SRMUN CHARLOTTE 2024
March 21-23, 2024
sc_charlotte@srmun.org

III: Increased Threat of Cyberattacks on International Peace

Introduction

The explosive growth of digital technology has opened new domains for conflict as both State and non-State actors gain the ability to carry out attacks across international borders.[1] International peace and security in cyberspace is one of the most prevalent topics of discussion within the United Nations Security Council (UNSC), as seen in the High-Level Open Debate on “Maintaining International Peace and Security in Cyberspace” in Estonia in 2021.[2] The meeting highlighted the importance of the cybersecurity by citing the continual growth of information and communications technology (ICT) under the *2030 Agenda for Sustainable Development* and addressed the surge in recent cyberattacks that threaten Member States’ stability and overall security.[3] In addition, the United Nations International Telecommunication Union (ITU) labelled cyber criminals as, “state-sponsored cyber espionage groups to mass-mailing ransomware gangs.”[4] Cyberattacks conducted by these criminals have increasingly grown more sophisticated, reaching alarming levels of disruption on a global scale while, requiring only simple and attainable equipment.[5] Threats have increased continuously to a new five-year high as the increased accessibility to mobile devices, robotics, and the other telecommunication equipment brings new vulnerabilities.[6]

Addressing Cyberattacks

The United Nations Institute for Disarmament Research (UNIDIR) defines cyberattacks “as the unauthorized penetration of computers or digital networks.”[7] Despite the UNSC becoming progressively more involved in addressing cyber threats to international peace and security, no legally binding document has been implemented since the Budapest Convention in 2001; which has remained the single regional treaty regarding cyberattacks in the European Union (EU).[8] In 2004, the General Assembly First Committee (GA First) installed the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (GGE), which is a UN-mandated working group comprised of 15 experts appointed by the Secretary-General to examine potential and existing cyber threats.[9] Since its establishment, the GGE has conducted six investigative studies, which has produced 4 substantial reports, on threats posed by the use of ICTs in the

[1] United Nations, Security Council. *Explosive’ Growth of Digital Technologies Creating New Potential for Conflict, Disarmament Chief Tells Security Council in First-Ever Debate on Cyberthreats*, June 29, 2021, https://press.un.org/en/2021/sc14563.doc.htm.

[2] “UN Security Council held its first ever open debate on maintaining peace and security in cyberspace,” *Digwatch,* June 29, 2021, accessed September 15, 2023, https://dig.watch/updates/un-security-council-held-its-first-ever-open-debate-maintaining-peace-and-security.

[3]“United Nations, Security Council. *Explosive’ Growth of Digital Technologies Creating New Potential for Conflict…”*

[4] International Telecommunication Union Telecommunication Development Bureau, *Understanding Cybercrime: Phenomena, Challenges, and Legal Response,* Geneva, Switzerland: Place des Nation, pg. 11. https://www.itu.int/en/ITU-D/Cybersecurity/Documents/cybercrime2014.pdf.

[5] Symantec, *Internet Security Threat Report 2017*, Mountain View, California, USA: 2017, pp. 7-8. 2017, https://docs.broadcom.com/doc/istr-22-2017-en.

[6] Symantec, *Internet Security Threat Report 2017*.

[7] United Nations Institute for Disarmament Research, *The Cyber Index: International Security Trends and Realities,* Geneva, Switzerland, 2013. https://unidir.org/files/publication/pdfs/cyber-index-2013-en-463.pdf

[8] “International and Foreign Cyberspace Law Research,” *Georgetown Law Library*, 2023, accessed September 15, 2023. https://guides.ll.georgetown.edu/cyberspace/cyber-crime-treaties#:~:text=Convention%20on%20Cybercrime%20(2001),techniques%2C%20and%20increasing%20international%20cooperation.

[9] “In Hindsight: The Security Council and Cyber Threats, an Update*,” Security Council Report*, January 31, 1011, accessed September 15, 2023. https://www.securitycouncilreport.org/monthly-forecast/2022-02/in-hindsight-the-security-council-and-cyber-threats-an-update.php

context of international security and recommendations how the UN should address them.[10] The conclusions and recommendation within these reports have been widely acknowledged and implemented by Member States with the latest 2021 report titled, *Group of Governmental Experts on Advancing Responsible State Behavior in Cyberspace in the Context of International Security,* affirming that cyberattacks will be governed by *International Humanitarian Law*, as outlined in the *UN Charter,* to prevent Member States from addressing the issue through legal vacuums.[11] However, the GGE has still yet to provide a means for Member States to respond to cybercrime and cyberattacks involving other Member States or State actors.[12] Overall, recent events have caused talks regarding cybersecurity to fade into the background with no significant headway.

Recent Developments and Conclusion

In July 2023, the UNSC held its first session to address the threat that artificial intelligence (AI) poses to international peace and security.[13] Secretary General Antonio Guterres addressed the necessity for a UN governing body regarding AI usage after the launch of ChatGPT app, which raised alarms potential usage for disinformation and manipulation.[14] Experts of the Open-Ended Working Group on Security and in the Use of ICT 2021-2025 (OEWG II) have addressed AI-enabled cyberattacks are already targeting critical infrastructure and peacekeeping and humanitarian operations citing the 2022 deepfake video of Russian President Vladmir Putin and Ukrainian President Volodymyr Zelensky declaring a false peace agreement.[15] The meeting further highlighted the absence of any existing organization or UN body that can properly become the "UN-watchdog" for AI to ensure peace and security, especially during armed conflicts.[16]

Member States are currently undergoing negotiations for a new international cybercrime treaty set to replace the Budapest Convention, also known as The Convention of Cybercrime.[17] The aim of the treaty is to make it enable Member States to share information on the significant rise of digital criminal activities like ransomware, denial-of-service attacks, and the exploitation of children online.[18] If signed, the treaty would become a major maker for how the UN and Member States can address cyberattacks and cybercriminal within and outside their borders.[19] However on September 1, 2023, it was reported that Member States were unable to reach consensus on the *United Nations Treaty on Countering the Use of Information and Communications Technologies for Criminal Purposes* (Cybercrime Treaty) due to differing policy on addressing cybercrimes committed by state and non-state actors.[20]

[10] "Developments in the field of information and telecommunications in context of International Security,*" United Nations Office for Disarmament Affairs,* accessed November 5, 2023. https://disarmament.unoda.org/ict-security/

[11]"In Hindsight: The Security Council and Cyber Threats, an Update*," Security Council Report*.

[12] Susan W. Brenner, "'At Light Speed' – Attribution and Response to Cybercrime/Terrorism/Warfare," *Journal of Criminal Law and Criminology*, vol. 97 (2007), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1008542#

[13] Farnaz Fassihi, "U.N. Officials Urge Regulation of Artificial Intelligence," *New York Times,* July 18, 2023, accessed September 15, 2023. https://www.nytimes.com/2023/07/18/world/un-security-council-ai.html.

[14] Farnaz Fassihi, "U.N. Officials Urge Regulation of Artificial Intelligence," *New York Times.*

[15] Mary Pratt, "Emerging Cyber Threats in 2023 from AI to Quantum to Data Poisoning," *CSO,* September 7, 2023, ccessed November 5, 2023, https://www.csoonline.com/article/651125/emerging-cyber-threats-in-2023-from-ai-to-quantum-to-data-poisoning.html

[16] U.N. Officials Urge Regulation of Artificial Intelligence," *New York Times.*

[17] Rishi Iyengar, Robbie Gramer and Anusha Rathi, "Russia in Commandeering the U.N Cybercrime Treaty," *Foreign Policy Report*, August 31, 2023, accessed September 15, 2023. https://foreignpolicy.com/2023/08/31/united-nations-russia-china-cybercrime-treaty/.

[18] Rishi Iyengar, et al. "Russia in Commandeering the U.N Cybercrime Treaty," *Foreign Policy Report*.

[19] Rishi Iyengar, et al. "Russia in Commandeering the U.N Cybercrime Treaty," *Foreign Policy Report*.

[20] "UN Cybercrime Treaty," *Global Initiative Against Transnational Organized Crime*, November 3, 2023, accessed November 5, 2023. https://globalinitiative.net/analysis/un-cybercrime-treaty-gitoc-positions-nov-23/