Committee: **DISEC 1**

Topic: **The Question of cyber-attacks and cybercrime.**

Chair: **Elodie Delort**

School: **Sainte Victoire International School (SVIS)**

Summary

Cybercrime is considered to be any criminal act related to computers and networks (such as hacking, phishing) or using a computer to commit any offences (in regards to child pornography and hate crimes), conducted through the Internet. It has seen a massive increase in recent years due to the rising number of connected people and devices.

Cybercrimes can generally be categorised into two varieties:
1. Crimes that target computer networks/devices. This includes viruses, denial-of-service (DoS) attacks, and hacking. It is generally a one-time event from the perspective of the victim.
2. Crimes that use computer networks to promote other criminal activities. This includes cyber stalking, phishing, botnets, piracy, identity theft, fraud, cyber pornography, cyber bullying, and in extreme cases cyber terrorism. These types of cybercrimes tend to be more serious, and are generally on-going series of events.

Background Information

Cybercrimes can create immense amounts of monetary losses. A 2012 report by Symantec stated that 1.5 million people are victims of some sort of cybercrime every single day. The average cost of damage per victim is estimated to be $197, adding up to more than $110 billion lost to cybercrimes worldwide every year. Roughly 80% of all cybercrime are committed by gangs of criminals recruited in highly organised operations.

Computer-related crimes date back to the origins of computing, however, greater connectivity through the Internet has brought the notion of cybercrime to the global public. The first traces of real cybercrime were in the 1980s with the proliferation of email. It then followed on to insecure web browsers that were more vulnerable to viruses. However, the biggest wave of cyberattacks started with the creation of Social Media, in the 2000s. Cyberattacks are becoming business opportunities available to anyone driven by profit and personal gain.

Definition of Key Terms

- **Cyber crime**

Any illegal or unethical activity through internet use or using computers as a tool. (Eg. Creating and selling broken software/untended software.)

- **Cyber security**

Protection of computer systems from theft or damage to their software or electronic data, as well as from disruption or misdirection of the services they provide.

- **Cyber security attacks**

Breaking into the cyber security systems to acquire private information.

- **Hacking**

Gaining unauthorised access to data in a system belonging to a person, company or country.

- **Denial Of Service**

Bringing down a server by flooding the machine with requests in attempt to overload systems.

- **Virus dissemination**

Direct or search for unauthorised access to a system by introducing malicious programs.

- **Phishing**

A malicious individual/group who scam(s) users by sending e-mails or creating web pages that are designed to collect an individual's online bank, credit, or other login.

- **Child Pornography**

A form of child sexual exploitation: any visual representation of sexually explicit conduct involving a minor.

- **Hate crime**

A crime that is motivated by prejudgement on the basis of race, religion, sexual orientation, etc…

- **Cyber stalking**

Use of electronic communications to harass or frighten someone.

- **Botnets**

The use of other' computers to send spam email messages.

- **Cyber terrorism**

Using the internet to perform international, wide-spread attacks that disrupt networks, spread violent messages, recruit terrorists, and plan physical attacks.

- **Malware/ Crimeware**

Software that is designed to cause damage to a single computer, server, or computer network.

- **Firewall**

A protection system for computers to prevent unauthorised access.

Major Countries and Organisations Involved

Global Programme on Cybercrime

Based on the General Assembly resolution of the twelfth United Nations Congress on Crime Prevention and Criminal Justice, and two resolutions on Commission on Crime Prevention and Criminal Justice, the Global Programme on Cybercrime is instructed to assist Member states against cyber-related crimes through capacity building and technical assistance.

The International Association of Cybercrime Prevention

The IACP is a non-profit organisation, "dedicated to the criminal law of computers, securing cyberspace and electronic exchanges to prevent and create awareness about cybercrimes." Its objectives are to "provide a forum for discussion, support and information for Internet users, and to enable improved knowledge on cybercrimes and cyber law governing the internet."

The Cyber Peace Foundation

The CPF is a Non-Governmental Organisation "with the vision of pioneering Cyber Peace Initiatives to build collective resiliency against cybercrimes and global threats of cyber warfare." It aims to reach out to citizens and governments "to provide a common platform on a global level."

The Organisation for Security and Co-Operation in Europe

The OSCE comprises 57 participating States in North America, Europe and Asia. The States are working on confidence-building measures to reduce conflict. These measures are designed to offer concrete tools including a mechanism to de-escalate rising tensions, and a platform for exchanging views.

The Russian Federation

In 2011, the Russian Federation published a convention on International Information Security. However, Russia has been accused of participating in numerous cyberattacks against many countries such as in the 2017 French elections, the 2008 Georgian presidential website hacking, 2016 and 2017 German cyberattacks, the 2009 ISP malfunction in Kyrgyzstan, the 2016 United Kingdom's Brexit referendum, the 2019 Venezuelan website shutdown, and many political interferences with the United States.

People's Republic of China

There have been many controversies regarding China's implications with Cyber security. China was one of the first countries to support Russia's resolutions, however, China has been accused of numerous cyber warfares in the previous years, including the 2013 blueprint incident in Australia, the 2014 computer system disturbance in Canada, the attacks on the Indian government networks, and numerous interferences with the United States.

The United States of America

"The United States Department of Defence recognises the use of computers and the Internet to conduct warfare in cyberspace as a threat to national security but also as a platform of attack." This insinuates that the USA would be ready to use cyber platforms as possibilities for attacks in certain circumstances.
The USA has been accused of performing cyberattacks such as the 2010 Student incident in Iran, the massive 2013 Edward Snowden incident with China, possibilities of 2019 electrical grid attacks on Russia.

Timeline of Events

Date	Description
1960s	First computers "hacked" by students in universities.
1982	First three viruses that attack Apple computers, making computers crash or leak information
January 2001	Resolution on "Combating the criminal misuse of information technologies."
23rd November 2001	Budapest convention on Cybercrimes
2004	Adoption of the Budapest convention on cybercrime
2008	Proposal for an International Cybercrime Convention from several member states

2009	US and Israel allegedly launch Student virus against Iranian facilities
March 2010	Resolution on “Creation of a Global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures.”
April 2010	Proposal for a global treaty on cybercrime rejected due to stalemate between LEDCs and MEDCs
14th September 2011	Russia and China propose an International Code of Conduct for Information Security
December 2011	ECOSOC event on cyber security and development
2013	Edward Snowden copied and leaked classified information from the National Security Agency
October 2013	UN approved the Russian Federation’s draft concerning cyber security
December 2013	Credit card and debit card information stolen from over 40 million US citizens
2015	Chinese Government accused after the United States Office of Personal Management hack
September 2015	Chinese President Xi Jinping and American President Barack Obama met and discussed issues related to cyber security.
2017	Equifax data breach: Largest data breach of credit card numbers and information, affecting over half of US citizens

Relevant UN Treaties and Events

International Telecommunications Union (ITU):
The ITU has a special thrust on cyber security activities as the facilitator of Action Line “Building confidence and security in the use of Information and Communications Technologies (ICTs).” Another essential action area of the ITU is internet policy and governance, its role is commanded in various resolutions regarding international public policy issues on the Internet and its management.

International Multilateral Partnership Against Cyber Threats (IMPACT):

IMPACT serves as a global platform that brings together approximately 152 countries to enhance their capabilities in dealing with cyber threats.
IMPACT is tasked by ITU with providing cyber security assistance and support to ITU's 193 member states and also to other organisations within the UN system.

United Nations Information and Communication Technologies Task Force (UN ICT TF):
The UN ICT TF is "intended to lend a truly global dimension to the multitude of efforts to bridge the global digital divide, foster digital opportunity and thus firmly putting ICT at the service of development for all."

Budapest Convention on Cyber crimes:
It was the first international treaty on crimes committed via the Internet, dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security.
The main objective was to strive for "a common criminal policy aimed at the protection of society against cyber crime."

Previous Attempts to solve the Issue

Since the General Assembly's First Committee in 1998, many UN organisations have become involved in the issue. There was a significant amount of debate concerning cyber security between 1998 and 2004, when the Budapest Convention on Cyber crimes came into force.

In the First Committee of 1998, Russia submitted a resolution concerning Internet security. The initial reaction of the United States of America was to automatically decline this attempt, however, in 2009, the US ended up co-sponsoring the draft resolution on cyber security that had been presented by the Russian Federation in 1998.

In September 2011, the Russian Federation proposed an 'International Code of Conduct for Information Security", with the aid of China, Tajikistan and Uzbekistan. Then, in October 2013, the United Nations approved of Russia's draft that was intended to keep the internet and mobile communications secure.

The Global Cybersecurity Index (GCI) was firstly published in 2014, followed by 2017, and accompanied by a draft published in 2018. The GCI is claimed to be "a trusted reference that measures the commitment of countries to cyber security." It seems to be sufficiently reliable and productive in terms of comparisons made and helps the United Nations to establish the regions in need of the most help.

The cybercrime repository was created in 2015, it is a central database of legislation, case laws, and lessons learned. This repository aims to assist countries to prevent and effectively prosecute cyber criminals.

Possible Solutions

International cooperation is essential to tackle the ever-growing threats of cyber crimes. There are, already, such actions to improve the cooperation such as the Intergovernmental Expert Group.

We should be touching on the ideas of law enforcement and training needs, particularly in developing countries, by exploring the cooperation mechanisms. We should also look into strengthening international communication between governments and UN systems. There should be an encouraged cooperation with organisations such as the Internet Watch Foundation, to report abuse images a protect certain groups from exploitation.
We must remember that prevention is the key to solving this issue; meaning that we ought to prioritise ideas such as heightening the awareness and educating of the general public, (including the education system, legal system, and justice system).

Finally, a paragraph from the United Nations Information Centre: “Countering cybercrime can save lives, grow prosperity and build peace. By strengthening law enforcement capacities and partnering with businesses so they can be part of the solution, we can go a long way in ensuring that the Internet can be a force for good.”

Bibliography

Fruhlinger, Josh. “What Is a Cyber Attack? Recent Examples Show Disturbing Trends.” *CSO Online*, CSO, 26 Nov. 2018, www.csoonline.com/article/3237324/what-is-a-cyber-attack-recent-examples-show-disturbing-trends.html.

Parmar, Kumar, director. *What Is Cyber Crime and Cyber Attack Types Explained in Short Time*. *YouTube*, YouTube, 6 July 2017, *www.youtube.com/watch?v=bOGmYF2oTZ0*.

Bhattacharya, Abhash, 2014 http://www.munish.nl/pages/downloader?code=spc104&comcode=spc1&year=2014

Rahaman, Mohammad Anisur. “Cyber Crime Affects Society in Different Ways.” *The Financial Express*, 4 July 2016, thefinancialexpress.com.bd/views/cyber-crime-affects-society-in-different-ways.

“Taking Action Where We Can to Stop Cybercrime.” *United Nations*, 30 Apr. 2018, unicwash.org/oped-cybercrime/.

ITU. “Global Cybersecurity Index.” *Global Cybersecurity Index*, 2019, www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx.

ITU. “UN Resolutions.” *UN Resolutions*, www.itu.int/en/action/cybersecurity/Pages/un-resolutions.aspx.

UNODC. “Cybercrime Repository.” *Cybercrime Repository*, 2015, www.unodc.org/unodc/en/cybercrime/cybercrime-repository.html.

MUN, Montessori. *Research Report Cyber Security*. 2016, montessori-mun.org/wp-content/uploads/2014/07/Final-Cybersecurity-Background-Guide.pdf.

“Cyber Peace Foundation.” *Cyber Peace Foundation*, www.cyberpeace.org/about-us/.

MUN, The Hague. *Research Report Cyber Security*. Abhash Bhattacharya, 2014, *Research Report Cyber Security*, www.munish.nl/pages/downloader?code=spc104&comcode=spc1&year=2014.

OSCE. “Cyber/ICT Security.” *OSCE*, www.osce.org/cyber-ict-security.