Cyber Espionage is Here to Stay: A Realist Approach to Cybersecurity

Author: Paige Smith (paigehannah.smith@mail.utoronto.ca)
Munk School of Global Affairs at the University of Toronto
GLA 2024H Intelligence & Cybersecurity
December 5, 2021

Introduction

In 2015, during his presidency, Barack Obama referred to cyberspace as the "new Wild West" in reference to its vastness and lawlessness; there isn't a sheriff in sight.[1] As technology continues to advance and change the landscape of politics and security, new challenges present themselves within this unregulated domain. While the number of state- and non-state entities acting in this space has significantly increased, the international community has failed to develop a consensus surrounding the legality of certain cyberoperations. This uncertainty has prompted a significant political debate within law and cybersecurity, which requires greater attention.

The literature is largely divided into two arguments: those who argue cyberspace should be left unregulated and those who argue states should work together to formulate international law on cyberspace.[2] Those in favour of greater regulation argue that cyberspace needs to be regulated in a similar way to other national threats within international law. This paper will counter the latter argument to conclude that states' vested interests in information gathering will inhibit the collective adoption of international regulatory policy for cybersecurity. Further, it aims to provide an insight into the complexities of the 'international regulatory vacuum' surrounding cyber espionage.[3]

Cyber espionage is defined as the method of using computer networks to gather confidential information from target governments or organizations.[4] States are attracted to cyber espionage behavior because of its low cost and covertness that allows them to attain valuable information without disclosing their intentions to the target.[5] Consequently, states favour today's

[1] Russell Buchan. *Cyber Espionage and International Law* (Bloomsbury Publishing: 2018).

[2] Abid A. Asonis. "International Law on Cyber Security in the Age of Digital Sovereignty," *E-International Relations* (2020).

[3] Dodik Setiawan Nur Heriyanto. "International Regulatory Vacuum of Cyber Espionage." *Atlantis Press: Advances in Social Science, Education and Humanities Research* (2019): 436.

[4] Ibid.

[5] Ibid.

lack of international law surrounding cyber activities because the implementation of legal regulation would infringe on their interests.[6]

First, this paper will introduce the current global context for cyber operations and cyber espionage. Next, it will highlight the exceptionality of cyber espionage and the lack of legal framework surrounding this topic. Then, it will present arguments in favour of stronger regulation and reasons why attempts to create frameworks have failed up to now. The reasons for these failures are then addressed in the next section when this paper analyzes state behavior through a realist lens and highlights the nature of power within cyberspace. Lastly, this paper will conclude by offering two options that stand as a 'middle ground,' acknowledging the obstacles standing in the way of regulation while offering guardrails for cyberspace behavior.

Background

A state-sponsored cyberattack is when a state either directly or indirectly employs hackers through military and government authorities to achieve its own political, commercial, or military interests.[7] The motivation for carrying out state-sponsored cyber-attacks, like cyber espionage, is the ability to reap high rewards at a relatively low cost.[8] Due to its covert nature, acquiring sufficient evidence to attribute an attack to a country is very difficult when it comes to cyber espionage.[9] With this in mind, many states intentionally adopt generic strategies and technologies to disguise themselves as the majority of amateur cyberattacks leaving them indistinguishable.[10] Most often, these tactics are known as 'advanced persistent threats' and provide long-term

[6] Ibid, 4.

[7] Crowdstrike. "What is Cybersecurity," last modified April 1, 2021. https://www.crowdstrike.com/cybersecurity-101/cyberattacks/cyber-espionage/.

[8] Ibid.

[9] Ibid.

[10] Ibid.

oversight of a target's sensitive data through hidden malware that in some cases might remain dormant for years.[11]

There exists very little public data available to outline the many ways in which cyber operations are utilized by state actors and this lack of transparency creates public concern. Today's major concerns surrounding cyberspace include the threat it poses to digital infrastructure and eCommerce platforms.[12] With ease, state and non-state actors can perform surveillance or destroy a target's digital networks. A case that drastically enhanced this concern was the 2010 self-replicating cyber worm, Stuxnet, which infected hundreds of computers and shut down the Iranian nuclear centrifuge facilities in the county of Natanz.[13] Research shows that the attack was a coordinated between Israel and the United States to disrupt Iran's nuclear capabilities.[14] The attack ruined one-fifth of Iran's centrifuges, infected 200,000 computers, and caused 1,000 machines to physically degrade.[15]

The Stuxnet worm was one of the first instances of a state actor harnessing the power of a "digital weapon" with an "intention to alter international power dynamics."[16] Since then, the political landscape for digital weapons and cyber warfare has shifted in response to a change in military weaponry. But even though concerns have risen, it remains largely unregulated. For example, hackers are being conscripted into the military and government.[17] In states with economies and employment that heavily rely on a singular infrastructure, the results of a digital attack could be devasting.[18] While these malicious attacks remain a major concern for national

[11] Crowdstrike. "What is Cyber Espionage."
[12] Ibid.
[13] Ibid.
[14] Ibid.
[15] Anjali Shiyamsaran. "State-sponsored Hacking is Still a Problem," *Reporter.* Last modified 20 October 2021.
[16] Jack Galligan. "The Cyber Vector of War: State Sponsored Hacking Attacks and the Rise of the Digital Mercenary." *Society + Space* (2018).
[17] Ibid.
[18] Ibid.

security, the persistence and advancement of cyber espionage have dynamically changed vulnerabilities and cyber-attack strategies.

The North Atlantic Treaty Organization (NATO) and other military alliances recognize the urgency to address cyberspace as an operational domain of international conflict.[19] For example, in 2014, NATO declared that cyber defense was included in its collective defence and in the case of a cyberattack, Article 5 would be triggered.[20] Cyberspace has been militarized and has therefore called for the recruitment of digital soldiers who are experts in the field and commissioned to carry out state-sanctioned attacks and political subterfuge.[21] It is clear that international organizations have acknowledged the need for greater attention to rising cyber threats, but it remains even more unclear how these organizations classify cyber espionage.

Lack of Legal Framework

With the advancement of cyber technologies, the cyber domain has become a new domain for warfare. Attacks are occurring at an increasing rate, prompting corporations and governments to debate this new security landscape. Indiscriminate and damaging ransomware and malware attacks, like WannaCry (2017) and NotPetya (2017), conducted by state actors like North Korea and Russia have highlighted major vulnerabilities within today's digital infrastructure.[22] Even though NotPetya cost approximately $10 billion in damages, no states came forward to say that the attack violated international law.[23] The reason for this is that there is no governance structure

[19] Ibid.

[20] Ibid.

[21] Ibid.

[22] Dennis Broeders and Bibi van den Berg. "Chapter 1: Governing Cyberspace: Behavior, Power and Diplomacy," *Governing Cyberspace* (London: Rowman & Littlefield, 2020).

[23] Ibid, 2.

in place to address issues in cyberspace and, similarly, there is no framework that outlines appropriate behavior in this new domain.

Even though there have been attempts to define what international law applies to cyberspace, these have either failed to provide adequate detail or have not achieved a consensus on a global scale. For example, the Tallinn Manual (2013) and the Tallinn Manual 2.0 (2017) provided an analysis of International Humanitarian Law and cyberspace to serve as a legal reference point but states have not used it in the context of cyberattacks.[24] Dan Efrony and Yuval Shany (2018) refer to the failure of the manual as a "rulebook on the shelf" and numerous other agreements and literature have followed similar patterns, such as the London Action Plan and the Tunis Commitment.[25] The lack of successful rules or guidelines specific to cyberattacks has left this global issue in a major grey area.

Most states have laws against espionage with penalties ranging from imprisonment, million-dollar fines, and even death in some cases, but there currently exists no *international* law making espionage illegal.[26] While it is certainly not encouraged, there exists a general, tacit acceptance that nations spy on each other.[27] Gary Brown and Keira Poellet (2012) explain that espionage is not endorsed but remains an "ill-defined policy space that permits it to occur without violating international law."[28] Today, cyber espionage is recognized in the same way by the international community and this has prompted major debates regarding whether there should be regulation to stop this tacit acceptance.

[24] Ibid, 3.
[25] Ibid.
[26] Ibid, 133.
[27] Ibid.
[28] Gary Brown and Keira Poellet. "The Customary International Law of Cyberspace," *Strategic. Studies Quarterly* 6, no.3 (2012):126-145.

Those who favour liberty within cyberspace argue that cyber technologies play a major role in national security by providing a military advantage for economies that can afford to invest in cyber technologies. For this reason, states with the economic means and cyber capabilities are reluctant to give up this power especially when they are unsure of other actors' behavior and intentions.[29] Actors who are the main drivers of cyberspace technology and surveillance tools are include the United States, China, Russia, the United Kingdom, Israel, Iran, and North Korea.[30]

States have recently allocated greater funding to programs within cybersecurity to ensure they maintain a competitive edge against rivaling technologies abroad. In 2021, the United States estimated a total of $18.7 billion for its cybersecurity budget, while China estimated a total of 170 billion yuan (approximately $25.8 billion).[31] It remains unclear how much of their respective budgets are invested in cyber espionage purposes, but it can be assumed that a significant portion is allocated to this clandestine behavior.

In contrast, those who favour applying an international legal framework to cyberspace argue that legal frameworks are necessary to address and regulate this new international security concern. However, the ever-changing landscape and technology surrounding these operations make it difficult to outline appropriate behavior and ensure legislation remains current. There have been several failed attempts to create these frameworks.

The first international treaty seeking to harmonize digital law was the 2001 Convention Cybercrime in Budapest which achieved a slight "consensus" on computer crimes by providing little detail and significant room for interpretation.[32] The Convention's vagueness and presence of

[29] Ibid.
[30] Ibid.
[31] Masha Borak. "China drafts three-year plan to boost its cybersecurity industry amid increasing concerns for safety." *South China Morning Post.* Last modified 13 July 2021.
[32] Jack Goldsmith, "Cybersecurity Treaties: A Skeptical View." *Koret-Taube Task Force on National Security and Law (*February 2021), 3.

loopholes meant that states were easily able to manipulate its regulations to serve their interests instead of its principal aims to facilitate cooperation and combat cybercrime. The failure of the Cybercrime Convention highlights the huge disparity in opinion surrounding digital practices in cyberspace and the inability to create international cooperation.[33]

According to Jack Goldstein (2021), the failure to establish international law is attributed to a non-alignment of interests on topics that exists too closely to those of national sovereignty and security.[34] He explains that successful treaties amongst powerful nations require the potential for mutual gain and without it, there is no incentive for states to comply.[35] Goldstein further argues that attribution stands as a major hurdle to any cybersecurity agreement, resulting in real difficulties to track attacks and exploits from around the world.[36] There exists no system for accurate tracing that the international community might use to attribute cyberattacks and cyber espionage.

Resolving and attributing cyber espionage is difficult since many cases do not go public due to the highly classified nature of information revealed within the courtroom.[37] Recent cases between U.S. and Chinese intelligence agencies highlight the nuance within cyber espionage cases and the fragility of diplomatic relations, as a result. Since 2017, the U.S. Department of Justice has brought forward at least a dozen cases against agents and spies for conducting cyber- and economic espionage on behalf of China.[38] It is evident that as "great powers" like America and China go head-to-head, there will be no battlefield for conflict but instead a clandestine race for information.[39]

[33] Ibid.
[34] Ibid.
[35] Ibid,4.
[36] Ibid,10.
[37] Mike Giglio. "China's Spies are on the offensive." *The Atlantic.* Last modified 26 August 2019.
[38] Ibid.
[39]Ibid.

Advocating for Greater Regulation

A common argument presented by scholars seeking greater regulation of state cyber operations, like cyber espionage, often uses Article 41(1) of the 1961 Vienna Convention to support their claims. This article of the Convention outlines the duty of all states to respect the laws and regulations of a recipient country and they are not obliged to interfere in domestic issues.[40] Dodik Setiawan Nur Heriyanto (2019) argues that cyber espionage is an illegitimate search for information because it is conducted without the target's knowledge and aims to attain confidential political, economic, or military information.[41] He explains that when one country engages in cyber espionage, they are directly violating the provisions of international diplomatic law outlined in the Vienna Convention 1961.[42]

Moreover, Heriyanto provides detail on the negative effects of cyber espionage to state diplomatic relations by explaining that the target state will become uncomfortable and disturbed by the cyber espionage practices carried out against them. In turn, this will lead to tense and fragile diplomatic relations.[43] Early signs of this damaged relationship can be seen when countries withdraw diplomatic representation from the country conducting the espionage.[44] In 2009, Indonesia withdrew its diplomatic missions from Australia after it was revealed that the country was tapping government officials' devices.[45]

In 2017, the former legal adviser to the State Department, Brian Egan, said that "states need to do more work to clarify how the international law on non-intervention applies to states'

[40] Dodik Setiawan Nur Heriyanto. "International Regulatory Vacuum of Cyber Espionage." *Atlantis Press: Advances in Social Science, Education and Humanities Research* (2019), 107.
[41] Ibid, 108.
[42] Ibid.
[43] Ibid.
[44] Ibid.
[45] Ibid.

activities in cyberspace."[46] He said this in reference to the 2016 Russian cyber interference in the U.S. presidential election that caused the spread of disinformation through its "hack and leak" operations.[47] While this incident prompted scholarly debate surrounding whether the principle of non-interference was violated, the majority of literature concludes that Russia's cyberattack did not violate it, especially in terms of coercion.[48] Although this does not directly speak to cyber espionage, it served as a major example of a state-led cyber operation that successfully extracted the information of interest.

Scholars advocating for the adoption of normative international law argue that states need to step up and accept responsibility for the cyber domain. They argue that the countries that permit or engage in cyber spying violate their obligation to respect the territorial sovereignty of other states.[49] Moreover, the rise of cyber espionage technologies provides a selective advantage to few and leaves developing countries as easy victims to these sophisticated tactics.[50]

The consequence of this political reality is that states with less resources are unable to keep up with the cyber operations of their peers and so must align themselves with major cyber powers.[51] Boeders and van den Berg (2021) argue that inequalities between sovereign states would likely suggest that small states favour the development of a rules-based order.[52] In this case, this could take form in 'cyber-norm entrepreneurship' in which these processes are adopted while still allowing for the desired ambiguity.[53]

[46] Nicholas Tsagourias. *Electoral Cyber Interference, Self-Determination, and the Principle of Non-intervention in Cyberspace*, November 2019.
[47] Ibid, 46.
[48] Ibid.
[49] Heriyanto,"International Regulatory Vacuum of Cyber Espionage," 109.
[50] Ibid.
[51] Ibid.
[52] Broeders and van den Berg. "Chapter 1: Governing Cyberspace: Behavior, Power and Diplomacy."
[53] Ibid.

While the claims that are presented in favour of developing a normative legal framework are compelling, the nuances of the cyber domain do not seem to appear as black and white as some scholars argue. Instead, states participating in cyber espionage programs are motivated by intrinsic views of power and competition within today's 'cyber-security dilemma.'

Applying a Realist Lens to the International Order

The international community turns a blind eye to these violations of territorial sovereignty because it is in the best interest of some of the most powerful states. Robert Reardon and Nazli Choucri (2012) said that "realist theories of deterrence, crisis management, and conflict may be used to understand whether cyberspace is stabilising or destabilising, whether cyber technologies will be a new source of conflict or peace, and whether states will engage in cyber arms racing."[54]

At the core of the realist theory is the idea that the international system is constantly in a state of anarchy in reference to a lack of overarching authority.[55] Hans Morgenthau's classical realist theory argues that nation-states are solely motivated by self-interest to gain greater power and security.[56] Although this serves to be a largely pessimistic view of states, it stands to be the dominant theory to explain today's landscape for cyber operations, specifically for cyber espionage. Cyberspace is dominated by actors who invest their money and resources in technology to attain information and further their interests.

An additional theory to further explain the motivations of state actors is Kenneth Waltz's neorealist theory which attributes behavior to power politics which emphasizes the unknown

[54] Anthony J.S. Craig and Brandon Valeriano. "Realism and Cyber Conflict: Security in the Digital Age." In *Realism in Practice.* (Bristol: E-International Relations Publishing).
[55] Ibid, 87.
[56] Ibid.

intentions of other states.[57] States are, by nature, suspicious of each other and with the rise of technological advances, states expend significant resources to remain informed and up to date.[58] This power dynamic is what drives states to attain greater power and limit their cooperation.

State actors are aware of the consequences of conducting cyber espionage and they accept the risks to their reputation and diplomatic relations to do so. Driven by egocentrism and fear of the unknown, states' behavior could be attributed to realist theories which would explain the lack of consensus or cooperation and the increase in cyber-attacks. Brown and Poellet (2012) explain that these state actors have no incentive to reach an agreement or create regulatory systems.[59] They argue that today's political environment cannot sustain the development of norms and customs through international negotiation and agreement unless cyber espionage was deemed separate from 'disruptive cyber action.'[60] States are committed to measuring their capabilities against those of their rivals and by understanding this obstacle to developing framework, it would be possible to develop frameworks that exclude this cyber operation. Brown and Poellet understand the exceptionality of cyber espionage for large state actors. To successfully create a legal framework, there would need to be not only incentives for cooperation to mediate the motivations driven by realist theory, but also a lack of disincentive by excluding regulations on cyber espionage.

Limitations of Cyber Espionage

Major states will need to balance concerns surrounding cyber espionage with growing concerns regarding escalations and misperceptions in cyberspace. Common cyber espionage

[57] Ibid.
[58] Ibid.
[59] James Lewis. "Shaping the ground for bilateral cybersecurity negotiations," *China International Strategy Review* (July 2021).
[60] Ibid.

tactics include watering hole, spear-phishing, and zero-day exploits, all of which could be detected as a malicious cyber-attack.[61] More specifically, some cyber espionage attacks involve social engineering to prompt the behavior or gathering of the information that is of interest or enabling the attack to take place through social means.[62] The dangers surrounding these cyber espionage attacks is that they could be mistaken for military attacks with major destabilizing repercussions.[63]

Russell J. Buchan (2016) highlights the ambiguous nature of cyberspace and how simple misinterpretations can lead to an escalation of conflict; this is what he calls the 'cyber dilemma.'[64] He explains that the stability of cyberspace "may be best served by consciously preparing for the moment that states wrongly interpret the actions of their adversaries."[65] Ensuring all states have defensive cyber technologies in place to defend themselves may help to mitigate major vulnerabilities for business and digital infrastructure globally.

In analyzing power relations surrounding cyber operations, some scholars remain skeptical as to whether cyber capabilities, like cyber espionage, give states coercive power to change the nature of conflict and warfare. These scholars are arguing that cyber operations may not have the brute force to compel or manipulate as they claim to hold. Erik Gartzke (2013) argues the limits of internet-based warfare: "It is one thing for an opponent to idle a country's infrastructure, communications or military capabilities. It is quite another to ensure that the damage inflicted translates into a lasting shift in the balance of national capabilities or resolve."[66] He argues that cyber operations alone will not alter the global order, the use of military operations would be necessary to have a lasting influence on global power structures.[67] A statistical study by Jensen,

[61] Crowdstrike. "What is Cyber Espionage."
[62] Ibid.
[63] Goldsmith, "Cybersecurity Treaties."
[64] Broeders and van den Berg. "Chapter 1: Governing Cyberspace: Behavior, Power and Diplomacy."
[65] Ibid, 9
[66] Ibid.
[67] Ibid.

Valeriano, and Marness (2016) confirm Gartzke's argument through analysis of cyber incidents between rival states. Their study concluded that coercive cyber actions aimed to manipulate behavior are often ineffective and cyber power is not indicative of transformative, coercive control.

Potential for a Middle Ground

Amid two competing narratives surrounding the regulation of cyber espionage, some scholars have argued that there exists a 'middle ground' that could mitigate concerns from both sides of the debate. There are two popular proposals that aim to provide some regulating framework to cyberspace while ensuring enough flexibility surrounding cyber espionage to ensure a state's willingness to participate. This section will first discuss the potential for successful norm-building and then discuss creating cyber treaties with exclusionary principles.

a. Establishing International Norms

Instead of implementing a legally binding framework, there exists the potential for creating non-binding, normative action within the international system. States that are by nature power-seeking and in competition are reluctant to commit themselves to agreements without knowing whether rival states will also comply. Instead, developing international cyber norms as a method of cyber deterrence might create some specific thresholds within cyber behavior.

However, norms are neither created nor interpreted equally, Liisi Adamson (2020) comments on the nuances behind creating and interpreting norms on a global versus regional level.[68] Global actors, like the UN GGE, propose global norms that are vague calls for cooperation.[69] Adamson argues that the biggest obstacle to norm-building is the varied

[68] Liisi Adamson. "International Law and International Cybernorms." 30
damson. "

interpretations. In some cases, actors might agree that the norm exists, but they do not agree on the application or applicability of the norm.[70] Adamson presents the case of the Stuxnet attack on the Iranian nuclear facility as an example of a contentious attack. Some arguments characterize it as an armed attack and under the UN Charter Article 51, Iran was permitted to use self-defence.[71] Others believe that the attack remained under the threshold necessary to term it an armed attack.[72]

Previously unsuccessful international norms have often lacked specificity and left room for misinterpretation. Concerns surrounding physical damage or injury, attacks from inside the state's borders, loss of functionality for cyberinfrastructure, and usurpation of government functions have been left to the interpretation of domestic actors.[73] For this reason, there have been major inconsistencies between reactions and consequences. As a result of this unsuccessful norm setting, there has been a lack of what Nori Katagiri (2021) explains as the 'trickle-down effect' on states which is when these actors are unable to gather the necessary evidence and are left to make "broad statements of ad hoc condemnation."[74]

Adamson (2021) concedes that the nature of cyber norms as voluntary and non-binding principles means that there exists no framework for implementing or enforcing them.[75] However, setting aside issues of enforceability, she argues that norms serve to differentiate what is acceptable and what is not for the international community at whole.[76] Adamson contends that even though these norms may be voluntary, nonbinding, and lacking legal consequences, other political actions like retorsion and 'naming and shaming,' can be used as effective consequences against state

[70]Liisi Adamson. "International Law and International Cybernorms." In *Governing Cyberspace (*London: Rowman &Littlefield) 2021, 32.
[71] Ibid.
[72] Ibid, 31
[73] Ibid.
[74] Ibid.
[75] Ibid.
[76] Ibid.

actors.[77] Broeders and van den Berg (2021) agree and propose a need for Confidence-Building Measures (CBMs) to serve in times when escalation of cyber conflict is unintentional.[78] In cyberspace, these measures would aim to reduce fear of attack and attempt to build trust and interpersonal communication to counteract the persistent "security dilemma."[79] Over time, the adoption of CBMs could lead to the establishment of new rules and practices that outline how states should cooperate and compete without escalating tensions.

b. Maintaining Exclusivity in Cyber Policies

With regard to cyberattacks, two main issues have resulted from a lack of legal or norm frameworks: the lack of threshold and the inability to attribute. To address these issues, scholars advocate for the adoption of international treaties that adequately address cyber-attack concerns but allow for cyber espionage to remain unregulated.

Not all cyberattacks should be treated the same.[80] Developing an international treaty on cybersecurity would likely cover topics ranging from cyber-arms control to cybercrime and regulation of software supply chains.[81] Spying on computer systems or making something less functional is different from cyberattacks that invoke irreversible damage and impact critical infrastructure.[82] Aggressive cyberattacks that result in physical destruction, like disabling electric power grids, are governed by traditional law in terms of warfare.[83] This physical damage or injury could warrant a military attack if its damages were substantial and for a significant amount of

[77] Ibid.
[78] Broeders and van den Berg. "Chapter 1: Governing Cyberspace: Behavior, Power and Diplomacy."
[79] Ibid.
[80] Ibid.
[81] Jack Goldsmith. "Cybersecurity Treaties."
[82] Ibid.
[83] Ibid, 137.

time.[84] However, these are not usually conducted by state actors or state-sponsored actors, with the exception of Stuxnet.

Richard A. Clarke and Robert Knake (2010) insist that a cyber treaty should ban cyber-attacks on civilian targets, but not ban military targets or cyber exploitation.[85] Their argument is convincing and stands to support the thesis of this paper in that it would require selective regulation of cyberspace. Clarke and Knake argue that such a treaty would ensure the safety of privately-owned networks but still allow for larger state actors to maintain their edge in cybersecurity.[86] In their article, they do not mention a ban or regulation on cyber espionage because they understand that states depend on these means for spying.[87] Perhaps another reason it was not mentioned was because of the difficulty in collecting evidence and attribution for this covert behavior.[88]

Conclusion

It is evident that as cyber capabilities continue to improve and expand, there is an urgency to engage in political debate surrounding their operations. This paper has provided a cursory look into the behemoth topic that is international cybersecurity and the nuances of creating frameworks to regulate rising concerns. Despite the sensibility of advocating for greater cyber regulation and creating legal frameworks to hold states accountable, this is close to impossible to achieve within the power-seeking and anarchical political landscape of cybersecurity. Large powers will likely continue to build stronger cyber arsenals to maintain their competitive edge while simultaneously spying on rival states to compare their capabilities.

[84] Ibid.
[85] Ibid, 2.
[86] Ibid.
[87] Ibid.
[88] Ibid.

One of the major challenges in proposing cyberspace policy is that as the technological landscape continues to evolve, solutions discussed today will be outdated and irrelevant soon. This also means that cyber operations are not easily understandable for policymakers or lawyers and will consistently rely on scholarly debate to stay informed.[89] Further research should look at the larger scope of cyber-attacks within international cyber law and to compare the role of state actors to non-state actors, and discuss these topics with an eye to wider-scope solutions. It could be concluded that the only way to realistically mitigate the effects of state-sponsored cyber-crime and espionage is to create stronger defensive systems to better identify and remove malware threats.

[89] Ibid.

Bibliography:

Adamson, Liisi. "International Law and International Cyber Norms: A Continuum?" In *Governing Cyberspace: Behavior, Power, and Diplomatic,* ed. Dennis Broeders and Bibi van den Berg, 19-44. London: Rowman & Littlefield, 2020.

Adonis, Abid A. "International Law on Cyber Security in the Age of Digital Sovereignty" *E-International Relations* (2020). https://www.e-ir.info/2020/03/14/international-law-on-cyber-security-in-the-age-of-digital-sovereignty/.

Borak, Masha. "China drafts three-year plan to boost its cybersecurity industry amid increasing concerns for data safety," *South China Morning Post.* Last modified 13 July 2021. https://www.scmp.com/tech/policy/article/3140963/china-drafts-three-year-plan-boost-its-cybersecurity-industry-amid.

Broeders, Dennis and Bibi van den Berg. "Chapter 1 Governing Cyberspace: Behavior, Power and Diplomacy," In *Governing Cyberspace: Behavior, Power and Diplomacy.* London: Rowman & Littlefield, 2020.

Brown, Gary and Keira Poellet. "The Customary International Law of Cyberspace." *Strategic Studies Quarterly* 6, no. 3 (2012): 126-145.

Craig, Anthony J.S. and Brandon Valeriano. "Realism and Cyber Conflict: Security in the Digital Age." In *Realism in Practice* (2018).

Crowdstrike. "What is Cyber Espionage." Accessed December 4, 2021. https://www.crowdstrike.com/cybersecurity-101/cyberattacks/cyber-espionage/.

Galligan, Jack. "The Cyber Vector of War: State Sponsored Hacking Attacks and the Rise of the Digital Mercenary". *Society + Space, 27 November 2018. https://www.societyandspace.org/articles/the-cyber-vector-of-war-state-sponsored-hacking-attacks-and-the-rise-of-the-digital-mercenary*.

Giglio, Mike. "China's Spies are on the offensive." *The Atlantic.* Last modified 26 August 2019. https://www.theatlantic.com/politics/archive/2019/08/inside-us-china-espionage-war/595747/.

Goldsmith, Jack. "Cybersecurity Treaties: A Skeptical View." *Koret-Taube Task Force on National Security and Law (*February 2021).

Heriyanto, Dodik Setiawan Nur. "International Regulatory Vacuum of Cyber Espionage." *Atlantis Press: Advances in Social Science, Education and Humanities Research* (2019). https://carnegieendowment.org/files/Hollis_Law_and_Cyberspace.pdf.

Hollis, Duncan. "A Brief Primer on International Law and Cyberspace." *Carnegie Endowment for International Peace (*2021).

Katagiri, Nori. “Why international law and norms do little in preventing non-state cyber attacks,” *Journal of Cybersecurity* 7, no.1 (2021).

Lewis, James. “Shaping the ground for bilateral cybersecurity negotiations.” *China International Strategy Review* 3 (2021):115-122. DOI:10.1007/s42533-021-00081-z.

Shiyamsaran, Anjali. “State-sponsored Hacking is Still a Problem,” *Reporter.* Last modified 20 October 2021.

Tsagourias, Nicholas. “Electoral Cyber Interference, Self-Determination and the Principle of Non-Intervention in Cyberspace,” SSRN Electronic Journal (2019).