Regulating Cyber Warfare Through the United Nations

Cadet Andrew Luzzatto

ABSTRACT

Cyber warfare is an emerging type of conflict threatening international establishments such as international humanitarian law and the norms guiding interactions between states. Currently, with no means to slow down their use, the rate at which cyber weapons are being produced and launched between states is growing. One organization that can change that is the United Nations. The United Nations possesses several facilities that make it a powerful tool to address the ever-expanding problem of international cyber security. While other options for imposing regulations exist, state governments should favor the United Nations as the premier platform to address this issue.

INTRODUCTION

Throughout the 21st century, a consensus of academics and policymakers agree that the continuing power and significance of modern cyber weapons threatens state norms and international law. Recent cyber-attacks have demonstrated blatant violations of international humanitarian law and the Universal Declaration Of Human Rights, as well as less concrete intrusions of national sovereignty. This stems partly from a lack of regulations addressing the issue. As of now, there is no internationally recognized definition for cyber weapons, no specific treaties that regulate them, and no means to prevent their use and rapid proliferation. Though there has been much discussion regarding different treaties and regulations that could be implemented to address cyber warfare, the question of how to implement these policies remain mostly unanswered. In other words, there is no present consensus on the means or the venue to discuss this problem. As the United Nations is a multilateral body with experience dealing with

Mr. Andrew J. Luzzatto is a fourth-year cadet at Norwich University majoring in Computer Security and Information Assurance. His coursework extends into cyberlaw, international relations, and ethics in computing and technology. For the past six years, he has participated in both high school and collegiate Model United Nation's programs. He is also member of the National Science Foundation CyberCorps Scholarship for Service Program, which pays for two years of undergraduate education in exchange for two years of service in the public cybersecurity sector.

unconventional weapons, it is the ideal organization to address this issue, as it possesses both the means and mandate to regulate cyber warfare.

ISSUES WITH CYBER WARFARE

Lack of a Standard Definition

Similar to terms like "terrorism" and "hybrid warfare," it is difficult to define what exactly "cyber warfare" and its related terms ("cyber-attack," "cyber-espionage," etc.) are. In fact, the definition of the word "cyberspace" itself is still a matter of debate, with different countries and international organizations prescribing different meanings in different situations.[1] While several proposals have been made by states and academics alike, no single definition seems to be comprehensive enough to fully encompass the issue and to address the concerns of most governments.[2]

An example of such an attempt to set these definitions as they related to international law is the Tallinn Manual on International Law Applicable to Cyber Warfare. Written in 2013 by a group of twenty international experts on the subject, the Tallinn Manual seeks to informally resolve the confusion regarding the regulation of cyber warfare.[3] The manual itself is made of a set of 95 rules that states should follow when conducting cyber operations.[4] Though this document effectively addresses several points of ambiguity surrounding international cyber warfare (including its related definitions), it functions only as an academic work.[5] This stipulation makes the document potentially useful for the creation of new international definitions and laws, but not suitable as a legally binding interpretation of international law.

Without a standard international definition, states can modify the meaning of the term "cyber warfare" according to their interests. For example, consider the Russian Federation's definition of an alternate term, "information warfare," which is defined in part as a

"conflict between two or more States in the information space with the goal of...carrying out mass psychological campaigns against the population of a State in order to destabilize society and the government."[6] This definition specifically addresses destabilization, which allows Russia to label social media posts, news stories, and blogs that oppose the interests of the Russian government as information warfare. The Shanghai Cooperation Group (of which Russia is a member) maintains a similar definition.[7] Critics of this definition of information warfare are concerned that it validates state censorship.[8] In an effort to sidestep this problem, states steer away from terms like "information warfare" and "information security" during international discussions on cyber regulations.[9]

Difficulty Applying International Norms and Laws

The way that cyber warfare relates to the established laws and norms that drive international relations is still unsettled. States and scholars do not yet know how the ideas of damage, sovereignty, and privacy apply to cyberspace. The relationship between cyber warfare and the principle of the use of force is chief among these concerns. According to the UN Charter, Chapter I, Article 2, Paragraph 4 and Chapter VII, Article 51, state actors can only use force as a form of self-defense against an armed attack.[10] Without proper international regulations that address the status of cyber weapons, states who consider cyber-attacks equivalent to armed attacks can justify their use of retaliatory strikes in the name of self-defense. While this has not yet occurred or been formally codified, the US has stated that it reserves the right to respond to enemy cyber-attacks "as we would to any other threat to our country."[11] Similarly, the North Atlantic Treaty Organization (NATO) has declared that it may, under currently undefined circumstances, consider a cyber-attack against any member state as an armed attack that would trigger the organization's Article V "collective defense measure."[12] Considering that these two entities have developed their own definitions for cyber warfare, and that these definitions differ from those of their competitors', namely the Shanghai Cooperation Group, there is a possibility that an unresolvable legal debate could erupt from a cyber-attack.

The attribution and identification of attacks are also major issues in cyberspace. Because cyber weapons are designed to exploit vulnerabilities unknown to the target, administrators often do not know they are being attacked until it is too late. The secret nature of cyber-attacks also makes it challenging, but not impossible, to identify the perpetrators of an attack.[13] It is even more difficult to address whether the culprit is working with a state government.[14] Even after a specific group or individual has been identified as the source of an attack, state governments can (and often do) deny any affiliation. Such was the case with the WannaCry ransomware virus. When the US attributed the virus to a member of the North Korean government, the North Korean Foreign Ministry promptly replied that the issue "has nothing to do with us."[15] States are easily able to deny and avoid affiliation with groups conducting cyber-attacks. This has disrupted the idea of deterrence, as retaliation against a state government could be interpreted as a first use of force and not as an act of self-defense.

Ethical Concerns

Several state actors, to include Israel, Iran, and Russia, have started utilizing civilians, private businesses, and critical health, water, and electrical infrastructure as targets in cyber warfare campaigns. Such a situation occurred in an exchange of cyber-attacks between Israel and Iran in the spring of 2020, when both states targeted elements of civilian infrastructures, including Israeli water treatment plants and privately owned business systems at Iran's Shahid Rajaee Port.[16] A similar incident occurred in December of 2015, when Russian hackers (who were possibly linked with the Russian government) launched a cyber-attack against several Ukrainian power plants, causing over 200,000 people to lose power.[17] State and non-state actor use of cyber espionage against civilian targets has also become immensely popular, though that practice is beyond the scope of this article.

International humanitarian law dictates that a distinction between combatants and civilians must be maintained in all forms of conflict.[18] In certain situations, this can be extremely difficult, as private infrastructure is usually intertwined and sometimes indistinguishable from military targets. Military organizations use the same computers, programs, networks, privately owned infrastructure, and cloud service providers as other internet users. In short, the dual-use nature of cyber infrastructure can leave civilian targets in the way of dangerous cyber-attacks.

OTHER OPTIONS FOR CONFRONTING THE ISSUE

Bilateral Agreements

Bilateral discussions and treaties play a crucial role in preventing and regulating all forms of warfare, including cyber. Whenever a cyber-attack occurs, the first channels used to discuss the issue are those established between the target and the perceived perpetrator. Within these venues, states can discuss possible resolutions to issues in cyberspace before escalating to other means. Additionally, discussions about cyber warfare within these forums allow states to gain a clearer understanding about each other's policies and objectives.[19]

The problem with bilateral agreements is that they, by their very nature, only settle disputes between two states. They fail to address the impact cyberspace has had on the world as a whole.[20] Additionally, bilateral treaties tend to be more fragile than larger, multilateral treaties.[21] This may be because of a lack of additional states and entities providing accountability for state actions. As accountability is one of the key concerns for cyber warfare, bilateral agreements alone cannot fully regulate the practice of conflict in cyberspace.

Regional Bodies

Regional bodies can help states collectively identify and classify cyber security threats. In these larger, multilateral organizations, discussions are centered around the larger, persistent security concerns faced by the group.[22] Groups like NATO and the European Convention on

Cyber Crime are a few examples of organizations effectively defining terms and regulating actions in cyberspace.[23]

There is skepticism within the international community as to how effective a regional body can be at accommodating and incorporating the policies of other countries into their framework. While regional bodies are effective at forming a consensus among like-minded parties, they fail to resolve conflicting ideas between separate groups, including differing ideas on definitions for cyber warfare. Such a concern was voiced by Brazil, China, and India regarding the European Convention on Cyber Crime. Though the convention has played a critical role in helping to define and regulate specific cybercrimes, these states still fear that the treaty is "inherently inapplicable to non-European countries."[24] Despite a lack of evidence to substantiate these concerns, with international politics, a country's perception is often just as important as the reality of the situation. Therefore, cyber warfare still needs a global platform where all state governments have a chance to impact the outcome.

WHY CHOOSE THE UNITED NATIONS

Bureaucratic Infrastructure and Mandate

Since its foundation in 1945, the UN mandate has and continues to address threats to international security, to promote the principles of self-determination and human rights, and to become "a centre for harmonizing the actions of nations" as they attempt to do the same.[25] As cyber warfare is intimately intertwined with each of these issues, the UN's responsibility to address the status of cyber weapons is indisputable.

To fulfill its mandate, the UN Charter establishes a comprehensive infrastructure of different subsidiary bodies, referred to in the Charter as "organs," capable of individually addressing specific aspects of multifaceted issues like cyber warfare. The unity of these various organs under a single body allows for the standardization, codification, and coordination of terms, treaties, and efforts to regulate cyberspace.

The General Assembly

The first and most well-known of these aforementioned organs is the General Assembly. The General Assembly is unique in that every member state (and some non-state actors) can participate.[26] For this reason, during certain parts of the resolution-writing process, the General Assembly is considered an equalizer among states of varying degrees of power.[27] With such a high rate of participation, the General Assembly provides what may be the only platform for discussing issues that require international consensus. Given that cyber warfare is an international issue that bleeds across geography, the General Assembly is well-poised to address issues in cyberspace.

While policy scholars are correct that the resolutions produced by the General Assembly are not legally binding,[28] these resolutions remain significant in the international community.

According to the late Oliver Lissitzyn, a renowned legal scholar, unanimous decisions like those made in the General Assembly can represent internationally recognized expectations for state behavior.[29] Discussions held in the General Assembly are equally invaluable in allowing countries to express their individual policies for specific matters of security. In effect, the General Assembly can clarify common ground between states on matters of cyber security.

The General Assembly also has the authority to launch studies into security issues like cyber warfare.[30] Such an action has already been taken by the UN under resolution A/RES/58/32, which declared the creation of a Group of Governmental Experts (GGE) to discuss the confluence of information and communication technology development and international security.[31] Since its first session in 2004, this group has produced several reports detailing concerns for interactions in cyberspace, including several of the aforementioned points found in part one of this article. These reports have effectively laid the groundwork for future efforts to regulate cyber warfare while simultaneously proving that the General Assembly can and has added meaningful contributions to the subject matter.

The Security Council

Another organ defined within the UN Charter is the Security Council. Unlike the General Assembly, the Security Council consists of five permanent members and ten additional members elected for two-year terms.[32] The Security Council has the unique capability to pass resolutions that all member states are required to follow.[33] This allows the Security Council to set legally binding precedents for international relations in areas like cyber warfare. Additionally, all initiatives passed by the Security Council have the full support of its permanent members, as a single vote by a permanent member against a resolution will prevent it from being accepted.[34] While this rule can delay the adoption of regulations, it grants the benefit of consensus from such major global powers as the United States, China, and Russia, all of which are permanent members of the Security Council.[35]

The Security Council has the authority to discuss matters that pose a significant and immediate threat to international security and human life.[36] Examples of this range from long term security situations, such as Iran's development of nuclear weapons,[37] to more specific events, such as the Six-Day War in 1967.[38] The international community can leverage the powers of the Security Council as a means to address situations where bilateralism fails to reduce tensions following a cyber-attack.

CONCLUSION

There are some well-founded concerns with using the UN to handle cyber warfare. First among these is the simple fact that the UN has failed to prescribe a definition to cyber warfare in nearly two decades of addressing the issue. As of now, most of the UN's efforts in cyberspace have been directed towards helping states build up their cyber defense capabilities. However,

it is important to remember that developing taxonomies and regulations for weapons systems is normally a slow process. The term "weapon of mass destruction" was only given an internationally recognized definition in 1977 through General Assembly resolution A/RES/32/84,[39] nearly three decades after the term was first used in a UN resolution in 1947.[40] The first treaty effective at regulating chemical warfare, the Chemical Weapons Convention of 1993, was first open for signing almost eighty years after the first use of chlorine gas as a weapon in World War I.[41]

Keeping this in mind, it should come as no surprise that the international community does not yet have a mechanism to completely address and counter cyber warfare. It is indeed possible that it may take the UN another five to ten years of discussion in the General Assembly before a definition is finally decided, and still decades more before a comprehensive treaty regulating cyber warfare is organized. Nevertheless, this should not dissuade countries from taking advantage of the functions and infrastructure that the UN provides.

DISCLAIMER

The views expressed in this work are those of the authors and do not reflect the official policy or position of the United States Military Academy, the Department of the Army, or the Department of Defense.

NOTES

1. Alexander Klimburg, ed. *National Cyber Security Framework Manual* (Tallinn, Estonia: NATO Cooperative Cyber Defense Centre of Excellence, 2012), 8, https://www.ccdcoe.org/uploads/2018/10/NCSFM_0.pdf.
2. Ibid., 17.
3. Michael N. Schmitt, ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare*, New York: Cambridge University Press, 2013, accessed October 3, 2022, https://ebookcentral.proquest.com/lib/norwich/detail.action?docID=1113076.
4. Priyanka R Dev, ""use of Force" and "Armed Attack" Thresholds in Cyber Conflict: The Looming Definitional Gaps and the Growing Need for Formal U.N. Response," *Texas International Law Journal* 50, no. 2 (Spring, 2015): 384, https://library.norwich.edu/login?qurl=https%3A%2F%2Fwww.proquest.com%2Fscholarly-journals%2Fuse-force-armed-attack-thresholds-cyber-conflict%2Fdocview%2F1704865288%2Fse-2%3Faccountid%3D12871.
5. Dev, ""use of Force" and "Armed Attack" Thresholds in Cyber Conflict: The Looming Definitional Gaps and the Growing Need for Formal U.N. Response," 385.
6. The Ministry of Foreign Affairs of the Russian Federation, "Convention on International Information Security," Foreign Policy / Fundamental Documents, accessed April 20, 2021, https://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/191666.
7. Oona A. Hathaway, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue, and Julia Spiegel, "The Law of Cyber-Attack," *California Law Review* 100, no. 4 (2012): 825, http://www.jstor.org/stable/23249823.
8. Hathaway, Crootof, Levitz, Nix, Nowlan, Perdue, and Spiegel, "The Law of Cyber-Attack," 825.
9. Keir Giles, "Prospects for the Rule of Law in Cyberspace," Carlisle, Pennsylvania: Strategic Studies Institute, United States Army War College (2017), 9, http://www.jstor.org/stable/resrep11600.
10. Charter of the United Nations arts. 2 and 51, *adopted* June 26, 1945, U.S.T. 993, U.N.T.S., https://tile.loc.gov/storage-services/service/ll/lltreaties//lltreaties-ustbv003/lltreaties-ustbv003.pdf.
11. U.S. White House, I*nternational Strategy for Cyberspace*, (Washington, DC: Government Publishing Office, 2011), 14, https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.
12. North Atlantic Council, "Wales Summit Declaration," North Atlantic Treaty Organization, August 30, 2018, https://www.nato.int/cps/en/natohq/official_texts_112964.htm?mode=pressrelease.
13. Eva-Nour Repussard, "There is No Attribution Problem, Only a Diplomatic One," *E-International Relations*, March 22, 2020, https://www.e-ir.info/2020/03/22/there-is-no-attribution-problem-only-a-diplomatic-one/.
14. Repussard, "There is No Attribution Problem, Only a Diplomatic One."
15. Eric Talmadge, "N. Korea calls Song, Wannacry hack charges smear campaign," *The Associated Press*, September 13, 2018, https://apnews.com/article/80003a5e8f9440e0bb4cca664c63a132.
16. Gil Baram and Kevjn Lim, "Israel and Iran Just Showed Us the Future of Cyberwar With Their Unusual Attacks," *Foreign Policy*, June 5, 2020, https://foreignpolicy.com/2020/06/05/israel-and-iran-just-showed-us-the-future-of-cyberwar-with-their-unusual-attacks/.
17. Donghui Park and Michael Walstrom, "Cyberattack on Critical Infrastructure: Russia and the Ukrainian Power Grid Attacks," The Henry M. Jackson School of International Studies: University of Washington, October 11, 2017, https://jsis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-power-grid-attacks/.
18. International Committee of the Red Cross, "Rule 1. The Principle of Distinction between Civilians and Combatants," IHL Database, accessed April 20, 2021, https://ihl-databases.icrc.org/customary-ihl/eng/docs/v1_cha_chapter1_rule1.
19. Lucas Ashbaugh, "An Analysis Of International Agreements Over Cybersecurity," *University of Maine Electronic Theses and Dissertations* April 27, 2018: 42, https://digitalcommons.library.umaine.edu/etd/2876.
20. Ashbaugh, "An Analysis Of International Agreements Over Cybersecurity," 15.
21. Paul Meyer, "Cyber-Security through Arms Control: An Approach to International Co-Operation," *The Rusi Journal* 156, no. 2 (2011): 26, https://doi.org/10.1080/03071847.2011.576471.
22. Giles, *Prospects for the Rule of Law in Cyberspace*, 17.
23. Ibid., 21-23.
24. Ibid., 22.
25. Charter of the United Nations art. 1, *adopted* June 26, 1945, U.S.T. 993, U.N.T.S., https://tile.loc.gov/storage-services/service/ll/lltreaties//lltreaties-ustbv003/lltreaties-ustbv003.pdf.

NOTES

26. Ibid.
27. Diana Panke, "The Institutional Design of the United Nations General Assembly: An Effective Equalizer?" *International Relations* 31, no. 1 (March 2017): 13, https://doi.org/10.1177/0047117817690567.
28. Charter of the United Nations art. 10, *adopted* June 26, 1945, U.S.T. 993, U.N.T.S., https://tile.loc.gov/storage-services/service/ll/lltreaties//lltreaties-ustbv003/lltreaties-ustbv003.pdf.
29. Oliver Lissitzyn, *International Law Today and Tommorow,* 1965, quoted in Stephen M. Schwebel, "The Effect of Resolutions of the U.N. General Assembly on Customary International Law," *Proceedings of the Annual Meeting (American Society of International Law)* 73 (1979): 303, http://www.jstor.org/stable/25658015.
30. Charter of the United Nations art. 13, a*dopted* June 26, 1945, U.S.T. 993, U.N.T.S., https://tile.loc.gov/storage-services/service/ll/lltreaties//lltreaties-ustbv003/lltreaties-ustbv003.pdf.
31. UN General Assembly, Resolution 58/32, "Developments in the field of information and telecommunications in the context of international security," December 18, 2003, https://undocs.org/pdf?symbol=en/A/RES/58/32.
32. Charter of the United Nations art. 23, *adopted* June 26, 1945, U.S.T. 993, U.N.T.S., https://tile.loc.gov/storage-services/service/ll/lltreaties//lltreaties-ustbv003/lltreaties-ustbv003.pdf.
33. Charter of the United Nations art. 25, *adopted* June 26, 1945, U.S.T. 993, U.N.T.S., https://tile.loc.gov/storage-services/service/ll/lltreaties//lltreaties-ustbv003/lltreaties-ustbv003.pdf.
34. Charter of the United Nations art. 26, *adopted* June 26, 1945, U.S.T. 993, U.N.T.S., https://tile.loc.gov/storage-services/service/ll/lltreaties//lltreaties-ustbv003/lltreaties-ustbv003.pdf.
35. Charter of the United Nations art. 23.
36. United Nations Peacekeeping, "Role of the Security Council," United Nations, accessed April 20, 2021. https://peacekeeping.un.org/en/role-of-security-council#:~:text=The%20Security%20Council%20has%20primary,peace%20operation%20should%20be%20deployed.
37. United Nations Security Council, Resolution 1696, July 31, 2006, https://www.un.org/securitycouncil/s/res/1696-%282006%29.
38. United Nations Security Council, Resolution 242, November 22, 1967, https://undocs.org/S/RES/242(1967).
39. UN General Assembly, Resolution 32/84, "Prohibition of the development and manufacture of new types of weapons of mass destruction and new systems of such weapons," December 12, 1977, https://digitallibrary.un.org/record/623117?ln=en.
40. UN General Assembly, Resolution 41(I), "Principles governing the general regulation and reduction of Armaments," December 14, 1946, https://digitallibrary.un.org/record/209757?ln=en.
41. Vladimir Pitschmann, "Overall View of Chemical and Biochemical Weapons," *Toxins* 6, No. 6 (2014):1765, www.mdpi.com/2072-6651/6/6/1761/htm.