CIMUN VI Chair Research Report

Committee: The United Nations Commission on Science and Technology for Development (UNCSTD)
Issue: Addressing cybersecurity threats to global peace and stability in the era of AI
Student Officer: Leah Kim, President, Minjoo Kim, Deputy Assistant President

1. Committee Introduction

As a subsidiary body of the Economic and Social Council (ECOSOC), the main mission of the United Nations Commission on Science and Technology for Development (UNCSTD) is to provide the United Nations General Assembly (GA) and ECOSOC with high quality advice on current issues that are relevant to science and technology.

Established in 2005, UNCSTD functions as a forum for national Governments, intergovernmental organizations, and the civil society to hold timely discussions on global issues that impact the field of science, technology, and development. Such discussions tackle various challenges of access, governance, and equity to ensure that technological advancement can benefit all people. The committee also maintains strong bonds with other UN entities, including United Nations Trade and Development (UNCTAD), The Commission on Status of Women (CSW), International Telecommunication Union (ITU), the United Nations Educational, Scientific, and Cultural Organization (UNESCO), as well as other regional commissions.

With the rapid development of technology in our current society, UNCSTD is one of the most relevant committees where timely discussions can be conducted. The committee requires critical thinking and cooperative collaboration from member states to methodologically utilize science and technology as a tool for a better future.

2. Agenda Introduction

In an era of technological development, Artificial Intelligence (AI) has rooted its place in the everyday lives of citizens. The use of various AI platforms such as ChatGPT, Gemini, Quark, and more, has shown a rapid increase in number along with an era of unprecedented opportunities over the past few years. However, along with this substantial success, a major problem started to surface to the general public: cybersecurity. Although AI technology has vast potential to reach limitless possibilities and accelerate technological progress, its functions may

be a threat to cybersecurity. When there are those who decide to weaponize AI with a malicious intent, the technology can immediately transform into a threatening tool.

The agenda invites delegates to assess the dual use of AI technology, and to determine methods to ensure that global peace and stability is not threatened in the current society. Thus, it is crucial to explore various ways to alleviate the potential misuses of AI, prevent the technology from falling into the wrong hands, and develop plans to combat cybersecurity threats.

3. Definition of Key Terms

Cybersecurity

Cybersecurity is the defense against online threats for vital programs, networks, and systems. The cyber attacks often target sensitive information or extort money through ransomware, disrupting business procedures.

Artificial Intelligence (AI)

AI technology allows computers and other machines to mimic human intelligence such as comprehension, problem-solving, decision-making, creativity, and autonomy. The core skills often include visual perception, speech recognition, and translation, among others.

Deepfakes

Deepfakes are AI-generated videos that have been digitally altered to convincingly replace one person's image with another. The videos are often used for malicious purposes, such as the spreading of false information.

Critical Infrastructure

Critical infrastructures, as their name suggests, are systems and networks that are essential to maintaining normal daily life. These include complex networks of highways, communication systems, and energy infrastructures.

Zero-Day Exploit

A zero-day exploit is a type of cyberattack vector that exploits an undiscovered or unfixed security vulnerability in computer hardware, software, or firmware.

AI-enhanced Cyberattacks

AI-generated attacks are cyberthreats that use natural language processing and artificial intelligence to trick and compromise people.

4. Timeline of Key Events

[2010] Stuxnet Attack

Stuxnet is a computer worm discovered in June 2010. It was written with the purpose of causing industrial control systems to malfunction, and feeding false data to monitoring systems. For example, nuclear facilities in Iran were the target of a cyberattack in 2010, revealed to be sponsored by the state. This is the first time a cyberweapon has been known to cause physical harm.

[2017] WannaCry and NotPetya attacks

The WannaCry and NotPetya attacks in 2017 were global ransomware campaigns that affected more than 150 countries. The WannaCry outbreak had shut down computers in more than 80 NHS organisations in England alone, resulting in approximately 20,000 cancelled appointments, 600 surgeries having to revert to pen and paper, and five hospitals diverting ambulances due to being unable to handle any more emergency cases. It demonstrated how susceptible logistics and healthcare systems are to cyberattacks.

[2018] Start of Deepfakes

AI-generated videos surfaced online and gained popularity in 2018, sparking concerns from the public. The term came to be used for synthetic media in 2017 when a Reddit moderator created a subreddit called “deepfakes” and began posting videos that used face-swapping technology to insert celebrities’ likenesses into existing pornographic videos.

[2021] Colonial Pipeline Hack

In 2021, gas shortages occurred throughout the Eastern United States as a result of a ransomware attack that is now known as the Colonial Pipeline Hack. This again demonstrated the vulnerability of vital infrastructure. A hacker group identified as DarkSide accessed the Colonial Pipeline network and stole 100 gigabytes of data within a two-hour window. After the data theft, the attackers infected the Colonial Pipeline's IT network with ransomware, which affected many computer systems, including those used for billing and accounting.

[2023] AI ethics

The UN Advisory Body on AI Ethics was established in 2023. Made up of 39 members from a wide range of countries and sectors, its new advisory body began working to provide

recommendations on the new international agency for the governance of AI. The group has issued a report on “Governing AI for Humanity,” which proposes a variety of measures to strengthen the governance of AI and recommendations on ethical AI deployment and making AI more inclusive. Furthermore, the UN started a global initiative in 2023 to establish international standards for AI governance.

[2024] 78 Election Deepfakes

In 2024, fake media and AI-powered bots were employed to sway public opinion and threaten democratic institutions. In the U.S. presidential election, there was significant press coverage after a robocall featuring a fake Joe Biden voice instructed New Hampshire voters not to vote in the Democratic primary. AI-generated images from hurricane disaster areas, and AI-faked celebrity endorsements or viral deepfake images and videos misrepresenting candidates’ actions did not have as much effect as expected.

5. Positions of Key Member Nations and Bodies

United States

The United States champions global cooperation when addressing issues related to AI technology. Yet, the U.S. prefers non-binding norms over enforceable treaties. The U.S. has a strong private sector AI development, and is concerned about Chinese cyber operations. The U.S. remains cautious of the AI’s potential takeover of human job opportunities, as it will exacerbate the U.S.’ unemployment crisis. Nonetheless, the U.S. sees AI as a fitting tool to replace human labor for tedious and repetitive tasks.

China

China is currently undergoing rapid AI advancement and large-scale surveillance systems, aiming to become a global leader by 2030. Having launched the "Next Generation AI Development Plan" in 2017, China plans to leverage AI in various sectors, including manufacturing, defense, and even governance. China advocates for digital sovereignty and a state-dependent model of internet governance. China has a unique focus on algorithms and data when it comes to regulations, requiring transparency of algorithmic processes.

Russia

Russia believes in utilizing AI to strengthen their national security, particularly in the field of military applications such as drones or robotic systems. In terms of AI capabilities, Russia is undeniably behind China and U.S.; however, Russia is still a key actor in state-sponsored cyberattacks. As Russia remains skeptical of Western-led governance structures, Russia prefers

bilateral or regional pacts. Furthermore, Russia is willing to collaborate with BRICS to develop solutions to AI.

European Union (EU)

The European Union's greatest goal is to reach an appropriate balance between innovation and ethical use. The EU AI act reflects this goal, as it categorizes the risks that AI technology poses, and proposes regulatory frameworks to each risk. Further, the EU supports data protection and digital rights. At the same time, the EU seeks to be a global leader in AI.

India

India is pro-innovation, and prioritizes development over ethical codes. Thus, India is seeing rapid technological growth with privacy concerns. India currently does not have official, codified regulations regarding AI. Yet, India is actively in the process of developing frameworks for the responsible use of AI. India aligns with values of multilateral governance, especially for cyber capacity-building in the Global South.

African Union (AU)

The African Union recognizes the AI's potential for socio-economic transformation. One of the most significant objectives of the AU is to address challenges in the health, agriculture, and education sector by utilizing AI. The AU puts a strong emphasis on digital divide and seeks assistance for developing cybersecurity infrastructure and AI governance frameworks.

Private Sector

Companies such as OpenAI and Microsoft are heavily investing into AI, recognizing its potential to become a prevalent tool in the future. The private sector employs AI to increase efficiency and facilitate decision-making processes. Yet, the potential for AI to develop a bias against certain groups is a growing concern in the private sector. The private sector places its focus in improving AI safety and transparency, but is wary of excessive regulation.

6. Questions a Resolution Must Answer

Why is it important to address the issue of cybersecurity, and what are some details that should be considered when addressing this problem?

Would different nations receive equal or disproportionate impacts from cybersecurity threats?

What are solutions that can address cybersecurity on a global scale, not just individual countries?

What are the benefits and drawbacks of AI technology, and how can these characteristics be utilized in the context of cybersecurity?

What are ways to prevent, combat, and mitigate cybersecurity threats?

Why might nations have different stances on cybersecurity, and what can be done to create incentives for mutual goals?

Is it possible to completely block cybersecurity threats, or are different approaches more feasible?

What are the most effective and impactful measures that can be taken to alleviate impacts of cyber attacks after they have been implemented?

7. Bibliography

Kaur, Ramanpreet, Dušan Gabrijelčič, and Tomaž Klobučar. "Artificial Intelligence for Cybersecurity: Literature Review and Future Research Directions." *Information Fusion*, vol. 97, 2023, Article 101804. ScienceDirect, https://doi.org/10.1016/j.inffus.2023.101804.

Salem, Aya H., et al. "Advancing Cybersecurity: A Comprehensive Review of AI-Driven Detection Techniques." *Journal of Big Data*, vol. 11, Article 105, 2024. SpringerOpen, https://doi.org/10.1186/s40537-024-00957-y.

Ali Al Maqousi, Kashinath Basu, Ahmad Al-Qerem & Amjad Aldweesh. 2025. AI-Driven Security Systems and Intelligent Threat Response Using Autonomous Cyber Defense. AI-Driven Security Systems and Intelligent Threat Response Using Autonomous Cyber Defense 501 526 .

Faisal Aburub & Saad Alateef. 2025. AI-Driven Security Systems and Intelligent Threat Response Using Autonomous Cyber Defense. AI-Driven Security Systems and Intelligent Threat Response Using Autonomous Cyber Defense 79 104 .

Ofusori, L., Bokaba, T., & Mhlongo, S. (2024). Artificial Intelligence in Cybersecurity: A Comprehensive Review and Future Direction. *Applied Artificial Intelligence*, *38*(1). https://doi.org/10.1080/08839514.2024.2439609

Salem, Aya H., et al. "Artificial Intelligence in Cybersecurity: A Review and a Case Study." *Sensors*, vol. 14, no. 22, 2024, Article 10487. MDPI, https://doi.org/10.3390/s142210487.