Committee: Disarmament and International Security Committee

Topic: The Question of Preventing CyberTerrorism and Building a Sustainable International Cybersecurity

Student Officer: Dong Gu Ko

Position: Deputy Chair of Disarmament and International Security Committee

---

Introduction

Recently, we have seen a spate of smaller, less sophisticated, yet no less appalling acts of terrorism across geographies that involve mass casualties and fear-inducing events. This type of threat will continue to change as new technologies and opportunities reveal themselves to terrorist organizations: cyberterrorism is an example of a newly developing frontier within the peril.

As technology is steadily being developed, people are taking advantage in various fields. Especially, cyberspace is one of the things that benefit people these days. A number of people are using cyberspace as a way of collecting any information they need. However, as the technology of cyberspace is steadily improving, issues related to cyberspace, like cyberterrorism, are steadily increasing as well.

Cyberterrorism refers to using technology to cause fear and harm through online attacks. The widespread use of technology has significantly increased the frequency of malicious cyberterrorism, including malware, cloud attacks, and DDoS (distributed denial-of-service) attacks. A number of countries are suffering from these kinds of cyberterrorism these days. The two most dangerous countries of origin for cyber attacks are China(18.83%), and the United States of America(17.05%).

While the number of cases of cyberterrorism increases day by day, there are some solutions to it. One of the solutions for cyberterrorism would be the use of ICT (Information and Communication Technology). ICT is simply defined as a diverse set of technological tools and resources used to transmit, store, or exchange information. ICT takes responsibility for overseeing security system operations, including monitoring and controlling access to private information, ensuring safe data

transmission, and managing secure data storage and disposal. These ICT security measures are crucial in safeguarding confidential data from unauthorized access, modification, loss, or disclosure. The development of technology must address these pressing concerns to ensure data protection and privacy.

Definition of Key Terms

IT (Information Technology)

Information Technology encompasses the utilization of computers, storage, networking, and other tangible devices, as well as the underlying infrastructure and methodologies, to generate, manipulate, store, safeguard, and facilitate the exchange of diverse electronic data.

ICT (Information and Communication Technology)

Information and Communication Technologies is a broader term for Information Technology, which encompasses all communication technologies. This includes the internet, wireless networks, cell phones, computers, software, middleware, video-conferencing, social networking, and various media applications and services that empower users to access, retrieve, store, transmit, and manipulate information in a digital format.

Cybersecurity

Cybersecurity, also referred to as IT (Information Technology) security, encompasses the practice of safeguarding critical systems and sensitive data from digital attacks. Its primary objective is to defend networked systems and applications against threats that may arise from both internal and external sources within an organization.

Cyberterrorism

A cyber attack (cyberterrorism) involves exploiting computers or communication networks to cause significant disruption or destruction, aiming to instill fear and intimidate society into fulfilling an ideological objective. The internet can be used by terrorists to finance their operations, train other terrorists, and plan terror attacks. The more mainstream idea of cyber terrorism is the hacking of

government or private servers to access sensitive information or even siphon funds for use in terror activities. However, there is currently no universally accepted definition of cyberterrorism.

Hacking

Hacking entails the process of identifying and subsequently capitalizing on vulnerabilities within a computer system or network. Typically, this is done with the intention of acquiring unauthorized entry to personal or organizational data. While hacking is not always a malicious activity, the term has mostly negative connotations due to its association with cybercrime.

DDoS (Distributed Denial-of-Service) Attack

A DDoS (distributed denial-of-service) Attack is an intentional and malicious effort to disrupt the regular flow of traffic to a specific server, service, or network. This disruption is achieved by overwhelming the target or its surrounding infrastructure with an excessive flood of Internet traffic.

Malicious Software

Malicious software, or malware, refers to any program or file deliberately designed to cause harm to a computer, network, or server. Various types of malware exist, such as computer viruses, worms, Trojan horses, ransomware, and spyware. These insidious programs execute actions such as stealing, encrypting, or deleting sensitive data, manipulating core computing functions, and clandestinely monitoring users' computer activities.

Antivirus Software

Antivirus software (antivirus program) is a security program designed to prevent, detect, search, and remove viruses and other types of malware from computers, networks, and other devices. Often included as part of a security package, antivirus software can also be purchased as a standalone option. Typically installed on a computer as a proactive approach to cybersecurity, an antivirus program can help mitigate a variety of cyber threats. Such cyber threats would include keyloggers, browser hijackers, Trojan horses, worms, rootkits, spyware, adware, botnets, phishing attempts, and ransomware attacks.

Background Information

The History of Cybersecurity

The beginning of cybersecurity was when researcher Bob Thomas created a computer program called Creeper that could move across the ARPANET (Advanced Research Projects Agency Network) in the 1970s. Ray Tomlinson, the inventor of email, wrote the program Reaper, which chased and deleted Creeper. Reaper holds the distinction of being the earliest instance of antivirus software and the pioneering self-replicating program, marking its role as the world's inaugural computer worm.

1987 was the birth year of commercial antivirus software although there were competing claims for the innovator of the first antivirus software. In 1987, Andreas Lüning and Kai Figge introduced their initial antivirus offering for the Atari ST. This year also witnessed the launch of Ultimate Virus Killer. Simultaneously, three Czechoslovakian individuals developed the first edition of the NOD antivirus. In the United States, John McAfee established McAfee and unveiled VirusScan.

In 1990, with the internet becoming available to the public, more people began putting their personal information online. Organized crime entities saw this as a potential source of revenue and started to steal data from people and governments via the web. It was the beginning of cybercrimes. Around the mid-1990s, there was a significant surge in network security threats, necessitating the widespread production of firewalls and antivirus programs to safeguard the general public.

During the early 2000s, criminal organizations commenced substantial funding of professional cyberattacks, while governments initiated stricter measures against hacking-related criminal activities, leading to considerably harsher penalties for those found responsible. Information security continued to advance as the internet grew as well but, unfortunately, so did viruses.

Major Related Issues

The Melissa Virus: In late March 1999, programmer David Lee Smith hijacked an AOL (America Online) account to post a virus-laden file on an Internet newsgroup named “alt.sex.” The Melissa virus spread rapidly by exploiting Microsoft Word and Outlook. It sent infected emails to contacts by

giving them names as “sexxxy.jpg” or “naked wife” or by deceitfully asserting, “Here is the document you requested ... don’t show anyone else ;-).” This caused havoc in email servers and disrupted about a million accounts. The virus inflicted $80 million in damages. With the FBI's help, Smith was arrested, pleaded guilty, and was sentenced to prison in 2002. The Melissa virus raised awareness about email attachment dangers, leading to improved cybersecurity. It prompted the FBI to establish its Cyber Division to combat online threats.

Adobe Cyber Attack: The Adobe Cyber Attack was one of the biggest data breaches of the 21st century. In October 2013, hackers stole login information and nearly 3 million credit card numbers from 38 million Adobe users. Adobe claims that only the passwords and credit card information of the first 2.9 million users were compromised, however, the remaining 35.1 million suffered the loss of their passwords and user IDs. Adobe paid just $1 million to settle a lawsuit filed by 15 state attorneys general over its huge data breach that exposed payment records on approximately 38 million people.

WannaCry Ransomware Cyber Attack: In May 2017, the WannaCry ransomware attack occurred, a global cyberattack executed by the WannaCry ransomware cryptoworm. A cryptoworm is a type of malicious computer software that spreads itself across a network by exploiting system vulnerabilities and encrypting files on an infected computer. This attack specifically aimed at Microsoft Windows operating system computers, encrypting data and demanding ransom payments in the form of Bitcoin cryptocurrency. After infecting a Windows computer, it encrypts files on the PC’s hard drive, making them impossible for users to access, then demands a ransom payment in bitcoin in order to decrypt them. WannaCry spread through a vulnerability in Microsoft Windows' implementation of the SMB (Server Message Block) protocol. This protocol facilitates communication among network nodes.

Cyber Attack on Marriott Hotels: In 2018, an internal security tool detected an unauthorized attempt to access Marriott's Starwood brands' guest reservation database, which led to an investigation. The breach, occurring in 2014 prior to Marriott's acquisition of Starwood in 2016, went unnoticed until then. The compromised Starwood network had not transitioned to Marriott's system by 2018, and this reliance on legacy IT infrastructure exacerbated the breach's scale. During the breach, hackers encrypted and extracted data from Starwood's system, potentially affecting up to 500 million guest records, though some were duplicates. The stolen information encompassed details like names, contact information, passport numbers, and preferences. A portion of the affected guests also had payment card data compromised.

RockYou2021: RockYou2021 is the largest password collection of all time that has been leaked on a popular hacker forum. A forum user posted a massive 100GB TXT file that contains 8.4 billion entries

of passwords, which have presumably been combined from previous data leaks and breaches. The passwords contained in these lists are all 6-20 characters in length, with whitespaces removed. The collection has been named 'RockYou2021' by the user on the forum, likely in connection to the well-known RockYou data breach from 2009. This breach involved hackers gaining unauthorized access to a social app website's servers and acquiring over 32 million user passwords that were stored without encryption in a file named rockyou2021.txt.

Efforts from the UN

The UN is putting various efforts into preventing cyber crimes and in developing ICTs. The ITU (International Telecommunication Union), a specialized agency of the United Nations, focuses on ICTs. ITU manages global radio spectrum and satellite orbits, establishes technical standards for seamless network connectivity, and strives to enhance ICT access for underserved global communities. Their commitment is to provide accessible and affordable ICT access to people worldwide, irrespective of various factors. Aligned with the SDGs (Sustainable Development Goals), ITU aims to leverage ICTs to address critical global challenges. These technologies can accelerate progress, bridge the digital divide, foster knowledge societies, and drive innovation across sectors such as healthcare and energy. The potential of digital connectivity, skills, and systems is vast, capable of reducing poverty, creating jobs, addressing climate change, and promoting transparency.

UNISSIG (The United Nations Information Security Special Interest Group) is a key mechanism within the UN system that promotes cooperation and collaboration among member organizations on information security. Its main goal is to enhance information security across these organizations. It achieves this by continuously assessing the UN system's exposure to both internal and external threats, aiming to reduce risks at all levels, especially strategic and operational ones. Member organizations understand that safeguarding UN system information assets builds trust with stakeholders, necessitating a comprehensive approach to information security and data protection. The UNISSIG manages organizational risk tied to the confidentiality, integrity, availability, and reliability of member organizations' information assets.

UNICC (The United Nations International Computing Centre) has been offering cybersecurity services to approximately two-thirds of UN system organizations for a while, with varying client usage for its 13 services. This aspect of UNICC's services has experienced notable growth, even though it represents a small portion of its budget. The assessment of these cybersecurity services among participating organizations has been uneven, with the Common Secure Threat Intelligence service standing out. In 2019, the JIU (United Nations Joint Inspection Unit) recommended UNICC

services in its Cybersecurity in the United Nations system organizations (JIU/REP/2021/3) report. The JIU is an independent and external oversight entity responsible for carrying out assessments, examinations, and inquiries within the United Nations. In 2021, the JIU conducted an evaluation of cybersecurity practices within the UN. As a result of this assessment, the JIU recommended that all UN Agencies make use of the expertise and capabilities of UNICC to enhance the overall cybersecurity readiness of the UN system.

Possible solutions

Strengthening Cybersecurity

Cyber terrorisms occur in cyberspace, which is a global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. The safeguarding of this digital realm is commonly referred to as cybersecurity, and it serves as the primary defense against cyberterrorism. So, the most fundamental way to prevent such cyber terrorism from happening in cyberspace would be strengthening cybersecurity. There could be various methods to strengthen cybersecurity, such as installing antivirus software, creating artificial intelligence to monitor any cyber threats, and raising white hat hackers. Governments could be in charge of these activities in order to strengthen their national cybersecurity.

Establishing International Laws

While several countries have enacted national laws addressing cyberterrorism – like India's Section 66-F of the Information Technology Act 2000, Pakistan's Section 10 of the Prevention of Electronic Crimes Act 2016, and Kenya's Section 33 of the Computer Misuse and Cybercrimes Act 2018 – there is no global consensus on the criminalization of cyberterrorism under international law. Because of this, nations should perceive cyber terrorisms as an international problem, and international laws should be needed in order to build sustainable international cybersecurity.

Associating with Non-Governmental Organizations

A NGO (Non-Governmental Organization) is an entity usually established separately from government influence. These organizations are commonly non-profit in nature, with a significant

presence in humanitarian efforts and social sciences. They encompass a variety of groups, including clubs and associations, that offer services to both their members and the wider community. There are several national and international NGOs related to cybersecurity, such as APWG 9Anti-Phishing Working Group), eNACSO (European NGO Alliance for Child Safety Online), and Spamhaus. The UN cooperating and associating with these NGOs would be appropriate for them to prevent cyber terrorisms happening in both international and national cyberspace. While NGOs are independent organizations with specific missions, often focusing on social or environmental issues, government-based organizations are public entities responsible for governance and public services. The distinction lies in their funding sources, structures, mandates, and levels of autonomy.

Educating Citizens

Cyber attacks are usually targeting citizens in a nation. However, there is no information for the citizens to discriminate about the form of cyber attacks, and how they should respond to cyberterrorism. Thus, there should be education conducted for every person in the nation in order to prevent cyberterrorisms happening worldwide. Education for the citizens could be done in various ways. Education could be about ways of responding to cyber attacks for citizens, cautioning citizens about unofficial or illegal websites, and training white hat hackers as educating students for national cybersecurity.

Major parties involved

United States of America

Although the United States is known for having the best infrastructure for cybersecurity, the United States stands as the top country which was hit by notorious traffic related to web applications with the percentage of 66%. It turned out that most of the attacks came from China and Russia. The United States is trying to respond to those by a variety of regulations and strategies. CISA (Cybersecurity and Infrastructure Security Agency), which is a part of the DHS (United States Department of Homeland Security), is focused on bolstering cybersecurity and protecting critical infrastructure. It coordinates with state governments, enhances government cybersecurity, and defends against private and nation-state hackers. In addition, according to the GCI (Global Cybersecurity Index) list, which is a trusted reference that measures the commitment of countries to cybersecurity at a global level, the United States is ranked first.

United Kingdom of Great Britain and Northern Ireland

The United Kingdom also has great cybersecurity and has been active in its efforts to strengthen its cybersecurity posture. The United Kingdom was hit by notorious traffic related to web applications, and the percentage is 3%, which is right behind the United States, Brazil, and Germany. Because of this, there are several policies and strategies. The NCSC (National Cyber Security Centre) in the UK helps protect the UK's critical services from cyber attacks, manages major incidents, and improves the underlying security of the UK Internet through technological improvement and advice to citizens and organizations. To add, the UK is ranked second in the GCI list with Saudi Arabia, which shows that the UK possesses well-improved cybersecurity infrastructures.

Kingdom of Saudi Arabia

Saudi Arabia is one of the world's leaders in cybersecurity development and preparedness. Saudi Arabia's consistent high rankings in global cybersecurity economies stand as a testament to the dedicated endeavors of significant institutions such as the NCA (National Cybersecurity Authority), which serves as a cornerstone of Saudi Arabia's national security apparatus. The NCA plays a dual role in cybersecurity, encompassing both regulatory and operational aspects. It maintains close collaboration with both public and private entities, aiming to enhance the nation's cybersecurity stance. Additionally, Saudi Arabia is ranked second in the GCI list with the United Kingdom.

Republic of Estonia

Estonia is recognized as one of the countries with the world's most advanced digital cybersecurity. One of the digital programs in Estonia is called e-Estonia, which is a digital society facilitating citizens' and residents' interactions with the state through ICT solutions. Starting from 2020, the e-Estonia program is providing Cyber Battle of Estonia, which is a series of cyber hacking events aimed at young people aged 15-24. The core mission of Cyber Battle of Estonia is to bring new people to cyber security, help them take their first steps, and get real hands-on experience. Moreover, Estonia is ranked third in the GCI list following the USA, the UK, and Saudi Arabia.

Republic of Korea

Republic of Korea is a world leader in many aspects of technology. Regardless of their global economic level, their telecommunications infrastructures, access, use, and skills in information and communication technologies were superior to other countries. Also, ROK is ranked fourth in the GCI list. However, ROK has faced several large-scale cyber attacks in recent years. Especially, cyber attacks suspected of originating from Democratic People's Republic of Korea have become increasingly sophisticated. DPRK has used cyber attacks to achieve its political goals in ROK by stealing information and millions of dollars, sowing a sense of vulnerability in Korean society.

People's Republic of China

The People's Republic of China probably poses the most extensive, dynamic, and enduring cyber espionage threat to both the US Government and private-sector networks. The nation's active cyber activities, coupled with its technology industry's export of related tools, heighten the risks of aggressive cyber operations targeting the US homeland. China undoubtedly possesses the capability to conduct cyber attacks that have the potential to disrupt critical infrastructure services within the US, including targeting oil and gas pipelines and rail systems.

Russian Federation

Russian Federation launches cyberattacks against other countries as a matter of routine. In some instances, these attacks coincide with military actions, such as in the ongoing conflict in Ukraine. Additionally, Russia employs cyberattacks to intentionally disrupt or undermine societies, as evidenced during the 2016 US Presidential election. The country also utilizes its powerful cyber capabilities to issue threats to governments in response to specific events, as seen when Finland invited Ukrainian President Volodymyr Zelensky to address its parliament in April.

Timeline Of Events

Date	Description of event
1998	The topic of information security was first discussed at the UN agenda when Russia introduced the draft resolution in the UN General Assembly's First Committee, which was adopted as resolution 53/70.
2004	Six GGE (Groups of Governmental Experts) have studied the threats posed by the use of ICTs in the

	context of international security and how these threats should be addressed.
December 2018	Through resolution 73/27, the General Assembly established an OEWG (Open-Ended Working Group), which is open to all Member States.
2019	OEWG began its work and held intersessional consultative meetings with industry, civil society, and academia.
2020	Via resolution 75/240, the General Assembly formed a fresh five-year OEWG for information and communications technology security. This group will convene regularly until 2025 and has a dedicated webpage.
March 2021	OEWG adopted a report by consensus at its final session. This final report and the recommendations contained therein were endorsed in General Assembly decision 75/564.
December 2022	A General Assembly resolution entitled "Programme of Action to Advance Responsible State Behavior in the Use of Information and Communications Technologies in the Context of International Security" was adopted for the first time as A/RES/77/37. The resolution requested a report of the Secretary-General on the proposal, taking into account the views submitted by States.

UN Involvement, Resolutions, Treaties and Events

Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures, 21 December 2009 (A/RES/64/211)

Resolution 64/211 highlights the importance of cybersecurity in global ICT systems. It recalls past resolutions on combating ICT misuse and fostering a cybersecurity culture. The resolution encourages nations to assess their cybersecurity efforts and share best practices. It emphasizes global cooperation to address cyber threats, promote ICT for development, and bridge the digital divide.

Countering the use of information and communications technologies for criminal purposes, 26 May 2021 (A/RES/75/282)

Resolution 75/282 tackles the misuse of ICTs for criminal purposes. It establishes an Ad Hoc Committee to craft an international convention on this matter, outlines its organizational aspects, and encourages stakeholder involvement. The resolution underscores considering existing cybercrime initiatives and allocating resources, especially for developing countries, to support the committee's work, enhancing global cybersecurity efforts.

Programme of action to advance responsible State behavior in the use of information and communications technologies in the context of international security, 7 December 2022 (A/RES/77/37)

Resolution 77/37 establishes a permanent program promoting responsible state behavior in ICT within international security. It underscores global ICT impact and the need to prevent misuse affecting stability. The resolution highlights cooperation, capacity building, and voluntary norms and engages stakeholders for enhanced cybersecurity. It seeks member states' input to refine the program's framework.

Ad Hoc Committee

By adopting Resolution 74/247, the General Assembly made the decision to create an open-ended ad hoc intergovernmental committee consisting of experts from various regions. The committee's purpose is to develop a comprehensive international convention focused on addressing the misuse of information and communications technologies for criminal activities. This effort involves a thorough consideration of existing international measures, as well as national, regional, and global initiatives aimed at combating the illicit use of technology, especially the work and outcomes of the open-ended intergovernmental Expert Group to Conduct a Comprehensive Study on Cybercrime.

Budapest Convention (2001)

The Budapest Convention, formally known as the Council of Europe Convention on Cybercrime, is the world's inaugural international treaty aimed at combating cybercrime. Established in 2001 and enforced from July 1, 2004, it encompasses three main objectives: enhancing investigative techniques, fostering international cooperation, and harmonizing national cybercrime laws. The convention requires participating countries to enact legislation criminalizing specific cyber-related offenses and

implementing clear rules for evidence gathering. It addresses a range of cybercrimes, such as illegal access, data interference, cyber fraud, child pornography, and copyright violations.

Bibliography

"Ad Hoc Committee - Home." *UNODC*, https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home.

"Budapest Convention - Cybercrime." *The Council of Europe*, https://www.coe.int/en/web/cybercrime/the-budapest-convention.

"Developing countries most vulnerable to cyberattacks – UN." *UN News*, 9 December 2011, https://news.un.org/en/story/2011/12/397922.

"Developments in the field of information and telecommunications in the context of international security – UNODA." *UNODA*, https://disarmament.unoda.org/ict-security/.

"Global Cybersecurity Index." *ITU*, https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx.

"The history of cybersecurity." *Cyber Magazine*, 4 October 2021, https://cybermagazine.com/cyber-security/history-cybersecurity.

"Index page for Global Cyber Security Index | Composite Indicators & Scoreboards Explorer." *Competence Centre on Composite Indicators and Scoreboards*, https://composite-indicators.jrc.ec.europa.eu/explorer/explorer/indices/GCI/global-cyber-security-index.

"Information Security Special Interest Group." *United Nations - CEB*, https://unsceb.org/unissig.

"International Telecommunication Union (ITU) .:. Sustainable Development Knowledge Platform." *Sustainable Development Goals*, https://sustainabledevelopment.un.org/index.php?page=view&type=30022&nr=2568&menu=3170.

"Services Overview." *UNICC*, https://www.unicc.org/what-we-do/services-overview/.

"Significant Cyber Incidents | Strategic Technologies Program." *CSIS*, https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.

"United Nations Cybersecurity in the United Nations system organizations." *Joint Inspection Unit*, https://www.unjiu.org/sites/www.unjiu.org/files/jiu_rep_2021_3_english.pdf.