1

Cyber Proxies: An Introduction

How societies organize force has intrigued people for centuries. The rise and legitimacy of the modern state itself is tied to the control over coercive capabilities, including those wielded by proxies.[1] As Harvard University professor Joseph Nye reminded an audience in November 2012, "Max Weber did not define the state as having 'the monopoly over the use of force' but 'the monopoly over the *legitimate* use of force.'"[2] This is an important distinction. On paper, the state has become tied to this monopoly, but very few have effectively possessed it. The sociologist Michael Mann even argues that "many have not even claimed it."[3] In other words, the idea of a monopoly over the legitimate use of force is very much linked to the European experience of the emergence of the nation-state and the Westphalian notion of sovereignty that became codified globally after World War II through the Charter of the United Nations (UN). Many countries outside this specific cultural and historical context are better described as brokers than as (aspirational) monopolists.[4] Meanwhile, the nature of the nation-state itself keeps evolving towards what's been called a market-state with increasing and systemic privatization.[5]

Fast forward to the twenty-first century and the new phenomenon of cyberspace. An analysis of how this technology is used to project coercive power and by whom must take Mann's observations into account, especially if the goal is to study this question at a global level. Comparing the proxy relationships in existing cyber powers such as China, Iran, Russia, and the United Sates requires a broader view of the state; it also requires us to revisit distinctions between private and public spheres that are blurred in countries where prebendalism reigns or where communist state structures and the party are still all-pervasive.[6] It also requires contending with Weber's explicit reference to "the legitimate use of *physical* force."[7] While offensive cyber operations can cause physical effects, so far hacking used for political or military purposes has primarily had nonphysical effects. Nonetheless, much of the debate over whether cyber war will take place is focused on the question of force and the likelihood of more than a thousand people dying within a year.[8] At best, this narrow focus ignores the full spectrum of political effects hacking has been used for, as the events in Ukraine and the malicious hacks during the 2016 US elections make

clear. At worst, it contributes to a mirror-imaging problem and tunnel vision that prevent a full appreciation of how other countries think about and use these capabilities – with all this implies for crisis prevention, escalatory dynamics, and signaling.

Another important observation to make at the start is that states wanting to project power through cyberspace find themselves in often complex and dynamic relationships with non-state actors. This chapter will therefore explore what non-state actors can be capable of and how they are likely to be used to project cyber power. It will discuss the pool of potential cyber proxies, the case selection for this book, and the attribution problem, and conclude by highlighting the bigger picture.

For the first time, non-state actors can have global reach through hacking, known in the US military bureaucracy's vernacular as "remote offensive cyber operations." Non-state actors can target a third party beyond a state's border with unprecedented ease and at a very low cost compared to conventional weaponry. And the effects can be significant. For example, in February 2016, hackers with alleged ties to North Korea attempted to steal nearly USD 1 billion from the Bangladeshi central bank.[9] If they had fully succeeded, the theft would have amounted to 0.58 percent of Bangladesh's GDP.[10] Attacks on this scale are not unprecedented. In 2015, a single group of cybercriminals stole USD 1 billion from financial institutions worldwide over a period of two years.[11] Moreover, it is clear today that malicious hackers could kill people.[12] Thankfully, not every theoretical possibility becomes reality, but incidents like these demonstrate that it is important to pay attention to these actors, especially when they have relationships with states who might want to use their capabilities and turn theory into practice.

While the Internet was initially a military project to provide a resilient communications network, it is perhaps unique in that the military left its development largely to a few geeks at universities. The military's lack of interest changed when the technology re-emerged out of the obscurity of academic institutions, became commercialized in the mid-1990s, and started to spread around the globe like wildfire. States discovered the Internet's potential not only as a resilient communications network and source for intelligence but also as a platform to project coercive power with an exponentially growing range. Even then, only a handful of states grasped its revolutionary potential and set up structures to take advantage of what would later be declared a new operational domain.[13] Only in 2010, with the front-page public revelations about the Stuxnet malware (reportedly designed by the United States and Israel) damaging centrifuges at the Natanz nuclear enrichment facility in Iran, did most states become aware of the technology's political and military dimension and decide to follow others in its exploitation.

For these reasons, most of the Internet's infrastructure as a global network evolved in private hands, and many of the earliest examples of malicious use are tied to non-state rather than state actors. For example, the first computer emergency response team was established in response to the Morris worm, malware developed by

a graduate student, not the malicious activity of a state. The history of cyber conflict itself arguably began with a proxy actor. According to Jason Healey, who edited a book on the topic, the history of cyber conflict "started in earnest in 1986, when German hackers searched through thousands of US computer files and sold their stolen materials to the KGB [the Soviet security agency]."[14] In other words, from the start non-state actors developed offensive cyber capabilities of interest to states and used by states to further the latter's political objectives. And with the dawn of the modern Internet, the pool of non-state actors with such capabilities has been steadily increasing. That is why Alexander Klimburg, director of the Global Commission on the Stability of Cyberspace, has argued that "[t]o create an integrated national capability in cyber power, the non-state sector must be induced to cooperate with government."[15]

Several normative issues cannot be ignored when discussing cyber proxies. Efforts encouraging states to pursue a monopoly over the legitimate use of force, for example, have an obvious normative undercurrent. In a democratic society, the people are sovereign; for effective accountability in a representative system, the state must retain tight control over its agents. Oversight mechanisms and policies defining what are and are not inherently governmental functions ensure such control. Obviously not all states are democracies. But there is a second normative undercurrent that emanates not from a state's political system but from the regime the international community has built to regulate the use of proxies. As far back as the sixteenth century, Niccolò Machiavelli argued that "[m]ercenaries and auxiliaries are at once useless and dangerous, and he who holds his State by means of mercenary troops can never be solidly or securely seated."[16] From his disdain for mercenaries to the nineteenth-century ban on privateering, the international community has clearly expressed a normative view that restricts the use of proxies.

Two of the modern landmark documents providing insight into how the international community thinks about the rules of the road for cyberspace explicitly discourage the use of "proxies." These are the reports by two groups of governmental experts that met under the auspices of the UN. In 2013, a UN Group of Governmental Experts (UNGGE) from fifteen UN member states, including the United States, China, Russia, the UK, France, and India, agreed in a consensus report that "[s]tates must not use proxies to commit internationally wrongful acts."[17] Two years later, a follow-up UNGGE report specified that "[s]tates must not use proxies to commit internationally wrongful acts using ICTs [information and communications technologies], and should seek to ensure that their territory is not used by non-State actors to commit such acts."[18] The new UNGGE group consisted of twenty member states, including the five permanent members of the UN Security Council as well as Brazil, Israel, and Pakistan. Part of the group's rationale was that proxies present new escalatory risks to international peace and security.

The term *proxy* is often limited to non-state actors with comparatively loose ties to governments. However, statements by Chinese and Iranian officials and scholars

suggest that they view certain companies and other non-governmental actors as tightly tied to Western governments. This points to the related challenge of distinguishing between private and public. Discussing the meaning of terms such as "mercenaries," "public," "private," "privatization," and "other slippery terms," the international relations scholar Deborah Avant observed that "all of this refers to the world of advanced, industrialized countries where the state, government, and public revolve around some notion of collective good. In parts of the developing world, state institutions and international recognition of them function mainly as mechanisms for rulers to achieve personal (private) gain."[19] This partly explains why distinguishing between political and economic espionage, as in discussions between the United States and China, has been particularly challenging.

Finally, cyber proxies are entangled in the broader normative questions around the definition of information security and cybersecurity; some states like Russia and China consider content an information security threat whereas others, including the United States, consider content and the free flow of information a human right. The latter states exclude content from their definitions and, to highlight this distinction, use the term *cybersecurity*, whereas other states frame their scope of concern as *information security*. Organizational theory and the literature on power are particularly useful analytical lenses that allow us to avoid being drawn into such normative debates.

PROXIES AND CYBER POWER

Some scholars have argued that cyberspace merits being considered its own sphere of power, much as the term "air power" emerged once mankind started exploring the skies. William "Billy" Mitchell, who was a driving force behind the establishment of the US Air Force, considered air power to be "the ability to do something in the air" while two professors at the US Naval Academy defined "sea power" shortly after World War I as "a nation's ability to enforce its will upon the sea."[20] Nye in turn defines *cyber power* as "the ability to obtain preferred outcomes through use of the electronically interconnected information resources of the cyber domain. Cyber power can be used to produce preferred outcomes *within* cyberspace, or it can use cyber instruments to produce preferred outcomes in other domains *outside* cyberspace."[21] Power is broader than just force, as Nye reminded us with his famous distinction between soft and hard power. In fact, in his discussion of cyber power, Nye also mentions circumvention technologies (technologies designed to circumvent government censorship and surveillance) and the Internet Freedom grant-making program by the US Department of State.[22] Cyber power therefore covers a wide range of effects influencing the targeted actor – including but not limited to coercion.

Proxies are used for the projection of power. Cyberspace has become a field for this general exercise of power due to three interconnected but analytically separate

trends. First, more and more machines – including cars and control systems in industry – are changing from closed manual and mechanical systems to interoperable digital systems. Second, more and more of these digital devices are connecting to the Internet. And third, ever greater numbers of people are gaining access to the Internet and these devices every day. All three trends expand the network, thereby raising its value, which in turn also increases the incentives for actors to exploit it for their political and military purposes.

The diffusion of reach – the ability to cause effects remotely not only over regional but also global distances – is arguably the most important aspect of cyber power, but it invites the question: what kind of effects can result from it? For example, in the cyber war debate, one of the underlying considerations was whether such a war would result in the deaths of a thousand people in the span of one year, a classic definition in political science.[23] This rather simplistic point quickly gave way to the broader political implications of offensive cyber operations and applications of the political science scholarship[24] discussing the difference between force and violence,[25] political use of force,[26] the power to hurt,[27] and coercive diplomacy.[28] For example, the political scientist K. J. Holsti made the incredibly prescient observation over fifty years ago that "[a]s technological levels rise, other means of inducement become available and can serve as substitutes for force."[29]

The necessary condition for cyber power as used in this book is *unauthorized access*. The notion of consent and authorization is a good baseline for conceptualizing hacking generally.[30] Malicious hacking, or *cracking* as it was once called, can be distinguished from non-malicious hacking in that the former takes place without the consent of the owner or operator of the system whereas the latter takes place with consent. The security researcher, hired to hack the system to identify its vulnerabilities and to subsequently protect it better, receives the authorization to do so.

Given this book's focus on international relations, it is only concerned with offensive cyber actions, which former US military service members Matthew Noyes and Robert Belk[31] term *external cyber operations*: "cyber actions with effects on systems not owned or operated by the actor."[32] Such effects can undermine the confidentiality, integrity, or availability of information.[33] Examples of external cyber action undermining the confidentiality of information include the now frequent data breaches that affect proprietary data of companies from law firms to the natural resources industry, to the hack of the US Office of Personnel Management, which undermined governmental data secrecy; such breaches often also violate individuals' privacy. DDoS attacks, in which targets are flooded with so much data traffic that they become overwhelmed and unavailable, are the most common malicious activity targeting the availability of information or systems. The integrity of information is ultimately the most critical issue. Manipulating the integrity of data is what enables sabotage acts such as Stuxnet and other actions to have potentially severe impacts.

In this book, the definition of cyber proxies is tied to such offensive cyber actions or operations.[34] Offensive cyber operations can be broken down into two components: access and payload. According to Herb Lin, a senior research scholar at Stanford University, "[i]n general, an offensive cyber operation gains access to an adversary's computer system or network and takes advantage of a vulnerability in that system or network to deliver a payload."[35] Malicious hackers can gain physical access or remote access. Remote access can be gained by social engineering, for example by using a fake email (so-called "spear phishing") to trick the user into sharing his or her legitimate credentials with the attacker, or by exploiting a vulnerability in the code. The vulnerability may be unintentional, a bug created due to a programmer's mistake, or it may be intentional – for example a flaw built in deliberately as a backdoor by a government agency. Once a malicious hacker has gained physical or remote access to the target system, the payload determines the hacking's effect and whether the data's confidentiality, integrity, or availability is undermined. The payload's effect can be limited to logical, non-physical observables, or it may have actual physical effects.[36] Proxies can develop, contribute to, and carry out any of the above, although gaining physical access raises the barriers and the cost significantly.

In sum, defining proxy actions as "offensive action" tries to account for the debate about the future of war, whether war necessarily involves physical effects, and the meaning of violence and coercion. Rather than limiting the definition to Weber's "physical force" or "coercion," "offensive action" is meant to include a broader set of activities. It is even possible that a state detecting persistent unauthorized access to part of its critical infrastructure (for example, the electrical grid) could respond by raising its readiness alert condition to the US equivalent of DEFCON 3. This in turn could be misread by other actors and lead to further escalation.

Also, the definition of cyber proxies is deliberately not tied to the effects caused by the offensive actions. While tying the definition to outcomes makes sense in other contexts, such as the discussion about norms or governmental decision-making,[37] it is not particularly helpful for an actor-focused study where the actor's intent and consequently effects of actions might change over time.[38] For example, the Iranian hackers mentioned in the US government's indictments boasted publicly about technically unsophisticated Web defacements made between 2010 and 2012; only three years later, they were trying to gain access to the control system of a dam. In short, the effects of cyber capabilities can evolve quickly compared to most conventional capabilities.

WHAT CYBER PROXIES ARE (THEORETICALLY) CAPABLE OF

An important question is whether non-state actors, and by extension cyber proxies, can wield the same cyber power – and cause similar effects and harm – as states. Some experts, like US Secret Service agent Baranoff, have argued that non-state

actors in fact are more powerful. The answer to the question of which is more dangerous is, it depends. First, states aren't equal. The United States has more sophisticated capabilities than Zimbabwe. Even among members of NATO or the G7, there are significant differences in capabilities. Comparing non-state actors to states therefore requires a case-by-case analysis. In addition, the ability to cause harm through hacking is only partially dependent on an actor's level of technical sophistication. Although Stuxnet created an impression that the ability to cause harm is correlated with an attacker's level of technical sophistication, that is only partly true.

The ability to cause harm is accessible to less sophisticated actors beyond a certain minimum threshold. That does not mean that any script kiddie can cause a worrisome degree of harm. As Beau Woods, a cybersecurity expert at the Atlantic Council, wrote in an email to me, "There's a wide gradation between skr1pt k1dd13 [script kiddie] and nation-state adversary. Whether someone acts as a proxy or not, they can cause harm. And they can go from low-skilled carder to taking down hospitals much, much, much faster than the time to react to their capability escalation."[39] In short, there is a threshold at which a small group of people, or even an individual, can acquire the ability to cause harm, including physical harm, across vast distances at a global scale. This threshold is lower for hacking than for most conventional military capabilities.

What Is Technically Possible

So what kind of effects can be caused by hacking today? First, it is important to remember that just because an effect is technically possible does not mean that it will actually happen. Risk is determined not only by the vulnerability, but also by who might have an interest to carry out malicious actions, the threat. Yet, many people still wonder what harm can be caused through hacking. In short, yes, it is possible to cause physical harm with hacking, including killing that occurs indirectly but nevertheless as a consequence of the hacking. Significant vulnerabilities exist, and accidents in the past have shown that people can die as a result of them. For example, in 2015, an Airbus A400 M plane crashed in Spain, killing four people onboard, because data had been accidentally wiped, leading to a software failure.[40] And in 1999, two children were killed when a gas pipeline ruptured because a computer failure prevented the pressure relief function from working properly.[41] Additional examples include the 2015 warning by the US Government Accountability Office that the increasing interconnectedness between aircraft and the Internet "can potentially provide unauthorized remote access to aircraft avionics systems."[42] Also in 2015, two security researchers successfully hacked into cars, a Toyota Prius and a Ford Escape. One assessment suggests that over 2 million Supervisory Control and Data Acquisition (SCADA) systems, the type of systems used in a lot of critical infrastructure, can be accessed remotely through the Internet.[43] Even nuclear power plants are vulnerable to malicious hacking and

malware. In 2014, staff at the Monju nuclear power plant in Japan discovered that a computer in the reactor's control center had been infected with malware and was communicating with an outside source.[44] Such vulnerabilities could cause death and destruction if successfully exploited. (However, the safety features that kicked in following accidental software issues at the Browns Ferry nuclear plant in 2006 and the emergency shutdown at the Baxley power plant in 2008 in the United States demonstrate the resilience ideally baked into critical systems.[45])

Such exploitation does not necessarily require highly sophisticated malware. The examples of security researchers being able to hack into and gain control of cars or the effect of unsophisticated disk-wiping malware show that the ability to cause harm does not depend on technical sophistication. In fact, sometimes hackers can succeed simply by trying default passwords or stealing legitimate credentials. For example, a power outage in western Ukraine in December 2015 was caused by hackers using stolen, legitimate credentials. The malware that was used during the operation did not do the actual damage; it served to obfuscate the attack and to delay recovery efforts.[46] Similarly, the hackers targeting the Bangladeshi central bank were able to transfer the money using legitimate credentials. The same technique could be used against chemical plants, dams, or pipelines. For example, hackers reportedly owned the control systems of the Water and Sewer Department of the City of South Houston, Texas.[47] The 2016 Verizon Security Solutions report mentions another example of hackers, reportedly with ties to Syria,[48] having "infiltrated a water utility's control system and changed the levels of chemicals being used to treat tap water. . . The system regulated valves and ducts that controlled the flow of water and chemicals used to treat it. . . It seems the activists lacked either the knowledge or the intent to do any harm."[49] Another example is disk-wiping malware. The cyber attack against Saudi Aramco, one of the world's largest oil companies, is one of the best illustrations. According to news reports, an IT worker at Saudi Aramco clicked on a link in a scam email and, within hours, some 35,000 computers were partially or totally wiped.[50] The effect of the hack included major disruptions of business operations and while oil production continued, the company started giving it away for free in Saudi Arabia. Its purchase of replacement hard drives drove up prices worldwide.[51]

These examples show that the main variable determining whether an actor can cause harm is not technical sophistication, not knowledge of specific vulnerabilities or development of sophisticated codes, but *intent*. If the intent is there, the capability can follow. Zero-day vulnerabilities (vulnerabilities unknown to the public, anti-virus companies, and the software vendor[52]) can be discovered or purchased by state and non-state actors alike.[53] Similarly, government officials and security experts are concerned most about Iran and North Korea as cyber threat actors "not because of their skill, but because they are motivated to cause destruction."[54]

In short, while it is not likely that people may be killed or that significant damage may occur due to accidental or intentional changes to computer code, it is

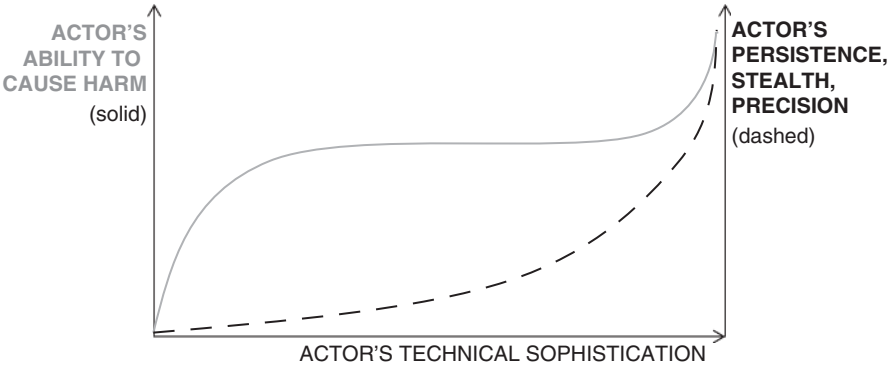

FIGURE 1.1 Relationship between an actor's technical sophistication and (1) the ability to cause harm as well as (2) persistence, stealth, and precision.

nonetheless possible. The likelihood is an open empirical question,[55] which needs to be re-evaluated constantly depending on the threat level from state and non-state actors. At present, there is no known case of somebody having been killed through an offensive cyber operation. The good news is that such acts of sabotage remain rare for most non-state actors, most of whom are criminals and so focused more on profit than on malicious harm. As cybercrime expert Brian Krebs pointed out, "Disabling infected systems is counterproductive for attackers, who generally focus on hoovering as much personal and financial data as they can from the PCs they control."[56]

How Technical Sophistication Matters

Increased technical sophistication can expand an actor's ability to cause harm (after the initial evolution from script kiddie to actual hacker), but in the context of cyber operations, it primarily expands the ability to target precisely and to do so stealthily.[57] Technical sophistication is most important when it comes to three other variables, namely: (1) the degree of persistence, or the ability of an actor to maintain unauthorized access to an infiltrated system; (2) the degree of stealth, or the ability of an actor to hide the malicious activity; and (3) the degree of precision, or the ability of an actor to limit the effect of the malicious activity to the targeted system. The caveat is, of course, that all of this is dependent on the target system's weakness in the first place: technology is constantly changing, a fact which might change the aforementioned dynamics in the future. With regard to the current state of the technology, Figure 1.1 visualizes this argument.

There are some situations where causing harm does require persistence and expertise, especially if the target includes industrial control systems, whose systems often differ significantly from other IT. The scholars Thomas Rid and Peter

McBurney have argued that "developing and deploying potentially destructive cyber-weapons against hardened targets will require significant resources, hard-to-get and highly specific target intelligence, and time to prepare, launch and execute an attack. Attacking secured targets would probably require the resources or the support of a state actor."[58] However, this does not mean that non-state actors cannot cause harm in such situations if they want to. The wording of Rid and McBurney's assessment reveals its limitations. In particular, the references to "hardened targets" and "secured targets" elide the fact that many critical infrastructure systems are not hardened or secured. An astonishing number of incidents in recent years were made possible because basic security measures (such as two-factor authentication) were missing. In such cases, causing harm is certainly within the reach of even relatively unsophisticated non-state actors.

While it is possible for non-state actors and proxies to cause significant harm through the Internet, it does not mean that it is easy. Jon Lindsay, professor at the University of Toronto and former intelligence officer with the US Navy, has observed that "[t]he latency between CNE [computer network exfiltration] and CNA [computer network attack] is more complicated than generally assumed."[59] In other words, just because you are able to access a system to steal data doesn't mean you are also able to carry out a cyber attack. In fact, two experts on industrial control systems, Robert Lee (a former US Air Force cyber warfare operations officer) and Michael Assante, have pointed out that "[industrial control systems]-custom cyber attacks capable of significant process or equipment impact require adversaries to become intimately aware of the process being automated and the engineering decisions and design of the [industrial control systems] and safety system."[60] This requires a higher level of sophistication in terms of persistence of access and expertise because industrial control systems differ significantly from regular IT.[61]

Why Some State Actors Do Stand Apart

Major states do stand apart from other states and non-state actors today in two ways: the level of resources they have available and their access to certain technologies. In terms of resources, for example, the US National Security Agency's (NSA) tailored access operations are carried out by some 600 people working at what is called the Remote Operations Center, which is staffed around the clock seven days a week.[62] The resources required to pay so many highly skilled individuals to work such hours for a prolonged period of time are generally only available to a major state (or corporation). At the same time, states that are able to maintain persistent access thanks to their resources don't necessarily exhibit the same degree of stealth. James Mulvenon, for example, an expert on China and cybersecurity, pointed to an important difference between Russian and Chinese actors in this regard, considering that Russia "abound[s] with highly talented programmers" while Chinese actors