H·I·S
HARARE INTERNATIONAL SCHOOL

66 Pendennis Rd, Harare, Zimbabwe

ZIMUN XII

The Cost of Innovation:

Navigating the Ethical Responsibilities of Technological Advancements and Societal Change for Inclusive, Sustainable Development in a Globalised World

General Assembly

Discussing the potential for technology and innovative solutions to cybersecurity threats and hacking

Committee: General Assembly

Issue: Discussing the potential for technology and innovative solutions to cybersecurity threats and hacking

Student Officer: Yohanna Masresha

Position: President Chair

INTRODUCTION

Cybercrime is defined as a wide range of criminal activities, carried out using digital devices or networks. A cybercrime often refers to a socially dangerous act committed using computer equipment against information that is processed and / or used in cyberspace. Cybercrime is split into five separate categories; unauthorized access, damage to computer data or programs, unauthorized interception of data within a system or network, sabotage to hinder the functioning of a computer system or network, and computer espionage (“Cybercrime”).

Cybercrime is a particularly relevant issue of the 21st century, as it is a growing threat that increases by the day. Accompanied by each new solution to the issue comes new vulnerabilities. Annually, cybersecurity threats and hacking drains billions of dollars from global economies. Every country, no matter their level of development, has faced cybersecurity threats, and will continue to, unless innovative solutions are developed. With such a complex issue, it is critical that the United Nations creates a multilateral solution (Gil).

According to the World Bank, in 2023, roughly 68 percent of the world’s population accessed the Internet. The global population relies heavily on connectivity for a number of tasks, from communication, to shopping, to advanced research and innovation. However, despite technology bringing extraordinary progress globally, it also creates new vulnerabilities. Connectivity exposes more than two thirds of the world's population to the risk of cybercrime. This lack of resilience further increases vulnerability and poses a larger international security threat. Cybercriminals exploit digital technology using ransomware, malware, and hacking as a means to steal money, data, and other valuable information. ICT (information and communications technology) are utilized to facilitate crimes like drug trafficking, arms smuggling, human trafficking, money laundering, and fraud. Cybercriminals exploit digital systems using malware, ransomware, and hacking to steal money, data, and other valuable information. Information and communications technology (ICT) are also used to facilitate crimes such as drug trafficking, arms smuggling, human trafficking, money laundering and fraud (Gil).

The WEF (World Economics Forum) 2020 Global Risks Report emphasized that organized cybercrime groups are joining forces across the globe to commit online criminal activities, with the estimated likelihood of their detection and prosecution being less than 1 percent in the United States ("Cybercrime"). This highlights the relevance of cybersecurity and its rapidly escalating threat in the modern day world.

DEFINITION OF KEY TERMS

- **Cyberwarfare** - cybercrimes, such as espionage, financial theft, etc., crossing international borders and involving the actions of at least one nation-state ("Cybercrime").
- **Black Market / Darknet Market** - a commercial website on the dark web that functions as black markets to sell or broker transactions involving drug, cyber-arms, weapons,

stolen credit card details, forged documents, unlicensed pharmaceuticals, steroids, counterfeit currency, and other illicit goods ("Darknet market").

- **Organized Cybercrime** - the premeditated, systematic, highly sophisticated and coordinated unlawful activity performed by structured groups of three or more individuals using digital technologies for illicit profit, power, or strategic advantage (Di Nicola et al.).
- **Hacking** - the act of exploiting weaknesses in a computer system or network to gain unauthorized access, to steal, corrupt, or manipulate data ("What Is Hacking? - Hacking - Definition, Types, Security, And More").
- **Cryptocurrency** - a digital currency in which transactions are verified and records maintained by a decentralized system, using cryptography rather than by a centralized authority ("cryptocurrency, n. meanings, etymology, and more").

BACKGROUND ON THE ISSUE

The issue of cybersecurity threats and hacking first began alongside the development of early technology and computer networks in the late 20th century. In the 1970s, as universities, large-scale corporations, and governments began utilizing computers, the first instances of digital sabotage and unauthorized access emerged. This showcased the threat of emerging technology and the new forms of crime it created. The issue escalated rapidly across the 1990s, with the public expansion of the internet, making digital systems globally accessible and more vulnerable. Over time, global connectivity has continued to rise, increasing the exposure to cyber threats. It is an international security threat that poses an increasing danger to the general public and to governments worldwide ("Cybercrime").

Particular regions, such as Southeast Asia, have been described as 'ground zero' for organized cybercrime operations. The threat posed by cybercrime is constantly escalating, undermining international economies, disrupting global infrastructures, and eroding trust in ever-evolving digital systems (Gil).

CURRENT CONTEXT

- **Silk Road & Ross Ulbricht**

Silk Road was an online black market, and the first modern darknet market. Launched in 2011 by American founder Ross Ulbricht, the marketplace operated as a hidden service on the Tor network, and allowed users to buy and sell products between one another anonymously. Transactions on Silk Road were conducted with bitcoin, and cryptocurrency played a detrimental role in protecting user identities and promoting anonymity. The Silk Road was a revolutionary technological milestone in cybercrime. Like an infection, darknet markets of the same kind began popping up across the web. Silk Road influenced later cybercrime marketplaces and increased the threat of cybersecurity. The platform showed how bitcoin enabled anonymous payments, bypassing traditional financial surveillance. Although some Silk Road supporters argue that it was a peaceful alternative to the often deadly violence of street drug trade, the online marketplace played a key role in the drug trade of the 2000s and led to the distribution of over 1 Billion USD of illicit items (Bilton and Ulbricht's). Since Silk Road was taken down, there have been countless other darknet markets inspired by it ("Preventing and countering cyber organized crime"). AlphaBay and Hansa were two of the biggest dark web marketplaces for illegal and illicit items like drugs and guns, post-Silk Road. Alpha Bay was 10 times larger than Silk Road, allowing users to sell and buy life-threatening opioids, leading to the deaths of numerous victims (Gibbs and Beckett).

- **Volt Typhoon**

Volt Typhoon is a Chinese nation-state sponsored cyber-espionage group that was publicly identified by United States and allied intelligence agencies in 2023. Allegedly, Volt Typhoon has staged cyber infrastructure attacks against critical sectors in the United States. The group represents a significant cybersecurity threat to international critical infrastructure. Volt Typhoon is notorious for carrying out long-term intrusions that can be leveraged during future geopolitical conflicts. The group's operations have raised international concerns in recent years about cyberwarfare preparedness. United States authoring agencies have observed that Volt Typhoon has compromises in Communications, Energy, Transportations Systems, and Water and Wastewater Systems sector organizations' technological sectors. Other victims of Volt Typhoon in the United States and its overseas territories include smaller organizations with limited cybersecurity capabilities that provide critical services to larger organizations or key geographic locations ("Volt Typhoon | NJCCIC").

MAJOR COUNTRIES AND ORGANIZATION INVOLVED

- UNODC

The United Nations Office on Drugs and Crime plays a key role in combatting global cybercrime. The UNODC, along with the UN General Assembly and other UN subgroups, are actively attempting to solve the issue. Through the creation of international legal frameworks, application of technical assistance to member states, and implementation of capacity building programs, the UNODC is finding innovative solutions to a modern-day issue that affects millions, if not billions, worldwide (Douglas).

- USA

The United States is a key actor in cybersecurity governance. The USA is frequently targeted by state-sponsored and criminal cyberattacks against infrastructure, elections, and private corporations. The nation itself may be considered to be partially responsible for the escalation of cybercrime in recent years as its cyber capabilities and offensive cyber doctrine pay a significant role in global cyber arms dynamics.Through the development of agencies like the CISA and government legislation like the Cybersecurity Information Sharing Act, the United States invests heavily in defensive technology, public-private threat intelligence sharing, and international cyber norms diplomacy ("Spotlight On").

- ITU, UNOCT, UNITAR

ITU (International Telecommunication Union) strongly supports national cybersecurity strategies, technical standards, and global cybersecurity indices ("International Telecommunication Union"). The UNOCT (United Nations Office of Counter-Terrorism) has addressed the use of CIT for terrorism and supports member states in cyber-related counterterrorism efforts (“UN Office of Counter-Terrorism | Office of Counter-Terrorism”). UNITAR (United Nations Institute for Training and Research) has provided training programs for government officials, including digital security and governance skills. This skill building has proved to be a useful aspect of preventing cyberwarfare on a smaller scale (“e-Workshop on Digital diplomacy and Cybersecurity”).

- China

The People’s Republic of China is a major cyber power and a central force in debates about cyber norms. Chinese private institutions and companies are frequent targets of intellectual property theft and cyber espionage. Western governments often allege that Chinese state-linked actors conduct cyber espionage campaigns, however, there is limited proof to support these allegations. China is a key participant to United Nations cyber negotiations, and has implemented its 2017 Cybersecurity Law (IT Advisory).

TIMELINE OF KEY EVENTS

-

23 November 2001 - Budapest Convention on Cybercrime Adopted

The Budapest Convention on Cybercrime was the first international treaty addressing internet and computer crime. It established common legal standards and cooperation mechanisms.

July 2002, Adopted January 2003 - UN General Assembly Resolution 57/239 on Cybersecurity

UNGA Resolution 57/329 addressed international collaboration and encouraged member states to develop national cybersecurity frameworks.

17 June 2010 - Discovery of Stuxnet Malware

In 2010, the first widely known cyberweapon that targeted industrial infrastructure was discovered. This event marked the beginning of modern cyberwarfare as it is known in the 21st century.

12 May 2017 - WannaCry Global Ransomware Attack

The WannaCry Global Ransomware attack was a massive cyberattack affecting over 150 countries demonstrated the vulnerability of global digital infrastructure.

16 November 2018 - Establishment of the US CISA (United States Cybersecurity and Infrastructure Security Agency)

The CISA, a sub-organization under the United States Department of Homeland Security (DHS) was created to coordinate national protection of critical infrastructure from cyber threats and improve the government's cybersecurity defense against private and nation-state hackers.

May 2023 - Public Disclosure of the Volt Typhoon Cyber Campaign

American intelligence agencies publicly warned of stealth intrusions into critical infrastructure networks across the nation and across non-continental United States territories.

1 July 2025 - UN Open-Ended Working Group (OEWG) Final Report Released

The United Nations OEWG report was created by the UN General Assembly to examine cyber threats, discuss norms for responsible state behaviour, explore capacity building for cybersecurity, and clarify the role of international law in cyberspace. The OEWG report affirmed the application of the UN Charter and international humanitarian law and human rights law to cyberspace.

RELEVANT UN RESOLUTIONS, TREATIES, & EVENTS

2002 – UN General Assembly Resolution 57/239: Creation of a Global Culture of Cybersecurity

https://undocs.org/A/RES/57/239

2003 – UN General Assembly Resolution 58/199: Creation of the Group of Governmental Experts (GGE)

https://undocs.org/A/RES/58/199

2013 – UN GGE Report on Developments in Information and Telecommunications

https://docs.un.org/en/A/68/98

2015 – UN General Assembly Resolution 70/174: Developments in ICTs in the Context of International Security

https://undocs.org/A/RES/70/174

2018 – UN General Assembly Resolution 73/27: Establishment of the Open-Ended Working Group on ICT Security

https://docs.un.org/en/A/RES/73/27

2021 – UN Open-Ended Working Group Final Report

https://undocs.org/A/75/816

POSSIBLE SOLUTIONS

1. *Deplores* member states conducting or knowingly supporting ICT activity contrary to its obligations under international law that may internationally damage critical infrastructure or otherwise impair the operation and use of critical infrastructure to provide services to the public of a nation
2. *Strongly Urges* the cooperation of member states in developing and applying measures to increase stability and security in the use of ICTs and to prevent harmful ICT practices or that may pose threats to international security and peace
3. *Encourages* intergovernmental organizations to provide long-term technical assistance and capacity building to strengthen the ability of national

authorities to deal with cybercrime, including the prevention, detection, investigation, and prosecution of such crime in all its forms; this includes but is not limited to the following organizations;

a. INTERPOL
b. UNODC
c. ITU
d. UNDP
e. UNOCT
f. UNITAR
g. EUROPOL

Works Cited

"About the Convention - Cybercrime." *The Council of Europe*, https://www.coe.int/en/web/cybercrime/the-budapest-convention. Accessed 21 February 2026.

Bilton, Nick, and Ross Ulbricht's. "Silk Road (marketplace)." *Wikipedia*, https://en.wikipedia.org/wiki/Silk_Road_(marketplace). Accessed 20 February 2026.

"cryptocurrency, n. meanings, etymology, and more." *Oxford English Dictionary*, https://www.oed.com/dictionary/cryptocurrency_n?tab=meaning_and_use. Accessed 18 February 2026.

"Cybercrime." *Wikipedia*, https://en.wikipedia.org/wiki/Cybercrime. Accessed 18 February 2026.

"Darknet market." *Wikipedia*, https://en.wikipedia.org/wiki/Darknet_market. Accessed 18 February 2026.

Di Nicola, Andrea, et al. “Criminological definitions of organized crime on the digital test bench: towards a physical–digital framework.” *Trends in Organized Crime*, 2025. *Springer Nature Link*, https://doi.org/10.1007/s12117-025-09575-3. Accessed 18 February 2026.

Douglas, Jeremy. “UNODC - Darknet Cybercrime Threats to Southeast Asia.” *Unodc*, https://www.unodc.org/roseap/uploads/archive/documents/darknet/index.html. Accessed 26 February 2026.

“e-Workshop on Digital diplomacy and Cybersecurity.” *UNITAR*, October 2020, https://unitar.org/sustainable-development-goals/multilateral-diplomacy/our-portfolio/core-diplomatic-training/e-workshop-digital-diplomacy-and-cybersecurity. Accessed 26 February 2026.

Gibbs, Samuel, and Lois Beckett. “Dark web marketplaces AlphaBay and Hansa shut down.” *The Guardian*, 21 July 2017, https://www.theguardian.com/technology/2017/jul/20/dark-web-marketplaces-alphabay-hansa-shut-down. Accessed 21 February 2026.

Gil, Laura. “Making the digital and physical world safer: Why the Convention against Cybercrime matters.” *UN News*, 24 December 2024, https://news.un.org/en/story/2024/12/1158526. Accessed 18 February 2026.

Gil, Laura. “Sixty-five nations sign first UN treaty to fight cybercrime, in milestone for digital cooperation.” *UN News*, 25 October 2025, https://news.un.org/en/story/2025/10/1166182. Accessed 18 February 2026.

“International Telecommunication Union.” *Wikipedia*, 25 July 2001, https://en.wikipedia.org/wiki/International_Telecommunication_Union. Accessed 26 February 2026.

IT Advisory. “Overview of China’s Cybersecurity Law.” *KPMG China*, February 2017, https://assets.kpmg.com/content/dam/kpmg/cn/pdf/en/2017/02/overview-of-cybersecurity-law.pdf. Accessed 26 February 2026.

“Preventing and countering cyber organized crime.” *United Nations Office on Drugs and Crime*, https://www.unodc.org/cld/zh/education/tertiary/cybercrime/module-13/key-issues/preventing-and-countering-cyber-organized-crime.html. Accessed 26 February 2026.

“Spotlight On.” *CISA*, https://www.cisa.gov/spotlight. Accessed 26 February 2026.

“UN Office of Counter-Terrorism | Office of Counter-Terrorism.” *the United Nations*, https://www.un.org/counterterrorism/en. Accessed 26 February 2026.

“Volt Typhoon | NJCCIC.” *NJCCIC*, https://www.cyber.nj.gov/threat-landscape/nation-state-threat-analysis-reports/china-linked-cyber-operations-targeting-us-critical-infrastructure/volt-typhoon. Accessed 26 February 2026.

“What Is Hacking? - Hacking - Definition, Types, Security, And More.” *Fortinet*, http://fortinet.com/resources/cyberglossary/what-is-hacking. Accessed 18 February 2026.