Forum: The Legal Committee (GA6)

Issue: Establishing an international legal framework for the improvement of cyber security laws

Student Officer: George Kanellopoulos

Position: Main Chair

INTRODUCTION

Last year, the Center for Strategic and International Studies (CSIS) published a report that estimated the global cost of cybercrime for the year 2018 to be close to 600 billion US dollars[1]. This piece of information resulting from the analysis of millions of reported cybercrimes leads to an important realization: cybercrime is not a thing of the future. In fact, it is one of the fastest growing crime sectors and in the next few years it will be one of the globe's most damaging issues from an economic, social and diplomatic standpoint.

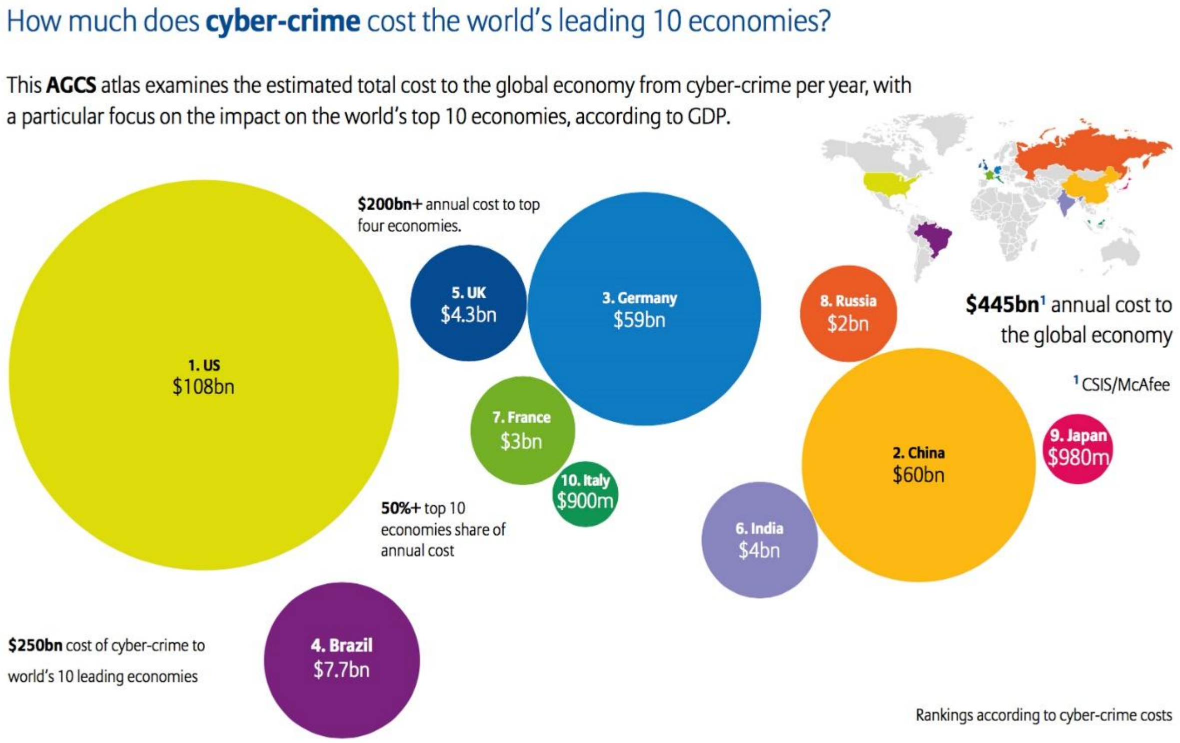
With its development linked to that of ICT (Information and Communication Technologies), it is exponentially growing in complexity and impact. Even though the international community has already recognized it as a serious problem from the beginning of the 21st century, it has up until now notoriously failed to reach a common understanding on resolving it.

Meanwhile, data breaches and other forms of cyber-attacks have exposed enormous amounts of personal information, hindered the function of entire public services including medical ones, and threatened the existence of multinational platforms, such as Twitter. The vast majority of perpetrators of these crimes have still not been put into custody, while a great number of them have not even been identified. This situation cannot be attributed only to the lack of technological know-how by law enforcement agencies but even more to the lack of international cooperation stemming from the lack of a global legal framework.

[1] Lewis , James Andrew. “Economic Impact of Cybercrime.” Economic Impact of Cybercrime | Center for Strategic and International Studies, 10 July 2019, www.csis.org/analysis/economic-impact-cybercrime.

The delegates of the legal committee are now more than ever tasked with reaching the compromise that is now needed in order to shield the inevitable development of technology from being exploited for malicious purposes. The fourth industrial revolution (the information revolution) is now considered to be well under way and a future without an international framework on cybercrime is proportional to a world without international law.

Figure 1 COST OF CYBERCRIME IN 2015[2]



[2] Kulkarni, Satish. "Cybercrime Costs the World $US465 Billion Annually." Cybercrime Costs the World $US465 Billion Annually | TCS Cyber Security Community, securitycommunity.tcs.com/infosecsoapbox/articles/2015/09/24/cybercrime-costs-world-us465-billion-annually.

DEFINITION OF KEY-TERMS

Jurisdiction

"The right of a state to affect persons and property within its territory through executive, legislative, or judicial power".[3]

Every state solely holds complete jurisdiction over its territory and no other state can have jurisdiction on foreign territory unless determined by a valid agreement. This exact case along with the absence of a commonly accepted international legal framework on cybercrime has been the cause of many incidents where the trial of persons accused of cybercrimes or cyberterrorism has been obstructed.

Network

"A group of two or more devices that can communicate. In practice, a network is comprised of a number of different computer systems connected by physical and/or wireless connections"[4]

Everything ranging from email services to sophisticated national security systems is comprised of one or a combination of networks and all hacking attempts are partially or completely centered on disrupting areas of networks.

Cyber Crime

"A crime, in which a computer is the object of the crime (hacking, phishing, spamming) or is used as a tool to commit an offense (child pornography, hate crimes). Cybercriminals may use computer technology to access personal information, business trade secrets, or use the Internet for exploitative or malicious purposes. Criminals can also use computers for communication and document or data storage."[5]

Even though an internationally recognized definition exists for cybercrime, there is not a definite list of actions that can be categorized as cybercrimes.

Cyber Security

"Measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack"[6]

[3] Shaw, Malcolm. "International Law." *Encyclopædia Britannica*, Encyclopædia Britannica, Inc., 7 Dec. 2016, http://www.britannica.com/topic/international-law/Jurisdiction.

[4] Schjølberg, Stein, and Ghernaouti-Hélie Solange. A Global Treaty on Cybersecurity and Cybercrime: a Contribution for Peace, Justice and Security in Cyberspace. 2nd ed., Cybercrimedata, 2011.

[5] "What Is Cybercrime? - Definition from Techopedia." Techopedia.com, http://www.techopedia.com/definition/2387/cybercrime.

[6] "Cybersecurity." Merriam-Webster, Merriam-Webster, http://www.merriam-webster.com/dictionary/cybersecurity.

Cyber security, as a term, encompasses a vast array of measures both physical and digital, including measures that aim to deter persons from even attempting to commit a cybercrime (e.g., public awareness campaigns on the implications of committing a cybercrime)

ICT (Information and Communications Technology)

"Information and communications technology is a field encompassing all kinds of technology that are related to media broadcasting, audiovisual processing and transmission systems and many other network-based functions."[7]

[8]

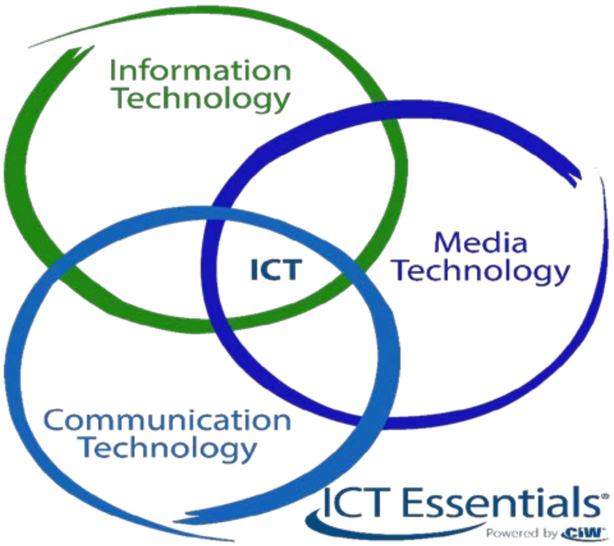


Figure 2 WHAT IS ICT?

[7] "What Is Information and Communications Technology (ICT)? - Definition from Techopedia." *Techopedia.com*, http://www.techopedia.com/definition/24152/information-and-communications-technology-ict..

[8] Partners, Certification. "ICT Essentials: ICT Technology Domains." ICT Essentials Powered by CIW, http://www.ictcertified.com/ict-essentials/ict-essentials.php.

BACKGROUND INFORMATION

Cybercrime is often solely correlated with hacking by the public. However, "hacking" represents only a part of all forms of cyber-attacks and even a smaller fraction of all illicit activities carried out through the manipulation or assault of ICT.

What is considered a cybercrime

Due to the fact that there is no clear internationally accepted classification of cybercrimes, this part will include all major recognized cybercrimes listed depending on their nature.

Identity Theft

This crime occurs when the perpetrator attempts to gain some of the victim's personal information to carry out a variety of actions, such as fund stealing, tax fraud, fake account registration etc. This is often achieved through sending malicious emails and URLs that, if opened, can give access to personal information or even to the computer of the victim. Identity theft is one of the most common and yet unreported cybercrimes with 14.4 million incidents being reported in the US alone last year.

Denial of Service Attacks

Ddos attacks are described as the attempt of the perpetrator to gain access to a computer system by overwhelming the network that this system is part of with fake traffic. This is done through botnets. These essentially are large networks of computers infected by malware, which allows the perpetrator to control these devices.

Cyber stalking

This type of cybercrime essentially covers the cases of harassment of a person through emails and the social media. The goal of the perpetrator is to intimidate the victims by posing threats to their safety or social integrity. The recent explosion in popularity of social media platforms has fueled the unfortunate surge of this cybercrime. Several deaths every year are attributed to cyber stalking and bullying.

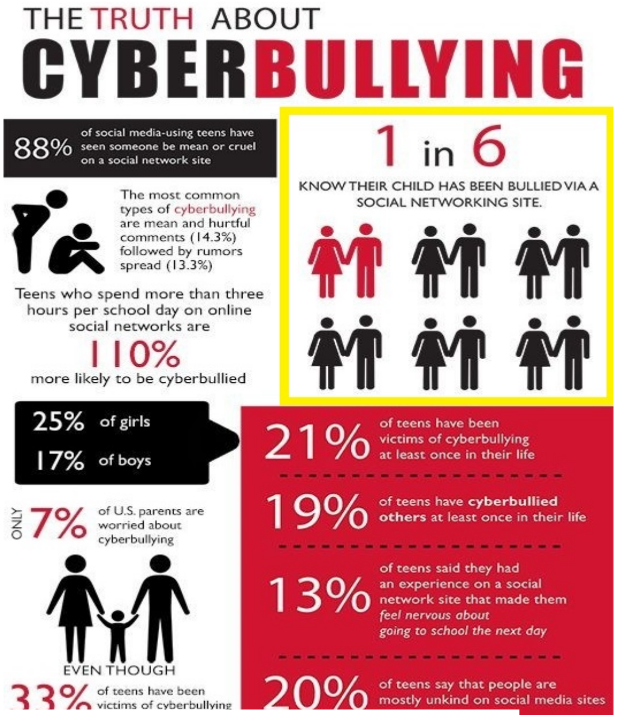


Figure 3 Cyber Stalking and bullying

Exploit Kits

These kits are essentially programs/pieces of code that after being provided with certain information on the target system, are made to exploit a bug (error in the code) in the software of the targeted machine allowing the perpetrator to carry out a variety of actions.

These actions can range from identity theft to complete destruction of the system. The fact that exploit kits have become a product easily usable and rapidly updated in order to overcome any new security patches raises a lot of concern on the part of cybersecurity industry. The producers and distributors of these systems most of the times cannot even be identified due to the hidden nature of the dark web and thus an immediate effective solution other than constantly providing security patches has not been found up until now.

One of the most recent and prominent examples of such attacks was the WannaCry ransomware virus attack of 2017. This virus exploited vulnerability in non-updated Microsoft windows machines, which allowed the installation of software that was able to lock access to the data of a computer unless a ransom was paid. The virus was said to have affected more than 200.000 systems all around the world. The perpetrators allegedly originating from North Korea were never arrested while the DPRK denied any connection to the incidence.

Distribution of Prohibited or Illegal Content

The creation of a part of the Internet that is not accessible through a search engine (dark web) is rumored to have been initially started in order to protect the Internet from the control of oppressive governments and companies. However, this part of the Internet, due to the fact that it consists of websites that cannot be accessed without the user holding the specific link to them, has made the dark web the perfect space for all forms of dangerous illicit activities. Child pornography, illegal substances and private information trade are amongst the most common illicit purposes that websites in the dark web serve.

MAJOR COUNTRIES AND ORGANIZATIONS INVOLVED

United States of America (USA)

The United States of America being amongst the pioneer states in the field of ICT play a very important role in most major attempts to establish an international legal framework on cyber security while also being the nation most affected by cybercrime. It helped form The Budapest Convention on Cybercrime as an observer state and after signing it has traditionally promoted it. Beside this, the US has also participated in the attempts of the Organization of American States (OAS)[9] to create common guidelines on tackling cybercrime.

On a national level, the US has been forming and updating cyber security acts for almost the past 25 years resulting in an extensive national legal framework for the prosecution of cybercrime. This system is also supported by numerous law enforcement agencies and subsidiary bodies. The flagship cyber security agency is the National Cyber Security and Communications Integration Center (NCCIC), which mainly acts as

[9] http://www.oas.org/juridico/english/cyber.htm

a center for public private cooperation, not only providing up to date measures that can reinforce the security of private computer systems but also accepting complaints and coordinating any attempts to track and eliminate ongoing criminal actions in the nation's cyber space.

Russian Federation

The Russian Federation, as one of the nations most involved in the issue of cyber security, has played a pivotal role in the formation of the "eastern approach to cybersecurity". On an international level, it is a signatory of the Shanghai Cooperation Organization's Information Security Agreement and a vocal supporter of attempts to create a new international cybersecurity legal framework through the proceedings of the UN. However, it has been accused multiple times of coordinating cyberattacks against other states' critical networks, with the most notable example being that of the 2016 US presidential elections meddling scandal[10].

China

China, following an even stricter approach on cyber security than that of the Russian Federation, bases its cyber security doctrine on the idea that the control of information and access to it are the most effective ways of eliminating terrorist, secessionist or other criminal activities in the cyber space. It is a signatory member of the Shanghai Cooperation Organization's Information Security Agreement and has also participated in regional training and cooperation programs with the ASEAN (Association of Southeast Asian Nations).

The most important example of China's endeavor in cyber security is the "Great Firewall of China"[11] project. The project, which was first publicized in 2000, aims at restricting access of Chinese Internet users to any sites, platforms or applications that are deemed illegal or dangerous by the Chinese Ministry of Public Security. This is achieved through a (firewall) system formed with the cooperation of the Chinese government with all national (Internet Service Providers) ISPs and other ICT companies, which essentially filters the content reaching the end users of the network. Despite the existence of this system, China is placed amongst the top countries affected by cyberattacks every year, a fact that challenges the effectiveness of the "Firewall" in regard to technically safeguarding its system from malicious actions.

European Union (EU)

The European Union has been and continues to be the source of new legislation revolving around the issue of cyber security. Throughout the last few years, it has

[10] Fandos, Nicholas. "Russian Hacking and Influence in the U.S. Election." The New York Times, The New York Times, 10 June 2019, http://www.nytimes.com/news-event/russian-election-hacking.

[11] pingp. "The Great Firewall of China: Background." Torfox, 1 June 2011, cs.stanford.edu/people/eroberts/cs181/projects/2010-11/FreedomOfInformationChina/the-great-firewall-of-china-background/index.html.

addressed issues ranging from intellectual property in the Internet to cyber security capacity building across the European, American and African continents.

With regards to its approach on cyber security, "The Budapest Convention on Cybercrime", is the most prominent example.

[12] Shanghai Cooperation Organization (SCO)[13]

The Shanghai Cooperation Organization constitutes another approach on cybersecurity through the Information Security Agreement. The organization currently has 8 member states all located in the Eurasian region.

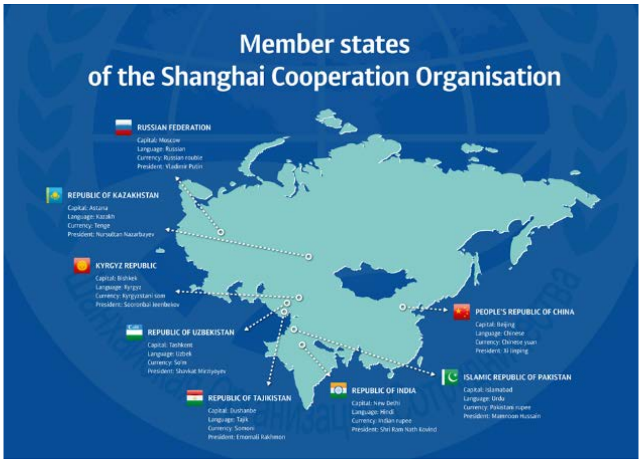


Figure 4 The members of

International Telecommunications Union (ITU)

The International Telecommunications Union is a specialized agency of the United Nations focusing on the ICT sector. Founded in 1865 as the International [14]Telegraph Union, the agency has the main responsibility of coordinating the use of radio communication and technology and acts as the main forum for international ICT cooperation and development. With regards to the topic, the ITU has directly assisted more than 80 countries all over the world by assessing their cyber security capacity, drawing a roadmap for the technical, legal and political framework that they should adopt and then providing consistent technical support for its implementation[15].

ITU serves as a great example of how research and information sharing can lead to the creation of innovative and inclusive solutions to the issue at hand.

Interpol

Interpol has made significant contributions towards an international framework for law enforcement, especially on cybercrime. Focusing on information gathering and distribution and international investigation coordination, Interpol fully takes advantage of its recognition in order to passively or actively support large cybercrime investigations. Its significant technical and intelligence gathering expertise has been displayed in

[12] "News Story: SCO Members Strengthen Anti-Terrorist Cooperation." Pacific Sentinel, pacificsentinel.blogspot.com/2017/09/news-story-sco-members-strengthen-anti.html.
[13] http://ipd.org.pk/pakistan-shanghai-cooperation-organization-friendship-forum/sco-map/
[14] https://dig.watch/events/itu-plenipotentiary-conference-pp-18
[15] Cybersecurity Programme, http://www.itu.int/en/ITU-D/Cybersecurity/Pages/default.aspx.

numerous successful operations, such as the dismantlement of a large international cybercrime server network in the Americas, or the prosecution and arrest of the leader of a multinational email scam scheme based in Nigeria in 2016. Moreover, its police personnel training offered all around the world should not be undermined. Such programs have assisted in the increase of the global cyber security capacity and are extremely valuable in the attempt to create a common standard approach.

Group of Governmental Specialists (UN GGE)

For the purposes of debating on this topic, the term GGE will refer to the UN GGE Developments in the Field of Information and Telecommunications in the Context of International Security. Throughout the 15 years of its existence, the group has been tasked with carrying out research and producing reports on various specific issues regarding cyber security (e.g., "the study of existing and potential threats in the sphere of information security"[16]). Many analysts, based on the fact that half of the meetings of the group concluded without official results claim that the group ultimately failed to meet the abovementioned goal.

Open-Ended Working Group (OEWG)

It was established with the adoption of resolution A/RES/73/27 during the last session of the UNGA and will hold its first meeting in June 2019. It is meant to serve a "negotiation process on security in the use of information and communications technologies"[17]. Its main goal is to "further develop rules, norms and principles of responsible behavior of states in cyberspace and their implementation; introduce changes to previously agreed norms or elaborate additional rules of behavior"[18]. The OEWG represents the Russian Federation's continuous attempt to create a completely new set of norms and principles under the auspices of the United Nations.

TIMELINE OF EVENTS

[16] Korzak, Elaine. "UN GGE on Cybersecurity: The End of an Era?" The Diplomat, 1 Aug. 2017, thediplomat.com/2017/07/un-gge-on-cybersecurity-have-china-and-russia-just-made-cyberspace-less-safe/.

[17] Brown, Deborah. "UN General Assembly Adopts Record Number of Resolutions on Internet Governance and Policy: Mixed Outcomes for Human Rights Online." UN General Assembly Adopts Record Number of Resolutions on Internet Governance and Policy: Mixed Outcomes for Human Rights Online | Association for Progressive Communications, APC, 10 Jan. 2019, http://www.apc.org/en/news/un-general-assembly-adopts-record-number-resolutions-internet-governance-and-policy-mixed.

DATE	**DESCRIPTION OF EVENT**
22nd January 2001	The General Assembly during its 55th session adopts the first resolution on cybercrime A/RES/55/63.
23rd November 2001	The European Union’s Budapest Convention is opened for ratification by all states.
1st July 2004	The Budapest Convention enters into force.
September 2004	First session of the UN GGE takes place.
16th June 2009	The Shanghai Cooperation Organization’s Information Security Agreement is ratified by its then member states.
27th June 2014	The African Union’s Cyber Security Convention is adopted.
10th of July 2015	Procedure of accession to the SCO’s Information Security Agreement starts for India and Pakistan.
12th of May 2017	Outbreak of the WannaCry ransomware virus.

RELEVANT UN RESOLUTIONS, TREATIES AND EVENTS

Resolution 55/63, January 2001

This resolution adopted by the UNGA during its 55th session is one of the first resolutions ever adopted on the issue of cyber security, with the exact topic name being "Combating the criminal misuse of information technologies". In terms of content, the resolution acts as a general acknowledgement of the key measures that need to be taken in order to combat cybercrime at both an international and national level.

More specifically, the measures range from law enforcement personnel training to interstate information sharing initiatives and the protection of personal data and right of access to information.

Resolution 56/121, January 2002

It specifies the key areas that need to be covered with regards to international cybersecurity. Notable points include not only the concept of risk assessment as a tool for creating more efficient national and international legal frameworks, but also the continuous reevaluation and updating of already existing laws and measures.

Resolution 64/211, March 2010

Adopted in the 64th UNGA, it makes statements regarding the role of the cooperation with the private sector developing an effective cybersecurity culture and law.

PREVIOUS ATTEMPTS TO SOLVE THE ISSUE

The Budapest Convention on Cybercrime

The Budapest Convention on Cybercrime[19] was drawn up by the Council of Europe and was opened for signature in Budapest on 23 November 2001. It essentially is a criminal justice treaty that includes:

- a list of actions considered to be attacks against or by means of computers.
- an outline of specific legal procedures, through which investigations on digital media related to cybercrime or any other crime can be carried out.
- the establishment of an international police and judicial cooperation framework on cybercrime.

Apart from setting common standards on the legal aspect of cyber security, the Convention also led to the creation of the Cybercrime Convention Committee. Currently, the committee has 63 member states and its role is to continuously assess the implementation of the convention by the signatory states, while also updating it to cover the latest developments in the ICT industry.

The convention is considered to be one of the most effective attempts to solve the issue, as it has created an environment of cooperation and capacity building between states from different geographical areas around the world. The majority of them have already reached the standards set by the agreement while the European Union along with other member states manage to effectively support LEDCs (Less Economically Developed Countries) also construct their national cybersecurity infrastructure.

However, the attempt of the convention to specifically define all actions that it considers as cybercrimes has led to objections by other states, such as the Russian Federation or China, which refuse to ratify the treaty in protest against their exclusion from the drafting process.

Shanghai Cooperation Organization's Information Security Agreement

On 16 June 2009, the then members of the SCO concluded their high-level meeting with the ratification of an agreement on information security. The ideas of this agreement are displayed in the two drafts of an international code of conduct for information security, circulated in the meetings of the UNGA during the years 2012 and

[19] "Budapest Convention and Related Standards." Cybercrime, http://www.coe.int/en/web/cybercrime/the-budapest-convention.

2015.[20] These codes contained general outlines of the responsibilities and rights of member states with regard to information security, including, among others, proposals for bilateral or multilateral information sharing agreements between nations, in order to exchange security strategies and avoid miscommunications.

Up until now, the agreement has only six signatory states, limiting any potential effect of its implementation. One of the main reasons that have made it controversial, was the right and responsibility of member states to “search for, acquire and disseminate information on the premise of complying with relevant national laws and regulations", a proposition, which, according to many states, provided the basis for governments to regulate information possibly violating fundamental human rights.

POSSIBLE SOLUTIONS

The task of reaching a consensus might seem almost impossible; however, delegates should keep in mind that handling a relatively new and evolving issue allows them the creative freedom to come up with new innovative solutions.

A complete resolution on the topic should cover the following aspects:

Raising Awareness

Many governments, especially LEDCs, do not show willingness to devote the resources necessary for building their cyber security capacity. A way to overcome this issue can be through further research and education, facilitated at a regional and or sub regional level through the organization of expert committees or specialized annual conferences. Other means of promoting awareness could be through international simulations of cyber-attacks.

Equally important to raising governments' awareness on the issue is informing the public about the significance of cybercrime. The significance of raising awareness is extremely critical in this case because a more informed public can persuade governments to take action. However, even more significant is that citizens realize that they should report possible cybercrimes to the responsible authorities, as many reports estimate that less than 50% of all cybercrime cases are actually reported yearly at a global level.

[20] https://ccdcoe-admin.aku.co/wp-content/uploads/2018/11/UN-150113-CodeOfConduct-1.pdf
https://ccdcoe-admin.aku.co/wp-content/uploads/2018/11/UN-110912-CodeOfConduct_0-1.pdf

Effective response

While forming a new framework on cybersecurity, delegates need to determine ways that will promote interstate and inter-agency information sharing and common law enforcement and strike capabilities in the likely case that a real cyber threat emerges.

The various international agencies that are already involved in the issue could prove really useful carriers of the proposed new mechanisms.

International legal coordination

To determine a universal and lasting solution on the issue of cybercrime investigations across multiple countries or regions, several approaches could be pursued;

A single treaty or set of treaties establishing a global regime regarding the exchange of information and free movement and operation of law enforcement units across countries could be proposed. In this case, states supporting the Budapest convention could argue for its ratification and application by all states. On the other hand, other states opposing the ratification of the Budapest convention or of any other already existing treaty could support or join one of the two working groups established during the last General Assembly.

Bilateral or multilateral cooperation treaties between states in a regional or socio-economic context could also be a more feasible way to achieve coordination of states. However, having multiple treaties does not ensure global cooperation, as the possible coexisting different standards could be conflicting.

Reassessment

Constant reconsideration of the framework on cyber security is necessary. Incorporating mechanisms similar to the Budapest Convention's aforementioned committee, as part of any proposed system, is of utmost importance.

Private-public cooperation can also prove extremely beneficial in the attempts of the system to remain updated.

Ensuring the protection of human rights

Assessment of any system proposed should not only focus on its effectiveness, but also on the adverse impact of its implementation on society. The issue of cyber security being closely related to information sharing networks and the Internet has also an ethical aspect.

Proposed systems should include provisions on the protection of private information, right of access to information and freedom of speech.

However, considering that this is one of the most controversial aspects of cybersecurity, delegates always keeping in mind their country's policy, should attempt to reach a consensus on what measures are deemed harmful to those rights.

BIBLIOGRAPHY

- Andreopoulos, George J. “Extradition.” *Encyclopædia Britannica*, Encyclopædia Britannica, Inc., 3 Aug. 2010, www.britannica.com/topic/extradition.
- Shaw, Malcolm. “International Law.” *Encyclopædia Britannica*, Encyclopædia Britannica, Inc., 7 Dec. 2016, www.britannica.com/topic/international-law/Jurisdiction.
- Schjølberg, Stein, and Ghernaouti-Hélie Solange. *A Global Treaty on Cybersecurity and Cybercrime: a Contribution for for Peace, Justice and Security in Cyberspace*. 2nd ed., Cybercrimedata, 2011.
- “What Is Cybercrime? - Definition from Techopedia.” *Techopedia.com*, www.techopedia.com/definition/2387/cybercrime.
- “Cybersecurity.” *Merriam-Webster*, Merriam-Webster, www.merriam-webster.com/dictionary/cybersecurity.
- “What Is Information and Communications Technology (ICT)? - Definition from Techopedia.” *Techopedia.com*, www.techopedia.com/definition/24152/information-and-communications-technology-ict.
- “Budapest Convention and Related Standards.” *Cybercrime*, www.coe.int/en/web/cybercrime/the-budapest-convention.
- https://ccdcoe-admin.aku.co/wp-content/uploads/2018/11/UN-150113-CodeOfConduct-1.pdf
- https://ccdcoe-admin.aku.co/wp-content/uploads/2018/11/UN-110912-CodeOfConduct_0-1.pdf
- “Shanghai Cooperation Organisation.” *CCDCOE*, ccdcoe.org/organisations/sco/.
- Ministry of Foreign Affairs. “The Budapest Convention on Cybercrime: a Framework for Capacity Building.” *News Item | Global Forum on Cyber Expertise*, Ministry of Foreign Affairs, 5 Dec. 2016, www.thegfce.com/news/news/2016/12/07/budapest-convention-on-cybercrime
- “Botnet Operation Disabled.” *FBI*, FBI, 14 Apr. 2011, www.fbi.gov/news/stories/botnet-operation-disabled.
- *Cybersecurity Programme*, www.itu.int/en/ITU-D/Cybersecurity/Pages/default.aspx.