International Law in The Context of Cybersecurity

Cyberspace and other digital elements are still relatively new in our world. We have had wars for hundreds of thousands of years, but the idea of a war or even crime taking place in a meta-physical place is pretty much brand new. International law is slowly catching up to this new form of warfare and crime. The concepts of international laws are even more important in this fight for global peace because "the fight against cyber-crime either is a global one or it makes no sense at all (Broadhurst, 2004)." This is due to the fact that more and more of these cyber and digital elements continue to become more pervasive and interconnected in all of our lives. Cyber attacks and cyber crimes can hit you from anywhere. Often times these attacks are across a multitude of different jurisdictional boundaries with attackers routing these attacks through various jurisdictions meaning that these attacks require cross-border co-operation and an international policing response (Adonis A., 2020). This paper will be discussing further the need for international laws in the context of cybersecurity, what the current international landscape looks like in context of cybersecurity, and the many challenges international lawmakers face when creating and enforcing these laws.

International law is incredibly important for keeping peace in the world and help assign accountability to the many states that make up our world. Most importantly international laws serve to protect sovereignty and protect states from the intervention into their 'internal affairs' (Moynihan, 2020). These laws include treaties which help bring wars to an end and allow peace to endure past hard times, human rights laws which hold countries to a standard, laws defining the rules surrounding environmental protections, and more. There are even laws setting out rules for areas we once did not know much about or even fully explored like space laws. One distinguishing factor that sets cyber law outside of these other different laws is the fact that governance of cyberspace did not begin with any state or government (Hollis, 2021). Governing of cyberspace began with academic institutions and private actors. With the internet's commercialization, information and commercialization technologies (ICT) organizations became major stakeholders in the entire cyber-sphere we live in today. What makes these ICT organizations even more important though is that their platforms act as a breeding ground or fence yard for the vast majority of cyber behavior (Hollis, 2021). This can range from someone posting a meme about the newest episode of the bachelor all the way to a cyber disinformation campaign. It could be someone sending an invitation to their wedding all the way to someone sending a phishing email or a malicious message filled with malware. Overall, it is not only the states that have some form of stake in the cyberspace. Organizations like Apple, IBM, Microsoft, Dell, Amazon, and more all have some kind of hand in the digital cybersphere we live in today. One example I believe exemplifies this fact is that state-sponsored activity or spying occurring on Apple and Google devices (Satter, 2023). States are going directly to mega-corporations like Google and Apple to request sensitive information on users. This leaves these massive ICT organizations in a precarious position filled with power and influence unlike anything else we have seen up to this point.

Currently there are three dominant parties in the fight on how the cyberspace should be regulated: liberal institutionalists, cyberlibertarians, and statists. Liberal institutionalists call for the importance of international institutions and rule-based multilateralism in managing cyber space (Adonis A., 2020). A cyberlibertarian are pretty much the exact opposite of liberal institutionalists, they believe that cyberspace should remain free from tyranny and any form of oppressive rule that may hinder the internet's liberty (Adonis A., 2020). Our last a final party, statists, believe that it is the states' own responsibility to formulate national and international law on how cyberspace should be governed (Adonis A., 2020). These three factions each fight for the development of international law in the cybersphere and also somewhat hinders their development due to the ongoing debates surrounding three core principles: jurisdiction, arbitration, and legal instruments and jurisprudences (Adonis A., 2020).

There are a ton of different actors or agents in the cyber realm. There are individuals who may just be scrolling through TikToks, individuals who are hackers who may be state-sponsored or acting independently, a range of different corporations, state actors, and more. All of these agents have the ability to conduct business, launch an attack, communicate, and just about everything else from one corner of the globe to the other. The major issue surrounding all of this though is how lawmakers can define when that action falls under the jurisdiction of international law. The internet inherently provides some form anonymity and the fact that the technology to maintain this anonymity continues to improve actually attributing or making the distinction between state and non-state sponsored activities has become increasingly difficult. With this anonymity also comes the challenge of determining where a potential violator of international law is really located. Bad actors can re-route themselves all over the place and make themselves untraceable. Altogether, all of these factors create major hurdles for lawmakers to jump through when creating international laws.

Arbitration ensures that these laws are enacted and that the members remain accountable to the law. When it comes to cyber security law, the wide range and diversity of agents in the cybersphere makes coming to a consensus on this issue incredibly difficult. Each of these agents have their own interests and as a result there is still no agreed legal norm on how we should dispute settlement mechanisms and arbitration (Adonis A., 2020). However, the Permanent Court of Arbitration in The Hague, Netherlands may be able to fulfill this blank space as they have already set mandates on other topics like outer space, energy, and environmental cases (Adonis A., 2020).

Then when we look towards the challenges legal instruments and jurisprudence, we can find a distinction between how states have already decided their rules on a national and international level. Countries like the United States or France have taken a stance and prioritized privacy over security concerns while Russia has thrown privacy to the side in favor of security (Adonis A., 2020). These different state actors have incredible different beliefs and interests which makes it incredibly difficult to come to any kind of consensus.

Aside from the Budapest Convention on Cybercrime and the African Union Convention on Cyber Security and Personal Data Protection international law does not really have any tailor-made rules for regulating cyberspace due to these issues (Hollis, 2021). The Budapest Convention on Cybercrime is an international treaty designed to focus on the sudden rise in cybercrime (Budapest Convention). This treaty aimed to improve investigative techniques, increase cooperation among nations, and harmonize national laws (Budapest Convention). 64 countries came together and laid out this legislation to outlaw certain cyber-related crimes along with defining several evidence-gathering rules (Budapest Convention). The not-yet-in-force African Union Convention on Cyber Security and Personal Data Protection aims to lay out a legal framework for addressing cybercrime and data protection in Africa (Sheik, 2023).

In addition to the difficulty of establishing these international laws there is also the massive debate as to how already existing international laws apply to cybersecurity (Hollis, 2021). These issues can be broken up into five different categories: silence, existential disagreements, interpretative challenges, attribution and accountability (Hollis, 2021). Many states have chosen to remain silent in the international debate as a way to avoid international disputes or because they lack the personnel or resources to understand the issues involved in applying international law (Hollis, 2021). This creates an issue when creating these massive international laws because it requires all of these different states coming to a consensus. Everyone needs to have some sort of say so we can all come to an agreement because the fight on the digital battlefield is a global one or no fight at all. Then when we look towards existential disagreements on what should be included or excluded in international law in context of cybersecurity. For example, in the UN, states have “challenged the availability of international humanitarian law, the right of self-defense, the duty of due diligence, and the right to take countermeasures with respect to online activity (Hollis, 2021).” All of these can have major implications on how international laws can be applied. More importantly, they have major consequences when we look towards how states partake in cyber operations during a war, how states respond to state-sponsored cyber activity, or how a state may protect other countries from internal malicious cyber activity aimed at a third party (Hollis, 2021). Interpretive questions come into play when we look towards topics like nonintervention, sovereignty, and human rights. These topics are completely new to our world. Our laws are not tailored to the digital environment. We have laws focused on the physical realm and figuring out how these physical rules apply to a digital world have caused a bit of a speedbump. Attribution is a major player in the headache that is international law in the context of cybersecurity. To apply international law in cyberspace you need to know who is responsible for the attack. Is this individual or group a state or state-sponsored actor? Is this individual or group acting on their own volition? These are incredibly difficult questions to answer in the digital age. This is what makes attribution so difficult. Technology advancements and different jurisdictions have created an even more toxic environment to form attribution and figuring out how to apply international law. So, they must identify where the attack is originating from which is near impossible. Then they must show evidence that the bad actor is state sponsored which is even more difficult because states often use proxies to conduct their cyber operations (Hollis, 2021). The final issue of accountability has been difficult because without proper legal framework on the international law states can not call international law on unwanted behavior because it may be considered legal under our current legal rhetoric (Hollis, 2021).

Overall, the situation may sound frightening and quite grim. One may wonder what the future of the digital age may look like and if we can really move forward. I believe that we are currently in the wild west stage of international law in the context of cybersecurity. These challenges and hurdles we are facing are inevitable when a new form of life-changing technology enters our domains. This technology is also unlike anything humankind has ever seen before. It would be unimaginable for someone living in 1940 to imagine a world where someone could launch massive attacks on a worldwide scale in a non-physical space. Figuring out the rules of the new game we are playing may take a while, but we will figure it out. As we move forward states look at how our current International Laws may apply and as we progress, we will come to a consensus on new laws to fill in the cracks in our existing infrastructure. One fight that sticks out to me is what end-state we will end up choosing (Hollis, 2021). Some states focus on protecting states from people while others aim to protect the people from the states. The former aims to protect the security of the states by taking a more authoritarian approach. They may want to create rules to protect states from individuals from produce subversive speech or anything that threatens the security of the state online (Hollis, 2021). The latter aims to protect the people from the states by creating data protection laws or prohibiting states from engaging in malicious cyber activity against critical infrastructure (Hollis, 2021). I believe we will end up somewhere in the middle. We will have to surrender some of our privacy to the states, but we are able to create laws that will protect our cyberspace and help create a safer cyberspace with proper rules so we can successfully hop over the hurdles that we face today.

References

Adonis A., A. (2020). International Law on Cyber Security in the Age of Digital Sovereignty. *E-International Relations*.

Broadhurst, R. (2004). Developments in the Global Law Enforcement of Cybercrime. *PIJPSM*.

Budapest Convention. (n.d.). Retrieved from BYJU's Exam Prep: https://byjus.com/free-ias-prep/budapest-convention/#:~:text=Primarily%20known%20as%20the%20Council,force%20on%20July%201%2C%202004.

Hollis, D. (2021, June 14). *A Brief Primer on International Law and Cyberspace*. Retrieved from Carnegie Endowment for International Peace: https://carnegieendowment.org/2021/06/14/brief-primer-on-international-law-and-cyberspace-pub-84763

Moynihan, H. (2020). The vital role of international law in the framework forresponsible state behaviour in cyberspace. *Journal of Cyber Policy*.

Satter, R. (2023, December 6). *Governments spying on Apple, Google users through push notifications.* Retrieved from Reuters: https://www.reuters.com/technology/cybersecurity/governments-spying-apple-google-users-through-push-notifications-us-senator-2023-12-06/

Sheik, S. (2023, April 24). *AU Convention on Cyber Security and Personal Data Protection | Malabo Convention.* Retrieved from Michalsons: https://www.michalsons.com/blog/au-convention-on-cyber-security-and-personal-data-protection-malabo-convention/65281#:~:text=In%202014%2C%20the%20African%20Union,signed%20up%20to%20it%20already.