Forum: Disarmament Committee

Issue: Measures to combat cyberattacks and cybercrime

Student Officer: Hazal Bulut

Position: Deputy Chair

Introduction

The Internet and technology are being increasingly used as weapons. In an ever globalizing world where wars were once fought with guns, we now see that wars are becoming internet-based. The scope of as to what is considered as cybercrime is broad: hacking, child sexual exploitation, sextortion, and infringement of copyright are all crimes committed via the Internet. Cyberattacks can be summarized as cybercrime committed with the purpose of causing harm, especially with a political or economic agenda, and thus is as wide of an issue as cybercrime.

With the internet becoming so ubiquitous, such crimes have become more high-profile. This means that in some cases, they have become state-sponsored. States have begun to use cyberattacks to further their political agenda, both nationally and internationally. The Russian meddling with the 2016 US Presidential election, where the Democratic National Convention's computers were hacked to boost the candidacy of Donald Trump, is one example of such an attack. This example is examined in greater detail in the General Overview section.

With the issue of cybercrime and cyberattacks being so broad, the measures taken to prevent them have to be all-encompassing in order to be effective. One of the most important measures that need to be taken is the establishment of global definitions of these terms, given that such definitions do not yet exist. Establishment of a convention and criminalization are other necessary steps that need to be taken.

Definition of Key Terms

Cyber Attack: Although there is no internationally adopted definition, cyberattacks can be defined as all acts in cyberspace intended to cause harm.

Cybercrime: United Nations Office on Drugs and Crime (UNODC) Global Programme on Cybercrime defines cybercrime broadly as “having cyber-dependent offences, cyber-enabled offences and, as a specific crime-type, online child sexual exploitation and abuse.” This means that all crimes committed on cyber space, or via the cyberspace are considered cybercrime.

Copyright Infringement: Copyright Infringement, or piracy, is to use, distribute, and/or display works that are protected by copyright law. All illegal uses of protected work are considered cybercrime.

Sextortion: Threats to expose sexual images of a person to get money or sexual favors. This is another form of cybercrime.

General Overview

In 2019, more than half of the global population has access to the Internet, corresponding to 4.3 billion people worldwide. With that percentage increasing worldwide, it is highly unlikely that cybercrime will not grow increasingly relevant.

Currently, cybercrime acts are distributed quite between financial-driven acts and computer-content related acts. Such acts can be cyber-dependent or cyber-enabled. Cyber-dependent crimes are those that employ malware or ransomware and can take down critical national infrastructure or websites. An example of cyber-dependent crimes would be taking down a website by overloading it with data, which is called a DDOS attack. Cyber-enabled crimes are those that do not necessarily require an ICT system (systems like The Internet) and can take place offline, but are facilitated by ICT systems. Frauds and purchase of illegal substances can be an example. Child sexual exploitation and sextortion are also cyber-enables crimes.

It is important to realize that cybercrimes, for the most part, do not occur on the parts of the internet accessed by the general public on a daily basis. Search engines can access approximately 4% of the internet. Another part of the World Wide Web is The Deep Web, which is not discoverable by search engines. This is where black-market weapons trade happens, as well as drug sales and the distribution of child exploitation. Any measures against cybercrime should also consider the Deep Web in order to be effective.

According to UNODC's 2013 Comprehensive Study on Cybercrime, "police-recorded crime statistics do not represent a sound basis for cross-national comparisons, although such statistics are often important for policy making at the national level. Two-thirds of countries view their systems of police statistics as insufficient for recording cybercrime." Therefore, another issue is knowing the true extent of cybercrime, and the means through which cybercrimes are committed, as police-recorded cybercrime rates show more so the level of specialization of the police force than the actual underlying crime rates.

Specialized structures for the investigation of cybercrime and crimes involving electronic evidence are necessary, as collecting evidence from service providers currently carries varying amounts of difficulty in different Member States. International cooperation should be developed in this regard, as existing agreements of cooperation are regional.

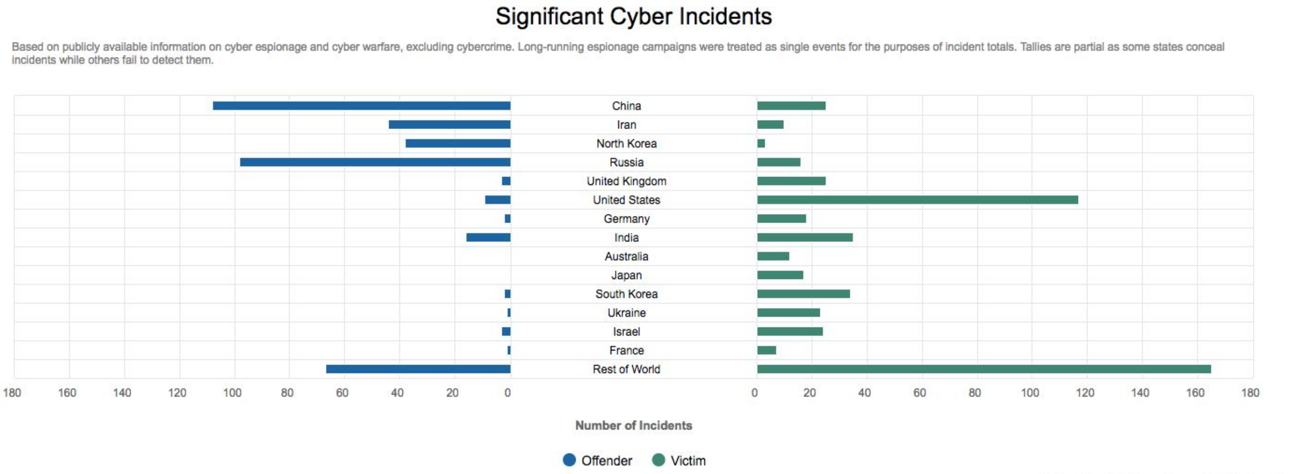
Cyberattacks should also be considered on a global scale, as they are increasingly being carried out by states, rather than individual groups. One example of such an attack was the 2016 US Presidential Election. The computers of the US Democratic National Convention (DNC) were hacked by Russian agents. The information gained from that attack was used to hurt the democratic nominee Hillary Clinton in order to boost Donald Trump's candidacy. Although it is not proven that this cyberattack was carried out by the Russian government itself, there is evidence to suggest that it was. In such cases, it can be observed that cyberattacks can be used to intervene in Member States' governmental affairs.

Major Parties Involved and Their Views

Russia

Britain, Australia and New Zealand have accused the Russian military intelligence of carrying out cyberattacks. “British Foreign Secretary Jeremy Hunt said in a statement Thursday that the country's National Cyber Security Centre (NCSC) had found that Russian GRU intelligence service operatives were behind cyber attacks believed to have cost the global economy millions of dollars” (CNN). The alleged state-sponsored attacks included the aforementioned DNC attack, as well as hackings of global agencies. Russia has not commented on any alleged involvement.

Graph: Significant Cyber Incidents where blye indicates the offender and green indicates the victim. (Center for Strategic & International Studies)



CSIS Technology Policy Program | Source: CSIS & Hackmageddon

China

China has also been accused by other countries of hacking global agencies and exposing sensitive information. Chinese hackers were found to expose the European Union’s communication systems. The US also has accused them of stealing documents from the US Navy, including missile plans. The Norwegian software firm Visma also revealed that hackers from the Chinese Ministry of State Security had targeted the company to steal trade secrets from the firm’s clients”(CSIS). China has also not commented on their involvement in these attacks.

Timeline of Events

6 August 1991	The Invention of the Internet
22 January 2001	The UN General Assembly debated Resolution 55/63, the first resolution on cybersecurity and information technologies.
3 April 2012	The UN General Assembly passed Resolution 65/230, requesting the Commission on Crime Prevention and Criminal Justice to establish an open-ended intergovernmental expert group, to conduct a comprehensive study of the problem of cybercrime and responses to it by Member States
February 2013	The draft of the study requested by 65/230 was published with the help of the UNODC.
17–18 June 2013	The attending countries agreed to cooperate on cybersecurity in the 39th G8 Summit.
2013	The Global Programme on Cybercrime was established with the mandate of helping countries tackle cybercrime in a holistic manner.

UN Involvement

United Nations Office on Drugs and Crime (UNODC) is the UN body that tackles this issue. As stated on their mandate, “UNODC draws upon its specialized expertise on criminal justice systems response to provide technical assistance in capacity building, prevention and awareness raising, international cooperation, and data collection, research and analysis on cybercrime.” The body oversees the Global Programme on Cybercrime as well as the Open-ended Intergovernmental Expert Group on Cybercrime.

Relevant UN Documents

Combating the criminal misuse of information technologies, January 2001 (A/55/63)

United Nations Commission on Crime Prevention and Criminal Justice (CCPCJ) Resolution on Cybercrime (Vienna, 12 -19 May 2010)

United Nations Congress on Crime Prevention and Criminal Justice Resolution on Cybercrime (Brazil, 12-19 April 2010)

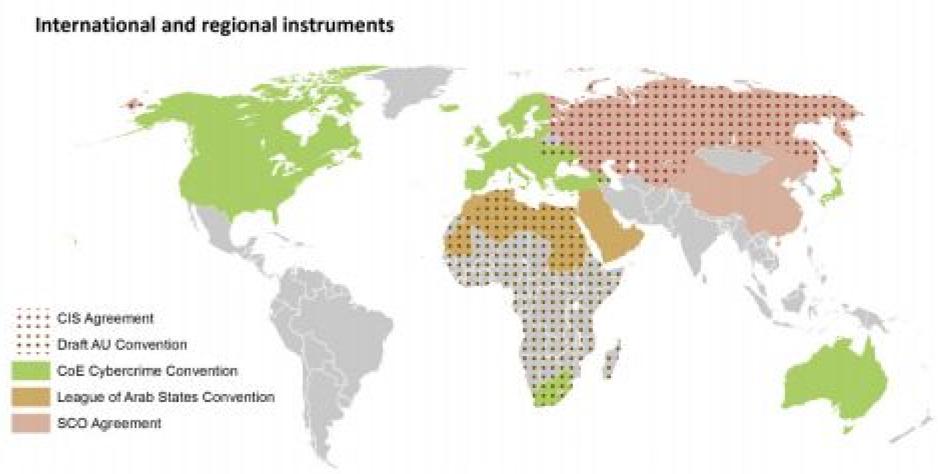
Twelfth United Nations Congress on Crime Prevention and Criminal Justice, April 2011 (A/65/230)

Treaties and Events

It should be stated that there is no international convention on cybercrime, the regional ones are demonstrated on the map above. (UNODC Study on Cybercrime, 2013)

According to the 2013 Comprehensive Study on Cybercrime, globally, 82 countries have signed and/or ratified a binding cybercrime instrument.

The Council of Europe Convention on Cybercrime is the most used multilateral instrument for the development of cybercrime legislation.


International and regional instruments
⁘ CIS Agreement
⁘ Draft AU Convention
🟩 CoE Cybercrime Convention
🟧 League of Arab States Convention
🟥 SCO Agreement

Evaluation of Previous Attempts to Resolve the Issue

All past attempts at solving the issue have been limited in region and scope. The UN resolutions have focused primarily on forming expert groups to prepare a report on the issue. However, the time to act is now. With the data collected, solid action should be taken, as will be discussed below.

Possible Solutions

The most significant necessary steps are legal measures to prevent and combat cybercrime. Criminalization, procedural powers, jurisdiction, international cooperation, and internet service provider responsibility and liability are all issues that need to be solved.

At the national level, cybercrime tend to focus on criminalization. The need for legislation in investigative measures, jurisdiction of police forces and collecting evidence is evident. Furthermore, the perpetrators of cyberattacks should be penalized internationally.

With the issue of cybercrime and cyberattacks being so broad, the measures taken to prevent them have to be focused yet all-encompassing to be effective. One of the most important measures that need to be taken are to establish global definitions of these terms, as one does not exist already. Establishment of a convention and criminalization are other necessary steps that need to be taken.

Notes from the Chair

Although this issue may seem abstract as there is no clear chronological development, please take a look at the UNODC report (linked here) to grasp the issue in its entirety.

Bibliography

“Action on Cybersecurity/Cybercrime.” United Nations System Chief Executives Board for Coordination, United Nations System Chief Executives Board for Coordination, www.unsystem.org/content/action-cybersecuritycybercrime.

Berlinger, Joshua, and Nina dos Santos. “UK Blames Russian Military for 'Reckless' Cyber Attacks.” CNN, Cable News Network, 4 Oct. 2018, edition.cnn.com/2018/10/03/uk/uk-russia-cyber-attacks-intl/index.html.

Diaz-Rhein, Agustina. “Cybercrime Repository.” United Nations Office on Drugs and Crime, United Nations Office on Drugs and Crime, www.unodc.org/unodc/en/cybercrime/cybercrime-repository.html.

Diaz-Rhein, Agustina. “EGM on Cybercrime.” United Nations Office on Drugs and Crime, United Nations Office on Drugs and Crime, www.unodc.org/unodc/en/cybercrime/egm-on-cybercrime.html.

Diaz-Rhein, Agustina. “Global Programme on Cybercrime.” United Nations Office on Drugs and Crime, United Nations Office on Drugs and Crime, www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html.

Lazarev, Ilya. “Treaties.” United Nations Office on Drugs and Crime, United Nations Office on Drugs and Crime, sherloc.unodc.org/cld/v3/sherloc/treaties/index.html?lng=en#/Regional.

Robinson, Michael, et al. An Introduction to Cyber Peacekeeping. Institute of Electrical and Electronics Engineers, 2018, An Introduction to Cyber Peacekeeping, arxiv.org/pdf/1710.09616.pdf.

Significant Cyber Incidents. Center for Strategic and International Studies, www.csis.org/programs/cybersecurity-and-governance/technology-policy-program/other-projects-cybersecurity.