Forum: Disarmament and International Security Committee (DISEC)

Issue #1: Discussing Measures to Develop International Legal Frameworks to Govern State Behavior in Cyberspace and Address Cyber Warfare

Student Officer: Soliana Solomon

Position: Chair of Disarmament and International Security Committee (DISEC)

Introduction

For centuries, technological innovations have shown to have boundless opportunities for the future. Technology has become a common part of our lives and is used all over the world, both positively and negatively. Throughout the years, the use of Cyberspace has become common for individuals, communities, and governments to use as the main source of information, communication, and networking. Cyberspace started in 1968, when the Danish artist Susanne Ussing first introduced the term (Castillo). The virtual environment of Cyberspace has many benefits such as enhanced communication which enables global connectivity and networking, has shown to promote economic growth due to E-commerce and remote work, and also enables convenient access to information (Acharry). Not only is Cyberspace an organized method of storing systems and data, it provides differe

`nt levels of security and access for governments and nations and Cybersecurity is a prominent part of them.

Cyberwarfare is now a security issue that impacts millions of people and governments around the world. In 2024, Cybercrime is predicted to cost the world $9.5 trillion USD and 75% of security professionals have reported an increase of cyber centered crimes in the past year (Fox).

Definition of Key Terms

Cyberspace: The interconnected virtual environment of digital communication platforms, the internet, and computer networks.

Cyber Warfare: Digital attacks by a nation-state to disrupt the computer systems of another nation-state, with the purpose to disrupt, manipulate, or damage.

Cyber Attack: Any attempt to expose, steal, or gain unauthorized access to a virtual environment.

Malware: Short for malicious software, it consists of viruses, worms, trojans, ransomware, and spyware to commit cyber attacks.

Phishing: A technique used by cyber attackers to trick people into compromising sensitive information by pretending to be a trustworthy entity.

Ransomware: A type of malware which encrypts a victim's files and demands ransom to restore access to the stolen data.

Advanced Persistent Threat (APT): A targeted cyber attack in which a person gains access to a system and remains undetected for a prolonged period of time.

Firewall: A security system for networks designed to monitor and control incoming and outgoing traffic based on preset security guidelines.

Intrusion Detection System (IDS): An application that monitors a system for malicious activity or policy violations.

Cyber Terrorism: The use of these systems to conduct violent acts to achieve political or ideological gains through threats.

Encryption: The process of converting information or data into code to prevent unauthorized access.

Cybersecurity: The practice of protecting systems, networks, and programs from digital attacks.

General Overview

Increase in Cyber Warfare Threats

For years, the threat of cyber attacks has grown to affect people on an individual level, to now, on a national level. Furthermore, the tactics used to commit these crimes have become far more sophisticated. Now, these crimes can go undetected for long periods of time. In 2020, it was expected and estimated that global Cybercrime costs would grow by 15% per year over the next five years, amounting to costs reaching $10.5 trillion USD per year by 2025, drastically increased from $3 trillion USD in 2015 (Morgan). The financial consequences of these increasing cyber attacks can be so severe that nations are implementing the latest software and technology to prevent having to pay the aftermath costs of falling victim to these crimes. The various consequences of these increasing cyber attacks are extremely severe as they cause irreversible economic loss, damage to nations politically and socially, and even loss of life. It is of utmost importance that nations understand the effects that cyber attacks can have on people from an individual to a global scale.

Lack of Comprehensive International Legal Frameworks

These attacks commonly transcend national borders impacting multiple nations at once. The current international policies and legal frameworks that have been put in place by nations related to cyberspace are often ambiguous and lack clear and well drawn out implementations of international legal systems. Because of this, crimes correlated with cyberspace and cyberwarfare fall into a legal gray area and it becomes challenging to hold perpetrators accountable for their actions and prevent other future malicious activities. Since cyberwarfare impacts multiple different nations at once, it is necessary that standardization in newly created legal frameworks establishes clear norms, rules, and punishments for state behavior in cyberspace. To start with, defining what an act of cyber aggression is, setting protocols for incident response after a system/systems are compromised, and creating institutions or bodies tasked with ensuring that crimes relating to cyberspace are monitored.

Major Parties Involved and Their Views

United States of America

The United States is one of the biggest advocates for comprehensive international norms and cooperation to deter cyber attacks and promote cybersecurity. In the past, the USA established the Cybersecurity and Infrastructure Security Agency (CISA) to enhance and create more protection for cyber security. Apart from in-state solutions, the nation has also engaged in multiple international collaborations such as the NATO Cooperative Cyber

Defence Centre of Excellence (CCDCOE). The United States has Imposed Sanctions on Foreign Entities and individuals involved in cyber attacks against the U.S and made their stance against cyber crime clear globally.

European Union (EU)

The EU supports the idea of bringing together and binding many different international legal entities and policies to create one comprehensive, global agreement between all nations. To protect personal data, they implemented General Data Protection Regulation (GDPR) which is a law that controls how personal information about people in the UK is collected and works to protect privacy and set guidelines in the cyber world. To improve the nation's cybersecurity capabilities, they established the EU Agency for Cyber Security (ENISA) and this agency works to provide advice, support, and coordination for people and organizations impacted by cyber warfare. The UK also initiated the EU Cyber Diplomacy Toolbox to respond to malicious cyber activities and address the substantial issue.

Russia

Russia has a different approach to combat the issue which has a focus on advocating for state sovereignty and establishing a framework that recognizes the right for all nations to control and regulate their own cyber activities without external interference. While this is true, Russia supports the idea of creating international rules and norms for all nations to align parallel with through negotiation through the United Nations. Russia has participated in a number of international forums, particularly the UN Group of Governmental Experts (UNGGE) in the context of Developments in the Field of Information and Telecommunications globally. Russia has also implemented the "Sovereign Internet" law which aims to create a domestic internet infrastructure that operates independently in the event of a national or international crisis and works to enhance cyber security and control.

China

Similarly, China also advocates for cyber sovereignty and emphasizes that nations should have control over their own internet and data between their borders and through that, should be able to regulate cyberspace according to their own laws and policies. China and Russia have a very similar stance on the topic as state sovereignty and multinational cooperation is a common theme seen in the values of the two nations.

Timeline of Events

Date	**Description of Event**
1998	The nation of Russia presents Cybersecurity issues to the

	United Nations by a draft resolution suggesting the need for international cooperation on information security. This marks the first major step toward global discussions on cybersecurity in the United Nations.
2001	The first international treaty named the Budapest Convention becomes the groundwork for future international cooperation on cybersecurity and aims to address cybercrime from levels of hacking to fraud.
2003	The Group of Governmental Experts (GGE) is established by the United Nations on the Developments in the Field of Information and Telecommunications in the Context of International Security and the group discusses international law and works to develop norms for state behavior.
2007	The nation of Estonia experiences very significant cyberattacks on its governments and financial institutions and this ended up highlighting the need for international frameworks on a global scale.
2010	Stuxnet is a computer worm and the discovery of it emphasizes the potential for cyber tools to be used in state-level conflicts and sparks multiple global debates on

	cyber warfare as the sophisticated cyber weapon targeted Iran's nuclear facilities.
2011	The European Union (EU) releases its first comprehensive Cybersecurity Strategy which emphasizes the need for international cooperation to address cyber threats and protect critical infrastructure.
2013	The UN GGE releases a report establishing norms for responsible international behavior in cyberspace and the importance of international law.
2014	The North Atlantic Treaty Organization (NATO), at the Wales Summit, declares cyberspace an operational domain which indicates that a cyberattack could trigger collective defense measures under Article 5 which considers an attack on one member as an attack on all.
2016	The publication of Tallinn Manual 2.0 explores how international law applies to cyber operations in both peacetime and during conflict.
2018	The United Nations Open-Ended Working Group (OEWG) is established as an inclusive platform for all UN member states to discuss norms, confidence-building measures,

	and the application of international law in Cyberspace.
2018	In the same year, France launched the Paris Call which is a multi-stakeholder initiative advocating for international norms to ensure the safety and stability of cyberspace.
2021	The UN GGE publishes a new and updated report refining cyber norms, emphasizing the protection of critical infrastructure and the importance of applying international law to state actions in cyberspace.
2021	The UN OEWG releases its final report which achieves a broad agreement on cyber norms and the applicability of international law in cyberspace.
2024	The UN OEWG continues to work on focusing on developing a comprehensive international legal framework for state behavior in cyberspace, addressing new challenges, and refining existing norms.

UN Involvement, Relevant Resolutions, Treaties and Events and Evaluation of Previous Attempts to Resolve the Issue

UNGA Resolution 70/237 (2015)

The UNGA Resolution 70/237 titled "Developments in the Field of International and Telecommunications in the Context of International Security" was adopted by the United Nations General Assembly on December 23, 2015. This resolution highlights many key points about the use of information and communication technologies relating to international security. This resolution is a part of a larger international framework which makes the effort to manage cyber security and establish rules and norms about how people and organizations operate in the cyber world. A common theme seen in the resolution is the call for international cooperation to take measures to ensure that information and telecommunications technologies are used effectively. This resolution emphasizes respecting the sovereignty of nations while also ensuring that cyberspace is not used negatively internationally as well as acknowledges the work of the UN Group of Governmental Experts (UNGGE) and tasks them with studying and recommending measures that will help to improve international cyberspace. The call for international cooperation is key in this resolution as it is one of the most prominent efforts made to combat cyber crime (*A/RES/70/237 General Assembly*).

UNGA Resolution 70/27 (2018)

The UNGA Resolution 70/27 was adopted on December 5, 2018 and builds onto the UNGA Resolution 70/237 titled "Developments in the Field of International and Telecommunications in the Context of International Security". This resolution has more of a focus on Information and Communication Technologies (ICT's) in relation to security. This resolution just builds upon the previous one by reaffirming previous UN resolutions and agreements relating to cyber security, emphasizing the importance of implementing international rules and norms relating to the cyber world, and works to enhance confidence building measures to enhance transparency and trust between nations. Additionally, this resolution clearly states its support for the continuation of the UNGGE's efforts to promote and establish international regulations.

OEWG First Report (2020)

The OEWG First Report stands for the Open-Ended Working Group (OEWG) on Developments in the Field of Information and Telecommunications in the context of International Security and it was established by the United Nations General Assembly in 2019. The OEWG was tasked with recommending norms, rules, and regulations to establish to promote international cooperation as many of the UN treaties and resolutions did not clearly establish any. This document heavily focused on emphasizing the need for clear international rules and norms governing state behavior in cyberspace and similarly to the previous resolution, it builds on agreements already established and promotes the need for international discussions on the topic through the United Nations and the UNGGE. This report, being one of the latest, provides guidance for future discussions and efforts in the OEWG and other international forums and aims to develop effective international norms and practices for cybersecurity ("Open-Ended Working Group – UNODA").

In the past, the most significant issue regarding attempts, efforts, and resolutions in the context of cyberspace is the lack of a clear, systematic legal framework which establishes global guidelines for responses to cyber attacks and this framework has still not been established even though cybercrime is one of the most serious threats against people and member states.

Possible Solutions

Cybercrime is an issue that needs to have action held against it to prevent serious events and complications from happening in the future. In this committee, delegates will be tasked with discussing how nations can prevent crimes and attacks like this from happening in a virtual environment, specifically by using an international legal framework or further developing the already established policies. Comprehensive frameworks can be made and ensuring that past ones are more specific and clear. Just like the previous resolutions mentioned above, clear international rules and norms need to be established after deep discussions on the topic. To create these international legal frameworks, nations must work together to ensure that all ideas and policies are implemented to the new, possible solutions. Multilateral cooperation fosters trust and alliances between nations which is essential for effective cyber governance.

Sustainable Development Goal (SDG)

SDG #16: Peace, Justice, and Strong Institutions

The topic of Cybersecurity and measures to govern state behavior in cyberspace relates to Sustainable Development Goal #16: Peace, Justice, and Strong Institutions as cybercrime is illegal and by developing an international legal framework, nations can create a strong international institution to bring justice to those who commit such acts. International discussion and forums also enhance the trust between countries as confidence-building measures are taken to ensure total transparency and trust globally.

SDG #17: Partnership for the Goals

Also relating to Sustainable Development Goal #17: Partnership for the Goals, international legal frameworks can not be created without international collaboration and partnership for the greater good. To create a solution to this significant global concern, nations have to work together, whether it be in discussions or while writing/brainstorming resolutions.

Appendix

A. https://carnegieendowment.org/posts/2021/06/a-brief-primer-on-international-law-and-cyberspace?lang=en
   1. This study breaks down the need for an international legal framework and all of the parts that are needed to ensure that it is functional, and establishes a global guideline for the issue of cyber crime.

B. https://www.csis.org/analysis/creating-accountability-global-cyber-norms
   1. The CSIS asalyzed how nations can create an international framework that works to create accountability for global cyber crimes.

C. https://www.state.gov/united-states-international-cyberspace-and-digital-policy-strategy/
   1. The United States created an international cyberspace and digital policy strategy that does well establishing regulations and guidelines.

D. https://www.youtube.com/watch?v=TYhH6Enm7rE
   1. A video from the United Nations Institute for Disarmament Research discussing the promotion of a legal framework to govern state behavior in cyberspace.

Bibliography

A/RES/70/237 General Assembly. 30 Dec. 2015.

Acharry, Arjun A. "What Is the Cyber World, and What Are Its Advantages and Disadvantages?" *Medium*, Medium, 22 Apr. 2023, medium.com/@arjunaacharry007/what-is-the-cyber-world-and-what-are-its-advantages-and-disadvantages-4ce25cd25c8d#:~:text=Advantages%20of%20the%20cyber%20world. Accessed 28 July 2024.

Castillo, Jose Antonio Hernandez. "Cyberspace Origin, Applications & Examples." *Study.com*, 27 Feb. 2023, study.com/academy/lesson/cyberspace-history-origin-overview.html#:~:text=Danish%20artist%20Susanne%20Ussing%20first,for%20the%20exchange%20of%20information. Accessed 28 July 2024.

Fox, Jacob. "Top Cybersecurity Statistics for 2024." *Www.cobalt.io*, 8 Dec. 2023, www.cobalt.io/blog/cybersecurity-statistics-2024. Accessed 28 July 2024.

Morgan, Steve. "Cybercrime to Cost the World $10.5 Trillion Annually by 2025." *Cybercrime Magazine*, 21 Feb. 2018, cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/#:~:text=Cybersecurity%20Ventures%20expects%20global%20cybercrime. Accessed 28 July 2024.

"Open-Ended Working Group – UNODA." *The United Nations*, disarmament.unoda.org/open-ended-working-group/. Accessed 29 July 2024.