GA1 Chair Report

Topic 2: Developing International Norms for Cybersecurity and Protecting Critical Infrastructure from Cyber-Attacks

Table of Contents

Personal Statements

Chair – Khalid Tayeb

I am Khalid Tayeb, I'm a student at the international school of Stuttgart, this will be my first time chairing and I am very excited to be your chair in GA1. In my free time I enjoy playing sports, especially basketball. I will see you all at the conference.

Deputy Chair – Mithun Krishna Nithiyanandam

I am Mithun Krishna, from Cologne International School and I will act as the deputy chair for the General Assembly 1. This is going to be my second time in MUNISS, first time as a chair. This is going to be my 6th MUN Conference. Apart from MUN, my interests lie in watching movies and tv shows. I am very thrilled to be part of this committee and I am looking forward to meeting you all in the conference.

Introduction

The ever-increasing necessity of cybersecurity and protecting vital infrastructure against cyberattacks is the focus of this topic. The threat of cyberattacks is growing as governments, corporations, and individuals rely more and more on digital networks, endangering public safety, economic stability, and national security. Targeting vital industries including banking, healthcare, energy, and telecommunications, cyber threats have grown increasingly complex and include ransomware attacks, data breaches, and state-sponsored cyber espionage. In order to provide a coordinated response to cyber threats, important tactics for improving global cybersecurity include strengthening capacity-building in Less Economically Developed Countries (LEDCs), implementing comprehensive cybercrime laws, and encouraging international cooperation. To hold bad actors accountable and discourage cybercriminals, legal and regulatory structures must be strengthened. This involves updating current cybersecurity laws, stiffening sanctions for cybercrimes, and enhancing systems for identifying and apprehending transnational cybercriminals.

Additionally, by offering technical know-how, financial support, and resources to improve cyber resilience, capacity-building initiatives at LEDCs can aid in closing the cybersecurity gap. Many developing countries are more susceptible to cyber assaults because they lack the necessary cybersecurity workforce and infrastructure. These nations may strengthen their capacity to identify, stop, and handle cyber incidents by funding cybersecurity education, training initiatives, and the creation of national cybersecurity agencies. Because cyberthreats transcend national boundaries and necessitate a coordinated worldwide response, international collaboration is also essential. To improve global cyber defences, governments, international organisations, and private sector stakeholders must work together through partnerships, cooperative cybersecurity exercises, and intelligence-sharing agreements. Multilateral cooperation is greatly aided by initiatives like the United Nations' work on responsible state behaviour in cyberspace and the Budapest Convention on Cybercrime.

In addition, the development of clear international standards and frameworks can support responsible state conduct in cyberspace while

shielding vital infrastructure from malicious cyber activity. Cyberspace disputes can be avoided and openness can be increased via agreements on cyberwarfare, digital sovereignty, and ethical hacking norms. By incentivising companies to adopt robust security measures and provide governments with cyber threat intelligence, public-private partnerships can further improve cybersecurity. Cyber resilience can also be increased by putting cutting-edge technology solutions into practice, such as zero-trust architectures, blockchain security mechanisms, and artificial intelligence-driven threat detection. The international community can reduce cyberthreats and guarantee the safety and stability of the digital environment by adopting a proactive and cooperative strategy.

Glossary

- UNDP (United Nations Development Programme): Supports global cybersecurity development.
- EU (European Union): Regulates cybersecurity and data protection (e.g., GDPR).
- NATO (North Atlantic Treaty Organization): Military alliance addressing cyber threats.
- ASEAN (Association of Southeast Asian Nations): Promotes regional cybersecurity cooperation.
- Critical Infrastructure: Essential systems like power grids and finance, vulnerable to cyberattacks.
- Cyber Warfare: State or non-state cyberattacks on nations' infrastructure or security.
- Ransomware: Malware that locks data and demands payment.
- GDPR (General Data Protection Regulation): EU law setting global data protection standards.
- Budapest Convention: First treaty on cybercrime cooperation.
- Stuxnet (2010): Cyberattack on Iran's nuclear program, showing cyber warfare risks.
- Zero-Day Vulnerability: Undetected security flaw exploited by hackers.

Issue Explanation

In the current digital age, interconnected computer systems and digital networks are crucial for providing basic services including transportation, healthcare, water, and power. These developments increase accessibility and efficiency, but they also make vital infrastructure more vulnerable to cyberattacks. These systems are targeted by cybercriminals, such as state-sponsored hackers, organised crime groups, and rogue individuals, for monetary gain, political ends, or to create extensive disruption. Creating strong cybersecurity standards and defences against more frequent and sophisticated cyberattacks has become a top priority worldwide. Cyber dangers endanger public safety, economic stability, and national security in the absence of robust security frameworks.

Problems and Consequences

The introduction of harmful software, like ransomware, into vital systems is one of the main dangers of cyberattacks. These assaults are used by cybercriminals to encrypt or block critical functions, then demand ransom payments before granting access again. Data breaches, monetary losses, and operational delays that can last for hours, days, or even weeks are just a few of the dire repercussions that victims of these assaults must deal with. Many companies are compelled to pay the ransom in order to recover control of their systems, particularly those with insufficient security measures. Businesses frequently have to spend millions on cybersecurity specialists and forensic investigations to get rid of malware and fortify their defences, even if they don't comply.

Cyber breaches seriously harm a company's reputation and undermine public trust in addition to causing financial losses. Companies who neglect to safeguard private client information risk fines, legal action, and a permanent decline in their clientele. For instance, e-commerce sites, healthcare facilities, and financial institutions manage enormous volumes of financial and personal data, which makes them attractive targets for hackers. Customers may lose faith in these companies' ability to protect

data when they have breaches, which could result in a drop in business or possibly their permanent closure.

Critical infrastructure cyberattacks have considerably more dire repercussions. A good illustration of how cybersecurity flaws can affect millions of people is the 2021 Colonial Pipeline ransomware attack. After the pipeline's computer systems were compromised by the DarkSide ransomware organisation, the business was forced to cease operations. Fuel shortages, panic purchasing, and price surges resulted from the Colonial Pipeline, which provides about 45% of the fuel used along the U.S. East Coast, becoming offline for a few days. A shortage of jet fuel led numerous airlines to cancel flights, and petrol outlets in several states ran out of fuel. The business paid the hackers $4.4 million in ransom in an attempt to swiftly resume operations, albeit law authorities subsequently retrieved some of this money. This event showed how catastrophic cyberattacks can be to a country's infrastructure, causing supply chain disruptions, economic damage, and even death threats.

Attacks on hospitals, water treatment plants, and electrical grids can also have catastrophic consequences. A cyberattack on a hospital's systems has the potential to destroy patient data, postpone necessary medical procedures, or even interfere with life-saving equipment. A patient died in 2020 as a result of a cyberattack on University Hospital Düsseldorf in Germany, when system malfunctions prevented the patient from receiving prompt medical attention. The actual risks of cyber threats to public safety are brought to light by attacks on water facilities, such as the 2021 Oldsmar, Florida water plant cyberattack, in which hackers tried to contaminate the city's water supply by raising sodium hydroxide levels.

Because of our increasing reliance on digital systems, cybersecurity is becoming a major worldwide concern. Businesses, governments, and vital services will continue to be exposed to attacks that might disrupt economies, jeopardise national security, and endanger lives if robust defences are not in place. International collaboration, stringent cybersecurity laws, and continuous investment in cutting-edge security technologies are all necessary to meet these problems.

Perspectives of Parties Involve

United States: The Cybersecurity and Infrastructure Security Agency (CISA) leads efforts to secure critical infrastructure. CISA emphasizes global collaboration to mitigate risks to interconnected cyber and physical systems, aiming to enhance resilience against emerging threats

United Kingdom: In 2024, the UK hosted an international summit with experts from the EU, US, Australia, Canada, India, Japan, and the African Union. The summit focused on strengthening defenses against cyber threats and developing cybersecurity skills.

North Atlantic Treaty Organization (NATO): NATO is adapting to unconventional hybrid threats. The alliance is enhancing intelligence sharing, cyber defenses, and protection of critical infrastructure, with plans to adopt a comprehensive response strategy for hybrid attacks

Microsoft: The company has proposed a framework for international cybersecurity norms aimed at reducing conflicts in cyberspace and protecting critical infrastructure.

History of the Topic

The concept of cybersecurity was introduced after the incident in 1971 where Bob Thomas, a computer programmer with BBN, created and deployed a virus that served as a security test. It was not malicious but it did highlight areas of vulnerability and security flaws in what would become the internet. But the very first cyberattack occurred in France in 1834. Two thieves stole financial market information by hacking the French Telegraph System. The largest data breach that ever happened would be Cognyte. They reported a data breach was in excess of 5 billion records. Over a four day period, the database was exposed, leaving 5,085,132,102 records vulnerable that contained information including: Name, Email Address, Password and Data Source.

The development of international cybersecurity can be broken down into distinct phases:

Early Phase (1990s-Early 2000s)

- The US emerged as an early leader, creating the first national cybersecurity policies
- Most other nations had limited understanding or policies around cyber threats
- Focus was primarily on domestic protection rather than international cooperation

Transition Phase (Mid-2000s-2010)

- The UN began facilitating global cybersecurity discussions through its Group of Governmental Experts
- Two distinct approaches emerged:
- Russia and China advocated for strict international treaties
- Western nations preferred flexible, non-binding guidelines
- Countries started recognizing the need for international collaboration

Cooperation Phase (2010-2015)

- UN member states agreed on basic voluntary guidelines for cyber behavior

- The EU developed comprehensive regional cybersecurity strategies
- Nations began sharing threat intelligence and best practices

Divergence Phase (2015-2020)

- Countries strengthened their domestic capabilities:
- US created CISA to protect critical infrastructure
- Japan and Canada enhanced their national frameworks
- Different philosophical approaches to cyber governance continued between East and West

Current Phase (2020-Present)

- Renewed focus on international cooperation while maintaining strong national programs
- All UN members agreed to basic frameworks for responsible behavior
- Countries like the US and Canada are implementing stricter infrastructure protection laws
- Increased emphasis on public-private partnerships and cross-border collaboration

Overtime, the number of cyberattacks on critical infrastructure has worsened. Between January 2023 and January 2024, critical infrastructure worldwide experienced over 420 million attacks, marketing a 30% rise from the previous year. In 2024, the US utilities saw a 70% surge in cyberattacks compared to the same period in 2023. These trends highlight the escalating threat to essential services, underscoring the need for enhanced cybersecurity measures and international cooperation

Potential Solutions for the issue:

NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE): Since its establishment in 2008, the NATO CCDCOE has been addressing the subject of 'cyber norms.' The Centre has focused on how existing international legal norms apply to cyberspace, notably through the Tallinn Manual process.

UN Resolution 58/199 (January 2004): This resolution focuses on creating a global culture of cybersecurity and protecting critical information infrastructures

UN Resolution 64/211 (March 2010): This resolution emphasizes the creation of a global culture of cybersecurity and reviews national efforts to protect critical information infrastructures

International Chamber of Commerce (ICC): The ICC has developed guidelines for protecting the cybersecurity of critical infrastructures and their supply chains. These guidelines offer actionable insights and a holistic approach to addressing evolving cyber threats, emphasizing the balance between regulation and sustainable controls supported by both the private sector and governments

Bibliography

Brandon Wales. *CISA Global*. 2021, www.cisa.gov/sites/default/files/publications/CISA_Global_Print-021721_508.pdf.

Coker, James. "How Countries Are Protecting Critical Infrastructure from Cyber Threats." *Infosecurity Europe*, 18 Apr. 2024, https://www.infosecurityeurope.com/en-gb/blog/regulation-and-policy/how-countries-protect-critical-infrastructure.html.

CopyCEI. "The Consequences of Cyber Attacks and Their Impact on Cybersecurity." *CEI*, 26 Apr. 2023, copycei.com/the-consequences-of-cyber-attacks-and-their-impact-on-cybersecurity.

Daniels, Michael, and Allan Cullison. "As Russia and China Rewrite Rules of War, NATO Adapts Its Game Plan." *Wall Street Journal*, 8 Dec. 2024, www.wsj.com/world/europe/as-russia-and-china-rewrite-rules-of-war-nato-adapts-its-game-plan-76432a2e.

Khan, Mehreen. "World Experts Gather to Tackle Cyber Threats." *The Times*, 15 Sept. 2024, www.thetimes.co.uk/article/world-experts-gather-to-tackle-cyber-threats-c78mkg6lt?.

Lewis, James Andrew. "Creating Accountability for Global Cyber Norms." *Center for Strategic and International Studies*, 23 Feb. 2022, https://www.csis.org/analysis/creating-accountability-global-cyber-norms.

Microsoft. "International Cybersecurity Norms Reducing Conflict in an Internet-Dependent World." *Microsoft*, 2014, query.prod.cms.rt.microsoft.com/cms/api/am/binary/REVroA.

Monroe University. "Cybersecurity History: Hacking and Data Breaches." *Monroe University*, www.monroeu.edu/news/cybersecurity-history-hacking-data-breaches#:~:text=Cybersecurity%20history%20is%20interesting%20indeed,would%20become%20%E2%80%9Cthe%20internet.%E2%80%9D.

"Protecting the Cybersecurity of Critical Infrastructures and Their Supply Chains - ICC - International Chamber of Commerce." *ICC - International Chamber of Commerce*, 29 Jan. 2025, iccwbo.org/news-publications/policies-reports/protecting-the-cybersecurity-of-critical-infrastructures-and-their-supply-chains/.

"Cyberattacks on Critical Infrastructure Increased by 30% in One Year." *Security Magazine*, 26 Aug. 2024, www.securitymagazine.com/articles/100982-cyberattacks-on-critical-infrastructure-increased-by-30-in-one-year.

"Cyberattacks on US Utilities Surged 70% This Year, Says Check Point." *Reuters*, 11 Sept. 2024, https://www.reuters.com/technology/cybersecurity/cyberattacks-us-utilities-surged-70-this-year-says-check-point-2024-09-11/.

"Why the World Needs a New Cyber Treaty for Critical Infrastructure." *Carnegie Endowment for International Peace*, 15 Mar. 2024, https://carnegieendowment.org/research/2024/03/why-the-world-needs-a-new-cyber-treaty-for-critical-infrastructure.

OPENAI. "ChatGPT." *ChatGPT.com*, OpenAI, 30 Nov. 2022, chatgpt.com.