Enforcing Global Cybersecurity in a Rapidly Digitizing Era

Forum: Disarmament Commission
Student Officer: Daniel Park, Deputy President

Introduction

The United Nations Office of Counter-Terrorism emphasizes the prominence of cybersecurity in current era

The United Nations Office of Counter-Terrorism Under-Secretary-General Vladimir Ivanovich Voronkov stated, "We must come together now, and we must do it fast, to mitigate this threat (technological attack) and ensure that new technologies remain a force for good rather than a force for evil." The rapid advancement of technologies, such as but not limited to development in Information Technology (IT); expanding global reality market, including Artificial Intelligence (AI), Virtual Reality (VR), and Augmented Reality (AR); and growing industrial technology, has assisted the world to be adapted to digitizing era in a short period of time. Nowadays, people are able to proceed with most of their tasks with the assistance of technologies. However, along with the technological convenience, which allows the population to save time in this urgent society, implementing global cybersecurity must become one of the essential targets that has to be widely recognized by the public.

The International Telecommunication Union (ITU) is a part of specialized agencies of the United Nations that has been established in 1865, for the purpose of promoting international communications in telegraphic networks. This agency is committed to unite the world's population by establishing technical standards to ensure telegraphic networks and technologies are interlinked. According to the International Telecommunication Union, cybersecurity indicates the accumulation of regulations, guidelines, devices, security strategies, protection systems, and risk management approaches that can be employed in order to defend the cyber environment of organizations, nations, and individual users. Cybersecurity aims to guarantee the acquisition and conservation of securing cyber information in the cyber environment.

Background

Cybersecurity directs to the procedure of defending and restoring data, digital programs, networks, and devices from any type of cyberattacks and cybercrimes. Significant amounts of online data on cyberspace contain data not only the data owned by individuals and companies, but also the data related to the governments, organizations, and military forces. Owing to the proliferation of malicious threats on these data, no one can be relieved by the danger of

cyberattacks and cybercrimes. Moreover, no one can guarantee that confidential data, such as records on national security, health reports, finance accounts, and personal information, will be secure without enforcing global cybersecurity. Governments, official corporates, and prominent organizations worldwide are inclined to form prevention in security, but regardless of how much they are secure, it is likely that cyberattacks will occur in any form.

According to the Statista, the number of cybersecurity incident reports by federal agencies in the United States of America has continuously increased from 2006 to 2015. The annual number of reported incidents in 2006 was 5,500, while in 2015, the annual number of reported incidents was 77,200. During the time period of 2006 to 2015, there was no phenomenon that the number of cybersecurity incidents has decreased than the number reported in the previous year.

The International Criminal Police Organization, Interpol, has announced that the evaluation of the impact of COVID-19 on cybercrime demonstrated critical target transferred from individual users and minor corporations on the governments and major corporations. The Secretary-General of Interpol, Jürgen Stock, stated, "Cybercriminals are developing and boosting their attacks at an alarming pace, exploiting the fear and uncertainty caused by the unstable social and economic situation created by COVID-19."

The statistical facts mainly prove that cybercrimes became significant issue that damage both individuals and societies.

Due to these reasons, the nations will have to put heads together, in order to find effective measures to apply global cybersecurity in a digitizing era. As this issue has been identified recently, the solutions to solve this issue must be different from the past.

On the field of cybersecurity, the North Atlantic Treaty Organization (NATO) focuses on defending networks and asserting that international regulations are still enforced in cyberenvironment

Places of High Concern

Cyber-attacks on Estonia

On January 10th, 2007, the Estonian government announced the procedure to relocate the Bronze Soldier and burial place of Tallinn, and around April 26th-April 27th in 2007, the excavation projects began near the Bronze Soldier. There were several violent protests, so authorities in Estonia chose to accelerate the process of the relocation project. On April 27th, 2007, Estonia became one of the first countries that encountered substantial cyber-attacks in the world. Cyber-attacks using Distributed Denial of Service (DDoS) were obstructing the public, and websites targeted by the attackers, such as Estonian governmental, political, financial, and other websites, were malfunctioning. These continuous cyber-attacks were arranged by Russian individuals and groups, due to the nation's conflict on the relocation of the Bronze Soldier and burial place of Tallinn. As the time flowed, the waves

Cyber-attacks on Estonia have been recorded as the first major cyber-attack in the world

of attacks strengthened, and from May 19th, 2007, the cyber-attacks hastily decreased. As a result of these cyber-attacks, Estonia had to confront the loss of billions of euros. This cyber event could have attenuated support on Estonian government from the Estonian citizen, which may affect Estonian governmental stability. However, along with support from different countries and the North Atlantic Treaty Organization (NATO), prompt reaction conducted by the Estonian government averted citizen's disbelief in the government.

Problems Raised

The proliferation of cyberattacks and cybercrimes

Cybercrime has grown into a substantial concern to nations. The United Nations Conference on Trade and Development (UNCTAD) asserted that the 154 countries had executed cybercrime legislation, and Europe recorded the highest cybercrime legislation establishment rate, 93%. At the same time, Asia was reported as the lowest cybercrime legislation adoption rate, 55%. As the storage capacity for the Internet rapidly expands every year, types of cyberattacks have become various. With different purposes, such as gaining monetary benefit, obtaining data, and manifesting a criminal's identity for acknowledgment, cybercrimes happen in this era are rampant. Cyber terrorists are strategic, and they are extremely fast in adaptation. Those terrorists will always be seeking approaches to take advantage of mobilizing new technologies. Numerous techniques of cyberattacks and cybercrimes have escalated, including Denial of Service (DoS) attacks, hacking, malware, phishing, spoofing, ransomware, and spamming.

"Denial of Service" (DoS) attack refers to an attack that interrupts and shuts down a device or a network. By transmitting the countless amount of unidentified data to a specific server or device, this process disallows regular users to access it properly. In most cases, Denial of Service (DoS) attacks make resources inaccessible for a relatively short time. However, in some cases, Denial of Service (DoS) attacks may completely shut down the server, which permanently rejects users from approaching data.

"Ransomware" is a malignant system that contaminates the user's device, and the software exhibits notations demanding payment in order to recover the system. This type of cyberattacks has been augmenting in recent years, and hackers require transactions to be done with cryptocurrencies, such as Bitcoin. Due to the characteristics and high anonymity level of cryptocurrencies, the process to track criminals would be obscure.

Communicating users through the undesired and illegitimate process is called a "spam attack." This attack often occurs on emails or message platforms by sending innumerable emails or messages to users. Usually, these messages are unauthorized and imitated for the purpose of advertisements.

Since citizens around the world may access the Internet anywhere around the world, cyberattacks and cybercrimes do not have specific regions or languages.

Cyberwarfare

The cyber-attack involving a nation or international organization with the aim of attacking and seeking to harm another nation's or organization's cyber data. Currently, several countries, including the United States of America, the United Kingdom, the Russian Federation, Iran, India, the Democratic People's Republic of Korea, and China, have the vigorous cyber ability for both offensive and defensive cyber actions. Since offensive cyber-attacks provide a wide range of choices without risks, various reasons lead countries to initiate a cyber strategy to undermine other countries' cyber data or obtain them through unauthorized procedures. As confidential data and military systems are highly connected to the cyber systems, cyberwarfare provides rising dangers for countries.

Nowadays, nations spend military budget in a measure to achieve more cyber information

Since the United States of America particularly relies on cyber data, the United States of America is greatly revealed to malicious hacking from national or international opponents. According to the United States Department of Defense Digital Service, the United States Army was hacked by 52 hackers during the time period of October 9th, 2019, to November 15th, 2019. Even though the United States is exposed to the risks due to a high level of military spending, the United States Army has advantageous technologies and abilities in both defense and offense in cyberwarfare.

While the United States of America holds the title of the world's largest military budget, the People's Republic of China ranked second in military spending. In the area of cyberwarfare, it is said that China has a similar system in the notion of cyberwarfare compared to the United States of America. The estimated range of cyber-attacking personnel, in other words, members in the army with hacking tasks, is around 50,000 to 100,000 members. Since the 1990s, many countries have presented the allegation of espionage on the Chinese government. Some western countries even accused China of employing spies in certain industries in the European region. Chinese government constantly claimed that China is not the assailant, but the victim for proliferating cyber-attacks. Along with these allegations, China is also accountable for causing cyber-attacks on institutions and corporations located in different countries.

Key Organizations

United Nations Office of Counter-Terrorism

The United Nations Office of Counter-Terrorism was instituted through the United Nations General Assembly, and the establishment of the Office is examined as the first significant institutional reform implemented by Antonio Guterres, the United Nations Secretary-General. The functions of the Office of Counter-Terrorism include developing clarity for the United Nations counter-terrorism attempts, ensuring coordination of the four pillars of the United Nations Counter-Terrorism Strategy, and etc. As the Office is significantly related to combatting terrorism, this Office may undertake duties related to cyberterrorism.

The United Nations Office of Counter-Terrorism examines the abuse of information and communication technologies (ICT)

United Nations Information and Communications Technologies Task Force

The United Nations Information and Communications Technologies Task Force facilitates a secure and sustainable future by utilizing innovative technology. The universal interconnectivity has been focused on as the Task Force's fundamental objective. The visions for the United Nations Information and Communications Technologies Task Force are to "be solution partners and agents of transformation," "be catalysts for innovative technology solutions for organizational transformation," "ensure solutions are agile, simple, reliable, innovative and secured," "stay client-centric, solution-oriented and business-driven," and "lead the United Nations through a digital journey to support the core work of the United Nations." From the visions, it is distinguishable that the Task Force values extensively exploited technologies. Internal of the United Nations Information and Communications Technologies Task Force, there is the United Nations Office of Information and Communications Technology. The Office was mandated with initiating an information risk management regime and assisting regulations. Moreover, in 2013, the United Nations Office of Information and Communications Technology adopted an action plan to deal with the most vital deficiencies and alleviate certain risks. Considering the relevance of the tasks managed by the Office and Task Force, the cybersecurity may also be addressed by this Office and the Task Force.

Possible Solutions

Establishing explicit interpretation of cybercrime legislation between nations

As previously mentioned, 154 out of 193 member states have already enacted cybercrime regulations and policies. Referring to the United Nations Office on Drugs and Crime, cybercrime legislation recognizes not only the standards of tolerable action for the Information and Communications Technology (ICT), but also sanctions on cybercrime,

mitigation of damage, and provision of cyber-protection for people, data, systems, services, and infrastructure. Since not all countries have the same cybercrime laws, nor all countries have adopted cybercrime-related laws, the member states should clarify on cybercrime legislation. Acknowledging the significance and differences in the cybercrime laws between nations will be necessary. Lastly, identifying measures to penalize cybercriminals should be addressed in the current agenda. The number of cybercrimes is interconnected between different nations, but there is no precise measure for pursuing cybercriminals and punishing cybercriminals.

Reaffirming the importance of the United Nations Global Counter-Terrorism Strategy

The United Nations Global Counter-Terrorism Strategy was adopted by the United Nations General Assembly on September 8th, 2006, through the resolution A/RES/60/288. The Strategy specifically presents a particular global constitution to enhance national, regional, and international efforts to counter-terrorism. The United Nations Global Counter-Terrorism Strategy claims not only the declaration that terrorism in any form or expression is unacceptable, but it also determines to consider pragmatic procedures to inhibit and combat terrorism. Nowadays, international societies are aware of the dangers of cyberattacks and cyber-terrorisms. Cyberterrorism became one of the critical terrorisms that exists in the world. The Plan of Action from the United Nations Global-Terrorism Strategy provides the structure to handle certain situations that require urgent actions. The Plan of Action includes, "Measures to address the conditions conducive to the spread of terrorism," "Measures to prevent and combat terrorism," "Measures to build States' capacity to prevent and combat terrorism and to strengthen the role of the United Nations system in this regard," and "Measures to ensure respect for human rights for all and the rule of law as the fundamental basis of the fight against terrorism." As these measures listed in the Plan of Action offer guidelines for the member states, this is the reason why the leaders from nations should reconsider the United Nations Global Counter-Terrorism Strategy to comprehend effective measures to respond and combat the urgent action.

The United Nations Global Counter-Terrorism Strategy was established on September 8th, 2006, by the United Nations General Assembly

Glossary

Cybersecurity: Procedure to secure computer systems and networks from cybercrime or harm on hardware, devices, software, data, etc.

Information Technology (IT): Utilization of computer technology to store, recover, transfer, and manipulate data or information.

Sources

"About OICT | Office of Information and Communications Technology." *United Nations*, United Nations, unite.un.org/about.

"About International Telecommunication Union (ITU)." *About ITU*, www.itu.int/en/about/Pages/default.aspx.

"Cyber Risk." *United Nations*, United Nations, unite.un.org/digitalbluehelmets/cyberrisk.

"Cybersecurity | Office of Counter-Terrorism." *United Nations*, United Nations, www.un.org/Counter-Terrorism/cybersecurity.

Cybersecurity, www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx.

"Cybersecurity | Office of Information and Communications Technology." *United Nations*, United Nations, unite.un.org/information-security.

"Data Security and U.S.-China Tech Entanglement." *Lawfare*, 5 Apr. 2020, www.lawfareblog.com/data-security-and-us-china-tech-entanglement.

Kaspersky. "What Is Cyber Security?" *Www.kaspersky.com*, 10 Mar. 2020, www.kaspersky.com/resource-center/definitions/what-is-cybersecurity.

Lapehn, Allison. "Why the U.S. Should Pay Attention to China's Draft Data Security Law." *SupChina*, 5 Oct. 2020, supchina.com/2020/10/05/why-the-u-s-should-pay-attention-to-chinas-draft-data-security-law/.

McGuinness, Damien. "How a Cyber Attack Transformed Estonia." *BBC News*, BBC, 27 Apr. 2017, www.bbc.com/news/39655415.

"UN Global Counter-Terrorism Strategy | Office of Counter-Terrorism." *United Nations*, United Nations, www.un.org/Counter-Terrorism/un-global-counter-terrorism-strategy.

"UN INFORMATION AND COMMUNICATION TECHNOLOGIES (ICT) TASK FORCE LAUNCHED TODAY AT HEADQUARTERS | Meetings Coverage and Press Releases." *United Nations*, United Nations, www.un.org/press/en/2001/dev2353.doc.htm.

"What Is Cyber Security? Definition, Best Practices & More." *Digital Guardian*, 5 Oct. 2020, digitalguardian.com/blog/what-cybersecurity.

Written by Alison Grace Johansen for NortonLifeLock. "Do You Worry about Cyber Safety? Learn Some Smart Defenses." *Norton*, us.norton.com/internetsecurity-malware-what-is-cybersecurity-what-you-need-to-know.html.