Committee Chair Report

GA1 - General Assembly 1

Topic 1: Establishing Norms and Regulations to Strengthen International Cybersecurity and Personal Data Privacy.

Chair: Yara Bazeih
Deputy Chair: Jady Yan

Personal Statements:

Chair – Yara Bazeih:

Good morning everyone, my name is Yara, I am 15 years old, I am from Lebanon and I go to ACS Hillingdon in London, England. This is my first time in MUNISS but I have been to many other conferences like THIMUN. MUNISS is an international conference where all people interested in Model UN can come to challenge themselves and work on their critical thinking and communication skills. I am very thankful I will chair this committee and wish all of you the best of luck during this conference. That said, I would like to welcome you to General Assembly 1, where we will be discussing important topics surrounding cybersecurity, arms trafficking and 3D printing weaponry. Since this is a beginner committee, we encourage every delegate, no matter their experience, to put themselves out there. Even if you're not sure what's going on, don't worry, most people don't. This debate is a first experience for most of you and so, don't be afraid to participate.

Deputy Chair – Jady Yan:

My name is Jady and I am 15 years old, and I had the experience participating in the Model United Nations MUNISS conference last year. In that conference, I was part of the World Health Organization (WHO) committee, where I discussed global health issues. I am excited to bring my experience and passion for international affairs to the General Assembly First Committee (GA1) as your deputy chair.

Introduction:

The Model United Nations International School of Stuttgart (MUNISS) conference is a platform that gathers students from around the country to engage in diplomatic simulations, creating an understanding on global issues. As a participant in MUNISS, I had the opportunity to engage myself in debates, resolution drafting, public speaking, and critical thinking.

Committee Overview:

The General Assembly First Committee (GA1) is one of the six main committees of the United Nations General Assembly. GA1 deals with disarmament, global challenges, and threats to peace that affect the international community. It provides a forum for all UN member states to discuss and address security issues, such as cybersecurity, which has become increasingly important in today's world.

According to the Charter of the United Nations, the General Assembly may:

- Consider and approve the United Nations budget and establish the financial assessments of Member States
- Elect the non-permanent members of the Security Council and the members of other United Nations councils and organs and, on the recommendation of the Security Council, appoint the Secretary-General
- Consider and make recommendations on the general principles of cooperation for maintaining international peace and security, including disarmament
- Discuss any question relating to international peace and security and, except where a dispute or situation is currently being discussed by the Security Council, make recommendations on it
- Discuss, with the same exception, and make recommendations on any questions within the scope of the Charter or affecting the powers and functions of any organ of the United Nations
- Initiate studies and make recommendations to promote international political cooperation, the development and codification of international law, the realisation of human rights and fundamental freedoms, and international collaboration in the economic, social, humanitarian, cultural, educational and health fields
- Make recommendations for the peaceful settlement of any situation that might impair friendly relations among countries

First-Time Delegates:

For many delegates, participating in GA1 could be their first experience in a Model United Nations. It is important to create an environment where first-time delegates feel comfortable to contribute their ideas and perspectives. We will provide clarity in procedures and provide guidance on debate etiquette and create discussions to help delegates navigate their first MUN experience.

Beginner Committee Functioning:

In a Model United Nations (MUN) setting, delegates engage in debates, negotiations, and resolution drafting to address global issues. Committees like GA1 provide a platform for delegates to represent their assigned countries' interests, perspectives, and collaborate on finding solutions to challenges. MUN procedures, such as the rules of parliamentary debate and the format for drafting resolutions are crucial for delegates to participate and contribute to committee sessions.

GA1 Chair Report

Topic 1: Establishing Norms and Regulations to Strengthen International Cybersecurity and Personal Data Privacy.

Introduction:

Cybersecurity has become a concern in today's world as advancements in technology can determine both unknown opportunities and new challenges. From state-sponsored cyberattacks to hacking by non-state actors, the threat of technology is evolving quickly, creating significant risks to people, businesses, and governments worldwide.

Summary of the Topic:

Cybersecurity measures aimed to protect computer systems, networks, and data from unauthorised access, exploitation, or disruption. Society's reliance on the digital world for communication and services has made cybersecurity a large issue for global stability. As cyber threats grow through national borders, cooperation and coordination between states are necessary to address the challenges created by cyber attacks and cybercrime.

Glossary:

1. Cybersecurity: Measures designed to protect computer systems, networks, and data from cyber threats, including unauthorised access, exploitation, and disruption.
2. Cyber Attack: Deliberate exploitation of computer systems, networks, or infrastructure to disrupt, damage, or gain unauthorised access to data or services.
3. State-Sponsored Cyber Attack: Cyber attacks initiated or supported by government entities to achieve strategic, political, or military objectives.
4. Non-State Actor: Entities that are not affiliated with or governed by any state, such as hacker groups, cybercriminal organisations, or terrorist networks.
5. Cybercrime: Criminal activities conducted through or targeting computer networks or digital devices, including hacking, identity theft, and financial fraud.

Issue Explanation:

The present situation in cybersecurity is characterised by a growing number of cyber threats and attacks. They target various sectors such as government, infrastructure, businesses, and individuals. These attacks create challenges leading to economic losses, breaches of privacy, etc

Failing to prevent cybersecurity threats could increase vulnerabilities and create more issues for the rest of the world. A lack of cooperation between member states in combating cyber

threats may result in reducing global trust in technologies and delaying socio-economic development. The most significant threats of cyber security include:

- Social engineering
- Third-party exposure
- Configuration mistakes
- Poor cyber hygiene
- Cloud vulnerabilities
- Mobile device vulnerabilities
- Poor data management

History of the Topic:

The beginning of cybersecurity as a global concern can be traced back to the early days of the internet. With the first recorded cyber attack dating back to the 1970s. However, the problem has grown in recent decades with the expansion of digital infrastructure and thereby increasing cyber threats.

Various countries, including the United States, Russia, China, and North Korea, have been implicated in state-sponsored cyber attacks targeting infrastructure, political institutions, and private companies. The cyber warfare capabilities have increased tensions in states and raised awareness about potential cyber conflicts.

The very first cyberattack occurred in France in 1834. Two thieves stole financial market information by hacking the French Telegraph System. There were other “hackers” who emerged over the years to interrupt phone service and wireless telegraphy, but it wasn’t until 1940, when Rene Carmille became the first ethical hacker. He was a computer expert and member of the Resistance in France during the Nazi occupation. He owned the machines that the French government used to process information. He discovered that the Nazis were using the machines to track down Jews, so he offered to allow them to use his machine. They took the bait, and he then used that access to hack them and disrupt their efforts.

According to Monroe College, “Cybersecurity is big business these days, especially now that the internet is a major part of our everyday lives and most businesses, as well as governmental agencies, rely on it for everything from record storage to operations. Cybersecurity professionals are employed or contracted with most corporations and

government agencies and a majority of mid-to-large sized businesses. It has become a necessity. As the internet has grown so, too, have the threats."

Cybersecurity helps protect individuals, businesses, and governments from people who seek to gain access to systems illegally and create havoc through:

- Viruses
- Phishing
- Man in the middle attack
- Password breach
- Denial of Service attack
- SQL Injection
- Ransomware

These attacks can destroy digital devices like smartphones, tablets, etc. They can trick individuals into giving out their login information. This can impact sectors such as financing, work, email, and other sensitive areas. Moreover, they can steal information, including people's identities, which leads to identity theft.

The biggest breach in history occurred in 2005 as business and governments transitioned from paper to digital records of information. This made data breaches increase in frequency and intensity.

In 2005, the Privacy Rights Clearinghouse reported 136 data breaches and more that 4,500 data breaches have been announced to the public. Experts have estimated that the numbers are actually higher.

Cognate, with the largest data breaches of all time, reported a data breach was in excess of 5 billion records. In the next four days, the database was exposed, which left more than 5 billion records vulnerable as it contains information that include:

- Names
- Email Addresses
- Passwords
- Data Sources (Canva, MySpace, Tumbler, etc)

On the other hand, hacking didn't always have a negative connotation. During the 1960s, engineering students used the term to indicate various methods of optimising machines and systems to better their efficiency. In fact, early hacking was more in line with ethical hacking.

By the 1980s and into the 1990s, as personal computers became more popular and more widely used, computer programs were used to store confidential records and personal information which caught the interest of hackers with bad intentions.

These “black hat hackers” became digital trespassers and thieves. They used their hacking skills to access private computers and destroy records, access financial accounts, steal data, and blackmail businesses into paying large sums of money.

These “white hat hackers” (ethical hackers) act as security specialists, exploring the system to identify security holes and areas that are vulnerable to hacking.

There are also “grey hat hackers”, a mix of ethical and unethical hackers, typically done at the national level for the security of government agencies.

Any Previous Attempts:

Attempts to prevent cybersecurity have been done, involving initiatives at the national, regional, and international levels. The United Nations has played a big role in promoting global cooperation on cybersecurity through the use of resolutions for cyber norms.

Additionally, governments, private companies, etc, have launched initiatives to improve cybersecurity capabilities, information sharing, and build against cyber threats. However, gaps remain in international cooperation that delay an effective response to the changing cyber challenges.

Media Contribution:

There is a wide variety of public opinion on cybersecurity. This reflects the diverse perspectives on the role of regulation, privacy concerns, and the impact of cyber threats on people’s everyday life. While some want stricter regulations and increased government involvement to prevent cybersecurity risks, other people emphasise how important it is for individual responsibility and cybersecurity awareness.

Bibliography:

1. "The Importance of Cybersecurity in the Digital Age." CyberNX, www.cybernx.com/b-the-importance-of-cybersecurity-in-the-digital-age.

2. "Cybersecurity: A Vital Safeguard in the Digital Age." Kiwop, www.kiwop.com/en/blog/cybersecurity-a-vital-safeguard-in-the-digital-age.

3. "Cybersecurity Policies." European Commission, Digital Strategy, digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies.

4. Toth, H. T. K. "Cybersecurity: An Ever Evolving Security Challenge." Sciences Po, Centre de Recherches Internationales, www.sciencespo.fr/ceri/sites/sciencespo.fr.ceri/files/art_htk.pdf.

5. "What Is Cybersecurity?" Cisco, www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html.

6. "What Is a Cyber Attack?" Check Point, www.checkpoint.com/cyber-hub/cyber-security/what-is-cyber-attack/#:~:text=A%20cyber%20attack%20is%20an,launch%20point%20for%20other%20attacks.

7. "State-Sponsored Cyber Attacks." Drishti IAS, www.drishtiias.com/daily-updates/daily-news-analysis/state-sponsored-cyber-attacks#:~:text=State%2Dsponsored%20cyber%20attacks%2C%20also,nations%2C%20organizations%2C%20or%20individuals.

8. "Nonstate Actor." ScienceDirect, www.sciencedirect.com/topics/computer-science/nonstate-actor#:~:text=Cyber%20war%20is%20an%20extension,threat%20against%20a%20nation%27s%20security.

9. "Cybercrime Definition." TechTarget, Search Security, www.techtarget.com/searchsecurity/definition/cybercrime#:~:text=Cybercrime%20is%20any%20criminal%20activity,directly%20damage%20or%20disable%20them.

10. "Cybersecurity: The History of Hacking & Data Breaches." Monroe College, www.monroecollege.edu/news/cybersecurity-history-hacking-data-breaches#:~:text=Cybersecurity%20history%20is%20interesting%20indeed,would%20become%20%E2%80%9Cthe%20internet.%E2%80%9D