Committee: United Nations Commission Science and Technology Development

Agenda: Addressing cyberterrorism through strengthening international cooperation and cyber protection

Student Officer: Suwan Lim

Introduction

The importance of the Internet to commerce and social life coupled with its vulnerability to disruption and misuse make its proper management a very complex contemporary issue. The decentralized structure of the Internet provides anonymity and unlimited use of time and place, making it difficult to control the resulting consequences.

In recent years, the rapid proliferation of Internet communications networks and the dramatic expansion of Internet-related industries have led to a focus on investing in Internet-related technologies and using the Internet to make money and increase profits. However, people are irresponsibly using the autonomy provided by the Internet to commit cybercrimes such as hacking, phishing, privacy invasion, and cyberterrorism. Among these, cyberterrorism causes particularly large financial and social damage. Some news outlets have predicted that cyberattacks using AI will increase in the future. For example, they warn that state-sponsored hacker groups could target the 2024 US presidential election.

The number of cybercrimes is increasing dramatically every year. The Global Database of Public Data Breaches reported that 1.9 billion data records were compromised in 918 data breaches worldwide in the first half of 2017. This is a 164% increase from the previous year. Malware is evolving in sophistication, and so are the technologies used to protect computer programs and software. The sophistication of malicious code is growing, and so is the technology that is used to protect computer programs and software. Detecting, responding to, and preventing cybercrime, including cyberterrorism, poses unique challenges for law enforcement and governments that require various approaches. The United States and the Republic of Korea Alliance seek to make robust and resilient national cybersecurity a policy priority. Finding effective strategies to strengthen cybersecurity and secure cyberspace is critical for future generations.

Definition of Key Terms

Cybercrime

Cybercrime is defined as "crime or illegal activity committed using the Internet." In fact, 'cybercrime' is not a legal term, and the crimes regulated by the laws of each country are communication crimes and computer-related crimes. Cybercrime that causes a lot of damage in Korea can be largely divided into new communication financial frauds such as phishing and smishing.

Cyberterrorism

Cyberterrorism Cyberterrorism refers to "damaging or destroying a computer system using the Internet for political or other reasons." The United States and the Federal Bureau of Investigation(FBI) defined it as a politically motivated attack on information, computer systems, and programs. It also includes violations such as invading the information systems of government or private organizations through computers or computer networks and causing serious damage or destruction.

Cybersecurity

Cybersecurity is defined as "work performed to protect individuals, organizations, or countries and their computer information from crimes or attacks committed using the Internet." To implement effective cybersecurity, technology must be developed and networks and related programs must be protected.

Malicious Code

Malicious code describes any code in any part of a software system or script intended to cause undesired effects, security breaches, or damage to a system.

History

The term cyber terrorism was first coined in the mid-eighties by Barry C. Collin, a senior research fellow of the Institute for Security and Intelligence in California (Akhgar et al., 2014).[1] At that time, he defined the term simply as “the convergence of cybernetics and terrorism”. Over the past years, cybercrime has become a huge business, a $1.5T industry with large segments of the cyber world being run by illegal companies masquerading as legitimate organizations. Some even offer technical leadership, team management, and customer service like actual companies do.

Technological developments are increasing the vulnerability of computer networks. The pace of advancement in cybercrime technology is incomparably faster than the pace of cybersecurity development worldwide. In addition, criminals are adapting to these defense systems and mechanisms, which makes critical infrastructure increasingly vulnerable over time. With the reliance on the Internet and cyber technology in our lives, cyberterrorism has become a serious concern over time.

In 2017, WannaCry and NotPetya were cyber-attacked and this had a huge impact on the economy. These two incidents affected organizations in more than 150 countries, prompted business interruption and other losses estimated at well over USD 300 million by some companies, brought reputational damage, and resulted in loss of customer data. WannaCry and NotPetya exposed a systemic risk and affected a broad cross-section of businesses without specific targeting, demonstrating the potential for escalation in the threat of cyber terrorism.

Today, the UN Office of Counterterrorism (UNOCT) launched several initiatives in the field of cybersecurity and brand-new technologies. The UNOCT cybersecurity and new technologies program aims to provide the ability to function and build up private organizations to counter cyber-attacks carried out by terrorist actors against critical infrastructure. Previous UNOCT projects have focused on using social media to collect open-source information and digital evidence to prevent terrorism while respecting human rights and ethics. Human rights and ethics should be protected by governments and organizations. Cybersecurity policies and administrations also need to be strengthened as internet transaction fraud, internet gambling, and personal information leaks through hacking.

Key Issues

Extreme and unpredictable damage

Directed attacks on the computer system can have serious consequences including financial losses, blackouts, and transportation delays. Hackers seek any vulnerable part of the cyber system to damage critical infrastructure where networks can be easily breached. A cyberattack on transportation infrastructure has this kind of potential of being assailed. If our car is attacked by hackers, our automobile is a computerized bomb on wheels. Also, according to a 2017 report from cybersecurity Ventures predicted ransomware damages would cost the world $5 billion in 2017, up from $325 million in 2015, an increase in just two years. Additionally, cyberterrorism has been used to spread propaganda and manage public ideas, as well as to steal delicate information, such as personal data and intellectual property.

Combining protection and resilience strategies

As sophisticated cyber threats like ransomware continue to grow faster in size and efficacy, thus the movement of organizations in every industry, trying to prevent such threats by building cyber resilience strategies is rising. Cyber resilience is the ability of an organization to accelerate its business (enterprise resilience) by preparing for, responding to, and recovering from cyber threats. Cyber-resilient organizations can adapt to known crises, threats, adversity, and challenges. The ultimate goal of cyber resilience is to help organizations thrive even in adverse situations, such as crises, pandemics, and financial volatility. Also, a government agency like CISA(Cybersecurity & Infrastructure Security Agency) aims to encourage business and critical infrastructure suppliers to heighten their awareness of the growing cyber-terrorism threat and take action.

Legal and regulatory frameworks

Various UN resolutions requested the need for international cooperation in combating cyber realism and promoting global cybersecurity. Moreover, countries have to enact laws that define cyberterrorism and

punish specific acts toward hackers. Recently, President Biden has made cybersecurity a top priority for the Biden-Harris administration. To advance the President's announcement, the government focused on tackling the immediate threat of ransomware and building a more potent and distinct workforce. Establishing cybercrime units within law enforcement agencies to handle cyberterrorism cases and building regulatory bodies like the European Union Agency for Cybersecurity(ENISA), which works to improve cybersecurity across member states can prohibit all those legal actions and infractions of law.

Major Parties Involved and Their Views

Countries

United States

The United States is one of the leading countries in building and strengthening cybersecurity strategies and technical systems. The U.S. has already created cybersecurity agencies like CISA(Cybersecurity and Infrastructure Security Agency) and NSA(National Security Agency) that contribute to providing cyber defense and insurance. Also, they collaborate with international cooperative initiatives like the Global Forum on Cyber Expertise (GFCE) and the Global Initiative to Combat Nuclear Terrorism (GICNT) to increase communication with other countries and strengthen strategies. On March 2, 2023, the Biden administration announced a new "National Cybersecurity Strategy (NCS)" about five years after the Trump administration. It was developed in collaboration with the private sector based on the National Security Strategy and National Defense Strategy reports.

The U.S. created cybersecurity agencies like CISA(Cybersecurity and Infrastructure Security Agency) and NSA(National Security Agency) that contribute to providing cyber defense and insurance. NSA officials instructed a team called "Red" consisting of 35 hackers to secure the U.S. national security systems. They were allowed to penetrate any Pentagon network but were restricted from breaking any U.S. laws, and they were supposed to only use hacking software that could be downloaded freely from the Internet. They also collaborate with international cooperative initiatives like the Global Forum on Cyber Expertise(GFCE) and

the Global Initiative to Combat Nuclear Terrorism (GICNT) to increase communication with other countries and reinforce programs. On March 2, 2023, the Biden administration announced a new “National Cybersecurity Strategy (NCS)” to develop in collaboration with private organizations and international cooperation for security protection.

China

The beginning of the Chinese government's cyber security strategy and policy is a gold shield process that began in the late 1990s, a method of focusing on basic intelligence and control based on the construction of an information censorship and surveillance system. In 2014, when Xi Jinping came to power, <Central Internet Safety Informationization Project> was established, and cyber security began to be recognized as a problem related to national ideology and status beyond simple technology competition. At the same time, the U.S.-China hegemony competition has increased the internal and external cyber threats, which has increased the need to establish a cyber security strategy. In response, the Chinese government immediately established and announced the 『National CyberSpace Security Strategy』 and 『CyberSpace International Cooperation Strategy』.

South Korea

According to a 2022 news report, the hacker secretly downloaded the User Certificate (GPKI) for access to the institution's internal system, which was stored on the PC of Officer A, and then used it to access the internal system of the institution with the account of Officer A and steal various secrets. As reported by ‘Cyber Security in South Korea’, the subjects that threatened national security in the past were hostile countries, terrorists, and international criminal organizations. They secretly infiltrated physical space, stole data, destroyed critical facilities, and killed lives. But recently, new threats have emerged, including the deprivation of industrial secrets through cyberattacks and system paralysis. Experts share that the Republic of Korea is also not free from the threat of cyber terrorism without borders.

India

India experienced about 429,847 cyberattacks in the financial/services sector in 2023 (about 112,474 in the first half of the year alone), and the frequency of cyberattacks has increased sharply, with about 70 government websites being hacked. In addition, it suffered an average of about 2,138 cyberattacks per

company per week, an increase of about 15% from the previous year. India has made efforts by earmarking about 60 billion (about 960 billion won) in the area of cybersecurity enhancement within its 2023/24 budget, but the demand for additional budget allocation within this year's budget is spreading in the face of the growing cyberattacks. The Indian cybersecurity market grew to about $6 billion (about 7.98 trillion won) as of 2023, with an annual cumulative growth rate of more than 30% over 2019-2023.

International Organizations

United Nations (UN)

A United Nations specialized agency for information and communication technologies(ICTs), the International Telecommunication Union (ITU) is the oldest agency in the UN. They facilitate international connectivity in communication networks. Also, they contribute to enhancing capacity and equal access and improving digital technologies in needless societies around the world.

NATO

NATO Cooperative Cyber Defense Centre of Excellence (CCDCOE) aims to support their member nations and NATO with exclusive interdisciplinary proficiency in the field of cyber defense analysis, training, and examining qualified areas like technology, operations, strategy, and law. South Korea is one of the contributing participants. Recently, they focused on collaborating cyber defense mechanisms with education systems.

European Union(EU)

European Union Agency for Cybersecurity (ENISA) focuses on improving cybersecurity across EU member states through policy development, capacity building, and promoting best practices. They were established in 2004 and started to strengthen cybersecurity in Europe and provide services and technology strategies to each other to boost the resilience of the union’s framework.

Europol’s European Cybercrime Center (EC3) was built by Europol to reinforce law enforcement as an acknowledgment of cybercrime in the EU and to protect citizens and companies who are vulnerable to those attacks. This agency can prevent online crimes and analyze preparation to combat.

Non-Governmental Organizations(NGOs)

Cyber Peace Foundation

Cyber peace foundations are introducing themselves as "endeavors to make the internet a more secure, stable, trustworthy and inclusive place for all netizens across the globe."[1] They can collaborate with private companies, law enforcement agencies, NGOs, universities, citizens, and more. This foundation has 4 main pillars, 'Cyber policy', 'Innovation and Research', 'Collaboration and Connection', and 'Inclusion and Outreach'.

Center for Internet Security(CIS)

The Center for Internet Security recognized emerging cyber issues like cyberterrorism, and cyber threats and sought potential solutions. They also provide a secure, on-demand, scalable computing environment in the cloud for safeguarding. CIS proves whether the security systems are reflecting the current circumstances of the Internet and cyberattacks to respond as quickly and efficiently as possible.

Carnegie Endowment for International Peace

Carnegie Endowment for International Peace is consistent with 170 experts from diverse perspectives and thinking skills with deep knowledge and experience of cybersecurity in international affairs. They mainly generate actionable policy-related ideas to reduce international conflict and advance cooperation.

Timeline of Relevant Resolutions, Treaties and Events

Date	Description of event
December 1996	United Nations General Assembly Resolution 51/210 was written by The UN collaborating with global corporations to combat terrorism, including emerging threats like cyberterrorism.
November 23, 2001	Budapest Convention on Cybercrime was held as the first international treaty to address internet and computer crime. It also aims to align national laws, improve investigative techniques, and foster global cooperation.
December 22, 2003	UN Resolution 58/199 was written by the UN and is about focusing on creating a worldwide cybersecurity culture and safeguarding critical information infrastructures.

[1] https://www.cyberpeace.org/about-us

January 1, 2004	The European Network and Information Security Agency was first established in 2004. They began operations to enhance cybersecurity and improve technical issues across the EU.
January 1, 2011	UN Resolution 66/24 was passed in 2011 and was about measuring to combat criminal use of information and communication technologies. The punishment has been reinforced since then.
May 2014	NATO established the Cooperative Cyber Defence Centre of Excellence in Tallinn, Estonia, to boost cyber defense capabilities through research and training.
June 2016	The EU introduced the General Data Protection Regulation to protect personal data and influence global cybersecurity practices.
May 2017	'WannaCry Ransomware Attack' was a global cyber incident affecting organizations worldwide highlighting the urgent need for international cooperation in cybersecurity. This ransomware attack spread through computers operating Microsoft Windows. The user's files were held hostage, and a Bitcoin ransom was demanded for their return.
January 1, 2023	The Global Forum on Cyber Expertise started to facilitate international collaboration among countries, organizations, and the private sector on cybersecurity best practices. They are a multi-stakeholder community, consisting of over 200 members and partners such as international organizations and governments around the world.

Evaluation of Previous Attempts to Resolve the Issue

There has been a critical evolution in combating cyberterrorism through increased international cooperation and cyber protection for a long time. The Department of Homeland Security in the United States, the European Network, and the Information Security Agency are the three examples of the different organizations to combat cyber threats from the early 2000s. The first collaboration with national institutions to the growing threat of cyberterrorism was initiated with the help of these projects. An historic agreement was reached in 2001 with the Budapest Convention on Cybercrime which was the very first convention to promote cooperation in the fight against cybercrime and harmonize regulations. Multilateral institutions such as the United Nations and NATO have implemented their agendas over time. Moreover, the UN has progressively redirected its attention towards cybersecurity with the formation of the NATO Cooperative Cyber Defence Centre of Excellence(CCDCOE) and the Group of Governmental Experts from supranational organizations. Cooperation between the public and private sectors is critical. One of the recent policies is the EU Cybersecurity Act (2019) which aims to enhance the cybersecurity of ICT products within

the EU. However, there continue to be worries about how fast cyber threats are growing and the constant need for technical changes. Thus, to counter complex cyberterrorist activities, further initiatives should focus on international cooperation, solid legal regimes, and timely sharing of intelligence.

The war against cyberterrorism has experienced its triumphs in overcoming challenges in the last 20 years due to improved international cooperation and cyber defense systems. Cyberthreats are not only a national or institutional problem, now they have become more related to individual issues. For instance, companies use their customers' privacy as a marketing use for their own good, therefore customers' privacy can't be protected by those crimes. After the 9/11 incident, the United States came to understand the increasing reality of cyberterrorism and formed the Department of Homeland Security with an emphasis on cyber protection. Furthermore, the European Union founded the European Network and Information Security Agency (ENISA) in 2001 to enhance network and information security throughout its member states. These early activities set the stage for the first structured national responses to the threat of cyberterrorism.

Numerous regional conferences and proper treaties are the beginning of the launch of international collaboration. The first attempts to advance that cooperation were carried out in the form of regulating global governance issues in cyberspace. Nations around the world have discussed cybersecurity policies and their application through implications towards international laws and potential future. To revise better laws in terms of companies and agencies which are vulnerable to cyber attacks, previous laws have made significant progress with the advent of improved defense systems. The UN and other specialized organizations have begun to develop more sophisticated methods of cybersecurity over time such as distinguishing the issues into five categories: silence, existential disagreements, interpretative challenges, attribution, and accountability. The research reveals that the adoption of technologies plays a pivotal role in combating cyberterrorism as well. NIST cybersecurity frameworks and other cooperation also suggested the proper guidelines to mitigate cybersecurity threats. Some countries like the US supported such public-private partnership programs as well to reduce the future possibilities of attacks.

The National Cybersecurity and Communications Integration Center (NCCIC) supports public-private partnerships. Among the new regulations that have been implemented are the establishment of cybersecurity certification systems for example the EU Cybersecurity Act (2019) which guarantees the dependability of ICT services, products as well as processes in the EU. However, it is important to recognize that the threats in the cyber world are still evolving at a fast pace. These include complexity, the need for constant innovation, as well as contradiction of purposes between nations. The counteraction to the constantly emerging threats of cyberterrorism must be regulated under specific laws and policies within the country and around the globe. Also, the future steps should address the enhancement of the legal regimes at the global level, increasing partnerships, and increasing the availability of up-to-date data. As

demonstrated by past experiences in countering cyberterrorism, there is a need to incorporate a collective and adaptive mechanism to sustain the robustness of global cybersecurity.

Possible Solutions

Cyberterrorism requires people worldwide to engage in some collective effort in this age of globalization. Our world has become globalized and interconnected, and the threats posed against each member state demand the collective improvement of cybersecurity. The ongoing creation of international cyber laws and friendly extradition measures with each country is imperative to avoid making cyber criminals escape the legal consequences just because they mask behind a screen. Conventionally, digital crimes are not straightforward and rarely leave any tangible traces that can be easily traced and acted upon legally. We should also be able to set up global-level working groups in cybersecurity and a central system for sharing threat intelligence sources. To protect against threats over the internet, measures such as artificial intelligence (AI) or blockchain may be adopted. Mandatory federal-level cybersecurity checkups and a strong base for the basic need services in case of cyber securities threats are the prerequisites. In total, these measures from the Snowden files help hinder terrorist acts in cyberspace and protect information.

Consumers and enterprises need to safeguard their data to avoid any critical attacks, loss, and monetary damages. To protect sensitive data and technologies, systems must be operated to monitor and control access records since needless data exposure makes the systems vulnerable to cybercrime. Today, major organizations and companies are hiring people who can utilize the systems and defend against attacks. Also, the investment in security technology and protection against terrorism is increasing noticeably, featuring firewalls, antivirus, and encryption. Organizations should prioritize security awareness to maintain data integrity and minimize vulnerabilities. As an individual, people should prevent these attacks by using uncrackable passwords, allowing two-step authentication, and not clicking on emails from unknown senders.

In the future, technical assistance should be provided equally to developing countries as developed countries to enhance their cybersecurity capacity and effectiveness. Thus, coming laws should ensure strengthened protection against cyberterrorism and secure adequate cybersecurity for all members of the global community whenever it’s international and national levels. International corporations like the UN and ITU should work with developed countries to provide the necessary financial and technical support and establish universal standards by inviting the flow of knowledge, technology, and practices through discussion forums and programs. To accomplish these tasks, designing standards and accommodating the adoption of advanced technologies will be the key factor that determines the cyberspace industry. Furthermore, continuing to secure governance and sensitive networks will lead to innovation that requires effective campaigning and coordination between public funding agencies and private sector entities.

Movements like these with other countries and community cooperation, can be a way for all individuals to gain a more secure internet.

Bibliography

1. Cheon, Gon, and Seong Kim. Analysis and Implications of U.S. Cybersecurity Strategy and Action Plan. Gon-woong Cheon, 22 Jan. 2024, www.google.co.kr/url?sa=t&source=web&rct=j&opi=89978449&url=www.kisa.or.kr/post/fileDownload%3FmenuSeq%3D20301%26postSeq%3D23%26attachSeq%3D1%26lang_type%3DKO&ved=2ahUKEwifr7q6r92GAxWcdvUHHYu7BMUQFnoECBAQAQ&usg=AOvVaw0izKpUxRVM9m1P7rQ0eBRR.
2. Plotnek, Jordan J., and Jill Slay. "Cyber terrorism: A homogenized taxonomy and definition." *Computers & Security*, vol. 102, Mar. 2021, p. 102145. https://doi.org/10.1016/j.cose.2020.102145.
3. 'The threat of cyber terrorism using AI generated next year will increase… 'It could be aimed at the general election.'" Digital Today, 17 Dec. 2023, www.digitaltoday.co.kr/news/articleView.html?idxno=498425.
4. Report World. "Causes and background of cybercrime." Report World, https://www.reportworld.co.kr/knowledge/12777#:~:text=%EB%AA%87%20%EB%85%84%20%EC%82%AC%EC%9D%B4%EC%97%90%20%EC%9D%B8%ED%84%B0%EB%84%B7,%ED%95%B4%20%EC%99%94%EB%8D%98%20%EA%B2%83%EC%9D%B4%20%EC%82%AC%EC%8B%A4%EC%9D%B4%EB%8B%A4.
5. "Cyber Terrorism: What It Is and How It's Evolved | Maryville Online." *Maryville University Online*, 23 Oct. 2023, online.maryville.edu/blog/cyber-terrorism.
6. Iftikhar, Saman. "Cyberterrorism as a global threat: a review on repercussions and countermeasures." *PeerJ. Computer Science*, vol. 10, Jan. 2024, p. e1772. https://doi.org/10.7717/peerj-cs.1772.
7. Iftikhar, Saman. "Cyberterrorism as a global threat: a review on repercussions and countermeasures." *PeerJ. Computer Science*, vol. 10, Jan. 2024, p. e1772. https://doi.org/10.7717/peerj-cs.1772.
8. *Cybersecurity and New Technologies | Office of Counter-Terrorism*. www.un.org/counterterrorism/cybersecurity.
9. *Significant Cyber Incidents | CSIS*. www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

10. United Nations. “Cybersecurity | Office of Counter-Terrorism.” *Www.un.org*, 2020, www.un.org/counterterrorism/cybersecurity.
11. Street, Chris. “Protecting America’s Roadways.” *Stories.uh.edu*, stories.uh.edu/magazine/magazine/spring-2024/protecting-americas-roadways/. Accessed 9 July 2024.
12. “Read “Science and Technology to Counter Terrorism: Proceedings of an Indo-U.S. Workshop” at NAP.edu.” *Nap.nationalacademies.org*, nap.nationalacademies.org/read/11848/chapter/6#50.Accessed 9 July 2024.
13. Panlogic. “Cyber Crime - National Crime Agency.” *Nationalcrimeagency.gov.uk*, 24 July 2019, nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime.
14. Fairleigh Dickinson University. “Cybersecurity and Cyber Terrorism.” *Fairleigh Dickinson University Online*, 2023, online.fdu.edu/program-resources/cybersecurity-and-cyber-terrorism/.
15. FBI. “Cyber Crime | Federal Bureau of Investigation.” *Federal Bureau of Investigation*, 2023, www.fbi.gov/investigate/cyber.
16. Plotnek, Jordan J., and Jill Slay. “Cyber Terrorism: A Homogenized Taxonomy and Definition.” *Computers & Security*, vol. 102, no. 102145, Mar. 2021, p. 102145, https://doi.org/10.1016/j.cose.2020.
17. Leaf. “10 Ways to Prevent Cyber Attacks.” *Leaf*, 2023, leaf-it.com/10-ways-prevent-cyber-attacks/.
18. Sciences, National Academy Of. “Science and Technology to Counter Terrorism.” *National Academies Press eBooks*, 2007, https://doi.org/10.17226/11848.
19. Hollis, Duncan. “A Brief Primer on International Law and Cyberspace.” *Carnegieendowment.org*, 14 June 2021, carnegieendowment.org/posts/2021/06/a-brief-primer-on-international-law-and-cyberspace?lang=en. Accessed 1 July 2024.
20. “International Cyber Law: Interactive Toolkit.” *Ccdcoe.org*, 2020, cyberlaw.ccdcoe.org/wiki/Main_Page.