FILLING IN THE GAPS OF INTERNATIONAL CYBERSECURITY IN THE UNITED STATES

CARISSE JOSEPH
College of Business
Florida Atlantic University

Abstract

With the widespread use of technology, a new host of threats appear that affect the American government, businesses, and civilians. This is why Cybersecurity is a global emergency that involves not only the United States, but all countries, and which makes it necessary for the gaps within international cybersecurity to be filled. Cyber security crosses all geographic boundaries and must be addressed wholistically in order to be effective. Current regulations within cyberspace are not adequate and in order to protect each state from cyber threats, it is imperative for the states to create a collaborative solution to the issues within the current cyberspace in order to maintain peace.

Introduction

Now, more than ever, technology is one of the most common means of communication between people. With billions of people using technology, it allows hackers to have multiple opportunities to facilitate cyberattacks. The use of technology and the internet are widespread throughout the world. This year, the number of devices connected to the internet is expected to reach over

46 billion.[1] Individuals use technology for various reasons, such as to work or to communicate with others. Technology and the internet have allowed people to complete tasks quickly and efficiently, making the lives of many easier. Due to the widespread use of technology, a new host of threats appear, however. Therefore, cybersecurity is important. Cybersecurity is the art of protecting networks, devices, and data from unauthorized access or criminal use.[2] Cybersecurity ensures that the confidential information of individuals, businesses, the government, and other entities is protected. The United States has made efforts to make sure that the people are protected. The most prominent Cybersecurity regulations in the United States are the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach Bliley Act, and the Homeland Security Act.[3] HIPPA ensures that the medical and health confidential information of a patient is protected.[4] The Gramm Leach Bliley Act requires financial institutions to be transparent about their information-sharing practices to their customers and to safeguard sensitive data.[5] The Homeland Security Act established the Department of Homeland Security after 9/11 and was created in the hope of preventing another terrorist

[1] *Internet of Things' Connected Devices to Triple by 2021, Reaching Over 46 Billion Units, Compare* the Cloud, 2021, https://www.comparethecloud.net/news/internet-of-things-connected-devices-to-triple-by-2021-reaching-over-46-billion-units/, (last visited March 15, 2021.)

[2]. *What is Cybersecurity, CISA*., 2021, https://us-cert.cisa.gov/ncas/tips/ST04-001, (last visited March 14, 2021.)

[3] Agarwal, H., *A Glance at The United States Cyber Security Laws*, 2018, https://www.appknox.com/blog/united-states-cyber-security-laws, (last visited March 15, 2021.)

[4] *Health Insurance Portability and Accountability Act of 1996 (HIPAA*), Centers for Disease Control and Prevention, https://www.cdc.gov/phlp/publications/topic/hipaa.html, (last visited March 27, 2021.)

[5] *Gramm Leach Bliley Act,* Federal Trade Commission, https://www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act, (last visited March 28, 2021.)

attack.[6] In 2018, the Cybersecurity and Infrastructure Security Agency was created to defend the nation against cyber-attacks.[7] While the United States has a good foundation within its borders, the issues within international cybersecurity need to be addressed. While the United States can regulate cybersecurity within the country, regulating it collaboratively with other countries has been challenging due to different viewpoints. The states also have different interpretations of various legal questions that arise. Each country has different cyber capabilities and viewpoints which makes it difficult for everyone to come to an agreement.

International Humanitarian Law

The United Nations established a group called the Open-Ended Working Group (OEWG) at the end of 2018 that discusses developments in Information Communications Technology (ICT).[8] In 2019, state representatives met to discuss different issues that would be addressed in later meetings. During this meeting, the applicability of International Humanitarian Law (IHL), a gap within cybersecurity, was discussed. International Humanitarian Law is defined as "a set of rules which seek, for humanitarian reasons, to limit the effects of armed conflict."[9] International Humanitarian Law protects innocent civilians whenever a war occurs. With the spread of technology, however, a new type of war has emerged - cyberwar. Cyberwar is "war conducted in and from computers and the networks connecting them, waged by states or their

---

[6] *The Homeland Security Act of 2002*, Homeland Security, https://www.dhs.gov/homeland-security-act-2002, ((last visited March 28, 2021.)

[7] *Cybersecurity and Infrastructure Security Agency*, CISA, https://www.cisa.gov/, (last visited March 28, 2021.)

[8]. *Open-ended Working Group on ICT*. Reachingcriticalwill.org. 2021, https://www.reachingcriticalwill.org/disarmament-fora/ict/oewg, (last visited March 28, 2021.)

[9] *What is International Humanitarian Law?*, Icrc.org. 2021, https://www.icrc.org/en/doc/assets/files/other/what_is_ihl.pdf, (last visited March 28, 2021.)

proxies against other states."[10] With cyber wars becoming a new threat, the states must identify how IHL can address some of its issues.

Cyberwar is unique from a typical war since it can occur anywhere in the world and can even be difficult to trace. Due to this, it is imperative to establish how IHL looks at cyberwars. IHL identifies cyberwars as an armed attack because they can lead to physical damage, injury, or death.[11] They can also damage important infrastructures, such as hospitals and nuclear plants. An example where International Humanitarian Law would apply would be if a hospital's computer systems were hacked and a patient who was seeking treatment died because they were unable to receive treatment due to a loss of information.

International Humanitarian Law focuses on protecting civilian objects like infrastructure, but a gap appears when we begin to discuss whether the personal information of civilians is protected under International Humanitarian Law. There appears to be some agreement among the members' that an attack is when a cyber operation intends to inflict physical harm or damage. The problem is that not all cyber-attacks will physically harm civilians. If the personal data of a civilian is compromised, it can severely impact their lives. Civilian data includes confidential information, such as tax records, medical data, social security information, and more. The states should consider filling this gap by looking at personal data as a civilian object to further protect civilians under International Humanitarian Law.[12]

---

[10] *Cyberwar*, Encyclopedia Britannica 2021, https://www.britannica.com/topic/cyberwar, (last visited March 28, 2021.)
[11] Laurent Gisel and Tilman Rodenhauser, *Cyber Operations and International Humanitarian Law: Five Key Points,* Nov. 2019, Humanitarian Law and Policy, https://blogs.icrc.org/law-and-policy/2019/11/28/cyber-operations-ihl-five-key-points/, (last visited March 28, 2021.)
[12] Id.

Attribution

Public attribution plays an influential role in international cyberspace. Attribution is "the allocation of a cyber-attack to a certain attacker or group of attackers."[13] Public Attribution is beneficial to victim states because it can be a useful mechanism for deterring cyber-attacks. When an attack occurs, investigators are called in to collect evidence to determine who is behind the attack. Investigators look at the technical forensics first to figure out who was behind the attack. They look at things such as the software and coding language used to help them get a better idea of the nature of the attack. The investigators can also identify the strategy that the attacker used, which can allow them to determine what their motive was.[14]

A notable example would be the 2014 indictment of Chinese military hackers. The hackers hacked into the computers of individuals who were indifferent to United States industries, such as the nuclear and solar industry. They stole the information they received through hacking for their own economic advantage. On the day of the indictment, FBI director James B. Comey claimed that "for too long, the Chinese government has blatantly sought to use cyber espionage to obtain economic advantage for its state-owned industries."[15] This hacking allowed investigators to identify the strategy that the Chinese were using to gain unauthorized access to their information.[16] The benefit of this is that investigators can help prevent and even predict future attacks because they are privy to the strategies that the Chinese hackers used. By placing the blame on those Chinese military officials, it helped them deter the officials from hacking

---

[13] Professor K. Saalbach, *Attribution of Cyber Attacks*, Universitat Osnabruk, Feb. 2017, https://repositorium.ub.uni-osnabrueck.de/bitstream/urn:nbn:de:gbv:700-2017022015577/2/Attribution_of_Cyber_Attacks_Saalbach.pdf, (last visited March 28, 2021.)

[14] Id.

[15] *U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage*, Justice.gov, 2021, https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor, (last visited March 28, 2021.)

[16] Id.

them for economic advantage.

Despite the benefits of attribution, there are some holes present in this method for deterring cyberattacks. It can be difficult for investigators to analyze both the strategic and technical aspects of an attack. If an attack is overly complicated, then it becomes more difficult for investigators to determine who is behind it. Experienced hackers also know how to conceal their identity, making the job of investigators more intricate. The United States has made investments in attribution technology a priority. However, not every state has that capability.[17]

Incorrectly attributing a state for a cyber-attack can have an impactful consequence within international cyberspace. It can lead to hostility between the victim state and the attacking state. Incorrectly attributing a state creates an unnecessary mark on the reputation of the blamed state in cyberspace as well. Currently, there is not an international law that governs placing the blame on other countries for participating in malicious cyber activities. The states have been discussing what norms should be established and their applicability. During the Open-Ended Working Group (OEWG) meeting in 2019, attribution was discussed, but the countries had differing viewpoints.

For instance, China was concerned that public attribution would lead to "great economic instability" while the United States believed that it would not invite conflict and would instead remind states to comply with the ethical norms. [18]A solution to this gap would be the creation of an international law that requires the victim state to provide evidence to prove that the state they are attributing the illegal action to was indeed behind the attack. The states would have to come together and decide what the evidence threshold would need to be. This

[17] *Final Report*, National Security Commission on Artificial Intelligence, 2021, https://www.nscai.gov/wp-content/upl. ads/2021/03/Full-Report-Digital-1.pdf, (last visited March 28, 2021.)
[18] Achten, N., *New U.N. Debate on Cybersecurity in the Context of International Security*. 2021, Lawfare. https://www.lawfareblog.com/new-un-debate-cybersecurity-context-international-security, (last visited March 28, 2021.)

way, the hostility between the victim state and attacking state will be mitigated because there is an established norm that allows the victim state to publicly come forward with the claims backed by evidence.

Prosecution in the International Cyberspace

Another gap within international cybersecurity is the issue of how to prosecute individuals who are behind attacks. There is no established international law regarding how states should prosecute individuals which makes the process challenging to navigate. A solution would be to apply the protective principle of jurisdiction to international cyberspace. The protective principle states that a country has the "jurisdiction to prescribe a rule of law attaching legal consequences to conduct outside its territory that threatens its security as a state or the operation of its governmental functions, provided the conduct is generally recognized as a crime under the law of states that have reasonably developed legal systems."[19]

Cyber threats can impact the security of a country tremendously because attackers can hack into government systems and steal classified information which would be detrimental to the country and its civilians. By applying a legal framework, it would allow states to circumvent prosecution arguments and would allow states to effectively prosecute attackers. States who are prone to cyberattacks due to having limited cybersecurity measures would benefit from this because they would be able to punish attackers. This principle may also aid in the reduction of cyber-attacks. When holes are present within the legal framework, it makes it easy for hackers to carry out their plans. If hackers know that they will be prosecuted if they attack a state, they will be

[19] *United States v. Zehe,* 601 F. Supp. 196 (D. Mass. 1985*)*, Justia Law. 2021, https://law.justia.com/cases/federal/district-courts/FSupp/601/196/1734505/,(last visited March 28, 2021.)

less likely to go through with an attack.

Conclusion

Technology will continue to spread in the future and the states must work to keep up with the changes in cyberspace. There will always be a need to modify the regulations within international cyberspace for the states to maintain cybersecurity. While the proposed solutions provide a way to fill the current gaps within international cybersecurity, it is important for discussions surrounding international cybersecurity to continue. This is a challenging, yet critical, aspect of international law that impacts the states profusely. State cooperation and collaboration are imperative to maintain international cybersecurity and protect the states against cybercrimes. Through collaboration, the states will have the ability to establish effective laws and prevent future cyberattacks.