Jason McCarthy

Dr. Karahan

CYSE 426

7/08/2024

International Law: The role it needs to play in Cybersecurity

International law has played a role in national security for nations worldwide for centuries. Such laws have allowed for close dialogue and avoiding escalated conflict where situations nearly get out of hand. In an ever-changing global landscape, the requirements and needs of humanity have begun to dictate that these international laws shift from covering not only the physical world but also the digital world that is expanding by the day. Implementing this is necessary as national governments have been increasingly digitizing or requiring digitization of records and information on their citizens and as the need for better safeguards around critical infrastructure rises. There have also been many calls by concerned citizens and legislators to implement more international laws as the number of attacks carried out daily targeting anything individuals use or benefit from in cyberspace climbs, and new technologies are rapidly developing.

International laws for Cybersecurity and Cybercrime are necessary as they signal that countries are willing to come together to find and work on solutions for these issues. The formation of these laws started occurring early on in Budapest on November 23rd, 2001, when the Convention on Cybercrime was put in place by the Council of Europe. The Council of Europe is the continent's leading human rights organization and boasts 46 members (Council of Europe, 2023). They have their main treaty, the European Convention on Human Rights, and it was signed by many representatives of the free world, including the United Kingdom, France,

Germany, Norway, Poland, Italy, and many others in Europe. Countries not located in Europe are non-members. This category includes the United States, Japan, Israel, Vatican City, Mexico, and Brazil, among others. The treaty for the Convention on Cybercrime, also known as Treaty 185, was signed on the day it is dated by the United States, among other countries who were present. The United States eventually ratified it and enforced it. It is valuable to note that none of the United States' cyberspace foes signed the treaty. This list would most recognizably include China, Russia, Iran, and North Korea.

The Convention on Cybercrime is very well laid out in detailing the issues it is designed to address. The treaty is not only enforced at the international level but also at the national government level for those who signed it. There are 48 articles in total and these are divided into four chapters. The cybersecurity topics covered in the treaty include illegal access, illegal interception, computer-related fraud, data interference, and misuse of devices, among others (Council of Europe, 2001). Although the Convention seems somewhat encompassing at face value, especially for the issues that existed at the time, this treaty is not comprehensive enough to address today's concerns and threats in Cyberspace. The more time goes on without widespread international conversations about the threats posed to the global cyberspace community and how to handle them, the more time technology has to leap ahead while international law continues to lack. The convention needs to be expanded further and new solutions for new and continuing problems may need to be provided in the form of other laws.

While the United States is not directly part of the Council of Europe as a member, this has not stopped the nation from implementing multinational cybersecurity initiatives through other mechanisms. At the 2024 NATO summit in Washington D.C., NATO allies, including the U.S., decided to create the NATO Integrated Cyber Defense Center (NATO, 2024). It is at their

strategic headquarters in Belgium. This Center implements a workspace for both civilian and military personnel to support the mission of increasing situational awareness and to boost the collective cyber defensive capabilities of NATO members. In addition to this, the center is focused on establishing norms in cyberspace when it comes to security.

The concerns at large since 2001 amid the creation of the Convention on Cybercrime and the continuing explosion of the internet itself are expansive. A united stance on cybersecurity needs to exist in the international community rather than having many partnerships and countries across the globe that merely interact with each other to deal with the same threats. Exacerbating this is the fact that there is no common view on what should be considered a standard way of approaching threats and activities in cyberspace (Burkadze, 2016). Handling threats in cyberspace and determining appropriate responses has been a struggle for quite some time now. Holding other countries and bad actors accountable for their actions in cyberspace is a key aspect of international law to shape as it is often difficult to determine who specifically is responsible for the crime or the attack. The technology used in these attacks allows individuals and organizations to remain anonymous, and they can't be positively identified (Burkadze, 2016). Even when they can be identified, how a country can respond is often limited. In 2012, The United States Department of State took the position that international law applies in cyberspace during the U.S. Cyber Command legal conference (Cherry & Pascucci, 2023). This aligns with a broader view of more sovereign states having the view that general rules of international law apply to conduct in cyberspace as well (Mačák, 2016). If some of the rules regarding attribution, or the burden of proof needed to place blame can be changed to some degree, and a consensus for this is met, it may be possible to enforce these international laws on a broader scale. Such change could involve a legal standard only requiring some kind of proof indicating that the

country of origin is doing nothing to prevent the possibility of such attacks. Part of this issue can be linked to the fact that countries are often hesitant to create and provide interpretation for new laws for cybersecurity to be implemented at the national level. This allows corporations and other entities, both good and bad, to come in and use the legal framework to their benefit with the absence of such regulation (Mačák, 2016).

When looking at standards for cybersecurity threats and what can be exploited through using internet-accessible information, one of the first topics to come to mind is data privacy. While data privacy may not seem like an international cybersecurity concern, a government's primary responsibility is to protect and act in the best interest of its citizens, and without data privacy, citizens are just as susceptible to cyberattacks as corporations. The data housed by corporations and critical infrastructure like phone, internet, and electric companies, alongside the healthcare industry, is largely connected to customers in some way. Across the pond, the GDPR in Europe, also known as the General Data Protection Regulation, is considered the gold standard (Saunders & Reifman, 2021). This regulation is recognized for its strong enhancement of data privacy, and it has shaped data privacy law in other countries (Saunders & Reifman, 2021). The GDPR lays out how companies are to collect, use, and destroy customer's data and multiple components are embedded including enforcement mechanisms, penalties, data breach notifications, and other requirements and utilities in the use of the data. The enforcement mechanism includes requiring privacy officials within companies with a position of data protection officer, which is somewhat comparable to how an inspector general works in a U.S. federal agency in the idea that they are mostly independent of the rest of the company in their duties and serve the public interest (Hoofnagle et al., 2019). The GDPR also enhances individual privacy rights by restricting how and when third-party companies can use customer data, and by

doing so, limits the threat of an external data breach (Hoofnagle et al., 2019). Europe has implemented information privacy in a way that heavily favors the consumer over the company because of its longstanding recognition of privacy as a human right. Europe also sees data protection as a requirement that data be used fairly for the right purposes and with proper authorization, and this view is aside from the idea of the right to private life (Hoofnagle et al., 2019).

In contrast, the United States has very little privacy law at the federal level. Any privacy guaranteed by federal law exists where predigital laws are understood to cover the same rights in cyberspace where laws were previously applied in the physical world. Most data protection or privacy laws have been conceived and adopted at the state level. United States data protection law is weaker compared to Europe to the extent that the European Court of Justice struck down, or invalidated, the US-EU safe harbor framework. This was done considering the surveillance activities Edward Snowden cast light on and these revelations attracted the attention of European countries as this went against their expectations for data privacy, whereas the United States has national security concerns to be heavily invested in (Bowman, 2021). Such differences in national priorities for each state will make it difficult to find common ground when it comes to safeguarding citizens personal data. As time goes on, and capabilities are developed in nations all over, a question that will need to be decided is whether not data protection is afforded under international humanitarian law (Cherry & Pascucci, 2023). It is at this point that the United States may need to make a final decision on the issue, as a country, rather than continuing to be undecided between the federal level and state levels across the nation.

As cyberspace continues to evolve, the global attitude towards the internet needs to adapt. For international law to successfully combat cyber threats, the framework of the laws being

written must be constructed with future technologies in mind. Forward-thinking is necessary as technology will always rapidly develop and progress faster than the laws exerting control over those technologies and how they are used. Some of the issues and technologies that are only now being seriously debated have been discussed in the theoretical for years. The obvious elephant in the room is artificial intelligence.

Today, Artificial Intelligence has very little legislative oversight at either the national or international level. The most useful type of artificial intelligence that has been widely implemented in recent years is machine learning (Burri, 2017). The implementation of such models has brought plenty of concerns with it. Growth occurs at an exponential rate, and with that growth has come the assertion that artificial intelligence needs to be examined to see if it meets the standard to qualify as being a legal person, or individual under the law (Burri,2017). Such a person would certainly be subject to international law in the country it resides. In the European Union, if one member state recognizes an A.I. entity as a person, then all other member states must as well. In such a situation, one could act as the parent, creating the algorithms for the entity, and profit from them (Burri, 2017). This creates many questions regarding personhood of an entity and its intelligence when it comes to the entity being classified as a type of being. When exploring the possibility of autonomous weapons systems that could be operated by A.I. in Geneva, it was maintained that these systems should be subject to human control in a capacity that could shut it down or take over (Burri, 2017). This all but guarantees that fully autonomous weapons will most likely be banned at some point. In relation to warfare, this goes beyond merely missiles or planes. As we edge closer to the first cyberwar, A.I. will likely have a major role to play when it comes to satellite imagery and surveillance, among other tasks to perform (Burri, 2017). As artificial intelligence continues to grow and receives

investment at a rapidly growing pace, it will be harder to study all the implications it brings with it, and to create ethical standards to counterbalance those implications. Currently, the IEEE has 10 public working groups on standards designed to address issues like transparency and privacy (Burri, 2017). Privacy is key when it comes to how the A.I. is using data owned by others, especially if it is being fed that data by human operators.

Military activities could potentially make extensive use of A.I. as a weapons system. Tools that are currently available and continuing to grow would allow an A.I. entity to become the ultimate cyber squadron mate (Guyonneau & Le Dez, 2019). Such an entity could give fighters access to information and an awareness of the battlefield they otherwise would not possess. This in turn could allow for better coordination and give commanders an enhanced level of control over the battlefield (Guyonneau & Le Dez, 2019). A.I. also has applications when it comes to augmented reality. It could potentially identify weapons, people, and places, among other things, giving a warrior all the intelligence they need during combat missions or undercover operations in support of combat missions (Guyonneau & Le Dez, 2019).

As A.I. continues to develop, it will be important to encourage cooperation between allies and international organizations to find solutions for ethical issues and create policy regarding the use of A.I. both domestically and militarily. Such power has the potential to be devastating if used for the wrong purposes, and there is a high probability that it will be used by our adversaries. When these policies and regulations are eventually written, both at a national and international level, it will be prudent to redetermine what constitutes deadly force or a serious enough act of agression. Once this determination is made, it can be used to determine appropriate response mechanisms when either the United States or its allies are attacked with such tools or weapons.

Great risk continues to be posed with a lack of international law regarding cybersecurity as threats continue to evolve and users, organizations, and governments are put at risk. As threats evolve, catching up on passing legislation to address concerns will become more trying, and working with our enemies rather than against them will become necessary for everyone's digital survivability. Russia and China have tried to propose international treaties, but these attempts have not garnered much support (Mačák, 2016). It will be crucial to involve nations like Russia, China, Iran, and North Korea in the discussion and development of treaties related to cybersecurity if we are to even hope to minimize the risk of cyberthreats or cyberwar. It is past time for the governments of the world to move away from relying on non-state-oriented forums for determining the application of international law in cyberspace (Hollis, 2021).

While countries move toward the goal of banding together to interface with each other and move towards the common goal of addressing these cybersecurity threats throughout the world, it is important to recognize that there is still much work to be done. As the physical world continues to integrate itself further with the digital world, countries need to align themselves on a common goal of securing cyberspace as no hard sovereign boundaries exist in the same way there, and where boundaries are needed, determine how they apply. This approach should involve having as many nations sitting at the table as possible. Cooperation can lead to fruitful progress, and we may find that we have more in common than we think as diplomatic relations are formed on the foundations of cybersecurity policy.

References

Bowman, C. M. (2021, March 3). *US-EU safe harbor invalidated: What now?*. Proskauer on Privacy. https://privacylaw.proskauer.com/2015/10/articles/european-union/us-eu-safe-harbor-invalidated-what-now/#:~:text=The%20CJEU%20went%20on%20to,requirements."%20See%20¶%2087.

Burkadze, K. (2016, May 20). *Cyber Security and international law*. Journal of Technical Science and Technologies. https://jtst.ibsu.edu.ge/jms/index.php/jtst/article/view/75

Burri, Thomas. (2017). International Law and Artificial Intelligence. *German Yearbook of International Law, 60,* 91-108.

Council of Europe. (2001, November 23). *Convention on cybercrime (ETS no. 185)*. European Parliament. https://www.europarl.europa.eu/cmsdata/179163/20090225ATT50418EN.pdf

Council of Europe. (2023, November 16). *Impact in 46 countries - the European Convention on Human Rights - www.coe.int*. The European Convention on Human Rights. https://www.coe.int/en/web/human-rights-convention/impact-in-46-countries

Cherry, L. M., & Pascucci, P. P. (2023, January 27). *International law in Cyberspace*. American Bar Association. https://www.americanbar.org/groups/law_national_security/publications/aba-standing-committee-on-law-and-national-security-60-th-anniversary-an-anthology/international-law-in-cyberspace/

Guyonneau , R., & Le Dez, A. (2019). *Artificial Intelligence in Digital Warfare: Introducing the Concept of the Cyberteammate*. The Cyber Defense Review. https://cyberdefensereview.army.mil/Portals/6/Documents/CDR%20Journal%20Articles/Fall%202019/CDR%20V4N2-Fall%202019_GUYONNEAU-LE%20DEZ.pdf?ver=2019-11-15-104106-423

Hollis, D. B. (2021, June 14). *A brief primer on International Law and Cyberspace - Carnegie Endowment for international peace*. Carnegie Endowment For International Peace. https://carnegieendowment.org/posts/2021/06/a-brief-primer-on-international-law-and-cyberspace?lang=en

Hoofnagle, C. J., van der Sloot, B., & Borgesius, F. Z. (2019). The European Union general data protection regulation: what it is and what it means*. *Information & Communications Technology Law*, *28*(1), 65–98. https://doi.org/10.1080/13600834.2019.1573501

K. Mačák, "Is the international law of cyber security in crisis?," *2016 8th International Conference on Cyber Conflict (CyCon)*, Tallinn, Estonia, 2016, pp. 127-139, doi: 10.1109/CYCON.2016.7529431.

North Atlantic Treaty Organization. (2024, July 10). *Allies agree new NATO Integrated Cyber Defence Centre*. NATO. https://www.nato.int/cps/en/natohq/news_227647.htm#:~:text=The%20Centre%20will%20bring%20together,enhance%20collective%20resilience%20and%20defence.

Saunders, D., & Reifman, S. (2021, April 27). *The case for a global data privacy adequacy standard*. International Association of Privacy Professionals. https://iapp.org/news/a/the-case-for-a-global-data-privacy-adequacy-standard