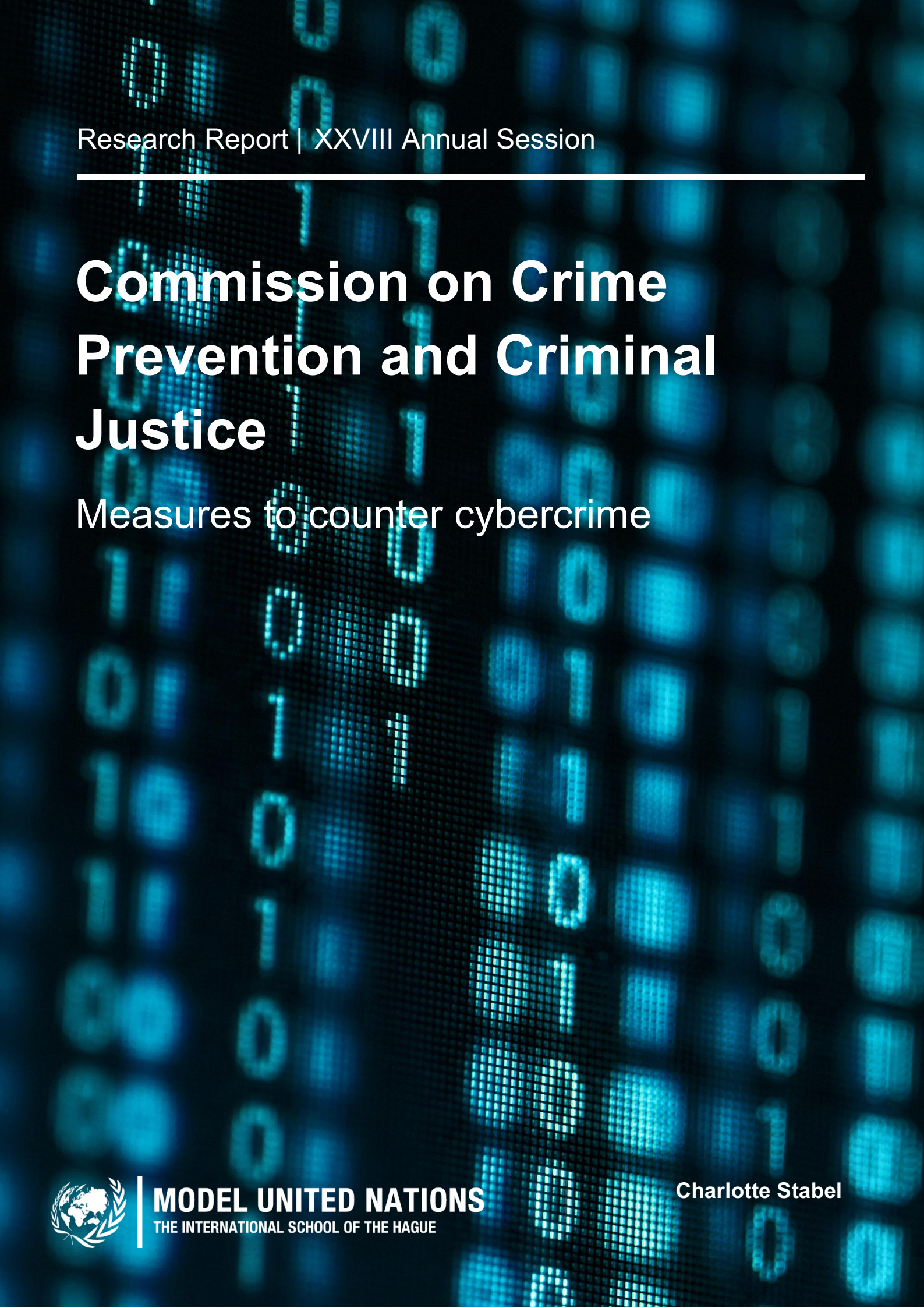

Research Report | XXVIII Annual Session

Commission on Crime Prevention and Criminal Justice

Measures to counter cybercrime

Charlotte Stabel

MODEL UNITED NATIONS
THE INTERNATIONAL SCHOOL OF THE HAGUE

Forum:	Commission on Crime Prevention and Criminal Justice
Issue:	Measures to counter cybercrime
Student Officer:	Charlotte Stabel
Position:	President

Introduction

In less than two decades, the Internet has consolidated itself as a very powerful platform evolving from a curiosity to an essential element of modern society changing forever the way we do business, and the way we communicate. It is one of the fastest-growing areas of technical infrastructures with over four billion people around the world using this platform today. This rapid expansion has proven itself to be very beneficial for many reasons, but with its growth has come a new type of criminal activity: Cybercrime. The internet provides a flexible platform that can be used quickly and easily to spread malicious software and to carry out attacks on individuals, companies and governments from anywhere in the world. Attacks can also be made against essential services such as water and electricity supply, information infrastructure and Internet services which have the potential to harm society in new and critical ways. Cars, traffic control, elevators, air conditioning and telephones also depend on the smooth functioning of this platform. These criminal activities attacks have also been the cause of great financial damage.

According to a study commissioned by the European Commission's Information Society and Media about the “Information Society” made in 2007, malicious software caused damages of up to USD 17 billion in 2003 alone. This number shows just how much power cybercrime has and how much damage this new activity can bring to companies and countries. To counterbalance this growth of criminal activity, cybersecurity plays an important

role in the ongoing development of information technology. Enhancing cybersecurity and protecting critical information infrastructures is essential to each nation's security and economic well-being and therefore a key element to counter and combat cybercrime. Consequently, the World Summit on the Information Society (WSIS) recognized the real and significant risks posed by inadequate cybersecurity and the proliferation of cybercrime. One of the reasons why the topic remains challenging is the constant technical development, as well as the changing methods and ways in which the offences are committed. A perpetrator can act from nearly any location in the world and take measures to mask their identity, and as a result makes this a difficult but very important issue to tackle.

Definition of Key Terms

Cybercrime

Cybercrime, also referred to as computer crime, is defined as an illegal activity which is conducted with the help of a computer and a network. The term is used to describe a brought range of crimes such as spamming, hacking, child pornography, cyberbullying or identity theft. Although there is no single universal definition of cybercrime, there is according to Interpol generally a distinction in law enforcement between two main types of cyber-related crimes:

- Advanced cybercrime, which is a constructive attack against computer hardware and software
- And cyber-enabled crime which refers to "traditional" crimes transformed through the use of internet, such as financial crimes, crimes against children or even terrorism.

Spamming

Spamming is the use of electronic messaging systems like e-mails to send unwanted messages. Although email spam is the most common form of spamming, others exist, like mobile phone messaging spam and social networking spam. Besides compromising user's rights and bothering them, they can have more damaging effects when they are being used for purposes such as infecting computers with viruses or selling illegal products.

Phishing

Phishing is the attempt to obtain financial or other confidential information from internet users by tricking them. More often than not, this act is performed by sending emails that seem to come from a legitimate organization, such as a bank, to obtain this private information.

Malware

Malware is a short term for "Malicious Software" and refers to software programs intentionally designed to damage or do other unwanted actions on a computer system.

Hacking

Hacking is used to describe the unauthorized access to a computer or confidential information.

Identity theft

Identity theft is the illegal use of someone's personal information such as a social security number or driver license numbers, without that person's permission.

Internet Bot

An internet bot, also known as a web robot, is a software that runs automated tasks over the internet. Bots are typically used to perform repetitive tasks at a much higher rate than would be possible for humans. Unfortunately, they are also frequently used for malicious purposes.

Botnet

The word botnet is a combination formed of the words “robot” and “network” and refers to a collection of internet-connected devices infected with malware that allows a third party to control them. A botnet attack, therefore refers to a type of attack that utilizes a botnet to produce damage on a large scale.

Cyberterrorism

According to the U.S. Federal Bureau of Investigation (FBI), cyberterrorism is defined as any “premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against non-combatant targets by sub-national groups or clandestine agents.

Cyberstalking

Cyberstalking is a crime in which an individual uses the internet to harass and or threaten someone.

Denial of Service (DoS) Attack

A Denial of Service (DoS) attack can be defined as an attack which slows or stops a machine or a network, making it inaccessible to its intended user.

Computer worm

A computer worm is a malicious computer program able to infect other computers by replicating itself and sending copies to other computers in a network without human interference.

General Overview

The internet is a worldwide system of interconnected computer networks. It traces its origins back to the 1960's when the US department of Defence wanted to link scientist and university professors around the world. What started as an innocent research project, is today used by over half of the world population. It is not owned by any company or country, and therefore free to be used by any individual on the globe but also threatened by any individual with unethical intentions. The difficulty with combating cyber criminality is the complex nature of the crimes as they take place in the border-less realm of cyberspace. Furthermore, the computer technology currently in use is basically the same around the world. Except from the language issues, there is very little difference between computer systems sold and used in Asia and those in Europe, therefore making it easier for

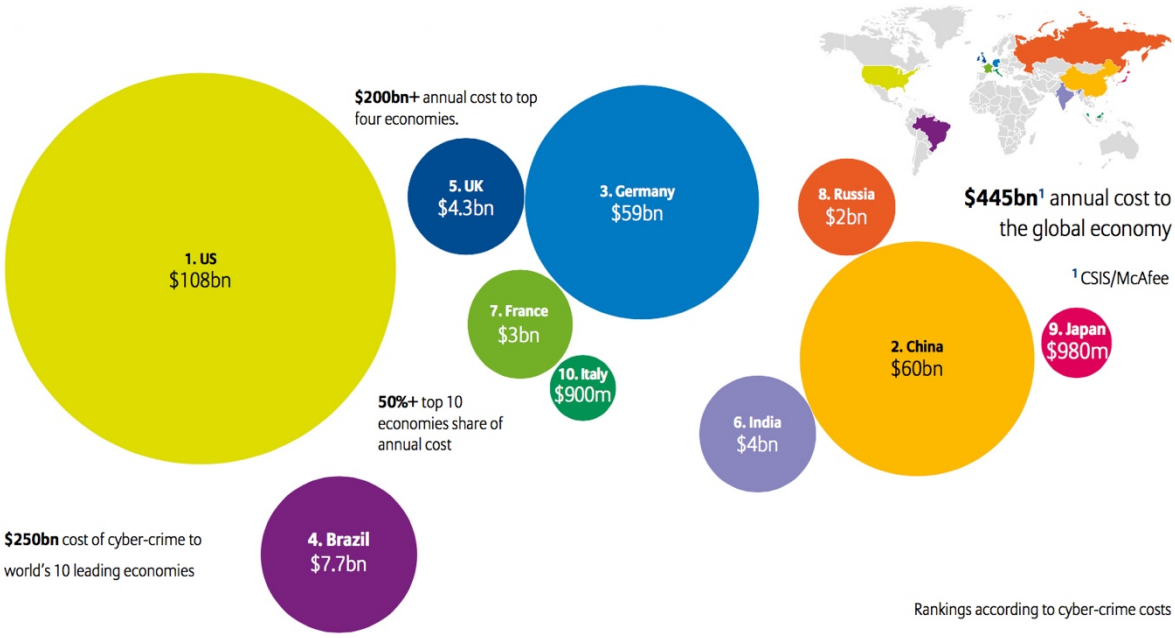

Fig.1. Kulkarni, Satish. "Cybercrime Costs the World $US465 Billion Annually" *Cyber security community*, 24 Sep. 2015.

international criminal activities. It is not only difficult to combat cyber criminality, but it will probably increase in the near future with the exponential growth of technology. And this growth comes along with the cost these criminal activities produce every year. This map is an estimation of the annual total cost to the global economy from cybercrime, with a specific interest on the impact on the world's top ten economies according to their gross domestic product (GDP). It is very clear that the country most affected cost wise by cyber-related crimes is the United States of America with an annual cost of $108 billion (Satish Kulkarni, 24 Sep. 2015). Not only does it cost a great deal of money, but this amount increases every year just as it shown on the graph below showing the development of the global average cost of cybercrime over five years.

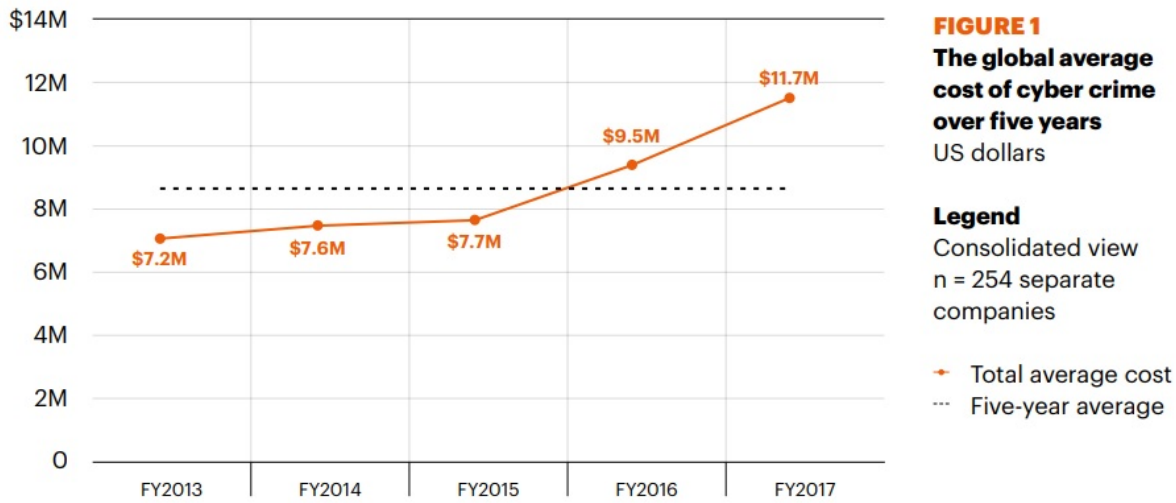

Fig. 2. "Cost of cybercrime study", *Ponemon Institute*, 2017

Legislation

While great efforts are being made every day to prevent cybercrime, the main problem is the lack of harmonisation and therefore of an international legal instrument. Also, there is a lack of national legislations against cyber-related crimes in certain countries such as Papua New Guinea. The reason this lack of national legislation affects the international community so much is that certain material that can lawfully be distributed in one country can easily be illegal in another country making this issue even more difficult. The map below

shows the different stages of legislation concerning cybercrime worldwide. It clearly displays the multiple countries where the issue has not yet been included in their national legislation.

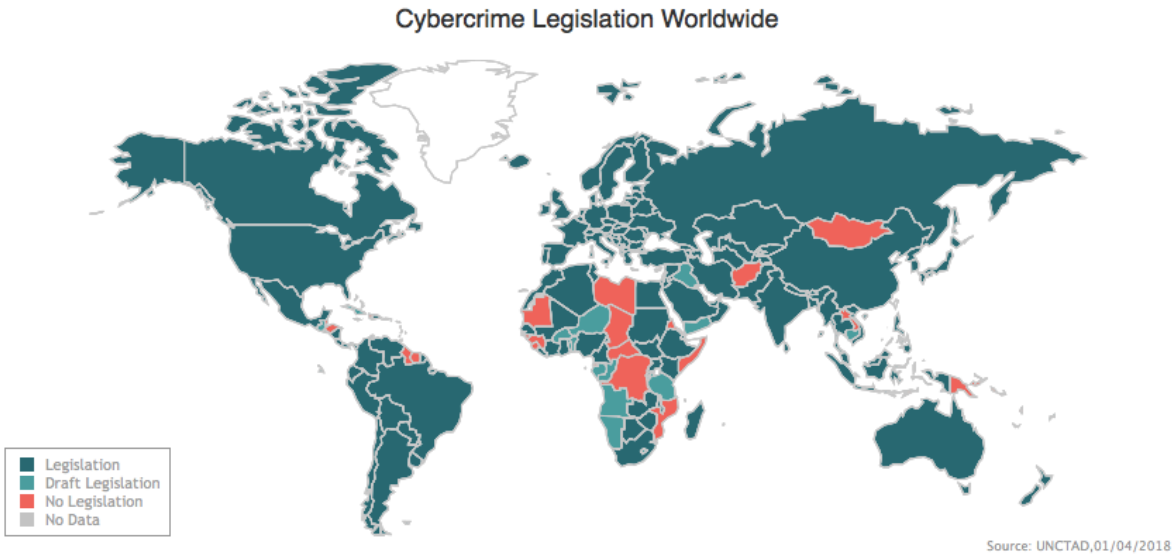

Fig. 3. "Cybercrime legislation Worldwide", *United Nations Conference on Trade and Development (UNCTAD)*, 1 April. 2018

Child pornography

One of the virtues of the internet is its ability to transmit great volumes of information at little cost anywhere in the world, and its ability to bring together people of common interests who would otherwise never meet. These qualities are facilitating illegal behaviour, which is especially dangerous for children. Child pornography is a form of sexual exploitation of children which constitutes a serious violation of human rights. It can be defined as a crime in which harm is caused to children by forcing them to engage in sexual activity. While it is very difficult to put an exact number on the number of offenses committed we can still compare these crimes to other types of cybercrime with this graph below which originates from a report called "The Comprehensive Study on Cybercrime", prepared by the UNODC in February of 2013 for the open-ended intergovernmental expert group on cybercrime. According to this study, in Europe the computer -related production, distribution or

possession of child pornography represents almost 30% of the most common cybercrime acts encountered by national police. Proving how present this type of cybercrime is.

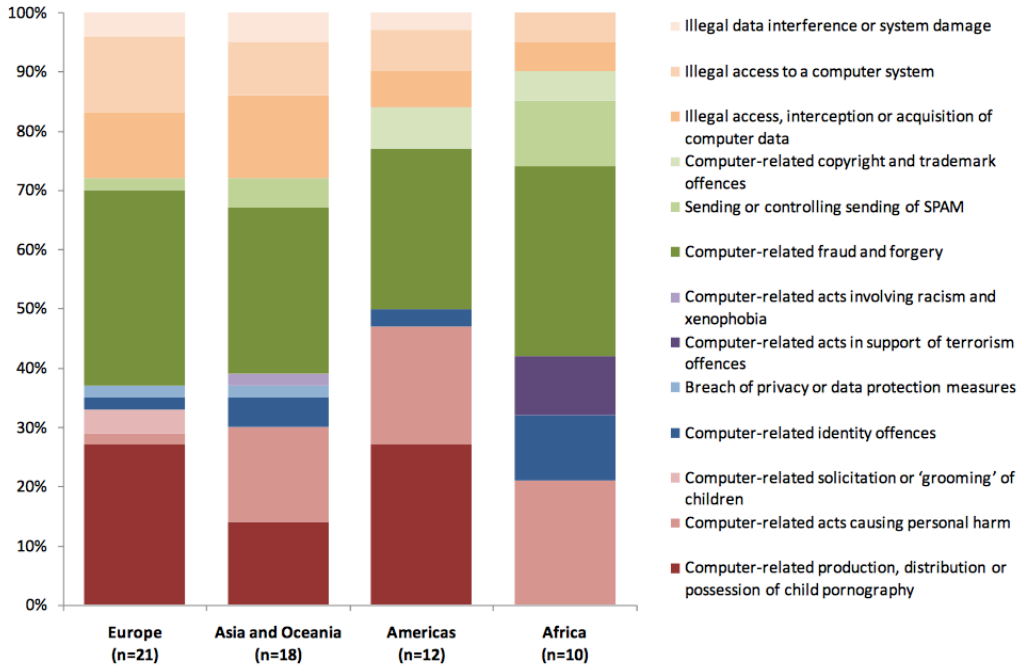

Fig. 4. "Most common cybercrime acts encountered by national police", *Comprehensive Study on Cybercrime*, Feb. 2013.

This crime is also mentioned in the Convention on Cybercrime made in 2001, where its states in the second chapter II - Measures to be taken at the national level, Section 1 – Substantive criminal law, Title 3 – Content-related offences, Article 9 – Offences related to child pornography, that each party of the convention has to adopt these legislations: "

- producing child pornography for the purpose of its distribution through a computer system,
- offering or making available child pornography through a computer system,
- distributing or transmitting child pornography through a computer sys- tem,

• procuring child pornography through a computer system for oneself or for another person,

• possessing child pornography in a computer system or on a computer data storage medium."

Major cases

Over the years, hackers and cybercriminals have shown the world that they have the power to harm and damage companies, governments, and individuals by using computers, internet and networks. Here are a few examples of notable cybercrimes, showing the outspread of these criminal activities.

2007

In April of 2007, hackers unleashed a wave of cyber-attacks that crippled dozens of government and corporate sites in Estonia making Estonia one of the first countries to come under a series of cyber-attacks. This online assault began on the 27th of April 2007 and followed Estonia's decision to move a Soviet World War II memorial from the centre of Tallinn. This statue, also referred to as the Bronze Soldier, symbol of the Red Army, represented for the Russian speaking population in Estonia, the victory over the German Nazis during the Second World War, but to the rest of the population it only reminded them of the long Soviet oppression. As a result, the removal of the statue from the centre of the capital, sparked protests and riots. These uprisings were followed by massive waves of cyber-attacks that lasted for three weeks. These attacks had significant consequences not only in Estonia but world-wide with the motivation to make cyber-attacks a criminal offence in the European Union and get NATO involved, establishing the Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn in 2008.

2014

In 2016, the internet-service company Yahoo! reported that at least 500 million accounts were hacked in 2014, today known as one of the biggest cyber breaches in history.

The attack on Yahoo! resulted in stolen names, telephone numbers, dates of birth, email addresses and other personal information from the users. The breach was only discovered two years after the attack and was only the beginning of a long history of online intrusions.

2015

In July of 2015, two hackers were able to take control of a Jeep Cherokee via its internet connected entertainment system. Chrysler is an American luxury car brand, creator and owner of the Jeep Cherokee model. This cyber-attack was a way for the hackers and researchers, Charlie Miller and Chris Valasek, to prove that it is possible to hack into this internet connected system present in a number of the Chrysler models. This led to the company recalling 1.4 million cars and trucks in the US and fixing their vulnerability and therefore making their system safer (David Goldman, July 2015).

Major Parties Involved

The International Criminal Police Organization

The International Criminal Police Organization (Interpol) is an international organization based in the Netherlands, that facilitates the international police coordination. They also play an important role in the fight against cyber criminality. They are committed “to the global fight against cybercrime, as well as tackling cyber-enabled crimes”. Because most cybercrimes are transnational in nature they are able to contribute on a very large scale.

Federal Bureau of Investigation

The federal Bureau of Investigation (FBI) is the domestic intelligence and security service of the United States and the lead federal agency for investigating cyber-attacks. They state that their priorities are among other things: “Protect the United States against cyber-based attacks and high-technology crimes” and “Combat transnational/national criminal

organizations and enterprises". With an annual budget of $8.7 billion, they have a large capacity to combat and counteract cyber related crimes (Andrew McCabe, June 21,2017).

European Union Agency for Network and Information Security

ENISA is the European Union Agency for Network and Information Security and is contributing to the security of Europe's information society and support cooperation under Member States. ENISA was established in 2004 under European Union regulations. Their main objective is to develop expertise to help assist the Member States in their fight against cybercrime.

United Nations Office on Drugs and Crime

The United Nations Office on Drugs and Crime (UNODC) is a United Nation office that was established in 1997. UNODC is mandated to "assist Member States in their struggle against illicit drugs crime and terrorism. They participate in the combat against cybercrime by offering technical assistance, raising awareness, helping international cooperation, and providing specialized expertise on the matter through research reports. They also started the global program on cybercrime and created the Open-ended intergovernmental expert group on cybercrime.

Timeline of Key Events

Timeline of events in reverse chronological order leading up to present day.

Date	Description of Event
November 1988	The first recognized computer worm ever distributed via the internet was called the "Morris Worm". The worm was the work of Robert Tappan Morris, who became the first person to be convicted under the Computer Fraud and Abuse Act.
26 March 1999	One of the first macro viruses, called "Melissa" was distributed as an email attachment.

13 March 2004	Establishment of the European Union Agency for Network and Information Security
1 July 2004	The convention on cybercrime (Budapest Convention) enters into force
April 2007	Estonian governments networks were harassed by a denial of service (DoS) attack after the removal of a war memorial from the centre of Tallinn.
Summer 2008	Computer systems of both republican and Democratic presidential campaigns were hacked.
January 2009	Israel's internet infrastructure suffers a massive cyber-attack during the January military offensive in the Gaza Strip.
January 2010	A group named the "Iranian Cyber Army" attacked the popular search engine "Baidu", the Chinese equivalent of Google.
January 2011	The Canadian government reported a major cyber-attack against two government departments.
11 January 2013	The European Cybercrime Centre (EC3) was launched.

Previous Attempts to Resolve the Issue

Open-ended Intergovernmental Expert Group on Cybercrime

The General Assembly requested 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. Their first session was held in 2011 and the last in 2017. This group was established in the hope to further clarify and extend the topic of cybercrime.

Global Program on Cybercrime

After the establishment of an open-ended intergovernmental Expert Group on Cybercrime in 2011 and the publication of a "Comprehensive Study on Cybercrime" 2013,

the UN created a Global Program on Cybercrime in 2013 mandated to assist Member states in their struggle against cyber-related crimes.

ITU Global Cybersecurity Agenda

The ITU Global Cybersecurity Agenda (GCA) was launched in 2007 and is a framework for international cooperation. Their aim is to coordinate the response to the challenges of cybersecurity and to share and transmit information on the matter

The convention on cybercrime

The convention on cybercrime also known as the Budapest Convention on Cybercrime or the Budapest convention is the first binding international treaty that concerned itself with Internet and computer crime and serves as a guideline for any country developing comprehensive national legislation against Cybercrime. It is a historic milestone in the fight against cybercrime and cyber threats. It was drafted by the Council of Europe in 2001 but only entered into force 2004. The convention is open for ratification even to states that are not members of the Council of Europe. However, despite its entry into force in 2004, twelve Member states of the European Union have signed but not yet ratified the treaty including Austria, Belgium, the Czech Republic, Greece, Ireland, Luxembourg, Malta, Poland, Portugal, Spain, Sweden and the United Kingdom. As a consequence, there are gaps in the legislation of the Member states.

The Protocol to the Council of Europe Convention on Cybercrime

In 2007, an Additional Protocol to the Convention on Cybercrime was adopted concerning the criminalization of “acts of a racist and xenophobic nature committed through computer systems”.

European Cybercrime Centre

In 2013, Europol set up the European Cybercrime Centre (EC3) which is body tasked to assist member states in their effort to combat cybercrime by developing tools and providing them with training. It also serves as a center of technical expertise on the matter. Moreover, they publish each year a report called the “Internet Organized Crime Threat Assessment” (IOCTA) which serves as a summary of the key findings and developments in cybercrime they managed to discover that particular year.

UN involvement, Relevant Resolutions, Treaties and Events

The United Nations, and in particular the United Nations Office on Drugs and Crime are invested on the issue of cyber criminality and have therefore worked on several resolutions relevant to the issue.

- Resolution 55/63, January 2001 **(A/RES/55/63)**: Combating the criminal misuse of information technologies
- Resolution 56/121, January 2002 **(A/RES/56/121**): Combating the criminal misuse of information technologies
- Resolution 57/239, January 2003 **(A/RES/57/239)**: Creation of a global culture of cybersecurity
- Resolution 58/199, January 2004 **(A/RES/58/199)**: Creation of a global culture of cybersecurity and the protection of critical information infrastructures

- Resolution 64/211, March 2010 **(A/RES/64/211)**: Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures

Possible Solutions

There are certain aspects and solutions which are unavoidable to effectively combat cybercrime. First and foremost, the continuation of implementing and harmonising legislations responsible to define and put a legal framework around this new area of criminal activity is key to combat cybercrime. Furthermore, it is important to ensure that those laws are followed by further coordinating and supporting law enforcement authorities. Also, it is crucial to further encourage capacity building which essentially means to retain the already existing knowledge, skills, tools and other resources. Finally, the training and education on this matter is also an essential part of this process, helping to further expand the knowledge and understanding of this subject. These are the four main aspects to combat cybercrime, but other solutions can be suggested and put into action. The Convention on Cybercrime is for example an essential part to respond to the growing threat of cybercrime in Europe and it is therefore important to encourage the European Member States who haven't ratified it yet to do so. On an international level, establishing a comprehensive international legal instrument to fight against cyberterrorism and other international cyber-related crimes is of utmost importance and thus should be emphasized upon. Authorities should also be encouraged to either improve or make national legislations concerning cyber-related crimes, and or following established models and frameworks as a guideline.

Appendices

Convention on Cybercrime

- http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf

Global Program on cybercrime

. https://rm.coe.int/2-2-unodc-cybercrime-coe-cebu-2017/168072bdb3

Protocol to the Council of Europe Convention on Cybercrime

. http://www.notohatespeech.com/wp-content/uploads/2016/08/AP-Cybercrime.pdf

Bibliography

Dennis, Michael. "Cybercrime" Encyclopaedia Britannica. 3 Sept. 2018. <https://www.britannica.com/topic/cybercrime>

"Global Programme on Cybercrime", *United Nations Office on Drugs and Crime (UNODC)*, 2018 <https://www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html>

"Understanding cybercrime: phenomena challenges and legal response", *International Telecommunication Union (ITU)*, Sep. 2012. <http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf>

"Cybercrime", *Europol*, <https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/cybercrime>

Morgan, Steve. "Cybercrime report", *Cybersecurity Ventures*, 2017. <https://cybersecurityventures.com/2015-wp/wp-content/uploads/2017/10/2017-Cybercrime-Report.pdf>

"Cybercrime Report The Human Impact", *Norton*, <https://www.symantec.com/content/en/us/home_homeoffice/media/pdf/cybercrime_report/Norton_USA-Human%20Impact-A4_Aug4-2.pdf>

"Comprehensive Study on Cybercrime", *United Nations Office on Drugs and Crime (UNODC)*, Feb. 2013. <https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf>

"Cybercrime", *United Nations Office on Drugs and Crime (UNODC)*, <https://www.unodc.org/documents/data-and-analysis/tocta/10.Cybercrime.pdf>

S. Shalini. "Budapest Convention on Cybercrime – An Overview", *Centre for communication Governance* (CCG), 3 Mar. 2016. <https://ccgnludelhi.wordpress.com/2016/03/03/budapest-convention-on-cybercrime-an-overview/>

"Estonia Cyber Attacks", *Afrinic*, <https://meeting.afrinic.net/afrinic-11/slides/aaf/Estonia_cyber_attacks_2007_latest.pdf>

McGuiness, Damien. “How a cyber-attack transformed Estonia”, *BBC News*, <https://www.bbc.com/news/39655415>

“About Cyber Defence Centre”, *NATO Cooperative Cyber Defence Centre of Excellence*, <https://ccdcoe.org>

Goldman, David. “Chrysler recalls 1.4 million hackable cars”, *CNN Tech*, <http://money.cnn.com/2015/07/24/technology/chrysler-hack-recall/index.html>

“A brief guide to the history of the internet”, *Investintech*, <https://www.investintech.com/content/historyinternet/>

“The history of cyber-attacks – a timeline”, *Nato Review magazine*, <https://www.nato.int/docu/review/2013/cyber/timeline/en/index.htm>

“About European Cybercrime Centre”, *Europol*, <https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3>

“Details of treaty No. 189”, *Council of Europe*, <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189>

Poremská, Michaela. “Child pornography on the internet in central Europe”, *Masaryk University Journal of Law and Technology*, <https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=5&cad=rja&uact=8&ved=0ahUKEwi6wNTmpezbAhWCKVAKHeqMC_MQFghIMAQ&url=https%3A%2F%2Fjournals.muni.cz%2Fmujlt%2Farticle%2Fdownload%2F2486%2F2050&usg=AOvVaw2o6cWmzwildhZb1dte-89h>

McCabe, Andrew. “FBI Budget Request for Fiscal Year 2018”, *Federal Bureau of Investigation (FBI)*, 21 June. 2017. <https://www.fbi.gov/news/testimony/fbi-budget-request-for-fiscal-year-2018>