Lab Assignment 03:

UN International Law

Micah Flack

Department of Computer Science, Dakota State University

CSC 840 DT1, Cyber Operations I

Dr. Michael Ham

September 16, 2022

UN Charter

Within the spirit of the laws set by the UN Charter, the articles should be enough to cover any form of cyber warfare. Regardless of whether those attacks are kinetic in nature or completely digital, the articles solely define the events warranting a response from the security council as any “threat to the peace, breach of the peace, or act of aggression” under chapter(7), articles 39 to 51 (Nations, n.d.). Given the formation of military units within governments like the United States, specifically United States Cyber Command (USCYBERCOM) or the rumored EquationGroup from the National Security Agency (NSA), we can assume that a broad international adoption of article 51 will be used to justify retaliatory military intervention.

However, this becomes an incredibly vague problem given permanent members of the security council engaging in unprovoked acts of aggression and, there are some who do not consider cyber-attacks a form of aggression unless kinetic forces are used. Specifically, article 27 of the UN Charter which provides that any permanent member of the security council (The Republic of China, France, the Union of Soviet Socialist Republics, the United Kingdom of Great Britain and Northern Ireland, and the United States of America) is allowed the right to veto any such decisions regarding acts of aggression. This means that if any of the permanent members were to engage in unprovoked warfare, it would be difficult to hold them responsible within the framework of the UN Charter because of their unilateral ability to block those actions (Madubuike-Ekwe, 2021).

Targets

Article 41 of the UN Charter says that the security council may use armed forces as a response to acts of aggression against targets that may include “complete or partial interruption of economic relations and of rail, sea, air, postal, telegraphic, radio, and other means of communication, and the severance of diplomatic relations”. Under international humanitarian law (IHL), or jus in bello, warfare is conducted in a way where efforts are made to minimize the suffering caused. It also specifies that certain targets are

prohibited, such as medical units and transports, cultural property, the natural environment, or works and installations containing dangerous forces (*What Objects Are Specially Protected under IHL? | The ICRC in Israel, Golan, West Bank, Gaza*, n.d.). Regardless of the target though, the goal is for any warfare to be carried out in way that minimizes the number of casualties (Marr, n.d.). Stuxnet is the textbook example used because of the discrimination between civilian and military targets, although this could be a violation considering the target contained dangerous materials and had things gone otherwise, we would be looking at it from a different perspective.

On a much smaller scale, in 2016 a group of Iranian hackers gained access to a SCADA system that controlled the Bowman Dam in Westchester County, New York (Berger, 2016; *Manhattan U.S. Attorney Announces Charges Against Seven Iranians For Conducting Coordinated Campaign Of Cyber Attacks Against U.S. Financial Sector On Behalf Of Islamic Revolutionary Guard Corps-Sponsored Entities*, 2016). Which, unlike the Hoover Dam that controls the Colorado River, if the Bowman dam were overflowed it would cause minimal damage and be far from a national incident. The reasons this might cause concern though is if a malicious operator were to gain access to a similar system that controls a major dam, like the one responsible for the Henan flood in China, it could cause not only massive damage to the natural environment or cultural sites but a loss of human life as well (Press, 2021; Wang & Plate, 2002).

Tallinn Alternatives

Opened for signatures in 2001 and fully enforced in 2004, 65 countries have since ratified the Budapest Convention as a global treaty for cybercrime (“Cybercrime Is Dangerous, But a New UN Treaty Could Be Worse for Rights,” 2021; Pawlak et al., n.d.). The treaty has since helped other countries to communicate international cybercrime more easily, while also providing avenues for developing countries to gain the necessary tools and resources to combat cybercrime within their own borders. Besides the Budapest Convention, there has been more participation on-behalf of intergovernmental organizations like G20, G7, BRICS, ECDC, NATO, WTO, ILO and OSCE. For example, Tallinn Manual 2.0 on

the International Law Applicable to Cyber Operations by the NATO which we have already discussed for this week. But most of international activity has been limited to generating awareness and suggestions or proposals for new resolutions and legislation (Tikk & Kerttunen, 2020).

There are, however, two promising initiatives currently being introduced. One is led by Microsoft, called the Digital Geneva Convention (*A Digital Geneva Convention to Protect Cyberspace | Microsoft Cybersecurity*, n.d.) that has persuaded 40 companies around the world to sign the Cyber Security Technology Agreement. It aims to create an international traceability organization for cyberattacks led by the signatories to identify and track threat actors while also providing governments, businesses, and the public with technical evidence. The other initiative is led by Russia in the form of a UN resolution for countering the use of information and communications technologies for criminal purposes ("Cybercrime Is Dangerous, But a New UN Treaty Could Be Worse for Rights," 2021). Although, this proposal has been met with opposition by many of the Budapest Convention signatories because they believe it is too loosely defined and would allow for human rights violations. Either of these proposals are significant since they will have some impact on cybersecurity, positive or negative, should they pass; it also increases public awareness and drives new discussions about how we need to interact globally in the digital age.

UN Charter Gap

We previously mentioned it before when discussing the UN Charter, but the language used within the articles is often seen as too vague and poorly enforced. Not to mention the other issues surrounding permanent members on the security council who cannot be removed, having absolute authority over decisions impacting responses towards acts of aggression which they provoked. This is especially relevant considering the recent war between Russia and Ukraine. And, in even earlier years the conflicts between Russia, Crimea, and Georgia. Which should also go without mentioning the numerous cyberattacks as they relate to these conflicts: Black Energy, Kill Disk, TeleBots, Industroyer/Industroyer2,

Crash Override, Eternal Petya, NotPetya, Grey Energy, Hermetic Wiper, Isaac Wiper, and Caddy Wiper (Greenberg, 2019). It would be fair to say then, that the UN Charter lacks the necessary power to enforce anything regarding cyberattacks in the 21st century.

References

A Digital Geneva Convention to protect cyberspace | Microsoft Cybersecurity. (n.d.). Retrieved September 16, 2022, from https://www.microsoft.com/en-us/cybersecurity/content-hub/a-digital-geneva-convention-to-protect-cyberspace

Berger, J. (2016, March 25). A Dam, Small and Unsung, Is Caught Up in an Iranian Hacking Case. *The New York Times*. https://www.nytimes.com/2016/03/26/nyregion/rye-brook-dam-caught-in-computer-hacking-case.html

Cybercrime is Dangerous, But a New UN Treaty Could Be Worse for Rights. (2021, August 13). *Human Rights Watch*. https://www.hrw.org/news/2021/08/13/cybercrime-dangerous-new-un-treaty-could-be-worse-rights

Greenberg, A. (2019). *Sandworm: A new era of cyberwar and the hunt for the Kremlin's most dangerous hackers* (First edition). Doubleday.

Madubuike-Ekwe, J. N. (2021). Cyberattack and the Use of Force in International Law. *Beijing Law Review*, *12*(02), 631–649. https://doi.org/10.4236/blr.2021.122034

Manhattan U.S. Attorney Announces Charges Against Seven Iranians For Conducting Coordinated Campaign Of Cyber Attacks Against U.S. Financial Sector On Behalf Of Islamic Revolutionary Guard Corps-Sponsored Entities. (2016, March 24). https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-announces-charges-against-seven-iranians-conducting-coordinated

Marr, C. (n.d.). *Cyberwarfare and Applied Just War Theory: Assessing the Stuxnet Worm through Jus ad Bellum and Jus in Bello*. 12.

Nations, U. (n.d.). *United Nations Charter (full text)*. United Nations; United Nations. Retrieved September 16, 2022, from https://www.un.org/en/about-us/un-charter/full-text

Pawlak, P., Abdel-Sadek, A., Dominioni, S., & Youmna, A. M. (n.d.). *GREAT EXPECTATIONS: DEFINING A TRANS-MEDITERRANEAN CYBERSECURITY AGENDA*. *22*, 85.

Press, T. A. (2021, July 21). China Blasts Dam To Divert Massive Flooding That Has Killed At Least 25. *NPR*. https://www.npr.org/2021/07/21/1018764692/china-blasts-dam-to-divert-massive-flooding-that-has-killed-at-least-25

Tikk, E., & Kerttunen, M. (Eds.). (2020). *Routledge handbook of international cybersecurity*. Routledge, Taylor & Francis Group.

Wang, Z.-Y., & Plate, E. J. (2002). Recent flood disasters in China. *Proceedings of the Institution of Civil Engineers - Water and Maritime Engineering*, *154*(3), 177–188. https://doi.org/10.1680/wame.2002.154.3.177

What objects are specially protected under IHL? | The ICRC in Israel, Golan, West Bank, Gaza. (n.d.). Retrieved September 16, 2022, from https://blogs.icrc.org/ilot/2017/08/14/objects-specially-protected-ihl/