This journal provides immediate open access to its content under the Creative Commons BY 4.0 license. Authors who publish with this journal retain all copyrights and agree to the terms of the above-mentioned CC BY 4.0 license

DOI: 10.2478/seeur-2020-0016

CYBERCRIME: A CHALLENGE TO LAW ENFORCEMENT

PhD. Candidate Dora Arifi, L.L.M
Faculty of Law, South East European University, Tetovo, North Macedonia
da24612@seeu.edu.mk

Assoc. Prof. Dr. Besa Arifi
Faculty of Law, South East European University, Tetovo, North Macedonia
b.arifi@seeu.edu.mk

ABSTRACT

When comparing 100 years ago and today, we always mention the social, economic and political changes that have influenced the emergence and development of the opportunities that we have today, with special emphasis on technological changes. Technology has evolved so fast that it seems that in the blink of an eye something new has just hit the market. Whether we like it or not, technology has become part of us, part of our lives, where we upon spend a great deal of the day with at least one of our technological devices with which we perform many tasks.

Nowadays there are limitless possibilities of gathering information, business, shop, and almost anything through the internet.

Although it is a very easy to make payments online, it can be quite risky, because not every website offers the security and convenience for purchasing the product we want and we may have doubts whether the money we have paid has gone to the right place and for the specific service, which we have paid for. The Internet has many positive as well as negative aspects,

since it also carries great danger because it is much easier to hind behind a false identity and commit illegal acts.

Cybercrime presents a new challenge to legal systems, considering that the more individuals use computer, and the Internet, the more the interest of hackers and perpetrators to commit these types of crimes increases.

Key words: cybercrime, hacking, cyber, technology, cybercrime laws.

INTRODUCTION

At the point when the expression "technology" is referenced, we are additionally connected for certain terms like the Internet, PCs, cell phones, tables and so on, which made it more convenient for us to complete tasks.

The importance of such technology does not need to be discussed because it is clear how dominant it is in our lives. Almost all of us grab our cell phones or surf the net once we wake up in the morning. The internet is not only used for socializing individuals through social networks, it is also used for news, lessons, etc, but also for doing a lot of work for a very short time.

Since all of us use the internet in our everyday life, it is normal that a part of our private life is exposed there, whether we like it or not. This happens because we upload out photos, personal data, share the locations of the places we frequent the most with friends etc. We also make payments and try to but certain products from anywhere in the world. Everything so far is fine. What is not right is the fact that by posting and exposing so many things from our lives, we make information accessible to hackers and we practically become a deliberate target. Consequently, we start facing cyber-bullying, identity fraud, cyber-stalking, etc. On the other hand, many payments through payment cards are made every day, on many websites, and it is precisely the insecurity on some websites that victimizes individuals because instead of successfully making purchases, they lose money, their credit cards and other data are hacked because they are attacked by cybercriminals. This includes credit card fraud, cyber-squatting, e-mail spoofing, intellectual property crimes, etc.

All these offenses are criminal offenses, and these offenses must be provided for in the laws or criminal codes of the states but also in international documents. This crime is costly because it

requires special preparation for investigation, expertise, court proceedings or even the incorporation of its types and forms, because there are many such crimes and even evolve quickly, that makes it difficult for the state. to keep up with these innovations.

Since cybercrime is present all over the world, a great difficulty is that not every country in the world has the professional staff, the right equipment, and the finances to invest so much in fighting these crimes. In many countries, cybercrime is not given as much importance because it is not considered "as important" as other classic crimes, such as murder, and therefore not much action is untaken. On the other hand, there are countries which spend large sums of money to professionalize the judiciary to prosecute these crimes. This means that the world is divided into two parts: states that try to fight cybercrime, states that do not consider cybercrime so dangerous yet. Nevertheless, the challenge is there and is for all states to face.

HISTORY OF CYBERCRIME

The question is often asked how cybercrime came about. Normally this is related to the invention of the computer and computer network but also the internet. As soon as it was widely recognized that computers store something of value (information), criminals saw an opportunity (Shinder & Cross, 2008, p. 42).

The history of the Internet goes back to the first telegraph in 1836. The telegraph revolutionized the way people communicated by using a code (the Morse code, which consisted of dots and dashes), which is similar to the way computers communicate today using 0s and 1s (Kremling & Parker, 2017, p. 31).

To discuss cybercrime, we will first define crime, which is an act or omission that harms any social, political, moral or legal good that is punishable by law. “Crime" consists of engaging in conduct that has been outlawed by society because it threatens the society's ability to maintain order (Brenner, 2010, p. 9).Cybercrime also disrupts order because it involves a series of activities that are illegal and harm individuals, businesses and data. The difference between crime and cybercrime in general is that the first, say a murder, requires a weapon, or a rape requires force, on the other hand, requires a computer. ‘Cybercrime’ broadly describes the crimes that take place within that space and the term has come to symbolize insecurity and risk online (Wall, 2007, p. 10). Cybercrime is relatively a new term, dating back to the 1960s and

tech enthusiasts may come up with a name related to cybercrime, which is MIT, the model of trains whose function was modified.

Before the invention of the cell phone, the Internet, deep-discount, long-distance calling programs and cards; and Skype (a free Web-based service that allows users to talk long distance with other subscribers via the Internet), a band of urban outlaws called **phreakers** developed (Ross & French, 2010, p. 19). Phreakers replaced the official message with one instructing callers that the police were too busy eating donuts and drinking coffee to respond to their calls (Ross & French, 2010, p. 37). In years, of course the perpetrators have consistently become sophisticated. For comparison purposes, in the ‘80s we only had the appearance of the first federal cybercrime that caused a stir and got media attention.

CYBERCRIME TODAY

Not so long ago, computers were large, cumbersome devices utilized primarily by government, research and financial institutions. The ability to commit computer crimes was largely limited to those with access and expertise (Clough, 2015, p. 5).

Today almost everyone in industrialized countries has access to computer technology; children learn to us PCs in elementary school, and people who cannott afford computers of their own can use PCs in public libraries or on college campuses for free, or they can rent computer time at business centers or Internet cafes (Shinder & Cross, 2008, p. 42)

The new millennium brought with it the growing popularity of new and exciting technologies, such as wireless networking and low-cost, high-speed “always-on” connectivity options through Digital Subscriber Lines (xDSL) and cable modems (Shinder & Cross, 2008, p. 52). The more opportunities and new technological innovations are offered to us, the greater the risk and possibility of new types of cybercrime. Therefore, we need to focus on the devices and the most vulnerable programs that can be more easily attacked from cybercriminals.

Cybercriminals love new technologies, including:

- Broadband
- Wireless
- Mobile computing and remote access
- Sophisticated Web technologies such as Java, ActiveX, and so on
- Fancy e-mail programs that support Hypertext Markup Language (HTML) and scripting

- E-commerce and online banking
- IM
- New operating systems (Shinder & Cross, 2008, p. 53).

Predictions are constantly being made based on statistics, cases, data, that cybercrime will cause many losses to humanity, amounting to large sums of trillions.

According to Sausalito, it is said :"If it were measured as a country, then cybercrime – which is predicted to inflict damages totaling $6 trillion USD globally in 2021 – would be the world's third – largest economy after the U.S and China"(Sausalito, 2020).

He also emphasizes that: "Cyber – security" ventures expects global cybercrime cost to grow by 15percent per year over the next five years, reaching $10.5 trillion, annually by 2025, up from $3 trillion in 2015" (Sausalito, 2020).

Hackers today are taking an advantage of everything, whatever opportunity is given to them. Since we are also in a time of pandemics, researchers have noticed that although this situation has become terrifying and boring too, with all the attention to human health issues, cybercriminals have taken an advantage and have been much more comfortable in realizing their plans.

TYPES OF CYBERCRIME

The term cybercrime is a new generalized term that includes forms or offenses related to the introduction and development of technology and that are becoming more common day by day across the globe. They target a computer or a computer network. Harm resulting from such crimes can be against property, against persons, or against both. There are also politically motivated crimes, controversial crimes and technical "non offenses" in the cybercrime world (Schell & Martin, 2004, p. 29). Crimes that can damage property include:

Viruses and worms - are programs encrypted for malicious purposes, which infect and delete data on the computer. A virus is a malware that, when executed, tries to replicate itself into other executable code. When it succeeds, the code is said to be *infected*(Aycock, 2006, p. 14). Both viruses and worms exploit weaknesses in computer software, replicating and /or attaching themselves to other programs (Schell & Martin, 2004, p. 61).

- Phreaking - is a kind of manipulation of phones usually to make free calls as described above.

- Intellectual Property Crime - is a crime that comes in many forms such as: piracy, patents, infringement of trademarks etc.
- Cyber Vandalism - typically involves cyber-attacks to achieve a malicious or vengeful intent (such as a denial-of-service attack launched in retaliation for some slight), to hurt and embarrass someone they are angry at, or simply to hurt people because they enjoy being destructive (Siegel, 2016, p. 562).
- Cyber Trespass - is a form of unauthorized access that deletes, damages or disrupts the computer or computer network.
- Cyber Squatting - Cyber squatting in general refers to the deliberate, bad faith, and abusive registration of the Internet domain names in violation of the rights of trademark owners (Finkelstein & Sims, 2005, p. 148). Cyber squatting means using somebody's name and creating a website for one's benefit. For example, if a random person, Joe, made a website called www.michaeljordan.com, pretending to be Jordan, etc, he would make unwarranted profits, and have an unfair advantage over his online colleagues in terms of revenue from advertising (Gehringer).

The following cybercrimes that affect individuals are:

- Hacking and Cracking - Hacking can expose vulnerabilities in a computer system, but more importantly, it can also damage the system and integrity of the organization that owns it, particularly its ability to store sensitive information(Ross & French, 2010, p. 37). Having gained unauthorized access, crackers destroy vital data, deny legitimate users service, or cause problems for their targets (Anonymous, 2003, p. 3).
- Cyber-Stalking - is a form of electronic harassment, often involving express or implied physical threats that create fear in the victim and that could escalate to real-life stalking and violent behavior (Shinder & Cross, 2008, p. 16).
- Child Pornography - involves a number of aspects: people who create pornographic materials using minor children, those who distribute these materials, and those who access them (Shinder & Cross, 2008, p. 16)
- E-Mail and SMS Spoofing – spoofing is a technique that allows attackers to send e-mails and text messages (SMS) to users that can lead to stolen bank accounts or stolen identities.
- Cyber-bullying - is a type of bullying which takes place over computers and cell phones, mainly saying over digital devices. Cyber-bullying tactics include humiliation,

destructive messages, gossip, slander and other “virtual taunts” communicated through e-mail, instant messaging, chat rooms and blogs (Staf, 2019, p. 11).

Some literatures also mention politically motivated cybercrimes which include:

- Hacktivism - hacker activists, or hacktivists, pairing their activism interest with their hacker skills to promote their platforms and missions.
- Cyber-vigilantism - the convergence of cyberspace and vigilantism (Schell & Martin, 2004, p. 30.

INVESTIGATION OF CYBERCRIME - BUILDING THE CYBERCRIME CASE

When a crime occurs and injures a victim, it is the plaintiff who files a lawsuit and notifies the judiciary. He files a criminal report or lawsuit, thus providing evidence of what happened and then the police and prosecution decide on his case. Investigating Internet Crimes is complicated. If a complaint received is about data found on a website the investigator needs to get clear and concise information as to the website involved in the complaint (Shipley & Bowker, 2014, p. 100).

Forensics comes into play after the commission of any kind of crime, depending on whether it is murder, rape, traffic offense, etc. Digital forensics refers to the scientific acquisition, analysis, and preservation of data contained in electronic media whose information can be used as evidence in a court of law (Reyes, Brittson, O'Shea, Steele, & Jean, 2007, p. 220).

All evidence found is taken and examined in laboratories and other appropriate places, and if there is evidence of a criminal offense, a file is prepared. After collecting the entire file with evidence against the defendant, the investigation is transferred to criminal proceedings.

DIFFICULTIES OF CYBERCRIME INVESTIGATION

According to Lexology, in the Internet Organized Crime Threat Assessment Report ("the Report"), Europol's European Cybercrime Center (EC3) of 2019, discussions have been made about the methods used by perpetrators to commit cybercrime and the threats posed by these crimes to society (Miralis & Miralis, 2020). The Report provides some insight into the five key challenges loss of data, loss of location, challenges associated with national legal frameworks,

obstacles to international cooperation, challenges of public-private partnerships (Miralis & Miralis, 2020). Prosecutors do not necessarily need to be trained in how to find and preserve digital evidence, but they do need to be trained in how to understand it and how to use it in court. The costs of training prosecutors in the intricacies and use of digital evidence therefore must be added to the costs involved in training law enforcement officers to collect and preserve digital evidence (Brenner, 2010, p. 158). A lack of appropriate expertise also presents barriers to the effective policing of cybercrime. Investigating such crimes will often require specialized technical knowledge and skills, and there is present little indication that police have appropriate training and competence, though inroads are being made, predominantly through the creation of specialized officers and units (Steinmetz & Yar, 2019, p. 18).

LAWS AND CRIMINAL CODES ON CYBERCRIME IN THE WORLD

According to UNCTAD, "while 154 countries (79 percent) have enacted cybercrime legislation, the pattern varies by region: Europe has the highest adoption rate (93 percent) and Asia and the Pacific the lowest (55 percent)" (UNCTAD, 2020).

a) German Criminal Code

In the German Criminal Code, in section 303b Computer sabotage it is said that:

"Whosoever interferes with data processing operations which are of substantial importance to another by destroying, damaging, rendering unusable, removing or altering a data processing system or a data carrier, shall be liable to imprisonment of not more than five years or a fine." (German Criminal Code Strafgesetzbuch – StGB)

b) Spanish Criminal Code

In the part "On damages", more precisely in article 278 it is stated:

"Whoever obtains data, written or electronic documents, computer media or other objects related thereto in order to discover a company secret, or who uses any of the means or instruments described in Section 1 of Article 197, shall be punished with a sentence of imprisonment of two to four years and a fine of twelve to twenty- four months (Criminal codes - Criminal Code of the Kingdom of Spain (1995 as of 2013)).

c) Criminal Code of Russia

Cybercrime is incorporated in Chapter 28 "Illegal Access to Computer Information"

"Illegal access to legally-protected computer information, if this deed has involved the destruction, blocking, modification or copying of computer information, - shall be punishable with a fine in the amount of up to 200 thousand roubles, or in the amount of a wage/salary or any other income of the convicted person for a period of up to 18 months, or with corrective labor for a term of up to one year, or with restraint of liberty for a term of up to two years, or with compulsory labor for a term of up to two years, or with deprivation of liberty for the same term" (The Criminal Code Of The Russian Federation No. 63-Fz Of June 13, 1996 p.135-136).

Also there are two other articles referring to cybercrime such as "Article 273 Creation, Use, and Dissemination of Harmful Computer Programs" and "Article 274 Violating the Rules for Operation of the Facilities for Computer Information Storage, Processing and Transmittance and of Information-Telecommunication Networks" (The Criminal Code Of The Russian Federation No. 63-Fz Of June 13, 1996 p.136-137).

d) Macedonian Criminal Code

Article 251 of the Criminal Code of the Republic of North Macedonia, in certain articles related to cybercrime and computer programs for malicious purposes, "Damage and unauthorized entry into a computer system", says that:

"A person who in a unauthorized way deletes, alters, damages, conceals or otherwise makes unusable computer data or a program or device for maintenance of the information system or will disable or complicate the use of computer system, data or program or computer communication, shall be punishable by a fine or up to three years in prison" (Criminal Code of the Republic of North Macedonia, 2002 p.112).

Some other articles related to cybercrime are: "Article 251-a "Making and importing computer viruses" and "Article 251-b "Computer fraud"(Criminal Code of the Republic of North Macedonia, 2002 p.113-114).

INTERNATIONAL IMPACT ON CYBERCRIME

International cooperation on combating and preventing cybercrime is seen at several points. First are the conventions such as The Council of Europe Convention on Cybercrime, the United

Nations Convention against Transnational Organized Crime (UNTOC) and its three protocols, Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, Additional Protocol to the Convention on Cybercrime Concerning the Criminalization of Acts of a Racist or Xenophobic Nature Committed Through Computer Systems,the Inter-American Convention on Mutual Assistance in Criminal Matters, the European Convention on Mutual Assistance in Criminal Matters. As the most important convention, The Council of Europe Convention on Cybercrime and its Protocol is mentioned. Then there are the establishment of certain rules for states to act in the face of these crimes and the increasing use of the option of international co-operation.

The EU did not have a dedicated cybercrime policy until 2007. In 2001 the European Commission published a Communication on information security and combating computer-related crime (Hayes, Jeandesboz, Ragazzi, Simon, & Mitsilegas, 2015, p. 28).

Thus, the European Union has taken steps to ensure that its Member States shall exercise jurisdiction over the online commission of crimes such as child pornography, racism and xenophobia, attacks against information systems and terrorism (Vagias & Dugard, 2014, p. 142). The following are some of the most important international documents on cybercrime:

a) The Council of Europe Convention on Cybercrime

The Cybercrime Convention was opened for signature in Budapest in 2001 (and it is therefore sometimes also known as the 'Budapest Convention' which follows the trend in international law to name treaties after the place they are signed) (Gillespie, 2015, p. 16). While in 2004 it entered into force and the states one by one began to sign and implement the same. The regulation of jurisdiction in the Cybercrime Convention constitutes the best available reflection of the International legal regime on the matter (Vagias & Dugard, 2014, p. 140). This convention is the first international convention in the world, with the aim to prevent crimes committed through the Internet, the computer network that violates freedoms and rights. The Convention is divided into four chapters, although these are themselves to significant subdivisions. The four chapters are:

- Use of terms (Chapter I).
- Measures to be taken at the domestic level (Chapter II).
- International co-operation (Chapter III).
- Final provisions (Chapter IV)(Gillespie, 2015, p. 17).

b) United Nations Convention against Transnational Organized Crime

This UN convention entered into force in 2003, the purpose of which is to develop international cooperation between states and their protection against organized crime in general. Although it does not talk specifically about cybercrime, it is considered to help a lot in this regard because organized crime is related to cybercrime and this convention provides a lot of information about crime prevention procedures and cooperation in combating the same. It also includes: special investigative techniques, transfer of criminal proceedings, protection of witnesses, assistance to and protection of victims etc.

c) Additional Protocol to the Convention on Cybercrime Concerning the Criminalization of Acts of a Racist or Xenophobic Nature Committed Through Computer Systems

According to this protocol it is said: "This Protocol entails an extension of the Cybercrime Convention's scope, including its substantive, procedural and international cooperation provisions, so as to cover also offences of racist or xenophobic propaganda (Additional Protocol to the Convention on Cybercrime, 2003). Thus, apart from harmonizing the substantive law elements of such behavior, the Protocol aims at improving the ability of the Parties to make use of the means and avenues of international cooperation set out in the Convention (ETS No. 185) in this area" (Additional Protocol to the Convention on Cybercrime, 2003 p.198).

d) Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse

Given the highest interest of children and on the other hand the abuse against them, there was a need to create a convention that would protect children from Sexual Exploitation and Sexual Abuse, because prostitution and child pornography are increasingly ubiquitous and persistent of these crimes. Article 1 "Purposes", of this convention stated: "The purposes of this convention are to:

- prevent and combat sexual exploitation and sexual abuse of children;
- protect the rights of child victims of sexual exploitation and sexual abuse;

- promote national and international co-operation against sexual exploitation and sexual abuse of children" (Europe, Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, 2007, p. 2).
-

CONCLUSIONS

Cybercrime is evolving on daily basis, it is being perfected so much that even the judiciary and professionals to fight these crimes constantly have a lack of knowledge or adequate tools because the perpetrator is always one step ahead. The existing laws must be updated in terms of dealing with cybercrime. On the other hand, the rapid spread of crime makes it difficult to create a new law that will cover all forms of cybercrime. Laws that regulate cybercrime must be more specific and clear in order not to doubt its applicability when dealing with court proceedings and criminal judgments precisely for these crimes. On the other hand, the continuous work of international organizations and agencies, which increases the efficiency of cooperation between countries the social awareness for the protection and prevention of cybercrime, through various different initiatives is to be welcomed.

If we all come together and help each other to learn more about these crimes and how to act before we are victimized by them we will significantly reduce the number of such crimes that have expanded and increased the fear of society so much.

Considering the above mentioned, we can conclude that the biggest challenge of law enforcement is the development and provision of technical skills and success in the work of investigations as well as the need to expand the cooperation of states especially when it comes to cybercrime and its investigation in many countries.

REFERENCES

Adopted by the State Duma on May 24, 1. A. (n.d.). The Criminal Code Of The Russian Federation No. 63-Fz Of June 13, 1996. Retrieved January 17, 2021

Anonymous. (2003). Maximum Security - Fourth Edition. Indianapolis, USA: Sams Publishing.

Aycock, J. (2006). Computer Viruses and Malware. Calgary, Canada: Springer, University of Calgary.

Brenner, S. W. (2010). Cybercrime: Criminal Threats from Cyberspace. Santa Barbara, California: Praeger.

Clough, J. (2015). Principles of Cybercrime - Second Edition . Cambridge, UK: Cambridge University Press , University Printing House.

Criminal Code of the Republic of North Macedonia. (2002). Retrieved January 15, 2021, from Official Gazette of the Republic of Macedonia "No. 80/99, No. 4/2002, No. 43/2003, No. 19/2004, No. 81/2005, No. 60/06, No. 73/06, No. 7/08, No. 139 / 08, number 114/09, number 51/11, number 135/11, 185/.

Europe, C. o. (2003, January 28). Additional Protocol to the Convention on Cybercrime. Retrieved January 18, 2021, from Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems: www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189

Europe, C. o. (2007). Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse. Lanzarote: Council of Europe, Council of Europe Treaty Series-No. 201.

Finkelstein, W. A., & Sims, J. R. (2005). The Intellectual Property Handbook: A Practical Guide for Franchise, Business and IP Counsel. Chicago, USA: American Bar Association, ABA Publishing .

Gehringer, E. F. (n.d.). Ethics in Computing. Retrieved January 15th, 2021, from Cybersquatting:https://ethics.csc.ncsu.edu/commerce/cybersquatting/study.php

German Criminal Code Strafgesetzbuch – StGB. (n.d.). Retrieved from Criminal Code in the version published on 13 November 1998 (Federal Law Gazette I, p. 3322) as last amended by Article 2 of the Act of 19 June 2019 (Federal Law Gazette I, p. 844): https://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html

Gillespie, A. A. (2015). Cybercrime: Key Issues and Debate. Lancaster, UK: Routledge; 1st edition .

Hayes, D. B., Jeandesboz, D. J., Ragazzi, D. F., Simon, D. S., & Mitsilegas, P. V. (2015). The law enforcement challenges of cybercrime: are we really playing catch-up? Brussels: Directorate-General for internal policies, Policy Department Citizen's rights andconstitutional affairs, European Parliament EU.

Knittel, J., & Soto, M. (2003). Everything You Need to Know About the Dangers of Computer Hacking. New York NY, USA: The Rosen Publishing Group, Inc.

Kremling, J., & Parker, A. M. (2017). Cyberspace, Cybersecurity, and Cybercrime. Thousand Oaks, California 91320: SAGE Publications, Inc.

Miralis, N. G., & Miralis, D. (2020, August 30). The 5 key challenges for law enforcement in fighting cybercrime. Retrieved January 17, 2021, from Lexology: https://www.lexology.com/library/detail.aspx?g=12513d17-cff3-4d8f-b7dc-cd91826f05d4

Reyes, A., Brittson, R., O'Shea, K., Steele, J., & Jean, C. B. (2007). Cyber Crime Investigations: Bridging the Gaps Between Security Professionals, Law Enforcement, and Prosecutors. Rockland, MA, USA: Syngress Publishing, Inc.

Ross, J. I., & French, J. L. (2010). Criminal investigations Cybercrime. New York Ny 10001: Chelsea House Publisher.

Sausalito, C. (2020, December 21). Cybercrime To Cost The World $10.5 Trillion Annually By 2025. Retrieved December 27, 2020, from Cybercrime Magazine: https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

Schell, B. H., & Martin, C. (2004). Cybercrime: A Reference Handbook. Santa Barbara, California: ABC-CLIO, Inc.

Secretariat, M. o.-G. (n.d.). Criminal codes - Criminal Code of the Kingdom of Spain (1995 as of 2013) . Retrieved January 16th, 2020, from Legislationline: https://www.legislationline.org/documents/section/criminal-codes/country/2/Spain/show.

Shinder, D. L., & Cross, M. (2008). Scene of the Cybercrime - Second Edition . Burlington, MA 01803: Syngress Publishing, Inc.

Shipley, T. G., & Bowker, A. (2014). Investigating Internet Crimes: An Introduction to Solving Crimes in Cyberspace. Waltham, USa : Syngress.

Siegel, L. J. (2016). Criminology: Theories, Patterns and Typologies 13th Edition. Boston, USA: CENGAGE Learning, University of Massachusetts, Lowell.

Singapore, G. o. (1993). COMPUTER MISUSE ACT Chapter 50A Original Enactment: Act 19 Of 1993 Revised Edition 31st July 2007. Retrieved January 16th, 2020, from COMPUTER MISUSE ACT: https://sso.agc.gov.sg/ACT/CMA1993#pr8-

Staf, T. N. (2019). Cyberbullying: A Deadly Trend. New York NY, USA: Rosen Publishing.

Steinmetz, K. F., & Yar, M. (2019). Cybercrime and Society - Third Edition. London, UK : Sage Publications, Inc.

UNCTAD. (2020, April 02). UNCTAD. Retrieved January 17, 2021, from Cybercrime Legislation Worldwide: https://unctad.org/page/cybercrime-legislation-worldwide

Vagias, M., & Dugard, J. (2014). The Territorial Jurisdiction of the International Criminal Court. Cambridge, UK: Cambridge University Press, University of Cambridge .

Wall, D. S. (2007). Cybercrime: The Transformation of Crime in the Information Age. Cambridge, UK: Polity Press.