International Social Science Review

Volume 96 | Issue 2 Article 3

Cyber Mercenaries: A New Threat to National Security

José de Arimatéia da Cruz

Stephanie Pedron

Cyber Mercenaries: A New Threat to National Security

Cover Page Footnote

José de Arimatéia da Cruz, PhD/MPH is a Professor of International Relations and Comparative Politics at Georgia Southern University, Savannah, GA. He is also a Research Professor at the U.S. Army War College, Strategic Studies Institute, Carlisle, PA and a Research Fellow of the Brazil Research Unit at the Council on Hemispheric Affairs in Washington, DC. Stephanie Pedron is a Political Science graduate student at Georgia Southern University.

Cyber Mercenaries: A New Threat to National Security

The birth of the Internet on October 29, 1969, propelled the world into an era of rapid technological development and structural innovation that fundamentally altered the way individuals and governments interact. Originally funded and designed by the Advanced Research Projects Agency (ARPA)—a branch of the U.S. Department of Defense—today's Internet generates an entire virtual landscape of information storage, processing, and communication that has been adopted by organizations and societies around the globe.[1] It has become an international pillar for commerce and networking. However, this electronic medium or "cyberspace" that a chunk of the world now operates on presents several security implications for private entities and nation-states.

Since the Internet's emergence outside of academic institutions, governments realized its underlying potential for intelligence-gathering and power projection across vast distances. Increased interconnectivity and information-sharing have a multitude of benefits. At the same time, they create cross-domain challenges that make nations, organizations, and individuals more vulnerable. According to Alexander Keith, a retired U.S. Army general and former director of the National Security Agency, Jamil Jaffer, Founder and Executive Director of the National Security Institute, and Jennifer Brunet, Director of Product & Strategy at IronNet Cybersecurity,

> Cyberspace has become a digital battleground where nation-states and their proxies, organized criminal groups, terrorists, hacktivists, and others seek to gain an advantage over one another… today the spread of advanced technologies and the increased connectivity of networked devices to physical systems make it more possible than ever before to create real-world effects through cyber activities."[2]

Warfare constantly changes. Strategies adapt to suit the situation and technology of the times. Accordingly, the Internet transformed the way nations conduct war. Cyber warfare is a

novel sphere of conflict that does not require geographic proximity between an attacker and their intended target. This ability to remotely cause harm introduced a degree of suspicion on the global stage. That cyber-attacks are dependent on the expertise of a group or even a single individual offers additional concerns. Tim Maurer, co-director of the Cyber Policy Initiative and a fellow at the Carnegie Endowment for International Peace, argues that, "The diffusion of power to an individual level is perhaps the most salient (if not unique) aspect of cyberspace compared to other security areas… an individual hacker can emerge as a cyber-power, one whose relative isolation, anonymity, and small footprint is a source of strength."[3] Those adept at exercising cyber warfare are capable of gross damage to a nation's infrastructure, from shutting down electrical grids and defense systems to stealing the personal information of millions of "netizens." Cyberspace has made it easier for competitors to remotely access the information networks of other societies and affect the operation of essential public and private institutions.[4]

There is no universal definition of what constitutes a cyber mercenary and current literature related to the topic is limited. Depending on one's perspective, a cyber mercenary can be a freedom fighter or a common thug renting his or her expertise to the highest bidder. Tim Maurer, in his book *Cyber Mercenaries: The State, Hackers, and Power*, presents a novel way of thinking about the dynamic between nation-states and their proxies,[5] although he does not clearly define the term cyber mercenary. Sitara Noor, in her article, "Cyber (In)Security: A Challenge to Reckon With" offers a basic description of cyber mercenary based on a dictionary definition of the traditional mercenary—that is, "a cyber mercenary can be defined as an individual or a group of experts who can offer their skills to anyone who will pay them a good amount of money."[6] Beginning with the common meaning of a word is helpful, but Noor's description neither places cyber mercenaries within the realm of cyber space, nor considers the selling of cyber tools or the

exchange of services for non-fiscal gains. Others also define cyber mercenaries as groups that carry out cyber espionage operations on demand,[7] although such definitions generally lack specificity.

According to Robert Knake, the Whitney Shepardson Senior Fellow at the Council on Foreign Relations (CFR) and author of *The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats,* a cyber mercenary is a criminal actor that will engage in offensive cyber operations for any country.[8] On the basis of this definition, cyber mercenaries may be considered a type of intermediary that contributes to a cyber-attack against a target. The use of intermediaries for conflict is common all around the world, and there is an opulent body of scholarship that traces the practice of hiring intermediaries, in particular mercenaries, throughout the centuries.[9] As such, there have been varying definitions of the word 'mercenary' based on different time periods. Scholars generally agree that mercenaries are conceptually distinct from other combatants in that they sell their skills to other parties, they are not integrated for prolonged periods of time into an armed force, they have not been sent by a third-party in an official capacity to assist with wartime efforts, and that they are recruited privately to avoid legal detection.[10] These attributes may still be applied to cyber mercenaries, although they would need to be updated to reflect modern innovation, as well as tied to the domain of cyberspace.

For the purpose of this paper, the authors define cyber mercenaries as intermediate actors with cyber-offensive capabilities that unlawfully peddle hacked intelligence, software exploits, or technical expertise to a beneficiary in exchange for financial or ideological gain. Beneficiaries range from nation-states to multinational corporations and wealthy individuals that gain advantage from the activities of these cyber mercenaries. Due to the explicit inclusion of nation-

states as a possible beneficiary, it is necessary to distinguish between state actors and state-sponsored actors. The authors do not include state actors employed by federal bodies recognized by domestic legislation. Contractors in such cases are subject to a notional set of standards and regulations that limit their autonomy and ensure that their activities do not breach laws or incite crimes. Therefore, contractors under the direction of the National Security Agency (NSA), the People Liberation Army (PLA), or the Iranians would not qualify. The authors do, however, include actors sponsored by a nation-state via active support or via the government willfully ignoring the activities that they conduct within their borders. For this paper, the authors will focus on a group of former state actors that were sponsored by a foreign nation-state and a group that sought to peddle hacked cyber weaponry.

Likewise, there are several competing definitions of cyber weapons that take into account the physical effects that these weapons cause, the context in which the weapon was used, and the intent of the user.[11] However, there is no international consensus regarding the definition of cyber weapons, rather, only the generic concept of 'weapon' is defined.[12] Even the *U.S. Department of Defense (DoD) Dictionary of Military and Associated Terms* does not define cyber weapons, although they have updated their list of terms to include several cyberspace-related jargon.[13] A traditional weapon is largely understood to be any device designed to "kill, injure, or disable people, or to damage or destroy property."[14] While cyber weapons have the capacity to harm groups and institutions en masse, the traditional definition of weapons does not encapsulate the diverse codes and software that have the potential to, but may not be used to inflict physical harm, thus intent and outcome play a crucial role in whether a malicious code should be deemed a weapon.

Technology and National Security Specialist Clay Wilson, in a 2006 Congressional Research Service report defines cyber weapons as "computer programs capable of disrupting the data storage or processing logic of enemy computers."[15] This definition, however, appears unconvincing for being under-inclusive. A cyber weapon defined by a simple capacity for inflicting harm or its possession of one or more offensive capabilities, in contrast, is over-inclusive and lacks the specificity necessary for legal regulation. Thomas Rid and Peter McBurney in their article, "Cyber Weapons," consider cyber weapons to be computer codes "used, or designed to be used, with the aim of threatening or causing physical, functional, or mental harm to structures, systems, or living things."[16] Their emphasis on intent is crucial, since technology may be repurposed for malicious use. In their view, a tool is a weapon when it is intended to be used as such. It is necessary then to consider both the outcome that the tool is designed to produce and the intent of the user to apply it in a manner that comports with its offensive capability. Intent, however, is a difficult element to measure and can raise several liability concerns.

Cyber Intelligence Research Director of the Italian Military of Defense Stefano Mele in his article, "Legal Considerations on Cyber-Weapons and their Definitions," provides a specific legal definition of cyber weapons within the context of warfare. Mele defines cyber weapons as "a part of equipment, a device, or any set of computer instructions, used in a conflict among actors both national and non-national, with the purpose of causing (directly or otherwise) physical damage to objects or people, or of sabotaging and/or damaging in a direct way the information systems of a sensitive target of the attacked subject."[17] Mele contends that a weapon can be an abstract concept, therefore program codes or computer instructions designed to inflict harm may be considered a weapon when used in specific circumstances. For the purpose of this

paper, the authors offer a tapered definition of cyber weapons that aligns with Stefano Mele's explanation in order to narrow the scope of discussion—cyber weapons are programs and software designed and used to deliver destructive outcomes on systems or networks. Destructive outcomes include manipulation, denials, disruption, degradation, and destruction.

This paper presents an explicit definition of cyber mercenaries and an overview of the reasons why nation-states might hire them. It considers the potential risks that cyber mercenaries pose and expands an existing framework for how nation-states might influence global actors that employ them. This paper is divided into five parts. The first examines the aspects of the Internet that allow cybercriminals to thrive, as well as the danger of privatized cyber capabilities in an increasingly plugged-in world. The second considers specific cyber mercenary groups based on the working definition outlined by the authors. Owing to the range of possibilities, this paper focuses on the motives and capabilities of two—Project Raven and the Shadow Brokers. These two groups were chosen to show variance among cyber mercenaries and their potential beneficiaries. They were analyzed based on what services or tools they peddled to beneficiaries and what they sought to gain in exchange. The third part of this paper analyzes the implications of the democratization and affordable access to information technology. The fourth considers an existing state-proxy framework, and the final segment provides recommendations for the future.

The Internet and Commercialized Cyber Capabilities

The Internet is a powerful mode of idea sharing and communication that is easily accessible to anyone with the means and the ability to operate it. In recent times, cyberspace has become a geopolitical arena that has resulted in the emergence of new channels of conflict and more intricate warfare tactics. The influence of independent actors and the offensive

competencies of small countries that lack large, physical militaries have been amplified as a result.

Accessibility and anonymity, two of the Internet's most prominent features, have made it possible for adversaries to inflict tremendous social and economic harm.[18] Former Assistant Secretary of Defense for Global Strategic Affairs Madelyn Creedon argues that the "low barriers of entry in cyberspace allow a range of adversaries to have effective capabilities against networks and computer systems, unlike those anywhere else—here, cyber criminals, proxies for hire, and terrorists could leverage capabilities that previously only governments possessed."[19] The openness of the online world, coupled with the privatization of offensive cyber skills raises concerns regarding liability and the loss of state control over cyber weaponry. The challenge of identifying those responsible—otherwise known as the 'attribution problem'—for cyber-attacks only adds fuel to the fire. Hackers are skilled at covering their tracks and may even plant evidence that implicates an innocent party.[20] The 'Ghostnet' hacker organization located in China for instance, which infiltrated political agencies and media companies worldwide. Even though authorities in affected countries knew where the attacks were coming from, they could not determine whether the computers being used were the actual computers of those responsible or previously infected computers used as relay points from a different location.[21]

States have begun to exploit these two web characteristics by outsourcing their virtual operations to third parties in order to achieve broader (often political) objectives. For the right price, countries, multinational corporations, and even wealthy individuals can purchase digital intelligence services and illicit access to high profile victims in a manner "akin to purchasing off-the-shelf elements of the National Security Agency or the Mossad."[22] The use of proxies for conflict between states is not a new strategy. Examples can be found all throughout history; the

Barbary pirates used by the Ottoman Empire or the Viet Cong supported by China and the USSR for instance. The expansion of the virtual world caused by more people gaining access to the Internet and current systems within the three main economic sectors (i.e. primary, secondary, and tertiary) changing from manual to digital incentivizes both state and non-state actors to exploit the cyber realm for their own purposes.

States may opt to hire cyber mercenaries for several reasons. On top of allowing them to maintain some semblance of deniability, cyber mercenaries permit them from engaging in direct conflict with an adversary. Indirect skirmishes may reduce casualties, costs, as well as domestic social repercussions such as a loss of electoral support in democratic societies. Furthermore, cyber mercenaries oftentimes have more experience using sophisticated technology than new cyber divisions established by the government. This gap incentivizes nation-states to take advantage of a cyber mercenary's previously learned skills.

The entrepreneurial state-sponsorship of cyber mercenaries underscores the dangers of non-obvious warfare, which is defined by Senior Management Scientist for RAND Corporation Martin Libicki as conflict where, "the identity of the warring side and even the very fact of warfare are completely ambiguous."[23] Ambiguity is a cause for doubt, which in turn breeds hesitance. Should a victim be unable to pinpoint an aggressor with confidence, then the victim might hesitate to respond.[24] Alternatively, even if the victim is certain of the culprit, without physical evidence, the globalization of politics and domestic news has resulted in a certain degree of caution. Should other world leaders have divergent opinions on who conducted a cyber-attack—or if the act can even be considered one—then the victim might again choose to subdue, or completely hold off, its response. In addition to identification issues, the shroud of anonymity may afford cyber mercenaries the opportunity to engage in other illicit activities.

They could even utilize the national resources of their state sponsors to fund these criminal undertakings.

Obscurity is arguably one of the cyber domain's greatest strengths. Although tracing network details like the Internet Protocol (IP) address might allow nations to determine the physical location of those perpetrating a cyber-attack that does not equate to locating the individual or group responsible. Hackers are not bound by geographic borders, nor do they need to be within the confines of their home state to carry out an invasive cyber operation. The Bangladesh Bank Cyber Heist is an example of the sweeping range of hackers and the complications that third parties can bring. In 2016, hackers from the Lazarus Group linked an IP address in North Korea to a server in Europe, which they used to control systems that they had already infected in an attempt to steal $951 million from the Federal Reserve Bank of New York account that belonged to the Bangladesh Central Bank.[25] Security hackers gradually familiarized themselves with the bank's daily procedures, before sending fraudulent instructions for thirty-five high dollar transactions via the SWIFT network, which is a global information system used by thousands of financial institutions for monetary transactions.[26] While the hackers only managed to get five of their orders through, the orders totaled $101 million. Due to a spelling error in one of the transfers, one transaction for $20 million was halted.[27] Cybersecurity experts concluded that North Korea was closely linked to the hackers that carried out the Bangladesh Bank attack, but the lack of immediate certainty stalled a response.

This not only undermined confidence in the safety of international transactions and the Federal Reserve, but also showcased the strategic advantages of empowering cyber mercenaries to conduct malicious activities. The South and North Korean governments established the Chosun Expo Joint Venture— also known as the Korea Expo Joint Venture (KEJP)—as an e-

commerce and lottery website.[28] When South Korea pulled out of the undertaking, North Korea continued operating the company. They expanded into different online enterprises and eventually used it as a front to hire hackers like Park Jin Hyok, who carried out an assortment of global cyber-attacks, heists, and intrusions, including the Bangladesh Bank Cyber Heist.[29] KEJP maintained its distance from the North Korean government, but still committed atrocities by collaborators working on their behalf. By allowing hackers like Park Jin Hyok to carry out these type of operations, North Korea managed to use his unique skillset to their advantage and deny knowledge of his actions when he was charged.

Given advancements in cyber security, groups remaining within compromised networks for months on end to steal information has become increasingly unlikely to go unnoticed for long. Due to this, more cyber mercenaries are likely to use precise hit-and-run approaches, where they only steal the information that is required from their targets and then abandon the network. The Advanced Persistent Threat (APT) group Icefog, for example, which focuses on attacking governmental institutions, tech and media companies, and telecom and satellite operators in Japan and South Korea.[30] An analysis of Icefog's attacks show that they were unusually focused; necessary files were identified, transferred, and then the targeted machine was abandoned. Despite the relative simplicity of their attacks, their hit-and-run tactics have successfully compromised several hundred targets.

The lack of central regulation governing cyberspace also allows cyber mercenaries to thrive. Stratfor global analyst Matthew Bey notes, "The absence of a global rules-based system means that the differences in laws, regulations, and litigation practices from state to state will only grow as countries try to exert greater control over the Internet."[31] While there have been efforts to introduce a series of fundamental norms that encourage the peaceful use of cyberspace

such as those proposed by the Global Commission on the Stability of Cyberspace, no intergovernmental organizations formally regulate the Internet, and consequently, the extensive field of cyber warfare. The lack of both an organizing body and transnational legislation contributes to the struggles that governments face when defending their national interests in the face of exploitive online aggressors.

This is not just an international issue; American laws overseeing digital warfare are not adequately equipped to address the speed of technological innovation or the privatization of specialized cyber capabilities.[32] In a *New York Times* article, reporters describe current American laws that control what former U.S. intelligence personnel can and cannot provide to foreign governments as "murky, outdated, and ill-equipped" and "meant to keep a leash on 20th-century warfare."[33] In other words, they do not comprise cyber skills that can be self-taught or learned from formal government agencies, and then further refined from anywhere in the world.

Addressing digital warfare requires an understanding of complex, continuously transforming technology.[34] Part of the security risks in the virtual world stems from the blurred lines between conventional warfare and cyberwarfare. What constitutes a threat has become more ambiguous, since the use of cyber weaponry does not fit traditional criterion of conflict. The international standards that determine whether entering a war is just (*jus ad bellum*) and regulations that outline the actions of wartime participants (*jus in bello*) provides little guidance about the legality of cyber-attacks or when such an attack becomes an act of war.[35] The many emerging types of cyber-attacks, as well as those that have only been hypothesized, also requires consideration. Several scholars have examined how existing laws, doctrines, and ethical principles might be applied to the virtual world, but none of them fully encompass the broad range of potential tools which may be used to cause harm.[36] Clear-cut determinations are crucial

for nation-states to evaluate offensive cyber operations, so that they might respond in a proportionate manner.

Cyberspace offers extensive opportunities for actors with advanced capabilities. If nothing is done to improve current capabilities of identifying, holding accountable, and sanctioning cyber mercenaries, as well as the states that contract their services, then governments that seek to covertly attack competitors without fully committing to the high cost of training or maintaining a digital army may continue to view cyber mercenaries as an easy, private alternative.[37]

Cyber Mercenary Group Examples

Group 1: Project Raven

Founded in 2009, Project Raven is a clandestine team made up of former intelligence operatives from the U.S. National Security Agency that were contracted to assist the United Arab Emirates in surveillance operations targeting political competitors, suspected terrorists, journalists, and human rights activists. According to a special report by Reuters, Raven is based in a converted mansion in Abu Dhabi known as the *Villa*.[38] Employing skills learned during their time spent serving in the U.S. intelligence community, Raven operatives utilized a wide range of cyber tools and methods to carry out covert cyber operations against a variety of targets chosen by UAE security forces. Early missions ranged from targeting users of Islamic Internet forums to assisting the UAE's National Electronic Security Authority (NESA) with combatting local terrorist networks like ISIS.[39] Operations ramped up in 2015 when agents were tasked to create malicious software like computer viruses that would infect website visitors en masse.

American operatives developed a strategy whereby missions would be handled in a step-by-step process. Every step was managed by a specific department or team. Together, these

divisions worked to conduct sophisticated cyber-attacks against Raven targets specified by NESA. The functions of each department are outlined below.[40]

- *Operations* – conducted hacking missions;
- *Management* – gathered relevant information on the identified target/s;
- *Infrastructure* – anonymously rented servers for Raven operatives to launch untraceable cyber-attacks;
- *Targeting* – scouted a target's devices and online accounts for vulnerabilities; developed suitable attacks to exploit a target's accounts; identified the target's associates and relatives for surveillance; and
- *Initial Access Development* – provided the Operations team with the necessary hacking tools.

Lori Stroud, a former intelligence analyst that left the NSA after backlash from the Edward Snowden leaks, joined Project Raven in 2014. She was officially employed as a contractor for the Baltimore-based cybersecurity firm, CyberPoint, which managed Project Raven for the UAE. In 2014, CyberPoint wrote a letter to the Department of Justice stating that their organization focused only on, "defend[ing] their [clients] critical systems and infrastructure from advanced exploitation techniques and the kinds of sophisticated threats where commodity solutions are inadequate."[41] Part of the ambiguity in cyberspace stems from the lack of distinction between cyberdefense and cyberoffense. However, the design and subsequent deployment of computer viruses that attack website visitors indiscriminately—as carried out by Project Raven in 2015—clearly does not fall under the former. Such wholesale attacks have the potential to affect the data and communication of citizens across the globe. Despite this, CyberPoint continues to present itself as a company focused solely on cyberdefense.[42]

Working in tandem with managers, Stroud assisted in crafting a policy by which Raven operatives must mark any data of potential American victims for deletion, and then notify others to remove them from subsequent collection.[43] Predictably, the flagged information continued to reappear in Raven's data caches. It was not until 2017 that Stroud discovered a targeting queue

filled with Americans, which had been limited to Emirati intelligence officers by Raven leadership. Even when Americans were not the direct target, legality was a recurrent concern for former U.S. agents because of the gray zones that cyber operations often fall into. For example, when hacking into the social media profiles or email accounts of non-Americans, the possibility of needing to break into servers located within the U.S. still exists.[44]

The most prominent cyber tool used by Project Raven was the espionage program Karma, which allowed agents to remotely access a user's iPhone. Karma was acquired by the UAE government from an undisclosed seller outside of the country.[45] Whether the seller engineered Karma or merely acted as a middleman is unknown, but without the creator of the tool present, Raven operatives only partially understood how Karma functioned. Karma exploited an undisclosed weakness in Apple's iMessage application, thus limiting the program's effect to Apple devices. Despite this restriction, it proved to be more valuable than other hacking tools because it did not require targets to directly download malware. Instead, Raven operatives could gain access to texts, emails, and even photographs by simply uploading phone numbers or email addresses into a preconfigured system. Between 2016 and 2017, Karma was successfully used against hundreds of targets, including prominent figures and journalists like the current Emir of Qatar Sheikh Tamim bin Hamad al-Thani, the chief editor of the Al-Arab newspaper *Abdullah Al-Athba*, the *Al-Jazeera* Chairman Sheikh Hamad bin Thamer bin Mohammed Al Thani, and more.[46]

Technically capable individuals or groups that develop sophisticated cyber weapons, and then sell them on the underground market have the potential to undermine global security. That the UAE was able to privately purchase such a potent tool alludes to a broader issue related to the commercialization of cyber weapons and how cyber mercenaries operate on the global stage.

Unlike state intelligence agencies that are often bound by agreements and conventional protocol in order to maintain positive multilateral relations, cyber mercenaries can act with more freedom. Additionally, cyber mercenaries often have little regard for the institutions that they are tasked to target because of other driving factors like monetary gain, which makes them perfect for conducting high-risk cyber operations. It is important to note, however, that the motivations of hackers are affected by a multitude of factors—all of which inevitably affect the type of cyber actions that they conduct and where they draw the line in terms of espionage. For Project Raven, many foreign operatives were likely driven by the lucrative salary offered by the UAE. Analysts like Stroud were reportedly paid upwards of $200,000 a year, while managers were paid over $400,000.[47]

The initial idea behind recruiting American contractors was to build-up Abu Dhabi's intelligence apparatus until Emirati specialists were capable of taking over. Outsourcing talent, as opposed to training individuals in-house, is done in many labor markets, not just those related to cyberspace. It allows organizations to tap the international talent pool for experienced individuals that can produce a greater quality of work in a more efficient, cost-effective manner. However, concern rose in 2015 when the UAE reportedly "grew more uncomfortable with a core national security program being run by foreigners."[48] Control over Project Raven shifted from CyberPoint to a domestic Emirati company called DarkMatter, which was founded in 2014 by Faisal al-Bannai, the creator of the mobile phone retailer Axiom Telecom.[49] Faisal al-Bannai has repeatedly denied any claims against DarkMatter for offensive hacking, zero-day exploits, or attempts to recruit foreign intelligence specialists for offensive cyber operations,[50] underscoring the difficulty of attribution and accountability in cyberspace.

Cyber weapons are proliferating, and control over them is not limited to the world's superpowers. Project Raven is an example of how small nations that lack large, physical militaries can amplify their offensive competencies to affect a range of virtual and physical communities or institutions. Furthermore, Project Raven illustrates the growing influence of intermediates acting within cyberspace, particularly the threat that former, highly-trained intelligence agents can pose when they are recruited by foreign organizations. The transformation of cyber warfare into a commodity has made it possible for anyone with the available resources to command advanced attacks against regional powers or other political adversaries.

Other highly-publicized cyber-attacks against recognized organizations in recent years, such as Sony Entertainment, Target, Yahoo, and J.P. Morgan Chase, has limned the need for organizations to hire individuals with cybersecurity expertise—demand, however, far outpaces supply.[51] According to a 2019 Cybersecurity Workforce Study by the International Information System Security Certification Consortium or (ISC)², the cybersecurity workforce gap in the U.S. is nearly 500,000.[52] This shortage can, expectedly, exacerbate cybersecurity issues, such as the number of data breaches within an institution. Since 2006, the Center for Strategic and International Studies (CSIS) has compiled a record of significant cyber incidents that focuses specifically on successful attacks carried out against federal agencies and businesses resulting in economic losses of over one million dollars.[53] From May 2006 to December 2010, the CSIS recorded seventy-five major cyber incidents. The following years until December 2017, it recorded 240 incidents. In 2018 alone, it recorded 104. A review of the upward surge in major incidents throughout the years, as well as the escalating financial costs outlined within each, alludes to the growing capabilities and boldness of cyber criminals.

Group 2: The Shadow Brokers (TSB)

The Shadow Brokers are an elite hacker group that first surfaced in August of 2016. They captivated the attention of media outlets and intelligence agencies across the globe when they started a public auction for computer exploits and hacking tools that they claimed to have stolen from one of the most sophisticated cyber-attack groups in the world, the Equation Group, which is believed to be linked to the U.S. National Security Agency.[54] The Equation Group has been described by journalists and security specialists as "omnipotent," the "Crown Creator of Cyber-Espionage," and the "apex predator of the APT world."[55]

TSB communicates by sharing links via Twitter, where they operate under the handle @theshadowbrokerss. Their motives have been widely speculated about, from retribution against President Donald Trump to a desire to publicly humiliate the NSA and stir internal chaos within the agency.[56] Their name, however, gives away one surefire drive—financial gain. It also provides insight into their initial desire to hold auctions for hacked data. The moniker references a fictional character from the video game series, Mass Effect. Founder of Comaelo Technologies, Matthieu Suiche, provides a description of the Shadow Broker from the game:

> "… an individual at the head of an expansive organization which trades in information, always selling to the highest bidder. The Shadow Broker appears to be highly competent at its trade: all secrets that are bought and sold never allow one customer of the Broker to gain a significant advantage, forcing the customers to continue trading information to avoid becoming disadvantaged…"[57]

Often, when hackers manage to access an adversary's cyber weaponry, they go to great lengths not to put themselves in the limelight. TSB instead opted to disclose their hacked caches, effectively releasing high-quality hacking tools into the public sphere. Since their appearance, TSB has published a total of four relevant leaks that contain a trove of cyber apparatuses from the NSA. Computer security specialist Bruce Shneier states that all of the current material

released by TSB was collected in 2013 "from an external NSA staging server, a machine that is owned, leased, or otherwise controlled by the U.S., but with no connection to the agency… the Shadow Brokers successfully hacked one of those caches."[58] Although the collection might seem outdated, custom-built hacking tools—particularly those designed by sophisticated attack groups—can be repurposed and used for years into the future. Randall Dipert considers the issue of repurposing software in his article, "The Ethics of Cyberwarfare," where he states that due to cyber weapons having no exotic components—unlike other advanced technological weapons such as biological—any computer is a potential cyber weapon.[59] Technology is constantly evolving. The potential of tools and programs to cause harm if restructured is a vital point to consider, and a major reason why adaptive techniques that take into account possible scenarios of varying significance are necessary.

The first leak by TSB was a data teaser that included a PasteBin page[60] with an invitation to an "Equations Group Cyber Weapons Auction," links to two encrypted archives, and auction instructions. To show their candor, the password for the first archive—which contained about 300MB of data—was given for free. According to Secure Trading Security Advisor Mustafa Al-Bassam, the cache contained "a set of exploits, implants, and tools for hacking firewalls."[61] The second archive, in contrast, was put up for auction. Also on their PasteBin page, TSB indicated that if they managed to reach their one million Bitcoin (BTC) goal, then they would dump more Equation Group files. However, after a series of low offers TSB called off the auction.

The second leak contained a list of foreign servers that were allegedly hacked by the Equation Group between 2000 and 2010, as well as a list of confidential cyber weapons.[62] Accompanying the information was a message that disjointedly called for the disruption of the 2016 U.S. presidential election.[63] The third, unlike previous leaks, included a message addressed

to President Donald Trump. TSB wrote that the leak was their "form of protest" against him for not upholding his campaign promises.[64] The end of the communication contained the password for the encrypted archive that TSB failed to auction during their first leak in 2016. This archive stored more hacking tools that could potentially compromise Unix and Linux operating systems.

The fourth leak is the most vital. It contained an array of what was originally thought to be zero-day exploits that predominantly targeted outdated versions of Microsoft Windows. Zero-day exploits target software vulnerabilities that manufacturers are unaware of.[65] When a hacker discovers and exploits these flaws, manufacturers would have "zero-days" to patch the issue.[66] In the wrong hands, zero-day exploits can be modified to destroy computer networks and steal information.[67] For example, Doublepulsar infected hundreds of thousands of computers mere weeks after TSB's leak. The NSA toolkit also contained the EternalBlue exploit that was used in tandem with Doublepulsar to conduct the WannaCry ransomware attack in May 2017. WannaCry crippled computers in over 150 countries and affected the operations of over fifty organizations. Economic loss estimates ranged from millions to billions of dollars.[68] Additionally, EternalBlue in conjunction with another leaked exploit, EternalRomance, and the hacking tool Mimikatz, were used to help propagate NotPetya malware one month after WannaCry. The NotPetya attack was dubbed the "most devastating cyber-attack in history" and resulted in damages of over $10 billion.[69] The un-redacted release of executable codes by the TSB harmed thousands of Internet users around the globe.

Notably, Microsoft released security patches addressing the targeted vulnerabilities a month before the TSB leaked them in April.[70] However devices that run older, unsupported versions of Windows or users that tinker with essential updating features on their personal devices remained vulnerable. Computers in larger organizations that tend to lag behind patch

schedules because of internal compatibility testing by administrators also remained at risk. Exploits effectively deliver malicious payloads, and are thus in high-demand by cybercriminals and other actors. The potential circulation of advanced cyber weaponry to third parties that either have the skills to use them or the means to hire individuals capable of doing so gives these parties the ability to cause immense destruction to a nation's infrastructure.

Implications

The democratization and affordable accessibility of information technology in the twenty-first century means that the only safe computers are the ones that remain unconnected to the World Wide Web. Nation-states must do whatever they can to protect their critical infrastructure (CI) against acts of terrorism, sabotage, or hacking by criminal elements. While the debate continues between the private sector and the government regarding who is ultimately responsible for protecting our CI, "illegal activities ignore national boundaries, ignore private-public distinctions, and leverage the public infrastructure to exploit its vulnerabilities."[71] The private-public sectors must come together "to effectively defend the information infrastructure" and "mitigate their impact effectively."[72]

Another important implication of the democratization of cyberspace, as the authors have previously stated, is the proliferation of non-state actors after the collapse of the Soviet Union. Given the porous borders of nation-states in the modern world, non-state actors constitute a growing concern for policy makers. Naval War College Chair of Science, Space, & Technology Joan Johnson-Freese in her essay, "A Space Mission Force for the Global Commons of Space," states that, "driven by such factors as economics and political ideology, non-state actors are more likely to deny, restrict, or disrupt common access and usage in pursuit of their objectives." [73]

The accessibility of cyberspace has also made less powerful nations view the Internet in a different light. They see cyber-power as a force multiplier and a part of their military arsenal when dealing with more powerful nations, including but not limited to, the United States, Russia, and China. Developing countries or rising powers such as India, Iran, and Brazil have developed their own cyber forces. While some developing nations may choose to cultivate their own cyber capable workforce, others may hire or recruit criminal elements to conduct their dirty deeds. As RAND senior engineer Dave Baiocchi and RAND engineering director William Welser states, "criminal syndicates could use satellites to monitor the patterns of law enforcement in order to elude capture, or a junta could use them to track rivals after a coup."[74] With the rise of plutocratic insurgency within the turbulent, interdependent world economy, criminal elements or syndicates have become the go to for nation-states and corrupt political leaders. While we traditionally think of insurgency as a rebel force attempting to overthrow the government, plutocratic insurgency aims to "carve out de facto zones of autonomy for themselves by crippling the state's ability to constrain their freedom of (economic) actions."[75] As Sarah Chayes demonstrates in her seminal book, *Thieves of State*, when corrupt politicians join forces with criminal syndicates, it is nation-states that end up paying the price because corruption threatens national and global security.[76]

Furthermore, American jurisprudence currently lags behind the advancement of cyber technology. U.S. laws do not translate well into the realm of cyberspace. At present, U.S. laws adequately address conventional forms of warfare, but when it comes to handling the growing number of sophisticated cyber-attacks, they have been painfully insufficient. As Senior Fellow at Potomac Institute for Policy Studies Melissa Hathaway points out, "wherever data is stored, it

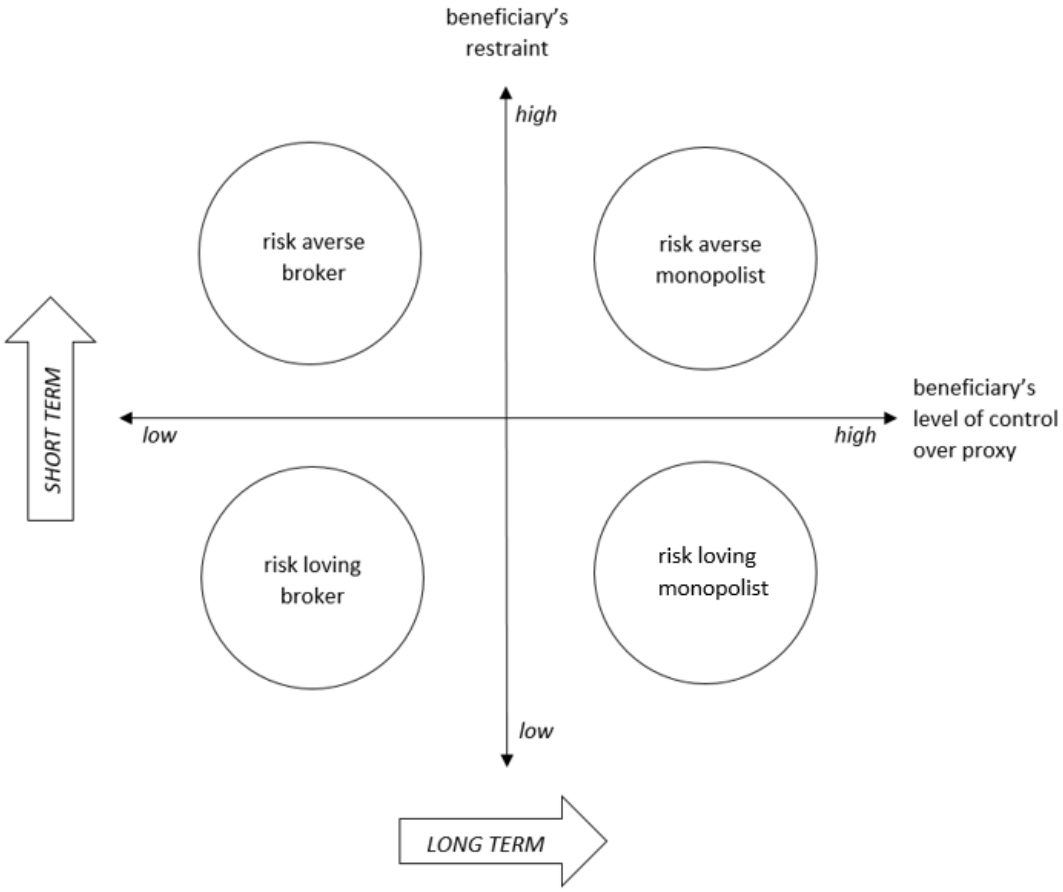
falls under the legal paradigm of that country. That includes the privacy laws. The U.S. does not have a single federal, government-wide data-breach law."[77]

Criminal enterprises and cyber mercenaries are also taking advantage of the democratization of technology to spread disinformation on the behavior of patrons in their patron-client relationship. Cyber is part of a nation's national power; it acts as a force multiplier in political warfare. Political warfare, as defined by George Kennan in the 1948 State Department memorandum: *Organizing Political Warfare*, is "the employment of all the means at a nation's command, short of war, to achieve its national objective."[78] One way cyber enhances a nation's political warfare is through the use of deepfakes. As law professors Robert Chesney and Danielle Citron argue, "deepfakes [are] highly realistic and difficult-to-detect digital manipulations of audio or video—it is becoming easier than ever to portray someone saying or doing something he or she never said or did."[79] Deepfakes allow for information cascades, especially in the realm of politics. Chesney and Citron suggest that when information cascades are utilized, "people pass information shared by others without bothering to check if it is true, making it appear more credible in the process."[80] When deepfakes become part of the democratic process, it creates political discord and resentment among voters and devalues the rule of law. Furthermore, all news, either legitimate or not, becomes "fake news" thus creating confusion among the electorate. As retired Reserve Colonel S.G. Chekinov and General-Lieutenant S.A. Bodanov argues, "the mass media today can stir up chaos and confusion in government and military management of any country and instill ideas of violence, treachery, and immorality, and demoralize the public. Put through this treatment, the armed forces personnel and public of any country will not be ready for active defense."[81]

Finally, while nation-states may employ cyber mercenaries as a way to avoid attribution or responsibility, there are some unintended consequences that must be seriously considered. Despite nation-states aggressively investing in their own cyber warriors, criminal syndicates and cyber criminals remain two steps ahead of law enforcement agencies. Cyber mercenaries may also be more technologically-prepared, and they enjoy the advantages of operating without the constraints of the rule of law or fear of prosecution. As U.S. Army War College Professor Steven Metz points out, "mercenaries became strategically important when they are more skilled than the fighters that states were able to keep under arms."[82] Metz focuses upon two key factors regarding the privatization of security—loyalty and discipline. He emphasizes the long-standing difficulties of keeping loyalty and discipline within professional military forces; therefore it is even more difficult to promote loyalty and discipline within cyber mercenaries that have no allegiance except to the highest bidder and the mighty dollar.

State and Proxy Relationships

Figure 1: Shaping Proxy Relationships through DIME(LE)



States that seek to transform their relationship or the relationship between other states and their cyber mercenaries might apply the elements outlined in the DIME(LE) model constructed by Tim Maurer.[83] This model covers several types of soft and hard power that governments have at their disposal, including diplomacy, information, military, economy, and law enforcement. The first involves engaging in international forums or the issuance of statements that urge heads of state to take action. The second and fifth elements work in tandem with one another; they concern the wilful spread of critical information and the public release of evidence by local law enforcement agencies. Both of these strategies essentially try to turn public opinion against the

state that the attack originated from. The third element, military force, is used to undermine trust between the state and its proxy through the exploitation of any power imbalances in their relationship. Lastly, economic sanctions may be imposed on a nation-state in a blatant attempt to force it to change its behavior.

The DIME(LE) model has distinguishable short-term and long-term goals. As shown in the figure above, in the short-term these elements may be used to alter a state's view towards risk, ultimately pushing the state towards greater restraint. In the long-term, how a state handles their proxy relationships may fundamentally shift to an arrangement where the state has more control over the proxy. It is important to take into account the risks associated with attempting to influence a state's proxy relationships, particularly if a government chooses to utilize a forceful element of the DIME(LE) framework, such as overt military action or economic sanctions. The priorities of cyber mercenaries often don't align with the priorities of their employers. Moreover, many cyber mercenaries do not have significant—if any—assets, which can make them harder for states to control in heated situations. Failing to regard vital factors in the bilateral relationship between a state and their proxy could result in unintended consequences ranging from severed trust and a loss of control over the cyber group to active state-sponsorship of similar organizations.

The authors of this paper suggest the incorporation of a sixth element when considering cyber mercenaries—cyber sanctions, which would be specifically aimed at identified groups or individuals responsible for or complicit in cyber-attacks. Sanctions would include travel restrictions, fines, incarceration, and the freezing or seizure of any assets. The inclusion of cyber sanctions can increase tensions between cyber mercenaries and their sponsors when they are

tasked to perform high-risk cyber operations. It may also deter future hackers and interested backers from aligning themselves with one another.

Conclusion

The rise of cyberspace transformed the conduction of warfare. Actors now have more tools to engage each other anonymously, indirectly, and across vast distances at a relatively lower cost. Nation-states that do not have the means to sustain large military forces can opt to hire or buy sophisticated cyber weapons from cyber mercenaries to amplify their power on the international stage. Cyber mercenaries can thus pose a security risk to countries that seek to maintain an asymmetrical advantage or to organizations that want to keep destructive cyber tools from proliferating. Nation-states can affect state-proxy relationships in a variety of ways, from spreading critical information online to applying trade embargoes or economic sanctions. Such tactics may also be helpful in deterring states from sponsoring cyber mercenaries or keeping hacker groups from forming relationships with certain parties. The lack of international law or governing institutions directly dealing with cyber incidents, as well as the variance of domestic legislation, results in a degree of ambiguity when the victims of a cyber-attack seek to retaliate in a proportionate way. Furthermore, current laws that describe what former intelligence personnel with the ability to build or operate dangerous codes and software are woefully underdeveloped in most countries. This lack of codified regulation may result in issues further down the line.

The proliferation of cyber-attacks in recent years necessitates the integration of cybersecurity at all stages of future systems development. In order to address the unique hazards posed by cyber mercenaries, heightened government oversight over intelligence agencies in the form of sweeping contract reviews, more intensive reporting requirements, and more profound information sharing might curb the risks associated with hiring outside talent. Since private

companies own networks and other critical infrastructure, the government cannot reduce national vulnerability to cyber-attacks on their own.[84] They may, however, be able to utilize existing legal authorities to their fullest capacity. For example, the U.S. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act signed by President George W. Bush on October 26, 2001, also known as the PATRIOT Act, facilitates information-sharing among agencies and grants law enforcement increased surveillance capabilities. If combined with Title 18 of the U.S. Code—which concerns America's criminal procedures—it may be used to monitor individuals that visit specific websites or access high-value information.[85]

Increased prioritization and investment by legislators into cybersecurity infrastructure is necessary. The creation of digital outreach teams that conduct frequent media blitzes in order to stimulate public opinion or remove confidential information spread by non-state actors on social media platforms may deter hacker groups from conducting certain activities. The passage of updated legislation encompassing the various aspects of cyber warfare would also be game-changing for agencies and courts attempting to navigate the litigation process. In addition, broadening intelligence networks and crafting a comprehensive (domestic and international) legal framework focused specifically on addressing cyber-attacks will alleviate some of the ambiguity when it comes to identification and response. Such an extensive security overhaul, however, is time consuming and may be met with broad political opposition. Until such procedures are established, states might begin augmenting their regulatory practices by first determining the fundamental operations that should only be performed by government institutions, particularly those closely tied to public safety. This, in turn, will establish clear boundaries regarding which functions may be delegated to third parties. Appropriate attention to

legal definitions of cyber mercenaries and cyber weapons are also vital for governments to begin addressing these urgent issues.

Most importantly, nation-states must acknowledge that they cannot address the danger of privatized cyber capabilities unilaterally. In the globalized and interdependent world of the post-cold war, global cooperation is essential in crafting effective regulatory structures for borderless hackers that have the capacity to impact societies via the Internet. International, proactive opposition against the employment of cyber mercenaries and plainly outlined sanctions for those that do could dissuade states from contracting their services.

ENDNOTES

[1] Doug Guthrie, "A Sociological Perspective on the Use of Technology: The Adoption of Internet Technology in U.S. Organizations," *Sociological Perspectives* vol. 42, no. 4 (1999): 583-603, 584.
[2] Keith Alexander, Jamil Jaffer, and Jennifer Brunet, "Clear Thinking About Protecting the Nation in the Cyber Domain," *The Cyber Defense Review* vol. 2, no. 1 (2017): 29-38, 29.
[3] Tim Maurer, *Cyber Mercenaries, the State Hackers, and Power* (Cambridge: Cambridge University Press, 2018), 13-14.
[4] William Bayles, "Network Attack," *Parameters*: *US Army War College Quarterly* vol. 31 no. 1 (2001), 44-58; Dombrowski, Peter and Demchak, Chris, "Cyber War, Cybered Conflict, and the Maritime Domain," *Naval War College Review,* vol. 67, no. 2 (2014): 71-96, 73.
[5] Maurer, 42.
[6] Sitara Noor, "Cyber (In) Security: A Challenge to Reckon With," *Strategic Studies* vol. 34, no. 2/3 (2014): 1-19, 6.
[7] Stefan Iovan and Alina-Anabela Iovan, "From Cyber Threats to Cyber-Crime," *Journal of Information Systems & Operations Management* vol. 10, no. 2 (2016): 424-433, 427.
[8] Personal correspondence with one of the authors on July 31, 2019.
[9] Alan Axelrod and Michael Dubowe, *Mercenaries: A Guide to Private Armies and Private Military Companies* (Thousand Oaks, California: CQ Press, 2014); John McCormack, *One Million Mercenaries: Swiss Soldiers in the Armies of the World* (London: Leo Cooper, 1993); Anthony Mockler, *The New Mercenaries* (London: Sidgwick & Jackson, 1985); & Janice Thomson, *Mercenaries, Pirates, and Sovereigns: State-building and Extraterritorial Violence in Early Modern Europe* (Princeton, NJ: Princeton University Press, 1994).
[10] Cécile Fabre, "In Defence of Mercenarism," *British Journal of Political Science* vol. 40, no. 3 (2010): 539-559; Deane-Peter Baker, *Just Warriors, Inc.: The Ethics of Privatized Force*

(London: Continuum, 2010); Deborah Avant, "From Mercenary to Citizen Armies: Explaining Change in the Practice of War," *International Organization* vol. 54, no. 1 (2000): 41–72; Peter Singer, *Corporate Warriors: The Rise of the Privatized Military Industry* (New York: Cornell University Press, 2003); & Sarah Percy, *Mercenaries: The History of a Norm in International Relations* (Oxford: Oxford University Press, 2007).

[11] Randall Dipert, "The Ethics of Cyberwarfare," *Journal of Military Ethics* vol. 9 (2010): 384-410; Stefano Mele, "Legal Considerations on Cyber-Weapons and Their Definition," *Journal of Law & Cyber Warfare* vol. 3, no. 1 (2014): 52-69; & Thomas Rid & Peter McBurney, "Cyber-Weapons," *The RUSI Journal* vol. 157, no. 1 (2012): 6-13.

[12] "U.S. Department of Defense Cyberspace Policy Report," November 2011, https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-059.pdf.

[13] U.S. Department of Defense, "Dictionary of Military and Associated Terms," updated January 2020, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf.

[14] Gregory Intoccia and Joe Moore, "Communications Technology, Warfare, and the Law: Is the Network a Weapons System," *Houston Journal of International Law* vol. 28, no. 2 (2006): 467-489, 480.

[15] Clay Wilson, "Congressional Research Service Report: Information Operations and Cyberwar: Capabilities and Related Policy Issues," updated September 14, 2006, https://fas.org/irp/crs/RL31787.pdf.

[16] Rid & McBurney, 7.

[17] Mele, 58.

[18] "The Cyber Threat Landscape: Confronting Challenges to the Financial System," Adrian Nish and Saher Naumaan, Carnegie Endowment for International Peace Report, updated March 25, 2019, https://carnegieendowment.org/2019/03/25/cyber-threat-landscape-confronting-challenges-to-financial-system-pub-78506.

[19] Madelyn Creedon, "Space and Cyber: Shared Challenges, Shared Opportunities: Edited Remarks to the USSTRATCOM Cyber and Space Symposium: 15 November 2011," *Strategic Studies Quarterly* vol. 6, no. 1 (2012): 3-8, 4.

[20] Scott Depasquale and Michael Daly, "The Growing Threat of Cyber Mercenaries," *Politico,* October 12, 2016, https://www.politico.com/agenda/story/2016/10/the-growing-threat-of-cyber-mercenaries-000221.

[21] Phillip Pool, "War of the Cyber World: The Law of Cyber Warfare," *The International Lawyer* vol. 47, no. 2 (2013): 299-323, 311.

[22] Mark Mazzetti, Adam Goldman, Ronen Bergman and Nicole Perlroth, "A new Age of Warfare: How Internet Mercenaries Do Battle for Authoritarian Governments," *New York Times,* March 21, 2019, https://www.nytimes.com/2019/03/21/us/politics/government-hackers-nso-darkmatter.html.

[23] Martin Libicki, "The Specter of Non-Obvious Warfare," *Strategic Studies Quarterly,* vol. 6, no. 3 (2012): 88-101, 88.

[24] Libicki, 89.

[25] Jim Finkle, "Cyber Security Firm: More Evidence Linked to North Korea Bank Heist" *Reuters,* April 3, 2017, https://www.reuters.com/article/us-cyber-heist-bangladesh-northkorea/cyber-security-firm-more-evidence-north-korea-linked-to-bangladesh-heist-idUSKBN1752I4. & Joshua Hammer, "The Billion-Dollar Bank Job," *New York Times,* May 3, 2018 https://www.nytimes.com/interactive/2018/05/03/magazine/money-issue-bangladesh-billion-dollar-bank-heist.html.

[26] Hammer, "The Billion-Dollar Bank Job." & "Swift: About Us" Swift, Retrieved from https://www.swift.com/about-us.
[27] Jamie Schram, "Congresswoman Wants Probe of 'Brazen' $81M Theft from New York Fed," New York Post, March 22, 2016, https://nypost.com/2016/03/22/congresswoman-wants-probe-of-brazen-81m-theft-from-new-york-fed/.
[28] Hammer, "The Billion-Dollar Bank Job."
[29] "North Korean Regime-Backed Programmer Charged With Conspiracy to Conduct Multiple Cyber Attacks and Intrusions," Department of Justice: Office of Public Affairs Press Release, September 6, 2018, https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and.
[30] "The 'Icefog' APT: A Tale of Cloak and Three Daggers," Kaspersky Lab Global Research and Analysis Team, 2013, https://media.kaspersky.com/en/icefog-apt-threat.pdf.
[31] Matthew Bey, "Great Powers in Cyberspace: The Strategic Drivers behind US, Chinese, and Russian Competition," *The Cyber Defense Review* vol. 3 (2018): 31-36, 35.
[32] Timothy Mckenzie, "Is Cyber Deterrence Possible?" *Air University Press*, 2017. 1-21, 5.
[33] Mazzetti, Goldman, Bergman, & Perlroth, "A new Age of Warfare: How Internet Mercenaries Do Battle for Authoritarian Governments," *New York Times.*
[34] Lucas Kello, "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft," *International Security* vol. 38, no. 2 (2013): 7-40; & Brian Mazanec, *The Evolution of Cyber War: International Norms for Emerging-Technology Weapons* (Lincoln: University of Nebraska Press, 2015), 161.
[35] Catherine Lotriont, "Cyber Operations: Conflict Under International Law," *Georgetown Journal of International Affairs* (2012): 15-24, 17; James McGhee, "Hack, Attack or Whack; The Politics of Imprecision in Cyber Law," *Journal of Law & Cyber Warfare* vol. 4, no. 1 (2014): 13-41, 23; Reese Nguyen, "Navigating Jus Ad Bellum" in the Age of Cyber Warfare," *California Law Review* vol. 101, no. 4 (2013): 1079-1129, 1081; & Roy Gutman and David Rieff, *Crimes of War: What the Public Should Know* (New York: W.W. Norton & Company, 1999), 223. To learn more about the concept of just war, please see A.J. Coates, *The Ethics of War: Second Edition*, Manchester University Press, 2016.
[36] Neil Rowe, "War Crimes from Cyber-weapons," *Journal of Information Warfare* vol. 6, no. 3 (2007): 15-25, 15; & Oona Hathaway, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue, and Julia Spiegel, "The Law of Cyber-Attack," *California Law Review* vol. 100, no. 4 (2012): 817-885, 839.
[37] Depasquale & Daly, "The Growing Threat of Cyber Mercenaries."
[38] Christopher Bing and Joel Schectman, "Special Report: Inside the UAE's Secret Hacking Team of US Mercenaries," *Reuters,* January 30, 2019, https://www.reuters.com/investigates/special-report/usa-spying-raven/.
[39] Ibid. & Lulu Garcia-Navarro, "Reuters Investigation Finds UAE Employed Former NSA Hackers As Spies," NPR, Radio Broadcast Episode, February 3, 2019, https://www.npr.org/2019/02/03/691058267/reuters-investigation-finds-uae-employed-former-nsa-hackers-as-spies.
[40] Bing & Schectman, "Special Report: Inside the UAE's Secret Hacking Team of US Mercenaries."
[41] Steven Bowers, "Request for Business Review," July 1, 2014, https://www.justice.gov/sites/default/files/atr/legacy/2014/10/06/309073.pdf.
[42] "About Us," CyberPoint Company, https://www.cyberpointllc.com/company.html.

[43] Bing & Schectman, "Special Report: Inside the UAE's Secret Hacking Team of US Mercenaries."
[44] Sam Biddle and Matthew Cole, "Team of American Hackers and Emirati Spies Discussed Attacking the Intercept," The Intercept, June 12, 2019, https://theintercept.com/2019/06/12/darkmatter-uae-hack-intercept/.
[45] Bing & Schectman, "Special Report: Inside the UAE's Secret Hacking Team of US Mercenaries."
[46] Ibid. & Christopher Bing and Joel Schectman, "Special Report: US Hackers Helped UAE Spy on Al Jazeer Chairman, BBC Host," *Reuters,* April 1, 2019, https://www.reuters.com/article/us-usa-raven-media-specialreport/special-report-u-s-hackers-helped-uae-spy-on-al-jazeera-chairman-bbc-host-idUSKCN1RD2PY.
[47] Ibid.
[48] Ibid.
[49] Alexander Cornwell, "Emerging Gulf State Cyber Security Powerhouse Growing Rapidly in Size, Revenue," *Reuters,* February 1, 2018, https://www.reuters.com/article/us-emirates-cyber-darkmatter-idUSKBN1FL451.
[50] Jon Gambrell, "UAE Cyber Firm DarkMatter Slowly Steps Out of the Shadows," Phys, February 1, 2018, https://phys.org/news/2018-02-uae-cyber-firm-darkmatter-slowly.html.
[51] William Parker, "Cyber Workforce Retention," Report. *Air University Press* (2016): 1-53, 2.
[52] "Strategies for Building and Growing Strong Cybersecurity Teams," (ISC)² Cybersecurity Workforce Study 2019, https://www.isc2.org/-/media/ISC2/Research/2019-Cybersecurity-Workforce-Study/ISC2-Cybersecurity-Workforce-Study-2019.ashx?la=en&hash=1827084508A24DD75C60655E243EAC59ECDD4482.
[53] "Significant Cyber Incidents," Center for Strategic & International Studies, https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents.
[54] Dan Goodin, "New Smoking Gun Further Ties NSA to Omnipotent "Equation Group" Hackers," ArsTechnica, March 11, 2015, https://arstechnica.com/information-technology/2015/03/new-smoking-gun-further-ties-nsa-to-omnipotent-equation-group-hackers/.
[55] Ibid; "Equation Group: The Crown Creator of Cyber Espionage," Kaspersky, Febrary 16, 2015, https://www.kaspersky.com/about/press-releases/2015_equation-group-the-crown-creator-of-cyber-espionage; & "The Equation Giveaway," Kaspersky, August 16, 2016, https://securelist.com/the-equation-giveaway/75812/.
[56] Josephine Wolff, "What Exactly are the NSA Hackers Trying to Accomplish?." Slate, August 17, 2016, https://slate.com/technology/2016/08/what-exactly-are-the-shadow-brokers-trying-to-accomplish.html; Scott Shane, Nicole Perlroth, and David Sanger, "Security Breach and Spilled Secrets Have Shaken the NSA to its Core," *New York Times,* November 12, 2017, https://www.nytimes.com/2017/11/12/us/nsa-shadow-brokers.html; & Sean Gallagher, "In Slap at Trump, Shadow Brokers Release NSA Equation Group Files," ArcTechnica, April 10, 2017, https://arstechnica.com/information-technology/2017/04/shadowbrokers-post-password-to-auction-file-of-alleged-nsa-hacking-tools/.
[57] Matthew Suiche, "Shadow Brokers: NSA Exploits of the Week," August 15, 2016, https://blog.comae.io/shadow-brokers-nsa-exploits-of-the-week-3f7e17bdc216.
[58] Bruce Schneier, "Who are the Shadow Brokers?," *The Atlantic,* May 23, 2017, https://www.theatlantic.com/technology/archive/2017/05/shadow-brokers/527778/.
[59] Dipert, 385.

[60] "Equation Group – Cyber Weapons Auction," Pastebin, August 13, 2016, https://archive.is/20160815133924/http:/pastebin.com/NDTU5kJQ.
[61] Mustafa Al-Bassam, "Equation Group Firewall Operations Catalogue," August16, 2016, https://musalbas.com/blog/2016/08/16/equation-group-firewall-operations-catalogue.html.
[62] "Shadow Brokers Reveal List of Servers Hacked by the NSA," Fortuna's Corner, November ,, 2016, https://fortunascorner.com/2016/11/01/shadow-brokers-reveal-list-of-servers-hacked-by-the-nsa-china-japan-and-korea-the-top-3-targeted-countries-49-total-countries-including-china-japan-germany-korea-india-italy-mexico-sp/.
[63] "Message #5 – Trick or Treat?," The Medium, October 30, 2016, https://medium.com/@shadowbrokerss/message-5-trick-or-treat-e43f946f93e6#.mo37m5ljp.
[64] "Don't Forget Your Base," The Medium, April 8, 2017, https://medium.com/@shadowbrokerss/dont-forget-your-base-867d304a94b1.
[65] Ablon, Lillian, Martin C. Libicki, and Andrea A. Golay, *Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar*, (RAND Corporation, 2014), 25.
[66] Adam Segal, "Using Incentives to Shape the Zero-Day Market," Report: Council on Foreign Relations, Septemeber 2016, www.jstor.org/stable/resrep05674.
[67] Paul Stockton and Michele Golabek-Goldman, "Curbing the Market for Cyber Weapons," *Yale Law & Policy Review* vol. 32, no. 1 (2013): 239-266, 240.
[68] Jonathan Berr, "WannaCry Ransomware Attack Losses Could Reach $4 Billion," CBS News, May 16, 2017, https://www.cbsnews.com/news/wannacry-ransomware-attacks-wannacry-virus-losses/.
[69] Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyber-attack in History," Wired, August 22, 2018, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.
[70] "Protecting Customers and Evaluation Risk," Microsoft Security Response Center, April 14, 2017, https://msrc-blog.microsoft.com/2017/04/14/protecting-customers-and-evaluating-risk/.
[71] Melissa Hathaway, "Toward a Closer Digital Alliance," *SAIS Review* vol. 36, no. 2 (2016), 57-67, 63.
[72] Ibid.
[73] Joan Johnson-Freese, "A Space Mission Force for the Global Commons of Space," *SAIS Review* vol. 36, no. 2 (2016): 5-13, 8.
[74] David Baiocchi and William Welser IV, "The Democratization of Space: New Actors Need New Rules," *Foreign Affairs* vol. 94, no. 3 (2015), 98-104.
[75] Nils Gilman, "The Twin Insurgency," *The American Interest* vol. 9, no. 6 (2014): 3-11.
[76] Sarah Chayes, *Thieves of State: Why Corruption Threatens Global Security* (New York: W.W. Norton & Company, 2015).
[77] Hathaway, 62.
[78] George Kennan, 'The Inauguration of Organized Political Warfare' [Redacted Version]," April 30, 1948, History and Public Policy Program Digital Archive, Obtained and contributed by A. Ross Johnson. Cited in his book 'Radio Free Europe and Radio Liberty', Ch1 n4. NARA release courtesy of Douglas Selvage. Redacted final draft of a memorandum dated May 4, 1948, and published with additional redactions as document 269, 'FRUS, Emergence of the Intelligence Establishment.' https://digitalarchive.wilsoncenter.org/document/114320.
[79] Robert Chesney and Danielle Citron, "Deepfakes and the New Disinformation War: The Coming Age of the Post-Truth Geopolitics," *Foreign Affairs,* vol. 98, no. 1 (2019): 147-155.
[80] Ibid.

[81] Keir Giles, *Handbook of Russian Information Warfare* (NATO Defense College Fellowship monograph Research Division, 2016), 25.
[82] Steven Metz, "The Privatization of Security is Coming: the U.S. Must Start Preparing For it. World Political Review (WPR)," World Politics Review, July 21, 2017, https://www.worldpoliticsreview.com/articles/22764/the-privatization-of-security-is-coming-the-u-s-must-start-preparing-for-it.
[83] Maurer, 140.
[84] Kate Charlet, "How the U.S. Approach to Cyber Conflict Evolved in 2018—and What Could Come Next," World Politics Review, December 26, 2018, https://www.worldpoliticsreview.com/articles/27071/how-the-u-s-approach-to-cyber-conflict-evolved-in-2018-and-what-could-come-next.
[85] Megan Penn, Joshua Miller, and Jan Schwarzenberg, "Countering Cyber Extremism: Interagency Paper No. 17," *Arthur D. Simons Center for Interagency Cooperation* (November 2015), 2.