CHAPTER 13

Offense and Defense in Cyberspace

Evan Perkoski and Michael Poznansky

In 2011, the Department of Defense (DoD) officially declared cyberspace "an operational domain for purposes of organizing, training, and equipping U.S. military forces."[1] Against this backdrop they created a new, subunified command that straddled both the National Security Agency and US Strategic Command. Now, only several years later, the DoD is taking steps to elevate US Cyber Command to a unified combatant command.[2] Each of these moves suggests that the US military is placing the cyber domain on par with land, air, and maritime—the more traditional warfighting domains of the American armed forces. The speed with which the United States has embraced cyberspace is a testament not only to its impact on global affairs in the present but also to the role it will surely play in the future.

Cyberspace offers actors of various stripes a vast tool kit with which to achieve a wide array of goals. It also presents some unique challenges, particularly for states. As former secretary of defense Ashton Carter noted, "We live in a wired world," and this has created new opportunities for nonstate actors to wreak havoc, for states to spy on friends and foes alike, and for militaries to engage one another.[3] None of these goals are new per se. But cyberspace is fundamentally altering the ways in which they are pursued.

The primary objective of this chapter is to familiarize students with the fundamentals of offense and defense in cyberspace. In the first section, we discuss how cyber operations differ from kinetic operations and what, if any, advantages they yield over more traditional methods. In the second section, we discuss some of the most common means by which perpetrators use cyberspace for offensive purposes and, equally important, the various ways in which would-be victims try to defend themselves. In the final section, we draw out several implications of the discussion. In particular, we focus on how cyber operations have affected the character of war, the future of military operations, and how the United States can achieve its strategic objectives in this increasingly "wired world."

Before we begin, though, a brief note on terminology is in order. We largely avoid using the term "cyber war" as a catch-all term since, as in other domains, there are a host of tasks that actors perform in cyberspace that do not constitute—or even come close to—acts of war. Some cyber operations, for example, seek to gain access to networks in order to exfiltrate information or otherwise spy on a particular target. Labeling acts such as these as

cyber war would verge on conceptual stretching. The same can be said of some operations conducted by nonstate actors. Consider how groups such as Anonymous and the Syrian Electronic Army often gain access to websites, including the DoD's, merely to rebrand them with a message and their personal logo. Thus, we mostly prefer the more general term "cyberspace operations."

SEPARATING THE NOVEL FROM THE FAMILIAR

"Cyberwarfare is like a soccer game with all the fans on the field with you and no one is wearing uniforms."[4] This statement from Coast Guard vice admiral Marshall Lytle reflects the popular sentiment that cyberspace is complex, ever evolving, and unique. Our aim in this section is to probe these notions by providing an overview of key differences and similarities between the cyber domain and the traditional domains of land, air, maritime, and space. As we hope will become clear, while cyberspace has some elements that are truly novel, there is also much that is deeply familiar.

Man-Made Domain

One of the ostensibly novel features of cyberspace that might set it apart from other domains is that it is man-made, wholly constituted of infrastructure developed by, and for, people. The fact that cyberspace could not have come into being without human agency does indeed make it qualitatively different from the traditional domains—all of which were created by divine intervention or cosmological accident. As cybersecurity expert Martin Libicki points out, however, "It is not the man-made nature of cyberspace that makes it different. Cities are man-made, but city combat shares many of the rules of country combat. What matters is that cyberspace is highly malleable by its owners, hence its defenders, in ways other media are not. Cities, although man-made, are not particularly malleable (at least not by those defending them)."[5] Indeed, cables can be cut, connections severed, and servers destroyed, all of which can alter the fundamental contours and reaches of the cyber terrain in an instant. In short, the adaptability and flexibility inherent in this man-made domain is much more novel and interesting than the mere fact that it would not exist without humans having created it.

Low Barriers to Entry

It is commonly argued that cyberspace is unique owing to the low barriers to entry. In some cases, only a moderately skilled operator with access to a computer and an Internet connection is necessary to carry out an operation. This is clearly not the case for conventional military operations, whether conducted on land, sea, or air, which almost always require quantities and types of resources that only states can provide. Yet, as with cyberspace, more traditional arenas also afford motivated actors an opportunity to execute missions on the cheap. The most obvious example that comes to mind is that of a terrorist, who can do enormous damage, wreak havoc, and sway public opinion wielding only a kitchen knife or a pickup truck. On the other hand, for large-scale cyberattacks like the Stuxnet operation or China's hack into the Office of Personnel Management, the barriers to entry for lone or nonstate actors may be prohibitively high, approximating the resources necessary to carry out more conventional

operations.[6] Thus, while there are indeed low barriers to entry in some cases, the costs associated with more complex operations remain substantial.

Unparalleled Rapidity

One area where the uniqueness of cyberwarfare shines through most clearly is in the speed of operations, which almost always exceed the pace of traditional, kinetic tools. Richard Clarke, a former cyberspace adviser to the president, writes that now, "as in the 1960s, the speed of war is rapidly accelerating. Then, long-range missiles could launch from the prairie of Wyoming and hit Moscow in only thirty-five minutes. Strikes in cyber war move at a rate approaching the speed of light."[7] A cyber operation launched from one continent can have an effect on another continent in a matter of milliseconds. It is certainly true, of course, that the planning necessary to successfully carry out a given cyber operation—particularly when success depends on extensive knowledge of the target's network and vulnerabilities—often takes far more time than the attack itself. Nevertheless, the fact remains that there are few if any analogs to the cyber domain's capacity to achieve results nearly instantaneously.

Layers of Secrecy

Another commonly discussed feature of cyberspace that is thought to set it apart from other tools of statecraft is that it offers perpetrators unparalleled opportunities to conduct operations under a dense cloak of anonymity. Former director of national intelligence James Clapper noted in 2012 that one of the greatest strategic challenges in cyberspace is "definitive real-time attribution of cyber-attacks. That is, knowing who carried out such attacks and where the perpetrators are located."[8] By routing their attacks through servers in different countries, cyber operators can easily take steps to cover their tracks and even falsely implicate someone else.

The cyber domain is clearly not the first arena where states have competed secretly with one another, as the many covert operations conducted throughout the Cold War and beyond demonstrate.[9] Yet the ease with which actors can achieve anonymity in the cyber domain is almost certainly greater than in any other arena.[10] This has nontrivial implications. For one, it is hard(er) for deterrence to function in cyberspace.[11] If one does not know with near certainty who attacked, credibly promising to retaliate will be fraught with challenges. As Jonathan Lindsay points out, though, the problem of anonymity and attribution may be most keenly felt for low-stakes operations; attribution, and hence deterrence, should be much easier when it comes to large-scale operations that only powerful, well-equipped states can undertake.[12]

While concealing one's identity in cyberspace is possible, concealing one's arsenal (and intentions) may be necessary. Unlike most conventional capabilities, announcing the capacity to levy some kind of attack in cyberspace is manifestly unwise since it affords the would-be victim an opportunity to close a vector or patch a vulnerability.[13] For this reason, actors of all stripes jealously guard their cyber capabilities. This makes estimating an enemy's capabilities much more difficult and any hope of cyber arms control, which would require monitoring and verification, exceedingly challenging. This is not to say that states willingly divulge all facets of their conventional capabilities; private information is rampant in international

politics.[14] All that we are arguing here is that the secrecy surrounding cyber capabilities is heightened relative to other domains.

Uncertain and Limited Effects

Finally, cyber operations may diverge from those in other domains in large part based on their effects. A popular refrain regarding these capabilities is that no one has directly died as the result of a cyberattack. This is technically true. To be sure, those warning of a "cyber 9/11" still worry about such outcomes, yet they have so far failed to materialize. In reality, the most likely scenario for deaths related to cyberspace is incidental fatalities stemming from a cyberattack on a power grid or traffic lights, for example. Yet there are essentially limitless nonlethal cyber outcomes. When it comes to their uses, then, cyber operations are most likely to be employed for intelligence collection, covert influence, sabotage, crime, political activism, or to support kinetic operations. They are less likely to substitute for, but will almost certainly complement, conventional military operations.

CYBER OFFENSE AND CYBER DEFENSE

This section investigates offensive and defensive operations in cyberspace.[15] The former refers to operations aimed at an adversary for exploitative or disruptive means. The latter captures efforts actors can pursue to safeguard against any such attempts.

Cyber Offense

There are several ways to distinguish among different types of offensive cyber operations. One is to look at ultimate ends. Along these lines, the DoD published a memo in 2010 titled "Joint Terminology for Cyberspace Operations," wherein it distinguished between computer network exploitation (CNE) and computer network attacks (CNAs). CNE is defined as "enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data about target or adversary automated information systems or networks."[16] CNAs are an entirely different beast. They refer to

> a category of fires employed for offensive purposes in which actions are taken through the use of computer networks to disrupt, deny, degrade, manipulate, or destroy information resident in the target information system or computer networks, or the systems/networks themselves. The ultimate intended effect is not necessarily on the targeted system itself, but may support a larger effort, such as information operations or counterterrorism, e.g., altering or spoofing specific communications or gaining or denying access to adversary communications or logistics channels.[17]

Thus, CNE operations are akin to espionage; they serve an intelligence function. CNAs more closely resemble sabotage; they aim to destroy, manipulate, or misdirect an adversary's data, computers, or network systems, often in conjunction with kinetic operations.

Although useful, the distinction between CNAs and CNE does not fully capture some of the most relevant distinctions among various types of offensive cyber operations. The strict focus on the intrusion's end goals leaves room for significant variation within each of the two

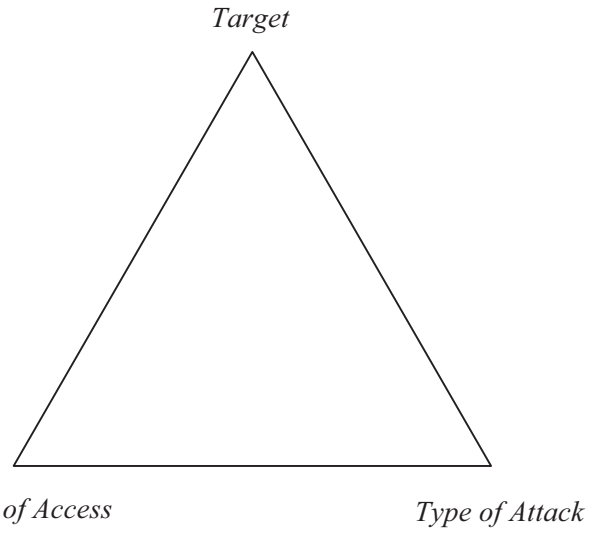

Figure 13.1. Cyber Effects Model

camps. An alternative way to understand the nature and scope of offensive cyber operations is the model displayed in figure 13.1. The model presents a clear way of categorizing offensive cyber operations, disaggregating them by target, the type of access used to conduct the operation, and the type of attack. We discuss each of these in turn.

TARGET

The first question to ask of any cyber operation is who, or what, is the intended target? Whether the target is a government network or a large bank may provide important clues about the type of perpetrator as well as their motivations. Even without knowing who exfiltrated data on millions of US federal employees from the Office of Personnel and Management (it was China), there would still be good reason to believe that this was the work of a nation-state. Who else would have both the resources and the incentives to pull off such a feat? Conversely, it may be reasonable to posit that operations targeting financial institutions are perpetrated by criminal groups seeking monetary gain. That said, North Korea's recent efforts to steal money from global financial institutions, including in Poland and Bangladesh, blur these lines.[18]

The most effective offensive cyber operations are closely tailored operations. For complex systems, months, perhaps years, of research, planning, defense probing, and preparation may be necessary. As Thomas Rid notes, for any perpetrator interested in carrying out an attack, "vulnerabilities have to be identified before they can be exploited; complex industrial systems need to be understood first; and a sophisticated attack vehicle may be so fine-tuned to one specific target configuration that a generic use may be difficult or impossible (consider a highly sophisticated rocket that can only be fired against one single target and at nothing else, even if some of its components may be reused)."[19] While unsophisticated, low-cost cyberattacks (e.g., distributed denial of service [DDoS]) can be rather generic and applied with little regard

to the target, their payoff is equally low. Conversely, cyber operations yielding the greatest rewards must be highly calibrated to their specific adversary and the particular task at hand.

As an example, infiltrating an enemy's air-defense system—a high-risk, high-reward operation—would first require a deep understanding of the network on which it operates, including any relevant vulnerabilities. Whether systems are new or old and whether they are connected to the Internet are all relevant pieces of information. Consider the different challenges that might arise during an operation against a superpower like the United States as opposed to a weaker, less advanced country like North Korea. "One of North Korea's biggest advantages is that it has hardly any Internet-connected infrastructure to target. . . . On the other hand, the US has tons of vulnerabilities a country like North Korea could exploit."[20] North Korea's dated, esoteric technology means that exploits need to be carefully tailored to its specific computing environment, which would likely require a meaningful intelligence-gathering operation and perhaps even physical access to its antiquated systems. This is not to say that targeting American systems would be easy but rather that the characteristics of a target's networks and systems, including how up to date they are, can dramatically affect the conduct and character of cyber operations.

TYPE OF ACCESS

Most cyber operations rely on flaws or vulnerabilities in an adversary's software, hardware, or both. According to the Internet Corporation for Assigned Names and Numbers (ICANN), the nonprofit organization that regulates Internet domains, a vulnerability is "a flaw in the measures you take to secure an asset. . . . They exist in operating systems, applications or hardware you use."[21] Vulnerabilities come in many forms. They may become relevant when users fail to update their software, since doing so may fix known "bugs" that adversaries can otherwise exploit. While much vulnerability arises from errors or oversights in software creation, they commonly stem from human error as well.

Software vulnerabilities that are unknown to developers and users are especially valuable. These are popularly known as "zero-days," referring to the fact that developers have known about the vulnerability for zero days—in other words, no time at all.[22] Zero-days are highly sought-after goods. Because the unwitting victims are entirely unaware of their existence, actors with malicious intent can easily exploit them for personal gain. Owing to their value, it should come as no surprise that there is a black market for them. Governments have also been known to stockpile zero-days for future use, identifying them on their own or buying them from cybersecurity researchers. The Stuxnet worm, for instance, utilized four separate zero-days.[23] There is often good reason for saving zero-days and not immediately burning them. Most notably, they can be used only once. After an intrusion with a zero-day, developers and system administrators will almost certainly patch the weakness in short order, rendering it unusable. But there are also downsides to waiting too long to use one. The previously unknown vulnerability may be discovered and subsequently patched, rendering the exploit useless.

There are other ways for actors to gain unauthorized entry into a network beyond hardware and software vulnerabilities. Humans—individual users—are commonly exploited through "social engineering" operations. Perhaps most common are spear-phishing attacks: operations intended to trick an individual into giving up their usernames and passwords, providing entry into a system without exploiting any software vulnerability whatsoever.[24]

For example, it has come to light that Russian hackers used spear-phishing techniques to access the email accounts of John Podesta and other Democratic National Committee staff members during the 2016 presidential election.[25] Intruders can also try to access a system through baiting operations, which includes doling out USB drives, CDs, or other removable media infected with malware (malicious software) in the vicinity of an organization they are interested in exploiting with the hopes that someone will insert the media into a computer. In doing so, the unsuspecting user may inadvertently install malware. While seemingly unsophisticated, most researchers believe that this is how the Stuxnet worm made its way into Iran's nuclear facilities.[26] "People, rather than technology, remain the weakest link in computer security."[27]

A final method of gaining access into an adversary's systems involves exploiting vulnerabilities that are intentionally created. Often called "backdoors," these vulnerabilities are baked into hardware and software. Benevolently, backdoors are added to give network administrators or technical support teams future access. Malevolently, however, states may pressure companies to create backdoors for their own use or insert them on their own using covert methods. This prospect generates a nontrivial fear, especially for governments, that certain products contain imperceptible backdoors that might grant unwanted access to foreign rivals. According to the *New York Times*, "American officials have long considered Huawei, the Chinese telecommunications giant, a security threat, blocking it from business deals in the United States for fear that the company would create 'back doors' in its equipment that could allow the Chinese military or Beijing-backed hackers to steal corporate and government secrets."[28] Regardless of how they got there, unsecured backdoors can provide an adversary with remote access and even control over a given network.

TYPE OF ATTACK

Although the field is constantly evolving, several types of cyberattacks are here to stay, including viruses, worms, trojans, and DDoS operations.[29] Viruses, worms, and trojans are all forms of malware that start working when they are installed onto the victim's systems. "A virus is a piece of code that, when run, will attach itself to other programs, which will again run when those programs are run."[30] A worm is "a program that propagates itself by attacking other machines and copying itself to them."[31] Viruses therefore become active only when its host is activated, whereas worms function and propagate on their own.[32] To briefly illustrate the difference, Stuxnet is considered a worm because once it found its way onto machines in the Natanz nuclear reactor, it activated and spread irrespective of user actions.[33] The Flame Virus, which shares code with Stuxnet, is a virus rather than a worm since it is activated when users launch Microsoft Word. As the *Washington Post* notes, "the code could activate computer microphones and cameras, log keyboard strokes, take screen shots, extract geolocation data from images, and send and receive commands and data through Bluetooth wireless technology. Flame was designed to do all this while masquerading as a routine Microsoft software update."[34]

A trojan is distinct from a worm or a virus. It is "a program that adds subversive functionality to an existing program."[35] In other words, it is malware disguised as harmless software. Once in place, it can install a backdoor—enabling outside access to one's network—or perform other malevolent actions such as broadcasting the user's data.

Other cyberattacks rely on relatively "brute-force" methods to overwhelm their targets, which is the case with DDoS attacks or "exploit[s] whose purpose is to deny somebody the

use of the service: namely to crash or hang a program or the entire system."[36] DDoS attacks work by coordinating bots—malware-infected, Internet-connected machines, often called "zombies"—that are "simultaneously and continuously sending a large amount of traffic and/or service requests to the target system. The target system either responds so slowly as to be unusable or crashes completely."[37] Flooding receivers or servers is nothing new, and such actions also have uses beyond simply denying access. When Israel conducted the Operation Orchard bombing raid against a Syrian nuclear reactor in 2007, it utilized the Suter network-attack system to essentially blind Syria's air defenses. "The technology allows users to invade communications networks, see what enemy sensors see and even take over as systems administrator so sensors can be manipulated into positions where approaching aircraft can't be seen, they say. The process involves locating enemy emitters with great precision and then directing data streams into them that can include false targets and misleading messages that allow a number of activities including control."[38]

Defense in Cyberspace

Defending against cyberattacks is a bit like defending against terrorism. As Erik Gartzke and Jonathan Lindsay put it, "cyber defense must succeed everywhere and every time, many argue, but attackers need only succeed once to compromise a system."[39] Even still, there are a range of steps—both small and large, simple and complex—that states and other actors alike can take to reduce their vulnerability to cyberattacks and unauthorized intrusions.

The DoD defines cyber defense as "the integrated application of DoD or US Government cyberspace capabilities and processes to synchronize in real-time the ability to detect, analyze and mitigate threats and vulnerabilities, and outmaneuver adversaries, in order to defend designated networks, protect critical missions, and enable US freedom of action."[40] One useful distinction is between preventive and deceptive cyber defenses.[41] Preventive methods aim to identify, forestall, and halt intrusions. Deceptive defensive methods are more interactive, operating in real time during an attack to trick, misdirect, and reveal the identity of intruders. Here one of the primary goals is to remove the cloak of anonymity and unmask the intruder, allowing for the possibility of retaliatory action.

Prevention

Some of the most common defensive methods include firewalls, antivirus software, intrusion-detection software, air gapping, and vulnerability detection. Among these, firewalls may be considered the workhorse of cyber defense. Nearly ubiquitous, a firewall is "a device or collection of devices which separates its occupants from potentially dangerous external environments (e.g., the Internet)."[42] Firewalls thus attempt to keep out unauthorized users while letting authorized traffic pass through. This is often the first line of network defense. Antivirus software is also incredibly common, scanning computers and networks for evidence of malicious programs. Antivirus software examines patterns of activity and compares it to known signatures and activities of malware. Since the efficacy of antivirus software is directly tied to its ability to identify *known* malware, it is critical to regularly update the software so that it has the latest information.[43] As a Defense Science Board task force notes, most "successful attacks reaching DoD networks today result from a personnel failure or out-of-date software in firewalls and detection systems."[44] Intrusion-detection systems, similar to antivirus software,

gather and analyze "information from various areas within a computer or a network to identify possible security breaches. In other words, intrusion detection is the act of detecting actions that attempt to compromise the confidentiality, integrity or availability of a system/network."[45] These systems tend to look for anomalies in ingoing and outgoing network traffic, rather than for specific pieces of malware.

Unlike the others, air gapping is a physical, and in many ways simpler, method of cyber defense. Air gapping refers to a system "in which there is no networking connection between the inner network and the external world."[46] By removing a network's external Internet connection, defenders hope to make it harder for unauthorized users to gain entry. Yet even this is not foolproof. USB drives and other removable media can still be used to transport malicious programs onto an air-gapped network, as was the case with Stuxnet. Nevertheless, the fact that compromising air-gapped networks requires another human to physically insert something into a system reduces the chances of an unwanted breach.

Finally, vulnerability detection and bug finding are attempts to uncover weaknesses preemptively before they can be exploited. Bugs are often found by individuals tasked with trying to break into a network in the service of greater security. One report finds that "the vast majority of publicly disclosed vulnerabilities are still found by fuzzing or manual auditing."[47] While organizations can do this internally, they often hire outsiders or pay individuals for reporting bugs through so-called bug bounty programs.

Deception

Network defenses relying on deception typically start working once an intruder has entered a system—in other words, when prevention has failed. "Defensive deception," as it is often called, "promises to delay significantly the intruder's exploitation of appropriated data, to burden opponents with false leads and sorting costs, and even to harm an attacker's technical infrastructure."[48] These methods have grown increasingly common in large part because the threat landscape is constantly evolving, making it difficult to thwart every intrusion from the start.

"Honeypots" are a good example of deceptive techniques. Honeypots are fake file folders, or destinations—which may appear particularly valuable—that system administrators can monitor for activity. Since they are fake, any activity with a honeypot is suggestive of anomalous behavior and perhaps an unauthorized intrusion. Files in the honeypot—called "honeytokens"—can also be designed to track the intruder upon exfiltration, helping administrators locate and identify the responsible party. Actors can also utilize honeypots to hide information that is in fact highly sensitive. These "'fake honeypots' . . . try to look like an obvious honeypot in order to scare attackers away."[49] Other forms of deception, including "tarpits," "honeynets," and "honeyclients," have similar goals.[50] This game of cunning, deception, and luck in many ways typifies the broader competition between offense and defense in cyberspace.

The most effective cyber defenses integrate both preventive and deceptive elements. This is because "achieving security cannot be done with single, silver-bullet solutions; instead, good security involves a collection of mechanisms that work together to balance the cost of securing our systems with the possible damage caused by security compromises, and drive the success rate of attackers to the lowest possible level."[51] Effective defensive strategies will therefore take steps to minimize the effect of inevitable, successful intrusions.

OFFENSE OR DEFENSE: WHICH IS EASIER?

At this point in the chapter, it may be useful to briefly comment on an issue that we have so far ignored: Is offense or defense easier? More formally, is cyberspace an offense- or defense-dominant domain? Deputy Secretary of Defense William Lynn argues for the former: "In cyberspace, the offense has the upper hand."[52] Similarly, Joseph Nye writes that "because the Internet was designed for ease of use rather than security, the offense currently has the advantage over the defense."[53] With an eye toward the future, Rid casts some doubt on the view that cyberspace is offense-dominant, writing that "the level of sophistication required to find an opportunity and to stage a successful cyber sabotage operation is rising. The better the protective and defensive setup of complex systems, the more sophistication, the more resources, the more skills, the more specificity in design, and the more organization is required from the attacker."[54] In short, cyberspace may be offense-dominant when it comes to unsophisticated, low-cost offensive operations but (becoming) defense-dominant when it comes to complex attacks that are most threatening. While this is beyond the scope of what we are after in this chapter, this debate will continue to rage on for the foreseeable future.

CONCLUSIONS

Notwithstanding the explosion of articles and commentary on the issue of cybersecurity in recent years, research and strategy in this domain is still very much in its infancy. While it is easy, and maybe even politically expedient, to argue that the cyber domain is entirely novel, it is noteworthy that similar arguments were being made in the 1950s and 1960s about nuclear weapons. Revisiting these and other debates can thus be extremely useful, shedding light on how new and rapidly evolving technologies can be effectively utilized and incorporated into America's strategic doctrine.

From a technical perspective, offensive and defensive tools are constantly being developed, raising the costs of complacency. With regard to the back-and-forth between terrorists and counterterrorism forces, Paul Wilkinson and Brian Jenkins write that "the history of attacks on aviation is the chronicle of a cat-and mouse game, where the cat is blocking old holes and the mouse always succeeds in finding new ones."[55] The same is true of cyberspace. Thus, vigilance, innovation, and layered defenses that can guard against surprise offensives are critical. The rapidity with which cyberspace evolves renders this a challenging but important task.

From a strategic perspective, policymakers and practitioners are still grappling with how cyber operations fit into the existing tool kit of both traditional and nontraditional options. Are cyber tools best suited for intelligence operations, used to eavesdrop on unsuspecting adversaries? Can they be used on their own to accomplish strategic objectives such as deterrence and compellence? Or are they most effective when they support kinetic operations? As US Air Force chief of staff Gen. David L. Goldfein recently noted, "So, the question for us is, does our development plan today ensure that throughout the continuum of learning, we are properly exposed to the operational art of how we bring air, space and cyber capabilities together and then knit them together with land and maritime capabilities and then pull them together with other elements of power—diplomatic, economic information—to be able to provide campaign design to the President so the President has options."[56]

Although answers to these and other questions are uncertain, recent comments suggest that policymakers are thinking hard about how to leverage their cyber arsenal in new ways.

During a business conference in 2016, the executive director of US Cyber Command, Shawn Turskey, revealed a plan to make cyber weapons readily attributable. According to Turskey, "in the intelligence community you never want to be caught, you want be low and slow, you never really want to be attributed. There's a different paradigm from where you are at in the intelligence community . . . But there's another space over here, where maybe you definitely want to be louder, where attribution is important to you and you actually want the adversary to know."[57] Rather than seeking to understand how the US government can work with cyber capabilities, it is perhaps more fruitful to imagine how cyber capabilities can instead be made to work for the US government.

When it comes specifically to offense and defense in cyberspace, there are several areas of ongoing debate. First, as alluded to above, there is growing uncertainty over the assumption that cyberspace operations will be dominated by anonymity. Actors can, and often do, claim credit for their attacks. Yet the assumption of perpetual anonymity in cyberspace is often cited as the main reason why they cannot be used to coerce an adversary. With the military seeking out "loud," attributable cyber options, this entire dynamic may be changing. Understanding the costs and benefits of credit-claiming in cyberspace, and what voluntary attribution can and cannot accomplish, is an important question for the future.

Second, there is no universal strategy for employing cyber weapons. Notably, different actors leverage cyber operations for very different goals, and they use them in very different ways as well. Nonstate actors often claim their cyberattacks to spread political messages. China has so far used its cyber capabilities to steal information and industrial secrets. North Korea has employed "cyber blackmail" in an attempt to prevent the release of a Sony film. And the United States and Israel leveraged their cyber capabilities to delay the construction of an Iranian nuclear weapon. Cyber weapons are indeed malleable tools that can be leveraged to accomplish a wide variety of operational and strategic goals. Understanding why actors are likely to pursue certain goals in cyberspace requires being sensitive to this heterogeneity.

Finally, the cyber sphere is in many respects a democratizing domain, both in terms of who can launch attacks and who can be targeted. Cyber defense is not merely a concern of states, but it is also an issue for businesses, nongovernmental organizations, and individuals alike. Cybercrime is estimated to cost the average American company $15 million per year, with the average breach costing nearly $6.3 million.[58] While this may seem trivial in terms of the overall threat it poses to states, it is worth bearing in mind that the US power grid is largely privately owned, and a coordinated cyberattack could wreak havoc on American commerce.[59] Recent cyberattacks against Ukraine's electrical grid, for instance, have caused hundreds of thousands to lose power, and it is not hard to imagine how such an operation could be used in conjunction with, or as the precursor to, a kinetic operation much closer to home.[60]

LEARNING REVIEW:

- What are the three elements of the Cyber Effects Model?
- Describe the differences between offensive and defensive cyber capabilities
- What are the operational advantages and disadvantages of cyberpower?

NOTES

1. Department of Defense, *The DoD Cyber Strategy*, 2015, 4, https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.

2. Jim Garamone and Lisa Ferdinando, "DoD Initiates Process to Elevate U.S. Cyber Command to Unified Combatant Command," Defense News, August, 2017, https://www.defense.gov/News/Article/Article/1283326/dod-initiates-process-to-elevate-us-cyber-command-to-unified-combatant-command/.

3. Department of Defense, *DoD Cyber Strategy*, 4.

4. Paul Szoldra, "This Top Military Officer Perfectly Captured the Strange Nature of Cyber Warfare in One Sentence," *Business Insider*, February 2017, http://www.businessinsider.com/admiral-unique-nature-cyber-warfare-2017-2.

5. Martin C. Libicki, "Cyberspace Is Not a Warfighting Domain," *I/S: Journal of Law and Policy for the Information Society* 8, no. 1 (2012): 324.

6. Jon R. Lindsay, "Tipping the Scales: The Attribution Problem and the Feasibility of Deterrence against Cyberattack," *Journal of Cybersecurity* 1, no. 1 (2015): 53–67.

7. Richard Clarke, "War from Cyberspace," *National Interest* (November/December 2009): 31–36.

8. James R. Clapper, "Worldwide Threat Assessment to the House Permanent Select Committee on Intelligence," Office of the Director of National Intelligence, February 2, 2012, https://www.dni.gov/files/documents/Newsroom/Testimonies/20120202_HPSCI%20WWTA%20-%20Oral%20Remarks%20as%20delivered.pdf.

9. Austin Carson, "Facing Off and Saving Face: Covert Intervention and Escalation Management in the Korean War," *International Organization* 70, no. 1 (2016): 103–31; Michael F. Joseph and Michael Poznansky, "Media Technology, Covert Action, and the Politics of Exposure," *Journal of Peace Research* (OnlineFirst, November 2016): 1–16.

10. Thomas Rid and Ben Buchanan, "Attributing Cyber Attacks," *Journal of Strategic Studies* 38, nos. 1–2 (2015): 1–2, 4–37.

11. Joseph S. Nye, "Deterrence and Dissuasion in Cyberspace," *International Security* 41, no. 3 (2017): 44–71.

12. Lindsay, "Tipping the Scales," 54.

13. Dave Aitel and Skylar Rampersaud, "Some People Want a Time Limit on the NSA's 'Zero-Day' Exploits—Here's Why That's a Terrible Idea," *Business Insider*, July 22, 2014, http://www.businessinsider.com/why-a-time-limit-on-zero-days-is-a-bad-idea-2014-7.

14. James D. Fearon, "Rationalist Explanations for War," *International Organization* 49, no. 3 (2015): 379–414.

15. For an excellent summary of offense and defense in cyberspace, including the dynamics of network intrusions and network defense, see Ben Buchanan, *The Cybersecurity Dilemma* (Oxford: Oxford University Press, 2016).

16. Gen. James E. Cartwright, "Joint Terminology for Cyberspace Operations," memorandum, Office of the Vice Chairman of the Joint Chiefs of Staff, November, http://www.nsci-va.org/CyberReferenceLib/2010-11-joint%20Terminology%20for%20Cyberspace%20Operations.pdf.

17. Ibid., 3.

18. Paul Mozur and Choe Sang-hun, "North Korea's Rising Ambition Seen in Bid to Breach Global Banks," *New York Times*, March 25, 2017, https://www.nytimes.com/2017/03/25/technology/north-korea-hackers-global-banks.html?_r=0.

19. Thomas Rid, "Cyber War Will Not Take Place," *Journal of Strategic Studies* 35, no. 1 (2012): 5–32.

20. Mark Clayton, "The New Cyber Arms Race," *Christian Science Monitor*, March 7, 2011, https://www.csmonitor.com/USA/Military/2011/0307/The-new-cyber-arms-race.

21. Internet Corporation for Assigned Names and Numbers, "Threats, Vulnerabilities and Exploits—Oh My!," ICANN (blog), August 10, 2015, https://www.icann.org/news/blog/threats-vulnerabilities-and-exploits-oh-my.

22. Kim Zetter, "Hacker Lexicon: What Is a Zero Day?," *Wired*, November 11, 2014, https://www.wired.com/2014/11/what-is-a-zero-day/.

23. Lindsay, "Tipping the Scales," 53.

24. "Spear Phishers: Angling to Steal Your Financial Info," Federal Bureau of Investigation, April 1, 2009, https://archives.fbi.gov/archives/news/stories/2009/april/spearphishing_040109.

25. Sean Gallagher, "Russia-Linked Phishing Campaign behind DNC Breach Also Hit Podesta, Powell," ARS Technica, October 20, 2016, https://arstechnica.com/information-technology/2016/10/russia-linked-phishing-campaign-behind-the-dnc-breach-also-hit-podesta-powell/.

26. Lindsay, "Tipping the Scales," 53–67.

27. Rebecca Slayton, "What Is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment," *International Security* 41, no. 3 (2017): 72–109.

28. David E. Sanger and Nicole Perlroth, "N.S.A. Breached Chinese Servers Seen as Security Threat," *New York Times*, March 22, 2014, https://www.nytimes.com/2014/03/23/world/asia/nsa-breached-chinese-servers-seen-as-spy-peril.html.

29. For a more extended, technical discussion, see Simon Hansman and Ray Hunt, "A Taxonomy of Network and Computer Attacks," *Computers and Security* 24, no. 1 (2005): 31–43.

30. Maria Kjaerland, "A Taxonomy and Comparison of Computer Security Incidents from the Commercial and Government Sectors," *Computers and Security* 25, no. 7 (2006), 522–38.

31. Ibid., 526.

32. "Interactive: Tracking Syria's Defections," Al Jazeera, July 30, 2012, http://www.aljazeera.com/indepth/interactive/syriadefections/2012730840348158.html.

33. For a case study of Stuxnet, see Jon R. Lindsay, "Stuxnet and the Limits of Cyber Warfare," *Security Studies* 22, no. 3 (2013): 365–404.

34. Ellen Nakashima, Greg Miller, and Julie Tate, "U.S., Israel Developed Flame Computer Virus to Slow Iranian Nuclear Efforts, Officials Say," *Washington Post*, June 19, 2012, https://www.washingtonpost.com/world/national-security/us-israel-developed-computer-virus-to-slow-iranian-nuclear-efforts-officials-say/2012/06/19/gJQA6xBPoV_story.html?utm_term=.3706cea29c7d.

35. Kjaerland, "Taxonomy and Comparison," 526.

36. Ibid.

37. S. T. Zargar, J. Joshi, and D. Tipper, "A Survey of Defense Mechanisms against Distributed Denial of Service (DDoS) Flooding Attacks," *IEEE Communications Surveys and Tutorials* 15, no. 4 (2013): 2046.

38. Ward Carrol, "A Closer Look at Israel's Syria Raid," Military.com, October 8, 2007, https://www.military.com/defensetech/2007/10/08/a-closer-look-at-israels-syria-raid.

39. Erik Gartzke and Jon R. Lindsay, "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace," *Security Studies* 24, no. 2 (2015): 322.

40. Cartwright, "Joint Terminology for Cyberspace Operations."

41. Sometimes called denial and deception—e.g., in Shushil Jajodia, V. S. Subrahmanian, Vipin Swarup, and Cliff Wang, eds. *Cyber Deception: Building the Scientific Foundation* (Cham, Switzerland: Springer International, 2016).

42. Kenneth Ingham and Stephanie Forrest, "A History and Survey of Network Firewalls," University of New Mexico tech report no. 37, https://www.cs.unm.edu/~treport/tr/02-12/firewall.pdf.

43. "What Is a Computer Virus or a Computer Worm?," Kaspersky Lab, https://usa.kaspersky.com/resource-center/threats/computer-viruses-vs-worms.

44. Slayton, "Cyber Offense-Defense Balance," 341.

45. Animesh Patcha and Jung-Min Park, "An Overview of Anomaly Detection Techniques: Existing Solutions and Latest Technological Trends," *Computer Networks* 51, no. 12 (2007): 3448–70.

46. Mordechai Guri, Gabi Kedma, Assaf Kachlon, and Yuval Elovici, "AirHopper: Bridging the Air-Gap between Isolated Networks and Mobile Phones Using Radio Frequencies," paper presented at the Ninth International Conference on Malicious and Unwanted Software: The Americas (MALWARE), Fajardo, Puerto Rico, October 28–30, 2014, 58–67.

47. Sean Heelan, "Vulnerability Detection Systems: Think Cyborg, Not Robot," report for the IEEE Computer and Reliability Societies, May/June 2011, https://www.computer.org/cms/ComputingNow/homepage/2011/0811/W_SP_VulnerabilityDetectionSystems.pdf.

48. Gartzke and Lindsay, "Weaving Tangled Webs," 343.

49. Ibid., 340.

50. Kristin E. Heckman, Michael J. Walsh, Frank J. Stech, Todd A. O'Boyle, Stephen R. DiCato, and Audra F. Herber, "Active Cyber Defense with Denial and Deception: A Cyber-Wargame Experiment," *Computers and Security* no. 37 (2013): 72–77.

51. Jajodia et al., *Cyber Deception*, 28.

52. Slayton, "Cyber Offense-Defense Balance," 72.

53. Joseph S. Nye, *Cyber Power*, Belfer Center for Science and International Affairs, 5, http://www.belfercenter.org/sites/default/files/files/publication/cyber-power.pdf.

54. Rid, "Cyber War Will Not Take Place," 28.

55. Paul Wilkinson and Brian Jenkins, eds., *Aviation Terrorism and Security* (London: Frank Cass Publishers, 2013), 24.

56. "Remarks by General David L. Goldfein, U.S. Air Force Chief of Staff," September 19, 2017, Air, Space & Cyber Symposium, Air Force Association, http://www.af.mil/Portals/1/documents/csaf/CSAF_AFA_2017%20Air_Space_and_Cyber_Symposium.pdf.

57. Chris Bing, "U.S. Cyber Command Director: We Want 'Loud,' Offensive Cyber Tools," FedScoop, August 30, 2016, https://www.fedscoop.com/us-cyber-command-offensive-cybersecurity-nsa-august-2016/ (emphasis added).

58. James Griffiths, "Cybercrime Costs the Average U.S. Firm $15 Million a Year," CNN Tech, October 8, 2015, http://money.cnn.com/2015/10/08/technology/cybercrime-cost-business/index.html.

59. "Quadrennial Energy Review: First Installment," Department of Energy, Office of Policy, https://energy.gov/epsa/quadrennial-energy-review-first-installment.

60. Dan Goodin, "Hackers Trigger Yet Another Power Outage in Ukraine," ARS Technica, January 11, 2017, https://arstechnica.com/information-technology/2017/01/the-new-normal-yet-another-hacker-caused-power-outage-hits-ukraine/.

This page intentionally left blank