefore, the decision to conduct an offensive cyber operation in response to adversary behavior demands that decision-makers weigh the potential costs of burning accesses and tools revealed through the operation. In other words, cyber operations have a "use it and lose it" quality.

Some might postulate that this attribute generates perceived windows of opportunity and vulnerability such that a state would be more likely to use any offensive capabilities it may possess at the moment out of the fear that they won't be available for future use.⁶³ While these incentives may exist when stakes are high, or for decision-makers with certain risk profiles, the reverse is also true: using a capability nearly guarantees that it won't be available for future use.

Second, beyond operational requirements for secrecy, states make political decisions to eschew attribution for offensive cyber operations.⁶⁴ States employ technical methods to avoid attribution (e.g., obfuscating points of departure of attacks by using spoofing, proxy servers, third-party infrastructure, compromised certificates, and other anonymizing capabilities) as well as make deliberate efforts to obscure command and control for cyberattacks (e.g., using cyber proxies with varying degrees of plausible deniability).⁶⁵ The time requirements for a targeted state to achieve attribution at a reasonable confidence threshold, as well as its willingness to share potentially sensitive intelligence information with allies or domestic publics to justify any escalatory responses, create additional temporal breaks for the pressure of a crisis situation to diffuse and for decision-makers to evaluate alternative courses of action.

Finally, related to the role of secrecy in cyber operations is the inextricable link between espionage—particularly cyber intelligence, surveillance, and reconnaissance (ISR)—and offensive cyber operations.⁶⁶ Cyber ISR is “an *essential predicate* and enduring companion to mission success in the cyber realm” [emphasis in original].⁶⁷ It includes information about a target collected through a variety of cyber and noncyber intelligence sources.⁶⁸ This is due to collection requirements against targets to plan and execute offensive operations. As Martin Libicki notes, the “notion that cyber-warriors can be assigned to any target on the fly may not be entirely the case. . . . This tenet understates how much intelligence preparation is required for a successful attack. Success at operational cyberwar depends to a great extent on knowing where the target is vulnerable.”⁶⁹ The time and resource requirements for intelligence about a target may exceed by orders of magnitude those needed to conduct an operation—potentially at a ratio of 100 to 1.⁷⁰

Intelligence collection is important not only prior to gaining access to a target's network or system (identifying vulnerabilities and developing exploits for them) but also oftentimes continues to play a role even after an actor has established a foothold in a network. Cyber weapons themselves may have built-in intelligence collection functions to gather information

about a target's network subsequent to penetration. This is because attackers must possess intimate knowledge of a network's structure and how components relate to one another—information that can often be gained only after breaching the network itself.⁷¹ This requisite underscores a key distinction between two types of cyber operations—computer network exploitation (CNE) and computer network attack (CNA). While they both require exploiting a vulnerability to gain access to a target, CNE involves clandestinely gaining access to observe and exfiltrate private information while CNA entails delivering some kind of effect against data at rest or in transit (e.g., disrupt, degrade, destroy, etc.).⁷² CNE, therefore, can be conducted to gather additional information as part of laying the groundwork for a forthcoming offensive operation.⁷³ For instance, an attacker might conduct an initial CNE operation to “map the network and make inferences about important and less important nodes on it simply by performing traffic analysis to determine what the organizational structure is and who holds positions of authority” for the purposes of identifying the key nodes to attack.⁷⁴

Intelligence is vital at every step of an operation, from collecting information about the specifications of a target's network or system and identifying vulnerabilities to serve as a foothold for an attack, to developing means of access and the exploit itself. It is also costly and intensive. As Austin Long notes, “The intelligence requirements for cyber options are immense, as the delivery mechanism is entirely dependent on intelligence collection.”⁷⁵ Laying the intelligence groundwork for an offensive cyber operation “can be extraordinarily difficult, even for advanced cyber actors.”⁷⁶ This is because states typically secure the critical systems that might be targeted through cyber means (e.g., nuclear power plants, electrical grids, or water filtration systems) because of their importance to social and economic functioning and national security. Therefore, developers of cyber weapons must collect intelligence on a target that is likely to be well defended and not connected to the Internet, as well as have intimate knowledge of the specific information or operational technology on which a particular system was built, which is often customized and not publicly known. Developing a capability that can interface with a custom-built system is difficult, but it is by orders of magnitude more arduous to develop the mastery necessary to manipulate the system to do something that it may have been designed to resist—to understand, for instance, how complex processes relate to one another or to identify key nodes that could be targeted to produce cascading failures.

The above discussion illustrates not only the immense intelligence work that underlies offensive cyber operations but also its value. CNE operations enabling actors to maintain persistent, stealthy presence in a target and collect information have critical strategic utilities in terms of their contribution to a state's intelligence collection efforts for espionage purposes as well as their support of potential future military operations. Indeed, data collected on state-conducted cyber operations indicates that the overwhelming majority of these are for intelligence or espionage.⁷⁷ The strategic worth of cyber intelligence activities—which are also required to support offensive operations—demands that governments conduct intelligence gain/loss calculations when evaluating the potential upside of conducting offensive operations that may jeopardize cyber intelligence assets. The fact that cyber operations have alternative and sometimes competing strategic utilities can reduce the probability of escalation via cyber means contingent on how decision-makers rank these different utilities.

One counterargument to the effects of intelligence gain/loss calculations on decisions about escalation is that there may be situations when the interests at stake are sufficiently high to warrant prioritizing offensive action over preserving intelligence. In general, when stakes are high in both cyber and noncyber realms, we should expect the probability of escalation to increase. However, the strategic value of cyber-enabled intelligence collection activities for both espionage and military purposes is an important factor militating against escalatory decision-making that is not as salient in other domains.

Willingness to Engage in Cross-Domain Escalation

Just as the limited ability of offensive cyber operations to generate meaningful and sustained costs against a target reduces their appeal as tools of escalation, it also diminishes the likelihood of cross-domain escalatory responses to a cyber incident. Cyber operations can cause significant economic and, in some instances, second-order effects on human life (such as cyberattacks against a power grid). However, they have not yet produced the physical violence and horrors of kinetic warfare or even terrorism that would engender a visceral public reaction to prod decision-makers into escalatory responses—particularly responses that would cross a key threshold from cyber to kinetic force. In other words, both the tangible and psychological costs of cyber operations may check domestic political willingness (or pressure) to escalate via cross-domain instruments in response to adversary cyber operations.


A counterargument to this logic, similar to the discussion above regarding cost generation, is the notion that sharply distinguishing between acts that harm people and break things versus those that generate less tangible costs may be limited to certain types of states. Analogous recommendations to improve cyber CBMs to promote transparency and stability would mitigate risks stemming from differing conceptions of cost.

Implications for US Policy Making

The above analysis suggests several important implications for policy making, particularly for the United States. First, our analysis should not be construed to imply that there are no circumstances in which we might expect to observe significant and risky escalation between rivals in cyberspace. In fact, our analysis suggests that the leading dangers lie in circumstances where the interests at stake are high and at least one party to a rivalry seeks to escalate. In these cases, when the latter may lack ability to do so using cyber means for the manifold reasons outlined above, a state may be incentivized to default to cross-domain, kinetic responses that would engender risks of spirals into unwanted conflict. We would expect this particular circumstance to be relatively rare, given that it is unlikely that a single cyber incident would be sufficiently costly in itself to trigger this chain of decision-making. Nevertheless, the potential consequences of such a low-probability, high-consequent event suggests that an important next step for researchers and practitioners is to theorize about more specific scenarios—such as those before, during, or after a great power conflict—that might approach these thresholds and explore how to build de-escalation pathways tailored to them.

Second, there is a growing recognition that the United States has historically been overly self-restrained in its approach to countering adversary behavior in cyberspace. For instance, it has chosen to largely employ diplomatic and legal instruments of power to address Chinese theft of national security intelligence property or Russian cyber-enabled influence operations that erode confidence in fundamental US democratic institutions. The 2018 DOD Cyber Strategy reflects a shift in this approach to a posture that is more active and engaged.⁷⁸ If our analysis above is correct, it would imply that the United States can safely engage its adversaries in cyberspace more assertively without invariably provoking dangerous escalation dynamics, although campaign planning should consider and conduct risk assessments of the types of scenarios outlined above that may trigger unwanted escalation. The reportedly first operational application of the “defend forward” concept, the US Cyber Command

operation to temporarily take the Russian troll farm, the Internet Research Agency, offline in the days preceding the 2018 midterm elections, provides initial (albeit limited) evidence that the United States can engage adversaries more directly in cyberspace without provoking escalatory spirals.⁷⁹ Additional evidence over time will provide further corroboration in either direction of the hypotheses presented in this analysis.

Finally, beyond the escalation implications of “defending forward,” our analysis highlights the limitations of cyber operations as independent tools of statecraft. To effectively alter the cost-benefit calculus of US adversaries, roll back existing adversary gains, and shape the future operating environment to better reflect US interests and values, policy makers should appreciate that cyber means are not a panacea for addressing cyber challenges. Any US strategy for cyberspace should incorporate the full range of instruments of power, particularly because the United States maintains an asymmetric advantage in noncyber instruments while facing peer and near-peer competitors in the cyber realm. Discerning how to integrate and apply cyber capabilities not only in conjunction with and in support of conventional military power, but also across the other instruments of power, represents a key imperative for policy makers in the current strategic environment and in a future possibly dominated by another great power conflict. 

Notes

1. Lawrence J. Cavaiola, David C. Gompert, and Martin Libicki, “Cyber House Rules: On War, Retaliation and Escalation,” *Survival: Global Politics and Strategy* 57, no. 1 (February–March 2015): 84–94; and Martin C. Libicki, *Crisis and Escalation in Cyberspace*, (Santa Monica, CA: RAND, 2012), 10, 93–97, 106–8, 114–19. In an earlier piece, Libicki also argues that the factors that distinguish the cyber domain from conventional ones make the former more escalatory, such as the uncertainty surrounding the effects of cyberattacks; the asymmetric nature of the vulnerability in the domain, which could prompt escalation to conventional kinetic attacks; and the greater credibility of retaliatory threats. See Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND, 2009), 69–74. See also Roger Hurwitz, “Keeping Cool: Steps for Avoiding Conflict and Escalation in Cyberspace,” *Georgetown Journal of International Affairs*, 2013–14, 17, <https://pdfs.semanticscholar.org/89c6/170c26f6f5b6f56271b7e1ee82af3f4e5e41.pdf>; David C. Gompert and Martin Libicki, “Cyber Warfare and Sino-American Crisis Instability,” *Survival: Global Politics and Strategy* 56, no. 4 (August–September 2014): 7–22; and Avery Goldstein, “First Things First: The Pressing Danger of Crisis Instability in U.S.–China Relations,” *International Security* 37, no. 4 (2013): 49–89.

2. “Joint Statement for the Record to the Senate Armed Services Committee, Foreign Cyber Threats to the United States, The Honorable James R. Clapper, Director of National Intelligence, The Honorable Marcel Lettre, Undersecretary of Defense for Intelligence, Admiral Michael S. Rogers, USN, Commander, U.S. Cyber Command, Director, National Security Agency,” 5 January 2017, <https://www.scribd.com/>.

3. For example, see Jason Healey, “The Cartwright Conjecture: The Deterrent Value and Escalatory Risks of Fearsome Cyber Capabilities,” in *Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations*, eds. Herbert Lin and Amy Zegart (Washington, DC: Brookings Institute Press, 2019). In a keynote address, Healey has also claimed that conflict in cyberspace is “the most escalatory kind of conflict we have ever come across.” Jason Healey (keynote address, CyberTalks, New York City, 8 September 2016). For a dissenting view, see Brandon Valeriano, Benjamin Jensen, and Ryan C. Maness in their book *Cyber Strategy: The Evolving Character of Power and Coercion* (Oxford: Oxford University Press, 2018) for a critique of the belief that cyberspace is escalatory.

4. Department of Defense, *Summary: Department of Defense Cyber Strategy 2018* (Washington, DC: Department of Defense, 2018), 1, https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF. For reactions to the strategy, see Max Smeets and Herbert Lin, “An Outcome-Based Analysis of U.S. Cyber Strategy of Persistence & Defend Forward,” *Lawfare*, (blog), Lawfare Institute in cooperation with the Brookings Institution, 28 November 2018, <https://www.lawfareblog.com/>; and Brandon Valeriano and Benjamin Jensen, “The Myth of Cyber Offense: A Case for Restraint,” Policy Analysis no. 862, Cato Institute, 15 January 2019, <https://www.cato.org/>.

5. Statement of Brandon Valeriano, PhD, Donald Bren Chair of Armed Politics, Marine Corps University, Reader in Digital Politics, Cardiff University, Adjunct Fellow of Cyber Security, Niskanen Center, “The International Cyber Conflict Threat Landscape,” Cyber Threats Facing America, Testimony before the United States Senate Committee on Homeland Security and Government Affairs, 10 May 2017, <https://www.hsgac.senate.gov/imo/media/doc/Testimony-Valeriano-2017-05-10-REVISED2.pdf>. See also Valeriano, Jensen, and Maness, *Cyber Strategy*, 66, where the authors note that “while cyber incidents are increasing [between 2000 and 2014], this increase appears to be directly associated with espionage and disruption campaigns, not the more malicious degradation activities that many fear.”

6. Valeriano, Jensen, and Maness, 76.

7. Erica D. Borghard and Jacquelyn Schneider, “Israel Responded to a Hamas Cyberattack with an Airstrike. That’s Not Such a Big Deal,” *The Washington Post*, 9 May 2019, <https://www.washingtonpost.com/>.

8. For seminal academic work on escalation see Herman Kahn, *On Escalation: Metaphors and Scenarios* (New Brunswick, NJ: Transaction Publishers, 2010); Richard Smoke, *War: Controlling Escalation* (Cambridge, MA: Harvard University Press, 1977); Barry R. Posen, *Inadvertent Escalation: Conventional War and Nuclear Risks* (Ithaca: Cornell University Press, 1991); and Bernard Brodie, *Escalation and the Nuclear Option* (Princeton: Princeton University Press, 1966).

9. Forrest E. Morgan, Karl Mueller, Evan S. Medeiros, Kevin L. Pollpeter, and Roger Cliff, *Dangerous Thresholds: Managing Escalation in the 21st Century* (Santa Monica, CA: RAND, 2008), 8, https://www.rand.org/content/dam/rand/pubs/monographs/2008/RAND_MG614.pdf.

10. Brodie, *Escalation*, 104.

11. Kahn, *On Escalation*, 23–24, 38; Thomas Schelling, *Arms and Influence* (New Haven: Yale University Press, 1966), chap. 3; Robert Jervis, “Cooperation under the Security Dilemma,” *World Politics* 30, no. 2 (January 1978), 167–214; Posen, *Inadvertent Escalation*; Scott D. Sagan, *The Limits of Safety: Organizations, Accidents, and Nuclear Weapons* (Princeton: Princeton University Press, 1993); and Graham T. Allison, *Essence of Decision: Explaining the Cuban Missile Crisis* (Boston: Little, Brown, 1971).

12. Herbert Lin, “Escalation Dynamics and Conflict Termination in Cyberspace,” *Strategic Studies Quarterly* 6, no. 3 (Fall 2012): 46–70, https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-06_Issue-3/Lin.pdf.

13. William A. Owens, Kenneth W. Dam, and Herbert S. Lin, eds., *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities* (Washington, DC: National Academies Press, 2009), 83–89. Zero days are the crown jewel of vulnerabilities. Zero days are vulnerabilities in hardware or software that exist “in the wild” and are unknown to defenders.

Therefore, patches have not yet been developed for them. Zero-day vulnerabilities are often revealed only after they have been exploited. Even then, it may take time for defenders to ascertain that a zero day was used.

14. For an additional discussion of access dependence, see Erica D. Borghard and Shawn W. Lonergan, “The Logic of Coercion in Cyberspace,” *Security Studies* 26, no. 3 (May 2017): 452–81. While nearly all cyber weapons require exploiting some kind of vulnerability to gain access to a target and deliver an effect, there are some exceptions. Distributed denial-of-service (DDoS) attacks, for instance, do not require gaining access but, rather, produce disruptive effects by overwhelming the target’s processing capacity (typically through jamming its bandwidth via the sheer volume of requests). However, at scale, the process of building large botnet armies to carry out DDoS attacks involves exploiting vulnerabilities in infected devices that are then harnessed as part of the botnet.

15. Chris Inglis, “Illuminating a New Domain: The Role and Nature of Military Intelligence, Surveillance, and Reconnaissance in Cyberspace,” in Lin and Zegart, *Bytes, Bombs, and Spies*, 25.

16. Jason Healey, “Claiming the Lost Cyber Heritage,” *Strategic Studies Quarterly* 6, no. 3 (Fall 2012): 14, https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-06_Issue-3/Healey.pdf.

17. Cost considers the resource requirements necessary to acquire access, risk includes physical as well strategic risks of different means of access, and reliability pertains to the likelihood of achieving a desired outcome.

18. A potential source of change is IT/OT convergence, which may reduce barriers to gaining access to OT networks and systems. See, for example, *IT/OT Convergence—Moving Digital Manufacturing Forward* ([San Jose, CA?]: Cisco, 2018), https://www.cisco.com/c/dam/en_us/solutions/industries/manufacturing/ITOT-convergence-whitepaper.pdf.

19. There are exceptions to each model. IT networks can indeed be closed and not connected to the open Internet, and OT networks can have access to the Internet. That said, OT networks having access to the open Internet are considered poor cybersecurity, and the convergence of the two networks is something most cybersecurity practitioners try to avoid. In one interesting study, Blake Rhoades et al. found maritime systems connected to the Internet. For further information see Jim Twist, Blake Rhoades, and Ernest Wong, “Navigating the Cyber Threats to the U.S. Maritime Transportation System,” in *Maritime Cyber Security*, eds. Joseph DiRenzo III, Nicole K. Drumhiller, and Fred S. Roberts (Washington, DC: Westphalia Press, 2017), chap. 4.

20. From a network engineering perspective, networks are layered in what is termed the Open Systems Interconnection (OSI) model. There are seven layers in the OSI model, ranging from the application layer, which is closest to the end user. From a broad technical vantage point, the lower the level of access, the greater the control and persistence a potential cyber capability can have over a compromised system.

21. For our purposes, it is not theoretically necessary to distinguish between software and firmware, but it is important to note that, from a technical perspective, they are different. Firmware is a type of software placed in hardware and is responsible for controlling some of the hardware’s basic functions. Like software, firmware can (and should, from a cybersecurity perspective) be updated.

22. Max Smeets, “A Matter of Time: On the Transitory Nature of Cyber Weapons,” *Journal of Strategic Studies* 41, nos. 1–2 (2017): 18.

23. Other types of cyber weapons are more modular or can be used in roughly the same form (or quickly repurposed in a slightly different and new form) against a range of potential targets. Examples of the latter include the recent proliferation of “malware as a service” markets, where individual can pay to rent botnets that distribute malware or families of ransomware, such as the evolution from Petya to NotPetya. See Department of Homeland Security (DHS), *Malware Trends: Industrial Control Systems Emergency Response Team (ICS-CERT), Advanced Analytic Laboratory (AAL)*, white paper (Arlington, VA: DHS, National Cybersecurity and Communications Integrations Center, October 2016), 2, https://www.us-cert.gov/sites/default/files/documents/NCCIC_ICSCERT_AAL_Malware_Trends_Paper_S508C.pdf.

24. Martin C. Libicki, "Second Acts in Cyberspace," in Lin and Zegart, *Bytes, Bombs, and Spies*, 133.
25. "Cyber-attack: US and UK Blame North Korea for WannaCry," BBC, 19 December 2017, <https://www.bbc.com/>.
26. Kim Zetter, "An Unprecedented Look at Stuxnet, the World's First Digital Weapon," *Wired*, 3 November 2014, <https://www.wired.com/>.
27. Steven Bellovin et al., "Limiting the Undesired Impact of Cyber Weapons: Technical Requirements and Policy Implications," in Lin and Zegart, *Bytes, Bombs, and Spies*, 269.
28. Herbert Lin, "Of-Neglect Cost Drivers of Cyber Weapons," *Net Politics* (blog), Council on Foreign Relations, 14 December 2016, <https://www.cfr.org/blog/oft-neglected-cost-drivers-cyber-weapons>.
29. From a defensive/cybersecurity perspective, the pace of DevOps (a conjunction of "development"—building computer programs—and "operations"—testing those programs) in a dynamic and continuous process reflects the dynamism of the environment.
30. Libicki, "Second Acts in Cyberspace," 133.
31. For research on the lifecycle of zero-day exploits, see Lillian Ablon and Andy Bogart, *Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and Their Exploits* (Santa Monica, CA: RAND Corporation, 2017), <https://www.rand.org/>.
32. "New CNMF Initiative Shares Malware Samples with Cybersecurity Industry," US Cyber Command, 5 November 2018, <https://www.cybercom.mil/>.
33. Martin C. Libicki, "Second Acts in Cyberspace," 133. Also see Smeets, "A Matter of Time."
34. Within the US government, for example, there is a Vulnerabilities Equities Process (VEP) that articulates standards for when the government discloses information about zero-day vulnerabilities. See White House, "Vulnerabilities Equities Policy and Process for the United States Government," 15 November 2017, <https://www.whitehouse.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF>. Governments and other actors must balance tradeoffs between the public security goods associated with information-sharing about vulnerabilities (which would enhance the overall security of information technology networks and systems) and the potential national security/intelligence benefits that come with stockpiling zero days. It is important to note that there is considerable variation in the time it takes different organizations to patch vulnerabilities.
35. Scott Shane, Nicole Perloth, and David E. Sanger, "Security Breach and Spilled Secrets Have Shaken the N.S.A. to Its Core," *The New York Times*, 12 November 2017, <https://www.nytimes.com/2017/11/12/us/nsa-shadow-brokers.html>.
36. Inglis, "Illuminating a New Domain," 29.
37. Austin Long, "A Cyber SIOP? Operational Considerations for Strategic Offensive Cyber Planning," in Lin and Zegart, *Bytes, Bombs, and Spies*, 120.
38. William T. Eliason, "An Interview with Paul M. Nakasone," *Joint Force Quarterly* 92 (1st Quarter 2019): 7–8, <https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-92/jfq-92.pdf>.
39. Department of Defense, Defense Science Board, *Task Force Report: Resilient Military Systems and the Advanced Cyber Threat* (Washington, DC: Office of the Under Secretary of Defense for Acquisition, Technology and Logistics, January 2013), 49, <https://apps.dtic.mil/dtic/tr/fulltext/u2/a569975.pdf>.
40. Erica D. Borghard, "The 'Known Unknowns' of Russian Cyber Signaling," *Net Politics* (blog), Council on Foreign Relations, 2 April 2018, <https://www.cfr.org/>.
41. See Erik Gartzke, "The Myth of Cyberwar," *International Security* 38, no. 2 (Fall 2013): 41–73; and Thomas Rid, *Cyber War Will Not Take Place* (Oxford: Oxford University Press, 2013).
42. Herbert S. Lin, "Offensive Cyber Operations and the Use of Force," *Journal of National Security Law & Policy* 4, no. 63 (2010): 63, http://jnslp.com/wp-content/uploads/2010/08/06_Lin.pdf.
43. For a discussion of the distinction between brute force and coercion, see Thomas Schelling, *Arms and Influence*. See also Robert J. Art, "To What Ends Military Power?," *International Security* 4, no. 4 (Spring 1980): 3–35.

44. For a more detailed discussion of this point, see Borghard and Lonergan, “Logic of Coercion in Cyberspace,” 452–481, 461–463.

45. Eric Talbot Jensen, “The Tallinn Manual 2.0: Highlights and Insights,” *Georgetown Journal of International Law* 48, no. 3 (2017): 736, <https://www.law.georgetown.edu/international-law-journal/wp-content/uploads/sites/21/2018/05/48-3-The-Tallinn-Manual-2.0.pdf>.

46. Herbert Lin, “Thinking about Nuclear and Cyber Conflict: Same Questions, Different Answers” (presentation, Hoover Institution/Center for International Security and Cooperation, Stanford University, CA, 15 May 2015), 4, <https://sipa.columbia.edu/sites/default/files/Thinking%20about%20Nuclear%20and%20Cyber%20Conflict-Columbia-2015-05-14.pdf>.

47. Max Smeets and Herbert S. Lin, “Offensive Cyber Capabilities: To What Ends?,” 10th International Conference on Cyber Conflict (CyCon), Tallinn, Estonia, 2018.

48. Some might claim that there have been indirect deaths associated with cyberattacks, such as the WannaCry ransomware attack in May 2017 that crippled the UK’s National Health Service. However, a 2018 National Audit Investigation by the British government does not even mention indirect casualties that may have resulted from the impact of the cyberattack on UK hospital and medical providers. Comptroller and Auditor General, Department of Health, *Investigation: WannaCry Cyber Attack and the NHS* (London: National Audit Office, 25 April 2018), <https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf>.

49. See for example, Joseph Marks, “Pentagon Researchers Test ‘Worst-Case Scenario’ Attack on U.S. Power Grid,” Nextgov, 13 November 2018, <https://www.nextgov.com/cybersecurity/2018/11/pentagon-researchers-test-worst-case-scenario-attack-us-power-grid/152803/>.

50. Eric S. Blake et al., “Tropical Cyclone Report—Hurricane Sandy (AL182012), 22–29 October 2012,” National Hurricane Center, 12 February 2013, 14–15, http://www.nhc.noaa.gov/data/tcr/AL182012_Sandy.pdf.

51. Blake et al., 14.

52. US Industrial Control System—Computer Emergency Response Team (ICS-CERT), Department of Homeland Security, “Cyber-Attack against Ukrainian Critical Infrastructure,” Alert IR-ALERT-H-16-056-01, 25 February 2016, <https://www.us-cert.gov>; and Industrial Control Systems (ICS), *Analysis of the Cyber Attack on the Ukrainian Power Grid: Defense Use Case*, Electricity Information Sharing and Analysis Center (E-ISAC) (Washington, DC: E-ISAC, 18 March 2016), https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.

53. Andy Greenberg, “The Untold Story of NotPetya, the Most Devastating Cyberattack in History,” *Wired*, 22 August 2018, <https://www.wired.com/>; and Matthew P. McCabe, “NotPetya Was Not Cyber ‘War,’” *Marsh & McLennan Insights*, August 2018, <http://www.mmc.com/>.

54. There is no international legal consensus on what specific behavior might be considered an “act of war or use of force” in cyberspace. Thus, the determination stems more from a political decision. The Tallinn Manual 1.0, which addresses questions of jus ad bellum for cyberspace, excludes cyberattacks carried out for “economic coercion” purposes from the “use of force” category. See Michael N. Schmitt, ed., *Tallinn Manual on International Law Applicable to Cyber Warfare* (Cambridge: Cambridge University Press, 2013), 48–52. President Obama, for example, deemed the North Korean cyberattacks against Sony Entertainment to be “cyber vandalism.” Sean Sullivan, “Obama: North Korea Hack ‘Cyber-vandalism’ not ‘Act of War,’” *The Washington Post*, 21 December 2014, https://www.washingtonpost.com/news/post-politics/wp/2014/12/21/obama-north-korea-hack-cyber-vandalism-not-act-of-war/?utm_term=.372998661031.

55. Bellovin et al., “Limiting the Undesired Impact of Cyber Weapons,” 272.

56. Herman Kahn, *On Escalation*, 218.

57. For more on cyber CBMs, see Erica D. Borghard and Shawn W. Lonergan, “Confidence Building Measures for the Cyber Domain,” *Strategic Studies Quarterly* 12, no. 3 (Fall 2018): 10–49, https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-12_Issue-3/Borghard-Lonergan.pdf.

58. Borghard and Lonergan, 31–32.

59. As applied to deterrence, Gartzke and Lindsay term this the “cyber commitment problem.” See Erik Gartzke and Jon R. Lindsay, “The Cyber Commitment Problem and the Destabilization of Nuclear Deterrence,” in Lin and Zegart, *Bytes, Bombs, and Spies*, 204. An interesting theoretical extension of this is to explore the implications for rationalist explanations for war. In this line of reasoning, war occurs because states disagree about the balance of power, and as information is revealed over the course of fighting about the true balance of capabilities and resolve, they should arrive at the outcome that reflects these. However, in cyberspace, revealing information about capabilities can actually change the balance of power as it removes those capabilities from the table for future use.

60. For a thorough discussion of different types of adversary OPSEC tactics, techniques, and procedures, see MITRE, “PRE-ATT&CK Techniques,” 2018, <https://attack.mitre.org/techniques/pre/>.

61. Blake E. Strom et al., *Finding Cyber Threats with ATT&CK-Based Analytics* (Annapolis Junction, MD: MITRE, June 2017), 17–21, <https://www.mitre.org/sites/default/files/publications/16-3713-finding-cyber-threats%20with%20att%26ck-based-analytics.pdf>.

62. Lillian Ablon, Martin C. Libicki, and Andrea A. Golay, *Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar* (Santa Monica, CA: RAND Corporation, 2014), chap. 4, https://www.rand.org/pubs/research_reports/RR610.html.

63. For more on how perceived windows of opportunity and vulnerability can generate inadvertent escalation risks, see Posen, *Inadvertent Escalation*.

64. See, for example, Thomas Rid and Ben Buchanan, “Attributing Cyber Attacks,” *Journal of Strategic Studies* 30, nos. 1–2 (2015): 4–37. For how secrecy can aid defenders, see Erik Gartzke and Jon R. Lindsay, “Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace,” *Security Studies* 24, no. 2 (2015): 316–348.

65. For further reference, see Clement Guitton and Elaine Korzak, “The Sophistication Criterion for Attribution: Identifying the Perpetrators of Cyber-Attacks,” *The RUSI Journal* 158, no. 4 (2013): 62–68. Rid and Buchanan argue that, at the strategic level, “attribution is a function of what is at stake politically”; see Rid and Buchanan “Attributing Cyber Attacks,” 7. Also see Erica D. Borghard and Shawn W. Loneragan, “Can States Calculate the Risks of Using Cyber Proxies?,” *Orbis* 60, no. 3 (May 2016): 395–416, for a discussion of why states delegate authority to proxy actors to conduct cyberattacks on their behalf; and Tim Maurer, *Cyber Mercenaries: The State, Hackers, and Power* (Cambridge: Cambridge University Press, 2017).

66. However, other sources of intelligence, such as human (HUMINT) and open-source (OSINT), can contribute to preparatory efforts.

67. Inglis, “Illuminating a New Domain,” 24.

68. Matthew M. Hurley, “For and from Cyberspace: Conceptualizing Cyber Intelligence, Surveillance, and Reconnaissance,” *Air & Space Power Journal* 26, no. 6 (November–December 2012): 14, https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Volume-26_Issue-6/F-Hurley.pdf.

69. Libicki, “Cyberdeterrence,” 154.

70. Libicki, 155.

71. Bellovin et al., “Limiting the Undesired Impact of Cyber Weapons,” 274.

72. Lin, “Offensive Cyber Operations,” 63–64.

73. Andru E. Wall, “Demystifying the Title 10–Title 50 Debate: Distinguishing Military Operations, Intelligence Activities & Covert Action,” *Harvard National Security Journal* 3, no. 1 (2011): 118–20, <https://harvardnsj.org/wp-content/uploads/sites/13/2012/01/Vol-3-Wall.pdf>.

74. Lin, “Offensive Cyber Operations,” 69.

75. Long, “Cyber SIOF,” 117.

76. Long, 117.

77. The Council on Foreign Relations Cyber Operations tracker identifies 290 distinct cyber operations that occurred from 2005 to 2018 as of 12 February 2019; see <https://www.cfr.org/interactive/cyber-operations>. Cyber activity encompasses a range of actions, including DDoS attacks, espio-

nage, defacement, data destruction, sabotage, and doxing. Of these, there are 8 cases of data destruction, 4 of defacement, 16 of DDoS, 4 of doxing, 237 of espionage, and 16 of sabotage; the remaining 5 are uncategorized in the data but, according to the descriptions, are additional instances of espionage. Similarly, Brandon Valeriano and Ryan Maness's Dyadic Cyber Incident Dataset (ver. 1.1) identifies 192 cyber incidents between 2000 and 2014. They code the incidents according to different types: vandalism, DDoS, intrusion, and infiltration. Intrusions are equivalent to the CFR's coding of espionage. In this dataset, there are 31 cases of vandalism, 33 of DDoS, 88 of intrusion (espionage), and 40 of infiltration.

78. For an excellent discussion of the evolution of US cyber strategy, see Jacquelyn G. Schneider, "Persistent Engagement: Foundation, Evolution and Evaluation of a Strategy," *Lawfare* (blog), Lawfare Institute in cooperation with the Brookings Institution, 10 May 2019, <https://www.lawfareblog.com/>.

79. Erica D. Borghard, "What a U.S. Operation against Russian Trolls Predicts about Escalation in Cyberspace," *War on the Rocks*, 22 March 2019, <https://warontherocks.com/>.

Erica D. Borghard

Dr. Borghard is an assistant professor at the Army Cyber Institute at the United States Military Academy at West Point and a research fellow at the Saltzman Institute of War and Peace Studies at Columbia University. She holds a PhD in political science from Columbia University.

Shawn W. Lonergan

Dr. Lonergan is a research affiliate of the Army Cyber Institute at the United States Military Academy at West Point and a cyber officer in the US Army Reserve currently assigned to 75th Innovation Command. He holds a PhD in political science from Columbia University.

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.