Chair Report | The Economic and Social Council

Forum: Economic and Social Council

Issue: Preventing Cybercrime and Ensuring the Safe Use of Cryptocurrency

Student Officer: Mordekai Gernes | gernesm@ismanila.org

Position: Head Chair

Student Officer: Hyeyeon Shin | 19-0377@sgen.edu.ph

Position: Deputy Chair

Welcome Letter

Welcome to SISC MUN 2024's Economic and Social Council (ECOSOC), delegates! Your chairs this year are Kai Gernes and Rosa Shin. ECOSOC is one of the six principal organizations of the United Nations, established in 1945. On May 9 & 11, this committee will be discussing contemporary challenges that relate to the economic and social aspects of the world, and formulating solutions as well as policy recommendations. The chairs look forward to diplomatic and fruitful debate throughout the course of this conference.

Background

In 1834, what is generally considered to be the first major cybercrime was committed. Two thieves accessed and stole data from the French telegraph system, giving them access to financial market information.

In the late 1870s, the telephone went public, and within two years individuals had broken into telephone lines and misdirected calls. Throughout the remainder of the 19th and into the 20th century, many cybercrimes were directed against phone lines.

In the 1980s, as email was popularizing, already the first phishing scams and malware contained in emails were being disseminated. Within the next decade, the internet itself became publicly available, and within a year of its introduction, the US Federal Bureau of Investigation discovered that a 10 year old boy going missing was attached to a ring of pedophiles who were virtually disseminating pornographic images of minors.

Since then, cybercrime has grown alongside the internet. With practically every new internet invention, there are people who seek to exploit these systems for nefarious purposes. In fact, these hacks and crimes have become sophisticated enough to take offline entire cities, which was demonstrated in Ukraine, taking offline entire sectors of the regional power grid. Another increasingly popular form of cyberattacks is ransomware, in which systems are infected and essentially held hostage until the victims satiate the demands of the hackers. A notable example of this type of attack was WannaCry, which was known as a "cryptoworm" for its ability to spread between systems and lock them down until ransom was paid.

The aspect of WannaCry that made it more notable was the method by which ransom payments were made, this being Bitcoin cryptocurrency. As cryptocurrency has no centralized source, it is incredibly difficult to trace, and thus can be easily

lost, making it harder for authorities to track down the perpetrators of this ransom attack. In the end, this attack cost roughly $4 billion USD in losses across the globe.

As a result of cryptocurrencies' near untraceability, it has gained popularity with criminal individuals and organizations as a method to extort their victims, creating many copycats at varying scales that persist today.

Domestic law enforcement agencies are often helpless to do anything about cyberattacks as the perpetrators may be well beyond their nation's jurisdiction, and therefore they cannot track them down, and if they do it can be incredibly difficult to properly prosecute them in an international court.

The issue of cybercrime has never been more pressing, with over 66% of the world's population being internet users. It is difficult to determine the exact cost that cybercrime exacted, but it is estimated the world lost $8.14 trillion USD in 2023 to cybercrime, a 15% increase from the year prior. With these alarming statistics, the time to address these issues is now, lest inaction should allow cybercrime to grow to such an extent that it cannot be rooted out.

Definition of Key Terms

Term	Definition
Cybercrime	An umbrella term referring to any number of crimes that are committed using digital devices and/or networks
Cyberattack	An assault launched by an individual or group of individuals with the express purpose of committing a cybercrime
Cryptocurrency	A digital currency which is designed to work as a medium of exchange through an encrypted network that does not rely on a central authority (such as a bank or government).
Crypto jacking	Cryptojacking is a type of cybercrime where a criminal secretly uses a victim's computing power to generate

	cryptocurrency
Hacker	An individual engaging in the unauthorized accessing of data

Major Parties Involved

The United States of America

The USA has engaged in possibly the most far-reaching efforts to tamp down cybercrime, through agencies such as the FBI and DHS. Furthermore, they have had some success in recouping losses exacted by cybercriminals, such as being able to track down and take back money from a North Korean hacking group. The USA has also been accused of engaging in large-scale cyber espionage against groups and nations, as well as cybercriminal groups operating in the USA.

The Russian Federation

Russia has been the source of several large-scale cyber attacks, some of which have been linked to their intelligence services, in the form of cyber espionage. Russia has implemented legislation, conducted law enforcement operations, and participated in international cooperation efforts to combat cybercrime.

North Korea

North Korea is notorious for its involvement in cybercrime, particularly through state-sponsored hacking groups such as Lazarus Group. These groups have been linked to high-profile cyber attacks, including the 2014 Sony Pictures hack and the WannaCry ransomware attack in 2017. North Korea allegedly uses cybercrime as a means to fund its regime and evade international sanctions.

Interpol

Interpol plays a crucial role in combating cybercrime by facilitating international cooperation and coordination among law enforcement agencies. Its global network enables the sharing of intelligence, resources, and best practices,

which are essential for investigating and prosecuting cybercriminals operating across borders. Interpol also provides training and capacity-building programs to enhance the capabilities of law enforcement personnel in tackling cyber threats effectively.

The People's Republic of China

China has demonstrated a commitment to combating cybercrime through the enactment of legislation and the establishment of specialized law enforcement units. However, concerns remain regarding the extent of state involvement in cyber activities and the enforcement of regulations. Additionally, China's role in the cryptocurrency landscape is notable, with efforts to regulate and manage digital currencies, balancing innovation with regulatory oversight to address potential risks such as money laundering and fraud.

Possible Solutions

- **Possible Solution 1**: Regulating cryptocurrency
    - Legislation to arrest the complete privacy of cryptocurrency and thus making it easier to track, at least for law enforcement, may make it harder for criminals to launder this money by passing it through a series of accounts before transferring it out.
- **Possible Solution 2**: Systems to assist victims
    - Some of these crimes will undoubtedly continue regardless, and being able to provide security to victims of these schemes in order to rebuild and insure themselves against future attacks would be valuable in fostering a successful economy. This could

also entail educating the public or businesses on best practices to avoid exposing themselves to cybercrime.

- **Possible Solution 3**: Information sharing
    - A platform or organization dedicated to ensuring the transfer of lessons learned and resources for combatting specific types of cybercrime, as well as actively fostering cooperation between nations who are combatting specific attacks in order to minimize damages and bring to justice the criminals involved.

Works Cited:

Charlton, Emma. "2023 Was a Big Year for Cybercrime – Here's How We Can Make Our Systems Safer." *World Economic Forum*, 10 Jan. 2024, www.weforum.org/agenda/2024/01/cybersecurity-cybercrime-system-safety/. Accessed 1 May 2024.

"Cyber Crime | Federal Bureau of Investigation." *Federal Bureau of Investigation*, 2016, www.fbi.gov/investigate/cyber. Accessed 1 May 2024.

"Cybercrime: History, Global Impact & Protective Measures [2022]." *BlueVoyant*, 2022, www.bluevoyant.com/knowledge-center/cybercrime-history-global-impact-protective-measures-2022. Accessed 1 May 2024.

"Extradition: Why Is the US Determined to Extradite European Hackers?" *Euronews*, Euronews.com, 5 June 2023, www.euronews.com/next/2023/06/05/extradition-why-is-the-us-determined-to-extradite-european-hackers. Accessed 1 May 2024.

"Famous Ransomware Attacks in History | the University of Tulsa." *Utulsa.edu*, 2024, online.utulsa.edu/blog/famous-ransomware-attacks-in-history/. Accessed 1 May 2024.

"Global Cybercrime Estimated Cost 2028 | Statista." *Statista*, Statista, 2023, www.statista.com/forecasts/1280009/cost-cybercrime-worldwide. Accessed 1 May 2024.

"Internet and Social Media Users in the World 2024 | Statista." *Statista*, Statista, 2024, www.statista.com/statistics/617136/digital-population-worldwide/#:~:text=As%20of%20January%202024%2C%20there,population%2C%20were%20social%20media%20users. Accessed 1 May 2024.

katharina.kiener-manu. "Cybercrime Module 7 Key Issues: Formal International Cooperation Mechanisms." *Unodc.org*, 2020, www.unodc.org/e4j/en/cybercrime/module-7/key-issues/formal-international-cooperation-mechanisms.html. Accessed 1 May 2024.

"Major Cases — FBI." *Fbi.gov*, 2016, www.fbi.gov/investigate/cyber/major-cases. Accessed 1 May 2024.

National Cybersecurity and Communications Integration Center. *WHAT IS WANNACRY/WANACRYPT0R?*

"The Prosecution of Cybercrime – Why Transnational and Extraterritorial Jurisdiction Should Be Resisted." *International Review of Law, Computers & Technology*, 2023, www.tandfonline.com/doi/full/10.1080/13600869.2022.2061888. Accessed 1 May 2024.

"What Was the WannaCry Ransomware Attack?" *Cloudflare.com*, 2017, www.cloudflare.com/learning/security/ransomware/wannacry-ransomware/. Accessed 1 May 2024.