Forum: Promoting Science Committee

Agenda: On measures to combat the rise of cybercrimes and its effect on political stability

Student Officer: Chan Kim

Introduction

Alongside rapid advancements in digital technology, cybercrime is becoming increasingly common. The most commonly practiced forms of cybercrime include phishing (Utilizing fake emails in order to attain personal online information), distribution of obscene and illegal material, and extortion (demanding payment from an online user via a threat against the victim). One of the largest consequences of cybercrime activity is the financial and economic burdens they bring. Cybercrime can result in the loss of intellectual property and confidential/sensitive business information, stock market manipulation, the additional financial burden of securing networks from cybercrime, etc. All of which can have varying degrees of harm to a nation's economic wellbeing. The cost of cybercrime as of 2022 is already up to 0.8% of global GDP (approximately 600 billion dollars per year). A 34% increase from 2014's 445 billion dollars, showing an average annual growth rate of 11.3% Indicating a consistent growth in the economic burden brought on by cybercrime, a growth that is likely continue accelerating with the development of more sophisticated cybercrime capabilities and the further digitalization of national/global economies. This issue should be taken with great consideration by the participants of the UN as the economic stability of a nation state will no doubt greatly determine a state's political one.

With politicians/political leaders in the modern age increasingly utilizing social media/the internet for communication and promotion for their political positions, cybercrime will undoubtably inversely experience an increase in relevance in regards to a countries political stability. The use of advanced technology predetermines new clashes and social tensions. In the context of social transformation, restrictions, ethnopolitical tensions and conflicts, these technologies and cybercrime can be used to reach political goals and cause the destabilization of nations. Politically driven and motivated cybercriminal activity commonly involves computerized attacks on critical information and infrastructure, using communication technology in order to promote terrorist activity and interference with internal political affairs of a nation state.

Key Terms

Cybercrime - Forms of criminal activity committed/perpetrated using computer technology. Major examples of cybercrime include: phishing scams, infringement of intellectual property, cyberextortion, malware attack, etc.

Cyberespionage - Cyberespionage is the act of gathering confidential information that is typically carried out by governments to gain political and or military information.

Cybersecurity - Proposed solutions (including laws, guidelines, technological safeguards etc.) to the threats posed by hacking and compromising computer systems.

Political Stability - The level of stability of a certain political group/entity.

Global Cyber Security Index - The Global Cyber Security Index (CGI) is a reference that measures the commitment of countries to cyber security at a global level. A nations level of cybersecurity development is measured by five pillars – (I) Legal Measures, (ii)Technical Measures, (iii)Organizational Measures, (iv) Capacity Development and (V) Cooperation.

General Overview

United States of America

The United States currently holds the highest place in the global cybersecurity index with a score of 100. However, the US still faces many challenges regarding cybercrime. Online criminal activity is increasingly becoming a bigger threat for US businesses. In 2018, the United States was the country most severely affected by the cybercrime purely in terms of financial damage, it is estimated that the US government faced over 13.7 billion dollars in costs that resulted from cybercrime. In the first half 2020 there were 4.4 million cyber-attacks on government customers which then rose by 917% in 2021 to 44.4 million cyber-attacks and cybercrime has caused 6 million us dollars in damage within 2022 alone.

The United States has stated in UN conferences regarding the usage of communication and information technologies for criminal purposes that their greatest concern regarding cybercrime are problems involving transnational cooperation between member states for mitigation of cybercrime. Washington has raised concerns on the evolution of cybercrime and their current transnational quality, that cybercrime organizations have expanded and broadened the scope of its level of cybercrime threats and cybercriminal activity by exploiting information and communication technologies to facilitate attacks and also to create online markets for stolen data. Another challenge raised by America was the limited national capacity and outdated national legal frameworks to tackle cybercrime. The United States in this regard faces challenges in working with associates to prosecute cybercrime within borders where there is limited ability for the government to update their domestic legal frameworks in order to more efficiently tackle cybercrime. Moreover, the United States have claimed that they face challenges in cases where laws regarding cybercrime and cybersecurity have been successfully adopted but have failed to have been effectively and legitimately implemented into their legal frameworks in actual practice. Due to this the United States has supported and recommended the prioritization of both legislative reform assistance and capacity building in order to ensure that new laws translate into action, in particular the US has emphasized this action regarding developing nations.

Russian Federation

The Russian Federation as of 2022 currently holds 5th place in the global cybersecurity index with a score of 71.43. Cybercrime has cost the Russian Federation approximately 49 billion dollars in 2020 and is predicted to cost a Russia 132 billion rubles by 2025. In recent years Russia has witnessed an increase in

cyber threats such as data breaches, malware attacks and digital fraud cases. Additionally, Russia is a big source of worldwide cybercrime activity. Russia is currently a major source of phishing attacks and in 2021, the Russian federation accounted for a quarter of the globes total unsolicited spam emails. The Russian Federation itself has also been directly involved in malicious cyberactivity with state-sponsored cybercrime (cyber espionage) being common. Russia has engaged in cybercriminal activity in order to perform cyber espionage, to suppress certain political and social activities, and to harm both regional and international adversaries.

In previous UN conferences Russia has also placed great emphasis on the issue of a lack of comprehensive Interntional framework for cooperation and a common terminological basis for cybercrime. Russia has stated that it supports the development of universal principles and norms that could be shared by all parties of interest and that they could lay the foundations for effective international cooperation in counter cybercrime. In Russia's view in the present context, the search for a political solution and consensus building should be conceived as the primary task. Russia has previously recommended the creation of a permanent forum in the general assembly to discuss all aspects of internationally cooperated fights against cybercrime in a balanced approach.

China

The Peoples Republic of China currently holds an average place of 69 in the global cybersecurity index with a score of 51.95. China has witnessed a sharp increase in cybercrime, the rapid growth of digital technologies but inadequate handling of cybersecurity has led to an increase and exacerbation of the issue. This increased vulnerability towards cybercrime could possibly have serious consequences for its economy and politics. The amount of cybercrime has grown annually in China by 20-30 percent, and reached a turnover of more than 14 billion us dollars in 2018. An estimated 400,000 people work in underground cybercriminal organizations in China. Additionally, there is widespread censorship of information and media within China, and cybercriminals have the potential to spread politically sensitive information that has the potential to harm the communist party's sovereignty and rule of China.

In previous United Nations conferences, China shared its views regarding cybercrime by stating that organized crime conventions could not adequately respond to new requirements for international cooperation to tackle cybercrime. China stated that the international community urgently needed the establishment of a global legal framework to counter cybercrime in hopes to the mitigate the increasingly dire situation. China has vehemently supported the view that all states should negotiate and establish a global convention against cybercrime open to all nations, under the guidance of the United Nations and drawing on the experience gained from already established regional conventions. According, to China international cooperation should help to effectively coordinate laws that can effectively provide practices to fight cybercrime and should provide universally agreed upon solutions for global governance of cybercrime. China believes that the convention should regulate the practice of cross border taking electronic devices and help to design a more efficient mechanism in taking evidence based on respect for state sovereignty and to safeguard the rights of corporates and individuals.

Germany

Germany holds a high position of 6th place in the national cyber security index with a score of 91% and a global cyber security ranking at 13th place with a score of 97%. Despite a high score in both national and global security indexes Germany is not immune from the effects of cybercrime and the issue has seen an increase in relevance in recent years. Germany overall has had the highest number of data breaches out of every country in the globe, with 106,731 breaches so far. It is estimated that cyberattacks in 2018 cost the German industry a total of 50 billion us dollars, the average cost of ransomware attacks was more than 1.73 million and average costs of data breaches in Germany in 2021 was 4.45 million dollars. Additionally, there have been recent reports that show a significant expansion of cybercriminal extortion methods and a dramatic increase in the variants of malware. Between may 2020 and may 2021, 144 million new variants were identified, a 22% increase compared to the previous year. Increased cybercriminal activity is largely believed to be caused by the growing sophistication and professionalism of cybercriminals compounded by the spread of more digital networking.

During earlier United Nations conferences regarding cybercrime, Germany shared its view that fighting cybercrime required sufficiently developed national legal frameworks but also functioning national cooperation across borders. Germany has underlined that special attention should be placed upon the implementation of cybercrime legislation and to making effective practical progress including through the provision of technical assistance. Germany believes that a challenge that should be considered by the member states is how to provide law enforcement entities with a sound legal framework and the necessary resources to secure electronic devices.

Brazil

Brazil currently holds 68th place in the national cyber security index with a score of 52% and holds the 18th place in the global cybersecurity index with a score of 97%. Cyberattacks are a major problem in modern Brazil. In 2017 more than 60% of Brazilian internet users of approximately 62 million people were victim to cybercrime with an overall loss of 22 billion us dollars and in 2018 this number increased to 70 million cybercrime victims. In 2018, it was estimated that Brazilian companies lost more than 20 billion us dollars to cybercrime attacks and the average annual cost of cybercrime for a Brazilian company was estimated to be 7.24 million us dollars in the same year. In 2022 it was reported that Brazil was the fourth most breached country in the world with over 3 million users breached by the second quarter of the year. Cybercrime initiatives have not been well developed in Brazil to adequately counter these new threats. Brazil has developed guidelines and practices to deal with cybercrime, but prevention methods and national security is considered lacking.

In previous united nations meetings, has stated that they faced difficulty whenever there was an international element to investigations and jurisdiction because the legal development of a case was often slowed by the divergences and disparities over the definition of privacy protection. Another challenge to international cooperation stated by Brazil was the volatility of digital evidence, since the amount of information circulating globally, and storage related costs make companies retain data for no longer than what is necessary for business. Brazil previously had shared their view that although the internet is a virtual space without any physical borders, its connections to with the physical world occurs in existing territories of a state. Brazil has stated that better and more efficient cooperation was needed and that multilateral

negotiation of an international instrument under the guidance of the UN could be a method through which a common minimum standard for exchange of information and evidence tackling to be established.

Australia

Australia currently ranks at 38th place in the national cybersecurity index with a score of 66% and holds 12th place in the global cybersecurity index with a score of 98%. Cybercrime saw a 13% increase in numbers in Australia in 2021 (around 76,000 reports of cybercrime per year) and based on reports Australia lost over 300 million dollars to cyber scam in 2021. These cybercrime threats have been increasingly taking a heavy toll on Australian businesses with average loss per cybercrime being 39,000 dollars for small businesses and 62,000 dollars for large businesses. Overall, it is estimated that cybercrime costs Australia over 40 billion dollars per year. Due to rising concerns, the Australian defense minister in 2022 stated that the Australian government would be reinforcing cybersecurity as a national priority for Australia.

Australia has previously stressed in UN conference meetings the importance of focusing on technical expertise to counter cybercrime. Australia believes that due to the complexity and constant advancements in cybercrime, addressing the issue requires constant attention, guidance and advice from of technical cybercrime experts. Australia has stated that the nation faced difficulties accessing and obtaining data to effectively pursue cybercrime and investigations and prosecutions. Additionally, regarding the issue of the adaptability of legal and operational frameworks, Australia has emphasized its commitment to maintaining adaptable domestic legislative frameworks that could keep up with rapid technological and behavioral advancements in cybercrime.

Major parties involved

United Nations Offices on Drug and Crime (UNODC)

The United Nations Offices on Drug and Crime is an office in the United Nations that primarily aims towards countering drugs and international crime. One of the five normative areas of activity that the organization bases itself around is to strengthen member states capacities to confront threats from transnational organized crime. With the rise and emergence of cybercrime, crime has become an interest of the organization. The UNODC helps member states to ratify and implement the UN convention against transnational organized crime and its protocols, and it desires to address new and emerging forms of crime (such as cybercrime).

International Court of Justice

The International Court of Justice is an international organization that serves as the principal judicial organ of the United Nations. The role of the organization is to settle legal disputes submitted to it by states in accordance with international law and to give advisory opinions on legal questions referred to it by authorized United Nations organs and specialized agencies.

International Criminal Police Organization (Interpol)

The International Criminal Police Organization is an inter-governmental organization that facilitates global police cooperation and crime prevention. It is the world's largest international police organization and has a total of 195 member states. The organization supports national efforts in combating across three global areas that it considers to be the most relevant and pressing in the modern world; terrorism, organized crime and cybercrime. Interpol coordinates law enforcement operations and delivers data sharing platforms, analysis and training in order to counter and prevent cybercrime.

Timeline of Events

Climate change will cause population movements by making certain parts of the world much less viable places to live; by causing food and water supplies to become more unreliable and increasing the frequency and severity of floods and storms. There are several events that have happened in the past:

Date	Description of event
2001	The commonwealth of independent states agreement on Cooperation in Combating Offenses in the field of computer information. The treaty was an attempt that agreement between different states to adopt national laws to implement the agreements provisions and to harmonize national cybersecurity laws.
Late 2001	The Convention of Cybercrime or The Budapest Convention, signed on November 23, 2001, in Budapest, is one of the first international treaties that attempted to tackle cybercrime by internationalizing national laws, improving techniques in investigations and increasing cooperation between nations. The convention was adopted by a total of 67 countries. As it stands, it is considered to be the most significant and important treaty on cybercrime to date.
2010	The Arab Leagues Arab convention on combating information and technology offenses. This convention mainly aimed towards strengthening cooperation between states in order to allow then to defend against and secure protection of their property, people and different interests from cybercrime. The Shanghai Cooperations Agreement on Cooperation in the Field of International Information Security. This treaty's focus went beyond simply cybercrime and cybersecurity to additionally include information security of member states as well as national control over systems and content.
2012	African Union Draft Convention on the Establishment of a Legal Framework Conductive to Cybercrime in Africa. This convention promoted the provisions and maintenance of human, financial and technical resources required to facilitate cybercrime investigations

2014	African Union Convention on Cybersecurity and Personal Data Protection. This convention included a call to African Union states to create and or amend national laws to adequately combat cybercrime, harmonize national laws, create mutual legal assistance treaties where they do not exist, facilitate information sharing between states, facilitate regional intergovernmental, and international cooperation and utilize existing means available to cooperate with other states and even the private sector.
2019	The United Nations General Assembly adopted a resolution that initiated a multiyear process of negotiating what could potentially become a global cybercrime treaty.

UN Involvement, Relevant Resolutions, Treaties and Events

- Since 2019 the United Nations have actively been negotiating for a potential global cybercrime treaty whose influence would be more far reaching then the Budapest convention. To coordinate the convention, the United Nations General Assembly accepted resolution 74/247 and established the Ad Hoc intergovernmental committee in order to elaborate a comprehensive international convention on countering the use of information and communication technologies for criminal purposes. Negotiations for this treaty are wide ranging and show a lack of unanimity concerning the definition of cybercrime.

Possible Solutions

The United Nations estimates that over 80 percent of global cybercrime is perpetrated by highly sophisticated and organized criminal groups. The advent of digital technology will increasingly make a nations border space permeable and will lead to an increased demand for national security requirements. Developing third world nations with less adequate funding, support and enforcement for more advanced cybersecurity measures are more vulnerable to cyber risks. Hence, transnational cooperation involving the aid of development for cybersecurity in developing countries will help to maximize the potential for domestic/global cybersecurity and cybercrime mitigation. For the United Nations cybercrime is a difficult and complicated issue to tackle due to there being no definitive single internationally agreed upon definition of cybercrime within the UN. By the United Nations cybercrime can be broadly defined as “having cyber-dependent offenses, cyber-enabled offenses and, as a specific crime type online child exploitation and abuse”. However, a consensus definition is non-existent. Such governance gaps between nations can create challenges and block the possible collective efforts towards the diffusion of cybercrime threats and hence should work as an important subject of discussion within the committee. However, due to the sheer difficulty of a multilateral cybercrime treaty, other measures such as the bolstering of mutual legal assistance treaties and other agreements can be carried out to maximize cybersecurity.

Bibliography

Security, H. N. (2008, August 4). *Cybercrime and Politics*. Help Net Security. https://www.helpnetsecurity.com/2008/08/04/cybercrime-and-politics/

Dataprot. (2022, October 4). *More Than 70 Cybercrime Statistics - A $6 Trillion Problem*. https://dataprot.net/statistics/cybercrime-statistics/

Wolff, A. (2021, September 7). *The Halfway Point: How Cybercrime Has Impacted Government in 2021*. SonicWall. https://blog.sonicwall.com/en-us/2021/09/the-halfway-point-how-cybercrime-has-impacted-government-in-2021/

Ohanian, C. (2022, October 17). *The UN Cybercrime Treaty Has a Cybersecurity Problem In It*. Just Security. https://www.justsecurity.org/83582/the-un-cybercrime-treaty-has-a-cybersecurity-problem-in-it/

Policies & Procedures Protect Against Cyberattacks. (n.d.). Trellix. https://www.trellix.com/en-us/security-awareness/cybersecurity/cybersecurity-policies.html

Cybercrime Legislation Worldwide. (n.d.). UNCTAD. https://unctad.org/page/cybercrime-legislation-worldwide

United Nations Cybercrime Treaty. (n.d.). Electronic Frontier Foundation. https://www.eff.org/issues/un-cybercrime-treaty

Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure | CISA. (n.d.). https://www.cisa.gov/uscert/ncas/alerts/aa22-110a

Mari, A. (2022, July 19). *Brazil surpasses US in breached users in Q2 2022*. ZDNET. https://www.zdnet.com/article/brazil-surpasses-us-in-breached-users-in-q2-2022/

Statista. (2022, July 6). *U.S. government and cybercrime - Statistics & Facts*. https://www.statista.com/topics/3387/us-government-and-cyber-crime/

Guides: International and Foreign Cyberspace Law Research Guide: Introduction. (n.d.-b). https://guides.ll.georgetown.edu/c.php?g=363530

Contact Information:

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

Chan Kim - Co- Chair

WeChat ID: chankim2007

Email: 25kchan@student.uiszc.org

Rosie Lee – Secretary General
23rlee@student.uiszc.org

Peter Pang – Head of Chair
24ppan@student.uiszc.org

Luke Ross Nuttall – Director of U2NESCO
lrn@uiszc.org