Forum: Promoting Science Committee

Agenda: On measures to create global agreements regarding cybersecurity laws and protocols

Student Officer: JiHye Kim

Introduction

Cybercrime and threats pose momentous threats from individuals, businesses, society, and government entities. Cybercrime and threats result in serious consequences affecting a broad spectrum. Operating businesses experience notable losses in their finances due to the theft of their funds, intellectual property or material, or sensitive data of the organization. Organizations often spend a lot of money investing in incident response, system recovery, and strengthening security measures after an attack. In addition, cyber incidents can lead to stock price declines and loss of investor confidence. Reputation damage causes customers to lose trust and loyalty, and organizations fall victim to cybercrimes and attacks, resulting in the business being impacted both in the short and long term of its operations. It also attracts attention from the media, making businesses deal with damaged reputations. Emotions of fear and anxiety can be built due to the consistent threat of cybercrime on an individual or organization, having a notable impact on one's performance on online actions. Cybercrimes aimed towards essential services including healthcare systems and power grids can threaten a whole range from public to national security. It not only could also jeopardize a nation's security through the exposition of information. Cyberattacks do not come to an end with a consequence within a single nation. It also promotes conflicts between nations as cybercrimes can increase rapid warfare between countries which leads to international tensions and conflicts. The potential for states to use non-state actors to carry out cyber operations is increasing, and geopolitical dynamics are becoming more complex. It further puts the burden on the government for the need to develop and allocate more resources towards cybersecurity measures, infrastructures, and training. An increased advancement in technology brings everyone interested in the topic of discussion on how their personal information is processed and utilized online, balancing between the morals of to what extent is it right to do with the information.

The developed modern society provides opportunities and benefits interconnecting individuals across the world. The technology used to protect our personal data from all over the globe is being ventured for the security and privacy of individuals, organizations, a nation. To protect all categorization of data from harm and theft, cybersecurity is crucial. Cybersecurity is defined as the practice of defending networks, systems, and programs from digital ambushes. It consists of a diverse range of Artificial Intelligence (AI), Machine Learning (ML), and zero-trust security models.

Cybercrimes occur comprehensively over the world ranging from more economically developed countries (MEDC) to less economically developed countries (LEDC). Statistics from the Identity Theft Resource Center (ITRC) reveal an annual data breach report showing a recorded quantity of 2,356 cyberattacks leading to data breaches in 2023. In comparison to 1,584 in the previous year and 754 in 2018, there has been a significant increase just only over the past few years. In the United Kingdom (UK), half of all its businesses and 32% of charities in the nation report being targeted by cyberattacks in a year.

As cybercrimes and threats become more prevalent and complicated, their impacts affect a complete scale from individuals, businesses, and governments, understanding the importance that cybercrime does not target specific groups. All nations definitely should use their foresight to build consensus on a global scale, generating rules and regulations on cybersecurity. It is a crucial need to ensure a coordinated answer to this common threat in order to provide a safer cyber environment for all.

Key Terms

Antivirus - This is a drug or treatment that is effective against viruses.

Computer worm - Type of malware that automatically propagate, spreading to other devices through networks, mainly the internet.

Computer virus – A program that spreads by infecting files or systems of a computer's hard drive, then duplicating itself.

Cyber compliance - This is the process that ensures an organization adheres to manufacturing regulations, quality, and rules and regulations as regards data privacy and safety.

Cyber security - Practices done to protect systems, networks, and various programs against digital attacks or crimes that are carried through the utilization of the internet. Attacks on data conventionally aim to access, change, or destroy data.

Cyber threats - Consists of any circumstances or events with the intention to negatively impact the industry's operation (organization reputation, mission, function, etc.) or assets. It could also be Unauthorized access, disclosure, or modification of personal information of an individual.

Cybercrime - Criminal activities that are carried out via computers or the internet.

Cyber hygiene - Practice organizations and individuals utilize in order to maintain a healthy, clean, and secure resilience of their systems, devices, and data on the internet. Its aim is to protect and secure data from attacks or threats.

Data breach - This is a consequence of personal, protected, or sensitive information being exposed to a group or individual that is not authorized to access.

Digital sovereignty - The ability to have control over one's own digital data.

Encryption - Process of converting data or information into a code specifically to protect the data from unauthorized access.

Interoperability - The ability of a computer system or software to exchange and make use of information.

Law – System of rules that a particular nation, society, or community recognizes as regulating the actions of its members and which it may enforce by imposition of penalties.

Threat intelligence - This is also referred to as "cyber threat intelligence" which is a piece of actionable detailed information to prevent and confront cybersecurity threats.

Protocols – An official procedure or system of rules governing affairs of state or diplomatic occasions.

General Overview

Cybersecurity engineers and analysts predict that cybersecurity to continuously be enhanced to face off the rapidly developing cybercrime and threats. Reports indicate a significant increase in both the size and complexity of crimes and threats that target organizations globally as of 2021. The estimated average cost of data breaches in 2021 was $4.24 million. It distinctly reflects the financial impact on organizations.

It has been reported by the United International Telecommunication Union (ITU) that over 4.9 billion individuals have access to the Internet, underscoring the urgent need for effective and secure cybersecurity measures for the purpose of protecting the increasing supply of online population.

According to the United Nations Office on Drugs and Crime (UNODC) report, cybercrime and threats are projected to cost the global economy an estimated $6 trillion annually by 2021, reflecting how anybody can become the victim of cybercrime and threats.

African Nation

As of 2021, it was estimated that 33% of the population in Africa had access to the internet which was a jump of 23% from 2018. Cybercrime began to become reachable in recent years as the development of digital technology and the internet boosted. African government has to continuously face unmanageable cybercrime and threats that are interminably evolving affecting a wide range from individuals to business organizations. If the problem is not handled properly, it will have serious consequences for the government's finances and security.

United States (U.S)

The United States has implemented various acts and legislation to protect against damages that could be caused by cybercrime some include the California Consumer Privacy Act (CCPA) is a law approved by government bodies and put into place on July 1, 2023. This legislation addresses residents of California, requiring businesses to give customers reasonable access to their data and authority over it. Additionally, as of December 18, 2023, previously publicly listed companies are required to follow the rules on the release of information about an incident developed by the Securities and Exchange Commission (SEC). As a result of the new changes, it’s now required of publicly traded corporations to communicate a cybersecurity breach within 4 business days after determining that such a breach is significant and may affect shareholding investment decisions. $4.2 billion exceeding loss was reported by the FBI’s Internet Crime Complaint Center (IC3) due to cybercrime as of 2020. There was a 68% increase in data breaches within a year from 2020 to 2021.

United Kingdom (UK)

The United Kingdom has enacted laws to combat cybercrime and protect its citizens, including: The Data Protection Act (DPA) is a law in the UK that governs the way people’s particular information is dealt with. It came into force in 2018 and now replaces the old Data Protection Act (1984), which set out the rules concerning data management, such as the organizations that deal with Managed Service Providers (MSP), giving customers the right to

know how their data is used. MSPs who intend to operate in the UK market should also comply with the European Union's new Network and Information Systems regulation NISD2. NIS1 was the directive that was replaced by NIS2 which will be effective from 17th October 2024. The NIS2 Directive mandated enhanced scrutiny measures for the entire governance framework as well as imposing increased penalties for failure to comply with regulations.

China

China has continuous practices to reduce incidents of cybercrime and treats as much as possible. An estimated value of $45 billion is invested in the cybersecurity market by the government. Over 10,000 websites including a variety of major social media platforms are blocked access by China as part of its internet management measures.

Japan

The Japanese government has plans to increase the budget for cybersecurity to $1.4 billion by 2025 to enhance cybersecurity, going against the developing threats of cybercrimes. It was reported by the Japanese government that an estimated 40% of cyber incidents in 2020, targeted critical infrastructure. A survey result showed nearly 60% of all Japanese organizations had experienced cyberattacks as of 2021.

Major parties involved

Governments and regulatory bodies

The government and regulatory bodies both develops and implements frameworks and policies for cybersecurity. They are mainly constructed to protect the rights of sensitive data from individuals and organizations from groups that are taking advantage from the internet. It is still now continuing, developing for the better to fight against cybercrime and threats.

Private sector/Organizations

Keystone technology businesses are heavily impacted by cybercrimes in various aspects. Major firms have the ability to quickly go against antiviruses and find solutions to protect their sensitive data. New start-up organizations frequently develop innovations for their security of data, preventing the occasions of cybercrimes and threats. Research and development (R&D) of cybersecurity is being heavily invested in in order to develop technologies including the major example of AI to detect crimes and threats, making machines have the analytical skill to predict

any source of cybercrime. Trainings are conducted to help address the skill gap and knowledge of cybersecurity in the industry.

Non-governmental organizations (NGOs)

Some of these organizations support incidents that happen due to cybersecurity, offering assistance to the affected community or businesses. NGOs frequently engage with advocacy, having a great deal of influence on governmental policies, balancing out the need for individual rights and security needs. Raising public awareness and educating individuals by creating campaigns that raise awareness on the risk of cybercrimes and safe online practices skills and knowledge to the public.

Timeline of Events

Cybercrime and threats would continuously develop and rise. Individuals and group targets sensitive data for their use, resulting in severe consequences and damages worth billions of dollars. As cybercrime becomes more easily accessible, the issues with cybercrimes and threats are not being resolved easily. These are several events that have happened in the past.

Date	Description of event
1970s	Cybersecurity was first introduced in the 1970s when a researcher named Bob Thomas innovated a computer program named Creeper. It could move across the Advanced Research Projects Agency Network (ARPANET) which was the forerunner of the internet, leaving trails wherever it went. The inventor of email, Ray Tomlinson generated Reaper, a program that chases and deletes Creeper. It was the very first exemplification of antivirus software and a self-replicating program. The Diffie-Hellman key exchange protocols revolutionize cryptography and secure communication as they enable both parties to derive a common secret key over an insecure channel that forms an indispensable premise for most modern encryption techniques.
1980s	Emerged to become the antivirus era as computer viruses developed and began to be proliferated in the 1980s. Efforts to combat viruses commenced with the introduction of antivirus software, setting the stage for an endless conflict

	between cybercrime and security. The ARPANET system was hacked by 414 hacker groups. It underscored the susceptibility of computer networks, having increased concerns about security and stimulating organizations to reevaluate their digital security.
1987	In 1987, the Vienna virus, an extremely simple virus that was a source code published noticeably times, accounting for its numerous variants known to be destroyed by antivirus programs was created. McAfee developed the first commercial antivirus software that provided users an essential weapon to combat emerging cyber threats which contributed significantly towards the advancement of creating secure programs.
1991	It was 1991 when Polymorphic virus, a malware that can adapt and change its physical forms to avoid detection and circumvent cybersecurity systems began to emerge. It brought antiviruses a significant challenge.
1995	Data Encryption Standards (DES) is a cryptographic key and algorithm applied to a set of data simultaneously was first adopted to secure electronic communications in 1995. It set a milestone in cryptography, laying the foundation for modern encryption standards to protect sensitive data.
1999	1999, the Melissa virus, created by David Lee Smith was a mass mailing macro virus that caused private documents to be revealed without the user being informed. Melissa could easily overload electronic servers. It imposes an estimated cost of $80 million worth of damage. Compelling organizations to make huge investments in cleanups and to mitigate the severe consequences of its widespread impacts on the computer.
Early 2000s	The Early 2000s was the starting point for numerous computer viruses and worms infecting computers globally. The outpouring of cyber-attacks promoted organizations to prioritize regulations. The Love Bug known as ILOVEYOU was a computer worm infecting an estimated quantity of over 10 million personal window computers

	spreading globally within just a few days. Causing billions worth of damages and gave the incentive to improved security measures. Code Red Worm (2001) was a computer worm attacking computers running Microsoft's Internet information services server. More than 359,000 computers connected to the internet were infected within less than 14 hours. SQL Slammer worm (2003) also known as Sapphire exploded the internet taking ten minutes to take over 90% of all unpatched laptops running SQL server on the internet. Mydoom (2004), is considered one of the worst computer viruses in history causing more than $38 billion work of damage by stealing email addresses from computers infected and sending them to the addresses.
2006	The Health Insurance Portability and Accountability Act (HIPPA) and Payment Card Industry Data Security Standard (PCI-DSS) compliance rules are established. It aimed to safeguard healthcare and financial data that are sensitive.
2010s	In the name of the Stuxnet worm, it targeted control systems in industries, clearly demonstrating the challenge associated with cyberwarfare in 2010. In 2017, the WannaCry ransomware attack occurred impacting an estimated 200,000 computers globally.
2022	Cybersecurity has evolved rapidly to combat developing cybercrimes and threats. Artificial Intelligence, ChatGPT was released in 2022, having dramatic impacts globally. AI, depending on how it is manipulated can become a useful tool to detect cybercrimes, or it can be taken as an advantage.

UN Involvement, Relevant Resolutions, Treaties and Events

- UN Counter-Terrorism Centre (UNCCT) is the center which promotes international collaboration to go against terrorism, supporting Member States in constituting the Global Counter-Terrorism method, looking upon peace and security.

- UN Office of Counter terrorism (UNOCT) The Global Counter-Terrorism Program on Cybersecurity and New Technologies was adopted in April 2020 with the aim of enhancing the capacities of Member States, international and regional organizations, and UN entities to raise awareness of the terrorist cyber-threat and enhance technical capacities to prevent, mitigate, and respond to terrorist and violent extremist groups misusing new technologies like the internet and Artificial Intelligence.

- The UNOCT/UNCCT Program on Cybersecurity and New Technologies contributes to strengthening the capacities of Member States and the private sector to prevent attacks against critical infrastructure by terrorist actors. It also tends to reduce the impact of an attack and recover and restore the attacked system in such cases.

- As of 2022, the UNOCT/UNCCT and INTERPOL has released the CT TECH imitative which aimed to enhance the capacities of law enforcement and criminal justice judication in chosen partner nations in order to counter taking advantage of recently developed emerging technologies for cyber-terrorist purposes. Additionally, it support Member States in manipulating new and appearing technologies to go against cybercrime and terror. CT TECH is funded by the European Union and administered under the UNCCT Global Counter-Terrorism Program on Cybersecurity and New Technologies.

- The Office also provides expertise in international fora on the use of unmanned aerial systems, as well as delivers capacity-building assistance in open-source intelligence, dark web, cryptocurrencies, and digital forensic investigations.

- Past UNOCT projects have included the use of social media to gather open source information and digital evidence in counter-terrorism and violent extremism while considering respect for human rights.

Possible Solutions

Cybersecurity risks are closely tied to bigger social, money, and political trends, making a tricky situation that needs complete answers. As one expert says “The link between digital systems means that weak spots in one spot can cause problems in others.” For instance, while lots of groups work on boosting their online protection, they often miss how much international teamwork matters in tackling these risks. The growth of cyberattacks not only puts single groups in danger but also harms country safety and money steadiness worldwide. It is thus key to see that good cybersecurity needs to think of different local situations and shared plans. This needs a many-sided way that has global pacts, idea sharing, and skill growth to deal with the main causes and effects of online crime. It is crucial for the international community to acknowledge the urgency of the problem and come together in order to carry out collective responses that include initiatives of:

International Cybersecurity Framework

Provide a comprehensive international framework laying out standardized cybersecurity laws and protocols. The framework should fit the legal systems of varying countries while promoting standards in best practices in terms of cybersecurity, incident reporting, and data protection.

Cooperative Information Sharing

Create a space for the cooperation of countries, organizations, and the private sector to share intelligence on cyber threats and adversity. This aspect of intelligent threat analysis would enable proactive attacks and fast responses to equally threatening advances.

Capacity Building and Training

Further strengthen capacity building in and training for governments, businesses, and individuals especially in the developing region. This must give value to equipping them with improved knowledge of cybersecurity skills to better enable them to prevent and respond to cyber incidents.

Joint Cybersecurity Exercise

Plan an international cyber-security exercise that will involve various countries and institutions. This helps to determine the weaknesses of the various established protocols, develop coordination between nations, and also provide methods of responding to possible threats.

Harmonized Regulatory Cooperation

Encourage cooperation on harmonized sets of cybersecurity regulations and compliance for national regulatory bodies. Within this regard, the entity will facilitate cross-border enforcement of cybersecurity laws. It will also galvanize a codified approach to cybercrime and improvements of overall security.

Bibliography

Martin, James. “How Many Cyber Attacks Occur Each Day? (2024).” *Exploding Topics*, 7 Feb. 2022, explodingtopics.com/blog/cybersecurity-stats. Accessed 22 Dec. 2024.

“Cybersecurity | United Nations - CEB.” *Unsceb.org*, 3 June 2024 unsceb.org/topics/cybersecurity. Accessed 19 Dec. 2024.

“All Courses | UNOCT LMS.” *Unoct-Connectandlearn.org*, 2020, learn.unoct-connectandlearn.org/course/index.php?categoryid=26. Accessed 19 Dec. 2024.

“All Courses | UNOCT LMS.” *Unoct-Connectandlearn.org*, 2020, learn.unoct-connectandlearn.org/course/index.php?categoryid=26. Accessed 20 Dec. 2024.

“Cybersecurity and New Technologies | Office of Counter-Terrorism.” United Nations, United Nations, www.un.org/counterterrorism/cybersecurity. Accessed 19 Dec. 2024.

Wolf, Arctic. “Polymorphic Virus | Arctic Wolf.” Arctic Wolf, 14 June 2023, arcticwolf.com/resources/glossary/polymorphic-virus/. Accessed 20 Dec. 2024.

Moore, David, et al. Code-Red. 1 Jan. 2002, dl.acm.org/doi/10.1145/637201.637244, https://doi.org/10.1145/637201.637244. Accessed 20 Dec. 2024.

Panko, Raymond R. “Slammer: The First Blitz Worm.” AIS Electronic Library (AISeL), 2024, aisel.aisnet.org/cais/vol11/iss1/12/. Accessed 21 Dec. 2024.

---. “Code-Red.” Proceedings of the Second ACM SIGCOMM Workshop on Internet Measurment - IMW ’02, 2002, p. 273, dl.acm.org/doi/10.1145/637201.637244, https://doi.org/10.1145/637201.637244. Accessed 23 Dec. 2024.

katharina.kiener-manu. “Cybercrime Module 8 Key Issues: International Cooperation on Cybersecurity Matters.” Unodc.org, 2020, www.unodc.org/e4j/ar/cybercrime/module-8/key-issues/international-cooperation-on-cybersecurity-matters.html. Accessed 24 Dec. 2024.

Manning, Sarah. “The History of Cybersecurity.” Maryville University Online, 24 July 2024, online.maryville.edu/blog/history-of-cybersecurity/. Accessed 24 Dec. 2024.

Davies, Vikki. “The History of Cybersecurity.” Cybermagazine.com, Bizclik Media Ltd, 4 Oct. 2021, cybermagazine.com/cyber-security/history-cybersecurity. Accessed 25 Dec. 2024.

Most. “Log In.” *@NordLayer*, 2021, nordlayer.com/blog/cybersecurity-statistics-2021-review/. Accessed 26 Dec. 2024.

Sobers, Rob. “157 Cybersecurity Statistics and Trends [Updated 2024].” *Varonis.com*, Varonis, 8 July 2022, www.varonis.com/blog/cybersecurity-statistics. Accessed 27 Dec. 2024.

Brands, Michael. “Cybersecurity Laws and Legislation (2024 Update).” *Connectwise.com*, ConnectWise, 6 May 2024, www.connectwise.com/blog/cybersecurity/cybersecurity-laws-and-legislation. Accessed 25 Dec. 2024.

and, Challenges. “Log In.” *@NordLayer*, 2024, nordlayer.com/blog/cybersecurity-for-ngos/. Accessed 26 Dec. 2024.

Contact Information:

Please contact the below person with any questions regarding the speech or report and good luck!

JiHye Kim - Co-Chair

WeChat ID: jhk_0510

Email: 26jkim@student.uisgz.org

Cowen Cui – Secretary General
25ccui@student.uiszc.org

Chan Kim – Head of Chair
25kchan@student.uiszc.org

Gladys Ndunge Mutinda– Director of U2NESCO
gnm@uiszc.org