INTERNATIONAL
HELLENIC
UNIVERSITY

Cybercrime and Incident Response

Evangelos Besas

SID: 3307170001

SCHOOL OF SCIENCE & TECHNOLOGY

A thesis submitted for the degree of

Master of Science (MSc) in Communications and Cybersecurity

JANUARY 2019
THESSALONIKI – GREECE

INTERNATIONAL
HELLENIC
UNIVERSITY

Cybercrime and Incident Response

Evangelos Besas

SID: 3307170001

Supervisor: Asst. Prof. Dr. Komninos G. Komnios
Supervising Committee Members:

SCHOOL OF SCIENCE & TECHNOLOGY

A thesis submitted for the degree of

Master of Science (MSc) in Communications and Cybersecurity

JANUARY 2019
THESSALONIKI – GREECE

Abstract

In today's wired world, cyber security incidents can have a great impact on organizations and critical infrastructure ranging from either economic, or damage in their reputation and credibility, to complete disrupt and destroy of operations.

Moreover, the ever-evolving nature of cybercrime poses more and more challenges that call for a collective approach in order to address them. A well-prepared incident response scheme might mitigate the risks, nevertheless, a solely act it was never enough.

What is needed is, cooperation and collaboration with other stakeholders, such as law enforcement, prosecutors, industry, etc. from across the globe to effectively and efficiently deal with old and new forms of cyber security incidents or cybercrimes.

Moreover, national as well as international laws should set the legal framework within which, each and every party should undertake their role towards the common goal of building and strengthening a cyber resilient public and private sector.

This dissertation firstly, goes on to discuss the cybercrime as a concept, the legal framework that relates to cyber issues and how to effectively respond when an incident occurs, and secondly, continues by making an observation along with a recommendation concerning on the one hand, the lack of total harmonization of national laws and on the other, the time-consuming process of international cooperation through the Mutual Legal Assistance Treaty (MLAT) or Letter of Rogatory (LOR) processes, that both have short and far-reaching implications in the fight against cybercrime.

Evangelos Besas

Acknowledgements

There are quite a few people to whom I would like to express my sincere gratitude for their contribution and support, not only throughout my time at the graduate school, but also during the preparation and writing of this Dissertation.

First of all, I am indebted to my thesis supervisor, Assistant Professor Dr. Komninos Komnios, who since the beginning of my graduate studies until the last day of writing and reviewing this Dissertation, offered me endless support and guidance. He taught me and provided me with in-depth knowledge of the legal framework particularly on privacy and data security laws at a national and international level and also which legislations address the cybercrime in all its phases. His expertise, passion to teach and active involvement gave me courage to go the extra mile and successfully complete this project.

Besides my supervisor, I would like to thank the rest of my dissertation committee members and also all my Professors at the MSc in Communications and Cybersecurity program for all their support and knowledge they gave me. Moreover, I would like to thank my external advisor Mr. Anastasios Papathanasiou who through our discussions he offered me valuable feedback and advice.

Last but not least, I would also like to extend my heartfelt gratitude to Dr. Marios Gatzianas who through his classes, he taught me fundamental knowledge about computer networking that not only gave me a good understanding of how things work on the Internet, but also a broader view and understanding on how, for example, malicious actors could take advantage of the computer systems and networks capabilities to disrupt and destroy. I am totally sure that the knowledge I gained will be useful, not only in my professional and academic career, but also in my personal life as well.

Finally, and most importantly, I would like to express my deepest gratitude to my family, my wife and my two children, Thomas and Helena, without their continued patience and endless support, this dissertation would not have been possible.

Evangelos Besas

Contents

Introduction

The fast pace with which new developments in the information and communications technology (ICT) emerge, have revolutionized the world we live in. In fact, all the technical infrastructure behind what we call as the Internet, has created a virtual wired world that we simply cannot live without it. From communicating and sharing information with others, learning news or doing research, to making online payments and doing business, the Internet has become so deeply ingrained in every aspect of our lives.

However, it is also curiously paradox of our Digital Age, the fact that, the very same technological achievements that helped us make our lives more convenient and empowered us to create even more, also empowered those who would be willing to disrupt and damage. And this is also sad to experience, when it was actually meant to advance rather than to destroy our daily lives, whether it is to a small or to a greater degree[1].

Nevertheless, malicious actors take advantage of these technological improvements and engage in criminal activities perpetrated through the Internet. And what is even more worry, is that these kinds of crimes constitute today the largest portion of criminal offenses, while they still keep increasing in numbers at exponential rates. These criminal acts which are committed through the Internet and make use of a computer system(s) or/and a network(s) are called cybercrimes, with some people though, using both the terms cybercrime and "computer crime" interchangeably and others making a slight distinction between them.

It is actually this definition issue, of the cybercrime or computer crime, that has given rise to some controversy over the past years, with some attempting to define it through its effects, others through its characteristics, and others giving a definition combining effects, characteristics and impact. This is confirmed by many authors in the field, with first and foremost, Eoghan Casey who finds it "problematic"[2] or according to Robert Taylor a "daunting and difficult task"[3], if one wants to define it sufficiently. Even a few years later, Majid Yar brings again to discussion the

[1] President Barack Obama, Remarks at Release of White House Cyberspace Policy Review (May 29, 2009), available at http://www.whitehouse.gov/the_press_office/Remarksby-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/

[2] Eoghan Casey, *Digital Evidence and Computer Crime*, Elsevier, 2004

[3] Robert Taylor, Eric J. Fritsch, John Liederbach, *Digital Crime and Digital Terrorism*, Pearson, 2015

issue of the 'absence of a consistent current definition of cybercrime, even among those law enforcement agencies charged with tackling it'[4].

Cybercrimes, and more specifically, those who commit them, though, do not care at all how they would be defined, and taking advantage of the cutting-edge technology, they have developed highly sophisticated ones, with their numbers dramatically increased in recent years and surpassing, of course, traditional crime rates. In fact, some of the characteristics that played significant role towards that direction, are also the low cost to commit a cybercrime, the high speed of its realization and effects, and, of course, the fact that it can be profitable.

Cybercriminals, thus, have all the motivations to realize their malicious intentions making it imperative for the legislators, law enforcement agencies and other involved parties, not only in the prosecution process, but also in the investigation, analysis, and follow-up procedures, to act fast, effectively and efficiently.

Moreover, it is widely agreed that, the growing evolution of the cybercrime along with its global nature, have also given rise to many challenges with first and foremost, the legislation and jurisdictions. Although national laws of today might deal with certain types of cybercrimes, there is also a need to keep adapting to the continuously evolving cyberspace and what that has to offer. Equally important is also the need for appropriate international laws to harmonize national ones as much as possible, in order to facilitate the process of the investigations and promote international cooperation among law enforcement and other stakeholders.

The first international treaty to deal with the cybercrime was the "Budapest" Convention on Cybercrime[5] that was adopted in 2001 not only by the European, but also by other States around the world. Although it does not explicitly instruct the states what specific countermeasures to take against cybercrimes, it creates a framework of laws that all participating countries should adopt in order to protect privacy and secure their data against cyber-attacks.

[4] Majid Yar, *Cybercrime and Society*, Sage Publications, 2006
[5] Council of Europe, *Convention on Cybercrime***,** European Treaty Series-No.185, Budapest, 23.XI.2001

The European Union cares too much about cyber laws and how to better protect its citizens against malicious cyber acts, that in 2013 it established the Cybersecurity Strategy[6] of the European Union, which all Member-States had to follow in order to ensure an "open, safe and secure cyberspace" where "fundamental rights, democracy" and the rule of law that govern the cyberspace, would be protected.

Moreover, and apart from the EU Cybersecurity Strategy, the European Parliament in 2016 adopted the Directive 2016/1148 on Security of Network and Information Systems (NIS Directive)[7] in order to achieve a high common level of network and information systems security among Member States and strengthen the resilience both for Operators of "essential services" (OESs) and Digital Service Providers (DSPs).

Furthermore, in 2016, the European Union adopted a more collective and strict approach towards the privacy and the processing of personal data, by introducing the General Data Protection Regulation (GDPR)[8] and giving certain rights to EU residents thus, even enabling them to take control over their own data. Moreover, the protection of personal data within the EU is considered fundamental right which organizations not only must respect, but also should be accountable for.

However, and although there is relevant legislation at both international and national level, that criminalizes certain types of cybercrime and also deals with other cyber related issues in Europe, there are still some cases in which things might be interpreted otherwise or the law itself would offer this kind of flexibility to Member States to act at their discretion, though, not without implications.

Although the challenges in the fight against cybercrime that the new era in the digital age has posed are pretty big, including but not limited to encryption, anonymization, virtual currencies, new technological instruments and lack of knowledge or training on them, there are also equally

[6] European Commission, High Representative of the European Union for Foreign Affairs and Security Policy, *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, 2013

[7] The European Parliament and The Council of the European Union, *concerning measures for a high common level of security of network and information systems across the Union*, Official Journal of the European Union, 6 July 2016

[8] Official Journal of the European Union, *Regulation (EU) 2016/679 of the European Parliament and of the Council,* 27 April 2016

huge challenges that come as a result from legislation discrepancies. These differences in laws among States create in turn, not just lack of harmonization, but also lack of effective international cooperation, due to the fact that the legal framework has always constituted the base upon which every procedure and policy could build and develop.

The existence of such challenges automatically entails the necessity for measures or procedures to deal with them. And the only way to address them, is to have a coherent plan where each and every stakeholder would act within the international cooperation framework. For example, the difference in the data retention period of time across Member States varies a lot, and that, has severe consequences to the investigation procedures by law enforcement and even to the prosecution of the perpetrators of criminal offenses by judges. Furthermore, the international cooperation in the framework of the Mutual Legal Assistance Treaty (MLAT) or Letter of Rogatory (LOR) has almost always been a time-consuming process that sometimes, if not most of the times, ended up nowhere. The user's data cannot be retained forever, and with different data retention periods of time could probably result in loss of vital data-evidence. For that reason, it is imperative that the legislation should be as harmonized as possible across Europe, perhaps with explicit references on that, and international cooperation between all stakeholders should be facilitated through well-established channels and based on explicit provisions.

Furthermore, cybercrime and incident response are terms that can hardly be separated, especially within the context of an interconnected world. Incident response plays a significant role in advancing cybersecurity and securing not only the Information and Communication Technology (ICT) systems of a nation's critical infrastructure, but also the ICT systems of each and every company regardless their size. This is a really critical point if we think that a cyberattack could easily go through different networks and even if its initial target was a small company or an individual affiliated to that company, with the appropriate cyber weapons, such as malicious software (malware), it could move laterally and infect the systems of bigger companies and critical infrastructure, thus putting at risk much more than in the beginning and even the national security and economic well-being.

The incident response scheme-program could indeed help in the fight against cybercrime by diminishing the threat and risk that cybercrime poses. The process through which the incident

response can have maximum results is a four-step procedure including a Preparation stage, a Detection, Identification & Analysis stage, a Containment, Eradication & Recovery, and lastly a Follow-up activity. Each and every phase of the Incident Response either involves proactive measures, such as getting prepared by creating an incidence response plan and team, etc., or involves responsive ones such as, containment, eradication & recovery and finally the follow-up actions in order to build on the lessons-learnt and avoid common mistakes in the future. However, as we have mentioned above, a solely act or course of action cannot bring the expected results and thus a more collective approach should be taken in the fight against cybercrime, though, under certain provisions and conditions.

This dissertation is divided into four chapters, an introduction as well as a conclusion-recommendations' section. Beginning with chapter 1, it provides a literature review and relevant background on cybercrime, how it is defined and also focuses on the proposed types of cybercrime. Chapter 2 discusses the European Union Cyber Strategy along with the most important legislation that governs cybercrime and cyber related issues mostly at the international level, however, with impact at the national. Chapter 3 analyzes the concept of incidence response in the case of a cybersecurity incident occurs, what are the steps to follow, who are the first responders, who is in charge, who else is in the team and which stakeholders might engage throughout the process. Chapter 4 discusses the goals of investigating a cybercrime and the challenges that arise during the investigation procedure until the prosecution of the perpetrators, and also stresses the importance of a common legal framework in the fight against cybercrime due to its global nature. Finally, in the Conclusions part of this Dissertation, some observations along with recommendations are discussed on how we could be better prepared to address a cybercrime and thus, diminish, if not eliminate, the risks in the information systems of the organizations and/or of the critical infrastructures that could, in turn, threaten the national security.

1. Cybercrime

Recent years have shown that electronic crimes have been more sophisticated and complex than before while at the same time statistical data have revealed that these features continue to grow at an exponential rate. What is more, is that according to recent reports cybercrime outpaces traditional crime in terms of the impact galvanized by the fast pace of technology and criminal cyber-capabilities. More specifically, according to the National Crime Agency *"…the cost of cybercrime to the UK economy is billions of pounds per annum – and growing*"[9]. Following the same report, it is clear that high-profile crimes have proven that common approaches to information and computer security are simply not sufficient no matter what countermeasures we take to tackle them. A case in example is unethical hackers, also known as 'black hats', who employ sophisticated attacks in order to compromise a computer system, take everything they deem worthy and then erase or make their tracks undetectable in less than twenty minutes[10]! Thus, the current trend proposes to respond by taking a more collective approach from the side of law enforcement, government and private sector to alleviate the existing vulnerabilities, prevent and address cybercrimes.

1.1 What is Cybercrime?

Cybercrime is all about all these features of a conventional crime that also involve cyberspace. In Literature there have been many attempts to define the term "cybercrime" by using various concepts to describe it either in broader or in more specific terms according to the type of criminal activities involved each time. However, there are still a great number of countries that perceive and interpret cybercrime in a vague way in their legislations and law texts, making this lack of a clear definition so problematic that it affects the ways they prevent and remediate it.

David Wall stresses the importance to understand first the impact of the internet on society and how information and communication technologies have shaped the world over the years and then try to define cybercrime[11]. Cyberspace provides tools and creates new opportunities for bad

[9] NCA Strategic Cyber IndustryGroup, *Cyber Crime Assessment 2016*, Version 1.2, July 7th, 2016
[10] Course Technology/Cengage LearningStaff, *Computer Forensics, Investigating Network Intrusions and Cybercrime*, EC-Council Press, 2010
[11] David S. Wall, *Cybercrime, The Transformation of Crime in the Information Age*, Polity Press, 2007

actors to commit illegal activities by taking advantage of its unique characteristics. These characteristics Wall named them as the *"key transformative impacts of the Internet"*, and are as mentioned bellow[12]:

1. "Globalization," which enables bad actors to surpass local or national boundaries.
2. "Distributed networks and grid technologies" which create new opportunities for victimization.
3. "Synopticism and panopticism", which enables remote surveillance capabilities on victims.
4. "Asymmetric rather than symmetric relationships", which do not justify the spend of resources in investigation or prosecution of small-impact victimizations distributed across jurisdictions.
5. "Data trails", which generate new opportunities for bad actors to engage in identity theft.
6. "Changes in the organization of criminal activities", which enable lone or group of criminals to perpetrate extremely complicated and far-reaching tasks that can be repeatedly performed countless times across the globe.

Wall David having in mind the above six transformative impacts of the Internet, defined cybercrime as a 'criminal and harmful behavior' which is 'transformed' and realized through the Internet. The latter simultaneously and automatically creates entirely new opportunities for offenders by providing them with speed, global range and the appropriate means to engage in such activity.

To fully understand how the Internet helps criminals to commit Cybercrimes by offering them new opportunities, Wall built a "matrix of cybercrimes" in order to depict the various levels of opportunities each type of crime creates and also demonstrate that cybercrimes are essentially a 'heterogeneous group of acts.'

In Table 1, is shown the impact of the Internet and technology in creating opportunities that are affected by criminal behavior. The three levels of the Internet's impact on criminal opportunity, are shown below on the Y-axis.

[12] David S. Wall, *'The Internet as a Conduit for Criminal Activity'*, pp. 77-98, 2005 (chapter rev. 2015) in April Pattavina (editor) *Information Technology and the Criminal Justice System*, Sage Publications, 2005

Crime Types ► ***Opportunities*** ▼	***Crime against machines/*** *Integrity-related / Harmful /Trespass*	***Crime using machines/*** *Computer-related Acquisition/ (Theft /Deception)*	***Crimes in the machine/*** *Content - related Obscenity/ Violence*
Cyber-Assisted Crimes – *Computers used by Traditional crime*	* Phreaking * Chipping	* Frauds * Pyramid Schemes	* Trading sexual materials * Stalking * Harassment (personal)
Cyber-Enabled Crimes *- Hybrid cybercrime* *New opportunities for traditional crime*	* Cracking/ Hacking * Viruses * Hactivism	* Multiple large-scale frauds * 419 type fraud * Trade secret theft * ID Theft	* Online Sex trade / * Camgirl sites * General Hate speech * Organized pedophile rings (Child abuse)
Cyber-Dependent Crimes *- True Cybercrime* *New opportunities for new types of crime (Sui Generis)*	* Spams * Denial of Service * Information Warfare * Parasitic Computing	* Intellectual Property Piracy distribution * Online Gambling *E-auction scams *Phishing, smishing, vishing	* Cyber-sex * Cyber-pimping * Online Grooming * Organized Bomb talk / Drug talk * Targeted hate speech [Social network media crimes]

Table 1. *The Matrix of Cybercrimes: Level of Opportunity by Type of Crime*[13]

In the first level of opportunity, there are the *Cyber-Assisted Crimes*, which are essentially crimes that occur in a conventional way, however, they also take advantage of technological assisting tools, but not special ones. For example, the Internet technology may be used via forums to gain information about how to commit more efficiently a crime or facilitate the distribution of illegal products (illegal import of alcohol, drugs, etc.) while diminishing the risk of getting caught. In that level belong crimes such as Phreaking and Chipping, Fraud, Stalking, etc.

[13] David S. Wall, *'The Internet as a Conduit for Criminal Activity'*, pp. 77-98, 2005 (chapter rev. 2015) in April Pattavina (editor) *Information Technology and the Criminal Justice System*, Sage Publications, 2005

In the second level, the Internet brought with it new opportunities for traditional crimes to transform to *Cyber-Enabled Crimes*, such as hacking and cracking, viruses, frauds, child pornography, etc. Perhaps, two of the most well-known cyber-enabled crimes are *Hacking* which actually attacks the CIA triad (Confidentiality, Integrity, and Availability) of an information security system within an organization and the distribution of C*hild Abuse Material (CAM)* because if, we supposedly could take down the Internet, such crimes would be eradicated or at least reduced to a great extent.

In the third level, the *Cyber-Dependent Crimes*, the Internet's impact has led to new forms of illegal activities, such as spams, DoS attacks, Phishing, Intellectual Property piracy, Online Grooming, etc. These types of crimes are so closely related with computer technology that are in essence dependent on cyberspace to be committed.

As for the Internet's impact on offender's behavior, the table depicts that on the X-axis there are three types of crime: "integrity-related (harmful trespass); computer-related (acquisition theft/deception); and content-related (obscenity and violence)". In the first type belong these 'least harmful' crimes that might also serve as precursors to commit other crimes as well, such as cyber-trespass, hacking-cracking, Viruses, DoS attacks, Cyber Warfare, etc. In the second type Wall includes 'acquisitive harm' offences within cyberspace that are computer -related or assisted, such as Identity theft, online Frauds, Phishing, Intellectual Property, etc. Finally, in the third type of crimes belong the most harmful behaviors with obscene and violent content, such as Online Child Pornography, Online Grooming, Hate Speech, etc.

However, the nature of cybercrime or computer crime is still a highly controversial matter and has given rise to too much discussion over the years concerning the solidarity of a clear definition that will impact upon every angle of prevention and remediation[14].

Donn Parker is the first author to write and deliver a definition of what is perceived as computer crime. Through his works (dating from 1976, 1983, and 1998) he kept in touch with computer

[14] Hamid Jahankhani, Ameer Al-Nemrat, Amin Hosseinian-Far, *Cybercrime Classification and Characteristics,* (chapter 12) in Babak Akhgar, Andrew Staniforth, Francesca Bosco, *Cyber Crime and Cyber Terrorism Investigator's Handbook*, Elsevier, 2014

crime evolution highlighting at the same time the key role of computers in what he described as 'computer abuse'[15].

For Parker the term '*computer abuse'* is clearly a 'higher-level definition' and describes it as *"…any incident involving an intentional act where a victim suffered or could have suffered a loss, and a perpetrator made or could have made a gain and is associated with computers"*[16]. Moreover, the four ways in which computers engage in computer abuse are when:

1. The "computer is the object", or the information in the computer is the object of the act (e.g. when someone steals or damages a computer).
2. The "computer is the subject", while it creates a unique environment or unique form of assets (e.g. when a virus infects or impairs a computer).
3. The computer is the medium or the tool of the act (e.g. when a computer is used to gain access to other computers).
4. The computer "represents a symbol" used to fear or to deceive (eg. a stockbroker pretending to have a secret computer software in a powerful computer in a Wall Street brokerage firm in order to earn a lot of money on rapid stock option trading).

However, over the years these categories have proved to be general enough to address the definitional issues on how to include both the "computer abuses" as defined by Parker in 1976, as well as the modern computer crimes the way we perceive them today.

Robert Taylor in his book "*Digital Crime and Digital Terrorism"* also outlines the problematic nature of defining computer crime by stating "Defining computer crime sufficiently is a "daunting and difficult task"[17]. Taylor following Parker's definitions (from 1976 to 1998) on one hand, and having in mind the evolution of technology that affected the nature of crimes on the other hand, he presented his four categories in a clearer way:

[15] Anthony Reyes, Kevin O'Shea, Jim Steele, Jon R. Hansen, Captain Benjamin R. Jean, Thomas Ralph, *Cyber Crime Investigations, Bridging the Gaps Between Security Professionals, Law Enforcement and Prosecutors*, Syngress, 2007
[16] Donn B. Parker, *Crime by Computer*, 1976
[17] Robert Taylor, Eric J. Fritsch, John Liederbach, *Digital Crime and Digital Terrorism*, Pearson, in Anthony Reyes, Kevin O'Shea, Jim Steele, Jon R. Hansen, Captain Benjamin R. Jean, Thomas Ralph, *Cyber Crime Investigations, Bridging the Gaps Between Security Professionals, Law Enforcement and Prosecutors*, Syngress, 2007

1. The computer as a target. In this category falls any attack to the system of legitimate users in order to render it inoperable or even destroy it (e.g. Denial-of-Service, virus infection, etc.).
2. The computer as a tool of the crime. For example, a computer might be used to access another computer and steal personal data.
3. The computer as "incidental to a crime". In that sense the computer is simply facilitating the crime. (e.g. money laundering, trade with child abuse material-CAM).
4. Crimes related to the dominance of computers. This involves crimes against the computer infrastructure, such as the theft of intellectual property and software piracy.

Eoghan Casey, also notes that is critical to develop a better understanding of how computers can be involved in a crime. While he shares the same view that, so far, a general agreement there has not been reached on the definition of the term *computer crime*, he stresses the norm of many authors throughout the years who have achieved a rather functional definition of it[18]. Casey's book *Digital Evidence and Computer Crime* focuses on digital evidence that is related to a crime and is in favor of a broader definition of computer crime that apart from computers and networks it also involves situations in which a crime does not 'rely heavily on computers' but to the fact that it still contains digital evidence. A case in point would be, an email that might contain incriminating information for a person, however the email itself would not have any active role in the realization of the crime.

Besides highlighting the importance of digital evidence, what Casey thinks problematic in defining computer crime, is the fact that many authors, like Parker, have categorized the role of a computer as an object, as a subject, as an instrument/tool to plan or commit crimes or even as a symbol (like Parker did), however, without anyone thinking of a computer as a digital evidence.

Majid Yar in his book *Cybercrime and Society*, argues that the 'absence of a consistent current definition of cybercrime, even among those law enforcement agencies charged with tackling it', is a major problem for its study[19]. He suggests that cybercrime should not be seen as a sole concept but rather as 'a range of illicit activities' whose 'common denominator' is the key role that the networks of information and communication technology (ICT) play in their commission.

[18] Eoghan Casey, *Digital Evidence and Computer Crime*, Elsevier, 2004
[19] Majid Yar, *Cybercrime and Society*, Sage Publications, 2006

Yar also shares *Thomas* and *Loader's* definition[20] who describe cybercrime as those 'computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks'. It is important to note that Thomas and Loader in their definition differentiates crime (which is any explicitly prohibited illegal act) from deviance (which is any act against social norms and rules and thus, undesirable or objectionable). However, from the criminology point of view this is not always the case and might not be separated one from the other.

Yar furthers his understanding on cybercrime by citing *Furnell* (2002) who distinguished between 'computer assisted crimes' (essentially traditional crimes that take advantage of cyber domain e.g. fraud, theft, money laundering, etc.) and 'computer-focused crimes' (offenses that have appeared at the same time with the advent of the Internet, and could not exist apart from it e.g. hacking, cracking, website defacement)[21].

Finally, Yar in order to better classify and interpret cybercrime and also enable everyone to link cybercrime to existing conceptions of not allowed and damaging acts, he provides the four categories presented by David Wall, that is, "Cyber-trespass, Cyber-deceptions and thefts, Cyber-pornography, and Cyber-violence", adding that the first two comprise 'crimes against property', the third has to do with 'crimes against morality', and the fourth relates to 'crimes against the person'. However, he also adds a fifth category 'crimes against the state', which are actions that infringe legislation securing the integrity of the state and its infrastructures (e.g. terrorism, espionage and disclosure of confidential or top-secret information).

The *Encyclopedia Britannica* refers to the term cybercrime and computer crime interchangeably and although there might be other disparities too, it outlines the absence of a digital computer that differentiates traditional criminal activity from cybercrime. According to its definition, the use of a computer is considered the tool to commit illegal activities, such as identity theft, fraud, distribution of child pornography material, trafficking of intellectual property, and infringement of privacy[22].

[20] Thomas and Loader, *Cybercrime: Law Enforcement, Security and Surveillance in the Information Age,* Routledge, 2000
[21] Majid Yar, *Cybercrime and Society*, Sage Publications, 2006
[22] Encyclopedia Britannica, *Cybercrime*, https://www.britannica.com/topic/cybercrime, accessed on11/21/2018

It is a fact that as technology advances more new criminal opportunities are created along with some new types of crime for bad actors to engage. Cybercrime, especially via the web, has grown in significance as the networked computers have become central to our lives, commerce, entertainment, and government. Besides, cybercrime in most cases prevail over traditional crime and will continue to do so in the years to come. That is simply because the advent of the Internet has brought with it knowledge, speed, ease and gave a global character to cybercrime that attracts cybercriminals to deploy their machinations.

The *Interpol* acknowledges too, that there is no global definition for cybercrime, however the Law Enforcement agencies, by and large, categorize the cybercrimes in two types: Firstly, those who are highly sophisticated and complex crimes (high-tech crimes) against computer hardware and software, and secondly, those who are cyber-enabled crimes such as, crimes against children, financial crimes. Interpol goes on to argue that a shift from simple forms of cybercrime to more complex and highly organized ones (criminal organization rather than individuals) has been made in recent years having a great impact in the global economy. Criminal rings by taking advantage of the new technologies they are becoming "widespread and damaging"[23].

In 2001, the *Council of* Europe (CoE), adopted its Convention on Cybercrime Treaty, also known as "Budapest Convention" in which recognizes certain activities to be cybercrimes (CoE, 2001):

- The illegal access to a computer system with the intent of obtaining computer data.
- The illegal interception of private (non-public) traffic of computer data to, from or within a computer system, "including electromagnetic emissions from a computer system carrying such computer data".
- The illegal interference on computer systems for purposes of damaging, deleting, deteriorating, alterating or suppressing computer data without being eligible.
- The serious preventing, without right, of the function of a computer system by "inputting, transmitting, destroying, erasing, deteriorating, modifying or suppressing computer data".

[23] https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime, accessed on 11/21/2018

- The internationally input, modification, erasure, or suppression of computer data, resulting in "inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, (forgery)".
- Any fraudulent or dishonest action such as, any interference, input, modification, erasure or suppression of computer data, for profit purposes.
- The production and distribution of child pornography material, distribution or transmission, offer or making it available, the procurement, possession in a computer system or on a computer-data storage medium.

1.2 Categories and Types of Cybercrime

As mentioned in sub-chapter 2.1, in Literature exist many definitions of what cybercrime is, however, in order to better define it some authors have gone on to classify cybercrime into a certain number of categories. For our purposes and in order to satisfy most the meaning behind cybercrime we will consider three main categories of cybercrime. That is, firstly, cybercrimes in which the computer is the target, secondly, cybercrimes in which computer is the tool to commit illegal activities, and thirdly cybercrimes in which computers are just facilitating other crimes.

Cybercrimes: Computers as a target

In this category fall all these cybercrimes in which a computer or information system becomes the target of a cyber-attack. In other words, all these illegal activities in which the perpetrators engage in and attack the computer or information system in order to obtain access, steal or destroy data, etc. Some of the main types of such cybercrimes are: hacking/cracking, malware (ransomware or destructive malware), denial of service (DoS or DDoS).

Hacking

Hacking or cyber-trespass[24], is the unauthorized access into a computer system that it is owned by a legitimate entity who has also established certain rights on it. The perpetrator of this type of

[24] David S. Wall, *'The Internet as a Conduit for Criminal Activity'*, pp. 77-98, 2005 (chapter rev. 2015) in April Pattavina (editor) *Information Technology and the Criminal Justice System*, Sage Publications, 2005

cybercrime is called hacker and might also engage in non-malicious activities, usually by altering equipment or processes. The most well-known techniques used by hackers are the following and not limited to, vulnerability scanner, password cracker, packet sniffer, key logger, spoofing attack, etc.

Cracking

Cracking is also a cyber-trespass, as David Wall has also written about, in terms of unauthorized access, however, the distinction is increasingly being made between principled trespassers (hackers) and unprincipled trespassers (crackers). While hackers might engage in a less harmful or even harmless cyber-trespass, crackers would undertake the most harmful activities by even destroying data, damaging computer systems, etc. Apart from the above, other cyber-trespassers are cyber-vandals, cyber- spies, and cyber-terrorists[25].

Ransomware

Ransomware is a type of malware (essentially a malicious software) that once it infects the targeted computer system it spreads rapidly across it and within an organization with the intention of blocking access of any legitimate user to the specific computer system or data. The ransomware is implementing by encrypting all important documents and files with a public key and then demands a ransom, typically in cryptocurrencies, to unlock them. Sometimes the ransomware is also called "scareware" as it pushes users to pay a fee (or ransom) by “scaring” or blackmailing them. Examples of ransomware are: Cryptowall (2014), Cryptolocker (2013), CryptoDefense (2014), TorrentLocker (2014), Wannacry, Petya, etc.

Destructive malware

This kind of malware is actually a program designed and specified by the attackers with the goal of destroying the data on a computer's hard drives, preventing the computer from running and resulting in a loss of information. Thus, once a destructive malware (eg. Trojan) infects a computer system, it will ultimately result in OS failures by randomly deleting files, folders, and registry entries.

[25] David S. Wall, *‘The Internet as a Conduit for Criminal Activity’*, pp. 77-98, 2005 (chapter rev. 2015) in April Pattavina (editor) *Information Technology and the Criminal Justice System*, Sage Publications, 2005

Denial of Service Attack/ Distributed Denial of Service Attack (DoS/DDoS)

A Denial-of-Service attack (DoS) is a cyberattack where the offender aims to render a device or network resource unavailable to its intended legitimate users by interrupting services of a host connected to the Internet, either temporarily or indefinitely. Denial of service is typically accomplished by sending countless requests to the targeted machine or resource in an attempt to overwhelm systems and hinder some or all legitimate requests from being fulfilled.

A Distributed Denial-of-Service (DDoS) is a cyber-attack where the perpetrator instead of one computer, he uses a network of infected computers — also known as ‘‘zombies’’— in order to send massive amounts of data at the target(s) of the attack. The legitimate owners of the compromised computers (zombies) usually have no knowledge about it due to the ‘‘bots’’ software that secretly infiltrates a computer system. The network of ‘zombie’ computers is called “botnet” and can reach really huge numbers such as millions of compromised computers[26].

Cybercrimes: Computers as an Instrument

Although computers can be the target of a perpetrator, they are often used as an instrument in order to commit their illegal activities. In this category fall types of cybercrimes such as, online fraud, phishing/spear phishing, identity theft, spam, spoofing.

Online Fraud

An online fraud is the deployment of any kind of machinations through the Internet and the use of its services in order to deceive victims and make illegal profit. The most well-known online fraud is the so-called scam ‘Nigerian fraud’ or else ‘419 fraud’ after the provision of the Nigerian Criminal Code which penalizes such schemes[27]. They usually email and ask for the victims’ assistance in order to gain access to a huge amount of money by promising a large share in the end. Once the recipient responds and shows interest then they persuade him/her using social engineering techniques to pay money in advance for the preparation of certain documents ending up in the loss of hundreds and even thousands of dollars or other currencies.

[26] Susan W. Brenner, *Cybercrime, Criminal Threats from Cyberspace*, Praeger, 2010

[27] R. G. Smith, M. N. Holmes and P. Kaufmann, *Nigerian Advance fee Fraud, Trends and Issues in Criminal Justice*, AIC, 1996

Phishing/Spear Phishing

'Phishing'[28] is the act of using fake emails or websites that might seem to be as the ones of the legitimate source (eg. Bank organizations, Insurance companies, etc) in order to scam the unsuspecting victims and try to make them divulge their personal, financial and sensitive information. Usually the phishing act is performed in conjunction with a spoofed e-mail that would ask the recipient to verify their account information for security reasons. The phishing method is also referred to as 'SMiShing' when offenders use SMS (cell phone) messages to deceive the recipients, 'Vishing' when they use VOIP (voice over internet protocol) to send out the messages, or even 'Pharming' when it is used to redirect victims into fake websites[29].

Spear Phishing is called the same method as explained above but now, the perpetrators have done preparation about the potential victim's background and personal information making their attack more targeted to the victim with increased possibilities of deceiving them.

Identity theft

Identity theft can be defined as the activity of stealing an individual's personal data (identity information), that might deem necessary in order make illegal profit without the victim's knowledge (eg. open bank accounts, credit cards, get loans, etc.)[30]. Methods that would enable the identitiy theft is phishing, social engineering techniques, through breaches in computer systems security, spyware, Trojan horse viruses, search in the rubbish the so-called 'dumpster diving', etc.

Spam

Email spam, also known as "junk email", are essentially unsolicited messages being sent by email. Although such email spam messages are sent mainly for commercial reasons, they can also be used to disseminate viruses or other malware programs, to include links which lead to phishing websites, etc.

[28] The word 'phishing' is a variant of 'phreaking', which was a term used to describe one of the early forms of hacking in which hackers would make free long-distance phone calls: Anti-Phishing Working Group: Origins of the Word 'Phishing' (2008), www.antiphishing.org/word phish.html, accessed on 10/20/2018

[29] Mohamed Chawki, Ashraf Darwish, Mohammad Ayoub Khan, Sapna Tyagi, *Cybercrime, Digital Forensics and Jurisdiction*, Springer, 2015

[30] Jonathan Clough, *Principles of Cybercrime*, Cambridge University, 2010

Spoofing

Spoofing usually refers to the email-spoofing and is the creation of email messages with a fake sender address (forgery of email headers). This happens with the intention to deceive the recipient about the source of the message, make them believe it has been sent by a legitimate source and finally open, or even reply to, a solicitation. Due to the fact that the core email protocols do not have any mechanism for authentication, it is common for spam and phishing emails to use such method in order to deceive unsuspecting users.

Cybercrimes: Computers as Facilitators

Although in literature there is a tendency to categorize cybercrimes in the above two only categories (and it is not wrong), however we can assume that there is a third category in which fall all types of cybercrimes where a computer's involvement is not that crucial, or at least is of less significance, in terms of whether the illegal activity itself would stop to exist if it were not for it. To make things clear, it would be better to think of those types of cybercrimes in which computers simply were neither the target, nor the instrument to perpetrate them. This category encompasses cases in which a computer is used in the process of the perpetration of a crime; however, its involvement is so trivial that it does not rise to the level of being so integral to the commission of the crime[31]. In order to understand the difference, it is always helpful to consider some examples such as, trading sex material, exchanging child abuse material, drug talk and trade, etc.

In all the above situations, we can agree that the crime itself exists from the very beginning, however the cyberspace plays the role of the facilitator which enables the communication and the sharing of illegal information as well as the trading of illegal materials.

[31] Susan W. Brenner, *Cybercrime, Criminal Threats from Cyberspace*, Praeger, 2010

2. Legal Framework on Cybercrime and Cybersecurity in Europe

Cybercrime and cybersecurity due to their global nature, in that they almost always involve more than one country, they require a collective approach to address them. Having this in mind the EU set its goal to achieve a common understanding among the Member States, to establish cooperation between them and the operators of essential services (OES) in order to enhance security for information systems and especially for critical infrastructure. Some of the main EU law texts concerning cyber issues are mentioned bellow and is important to note that these laws (the majority of which are directives) have to pass through the national legislation procedure of each and every Member State in order to be implemented[32].

2.1 Convention on Cybercrime – Budapest Convention

A crucial step to deal with the Internet and computer crime was the adoption of the first international treaty, the *Convention on* Cybercrime which aim was to harmonize national laws, improve investigative techniques, and also increase cooperation among states [33].

In 2001 the Council of Europe adopted the most comprehensive international legislative effort to tackle cybercrime. It was signed on November 23, 2001 in Budapest by 30 countries including four non-member states of the Council of Europe, Canada, Japan, South Africa, and the United States, that took part in its development. As of 31st December 2018, there were 62 states which had ratified it and entered it into force and 4 signatory states not having ratified it.

The Convention on Cybercrime was followed by the First Additional Protocol to the Convention on Cybercrime[34]. During the talks on the text of the Convention on Cybercrime, the issues of racism and xenophobic acts turned out to be controversial matters with some countries, which valued and protected freedom of expression, having concerns about such provisions in the Convention that would violate it.

[32] Most EU acts are directives and therefore require implementation in Member State national laws. However, such procedure might entail a risk of diverting interpretations.
[33] Council of Europe, *Convention on Cybercrime***,** European Treaty Series-No.185, Budapest, 23.XI.2001
[34] Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems, ETS No. 189, available at: http://conventions.coe.int., accessed on 12/23/2018

This situation was solved with a separate protocol on 'racist and xenophobic acts in cyberspace' being signed on January 28th, 2003 and entered into force on March 1st, 2006. Concurrent with both the convention and the protocol are explanatory reports. The Convention and its Explanatory Report was adopted by the Committee of Ministers of the Council of Europe at its 109th Session (8 November 2001). [35]

The Convention on Cybercrime today is recognized as a significant regional instrument to deal with the cybercrime and is backed by various international organizations. The main goal of the treaty is to create a common policy for all participating States that would protect them against cybercrime, including the adoption of appropriate national legislation as well as fostering international cooperation. In that way nations could tackle the rising problems of the global nature of cybercrime by enabling pursuit beyond the borders of a single nation.

In chapter II, the treaty describes all the measures that States have to take at the national level. More specifically, in Section I it describes the criminal offences against the confidentiality, integrity and availability of computer data and systems, that have to be established in their domestic legislation. Some examples of them are, illegal access, illegal interception, misuse of devices, system interference, data interference, computer-related offences such as, Computer-related forgery, and Computer-related fraud, other content-related offenses, such as, child abuse and many more criminal offenses[36].

In Section II, the treaty describes the common provisions of the procedural law. That is, each Party should adopt legislative and other measures necessary to establish the powers and processes for the purpose of specific criminal investigations or proceedings. Moreover, requires States to take legislative measures to order competent authorities to expedite preservation of stored computer data, to empower competent authorities to order on their behalf, to search and seize of stored computer data, to collect or record through the application of technical means on the territory of that Party, empower authorities to intercept of content data[37.] And in Section III, the treaty describes jurisdiction that each Party might establish over offenses.

[35] Mohamed Chawki, Ashraf Darwish, Mohammad Ayoub Khan, and Sapna Tyagi, *Cybercrime, Digital Forensics and Jurisdiction*, Springer, 2015
[36] Council of Europe, *Convention on Cybercrime***,** European Treaty Series-No.185, Budapest, 23.XI.2001
[37] Council of Europe, *Convention on Cybercrime***,** European Treaty Series-No.185, Budapest, 23.XI.2001

Furthermore, in chapter III, the treaty discusses one of the most significant concepts, the international cooperation. Apart from the general principles in international cooperation, mutual assistance, extradition, and the procedures pertaining to mutual assistance requests in the absence of applicable international agreements, the treaty mentions also all the procedures that should be followed by the States, in case of mutual assistance in terms of accessing stored computer data, expedite disclosure of stored computer data, etc[38].

Law enforcement agencies face certain limitations in their capabilities, which in the absence of international agreements, prevent them from investigating the cybercrime, prosecuting and arresting the offenders. However, the provisions of the Budapest Convention are focused on mitigating such boundaries.

Finally, the Budapest Convention success seems to relate on how many the participating States are. With so many countries already on board, some being close and others in the process of harmonizing their laws to meet Cybercrime Convention standards (whether they will join or not in the end), it is obvious that this first international treaty to address cybercrime was and is a successful instrument for international harmonization.

2.2 European Union (EU) Cybersecurity Strategy[39]

In order to ensure an "open, safe and secure cyberspace" the EU had to take certain measures to protect "fundamental rights, democracy and the rule of law" that govern the cyberspace. No illegal activities nor other incidents should endanger the reliability and interoperability of the Internet. However, as the technology keeps on improving the cybercriminals employ highly sophisticated and even more complex cyber-attacks highlighting the vulnerabilities of the digital world.

For that reason, EU governments needed to specify the roles and responsibilities both for the public and the private sector who not only owns and operates a significant part of the Internet,

[38] Council of Europe, *Convention on Cybercrime***,** European Treaty Series-No.185, Budapest, 23.XI.2001
[39] European Commission, High Representative of the European Union for Foreign Affairs and Security Policy, *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, 2013

but also has a leading role in that. This realized through a proposal for a Cybersecurity[40] Strategy of the EU, that was put forward by the Commission and the High Representative of the Union for Foreign Affairs and Security Policy (High Representative).

The *principles* that govern this strategy are the following:

- *'The EU's core values apply as much in the digital as in the physical world'*, meaning that the same rules and trends (norms) that apply to the everyday life apply also to the cyberspace.
- *'Protecting fundamental rights, freedom of expression, personal data and privacy*', meaning that cybersecurity must be based on fundamental rights and EU core values and also every action taken for implementing it, such as sharing of information, etc. must be compliant with EU laws.
- *'Access for all',* meaning that it will reassure seamless and secure access to the Internet for all.
- *Democratic and efficient multi-stakeholder governance*, meaning that the Cyberspace is not governed by a central authority or third party, instead there are many needed entities which are significant to support this multi-stakeholder cyber domain.
- *'A shared responsibility to ensure security*', meaning that not only the public sector, but also the private as well as individuals need to share the responsibility and create and preserve a safe and secure cyber domain including taking any action for that.

Priorities

The cybersecurity strategy involves specific actions taken either by the EU, Member States or industry in order to safeguard the Internet and are articulated in the following five strategic priorities:

- *'Achieving cyber resilience'*

  In order to provide cyber resilience, both public authorities and the private sector must cooperate to enhance their capacities towards a well-coordinated response in emergency

[40] Cyber-security refers to a set of actions that are necessary in order to safeguard the cyber domain and more specifically, to protect and preserve the confidentiality, integrity and availability of the information, programs and data against any attack, damage or unauthorized access. Moreover, cybersecurity applies both to the public and private sector as well as to military by protecting their networks and critical information infrastructure.

situations. Moreover, to enhance national capabilities in being able to prevent, detect and address effectively any cyber security incident that might happen, the strategy advises the Member States to designate national competent authorities for Network and Information Security, to set up a Computer Emergency Response Team-CERT, and adopt a national NIS strategy and a national NIS cooperation plan. Furthermore, mechanisms for prevention, detection, mitigation and response to incidents are necessary, along with the engagement of the private sector which owns and operates the larger part of the network and information systems. Finally, raising awareness of the risks is crucial too, and the European Network and Information Security Agency (ENISA) plays a significant role towards that direction through workshops, reports, promoting public-private partnerships, etc.

- *'Drastically reducing cybercrime'*

  High profiles cybercriminals take advantage of the cutting-edge technology and engage in sophisticated and complex attacks increasing the cybercrime rates globally. In order to deal with these issues a strong and strict legislation is needed by the Member States as well as cybercrime units with capabilities and operational tools to tackle cybercrimes. Furthermore, towards the same direction, law enforcement and judicial authorities, public and private stakeholders from the EU need to cooperate and coordinate their actions.

- *'Developing cyberdefense policy and capabilities related to the Common Security and Defense Policy (CSDP)'*

  Cybersecurity also involve the advancement of the EU cyber defense capabilities by creating a cyberdefense policy to protect networks and information systems within CSDP scope. Also, by offering Cyber Defense Training & Exercise Opportunities for the military staff, promoting dialogue and coordination between civilian and military actors and with international partners, including NATO.

- *'Develop the industrial and technological resources for cybersecurity'*

  It is crucial to ensure that both information system components (hardware, software) are secure and guarantee the protection of personal data. For that reason, a promotion of a single market for cybersecurity products is enhancing cybersecurity.

- *'Establish a coherent international cyberspace policy for the European Union and promote core EU values'*

By establishing norms of behavior, implementing rules and laws that apply to cyberspace, EU is creating a free and open Internet in which international partners and organizations will work together in an effort to build cybersecurity capacity.

Roles and Responsibilities

As mentioned above, cyber issues need a global approach because almost always more than one country is involved. Thus, to build strong relationships and cooperation among all players such as, law enforcement agencies, NIS competent authorities, CERTs and industry, is vital for strengthening cybersecurity. However, the EU has the role of coordinating this endeavor and guiding the Member States to establish communication channels with each other, share information and expertise in order to prevent and tackle cybercrimes.

At a national level, member states should create the appropriate structures and enhance their capabilities in cyber resilience, cybercrime and defense in order to meet the requirements of this Cybersecurity Strategy.

At the EU level, in order to promote cybersecurity as a way of addressing cyber issues, the EU include agencies such as the ENISA, Europol/EC3 and the EDA (European Defense Agency) which are focusing on NIS, law enforcement and defense sector respectively. These agencies along with the CERT-EU would support and create a safe digital environment for everyone.

At an international level, the Commission, the High Representative along with member states and international organizations such as Council of Europe, OECD, OSCE, NATO and UN, work to promote coordinated and innovative action plans, while at the same time they provide guidance and data analysis to member states.

2.3 The Directive on security of network and information systems (NIS Directive)

The Directive (EU) 2016/1148 on Security of Network and Information Systems (NIS Directive)[41] with the goal of achieving a high common level of network and information systems security across the European Union, basically focuses on strengthening the resilience for Operators of "essential services" (OESs) as well as for Digital Service Providers (DSPs).

Although the NIS Directive was adopted by the European Parliament on July 6th, 2016 and entered into force a month later, it was not until May 2018 that the Member States transposed the Directive into their national laws. However, they still need to identify those 'operators of essential services' (OESs), which also need to be compliant with the NIS directive, by November 9th, 2018. According to this Directive, OESs could be critical infrastructures that provide energy, water, health care, transport, banking and financial, and digital infrastructure (ISPs, DNS providers, etc.), whereas DSPs could be search engines, cloud computing services, and online marketplaces.

Moreover, the NIS Directive provides all the necessary steps and legal measures that Member States should follow and implement in order to enhance their common level of cybersecurity. More specifically, Member States should:

- Have a national strategy on the security of network and information systems along with explicit strategic goals and policy actions (ENISA might be requested to assist).
- Be well-prepared by introducing a national Computer Security Incident Response Team (CSIRT), also known as computer emergency response teams (CERTs) and a competent national NIS authority and build a network among them for a more effective operational cooperation.
- Contribute in setting up a network consisting of single points of contact, in order to support and facilitate strategic cooperation and the exchange of information.

[41] The European Parliament and The Council of the European Union, *Concerning measures for a high common level of Security of Network and Information Systems across the Union*, Official Journal of the European Union, 6 July 2016

- Promote a cooperation not only between the public and private sectors, but also between operators of essential services and digital service providers to ensure the security of network and information systems.
- Safeguard their ‘essential State functions’, in particular to safeguard national security by protecting State’s critical information, and to maintain law and order by allowing the investigation, detection and prosecution of criminal offences.
- Businesses in these sectors that are identified by the Member States as operators of essential services will have to take appropriate security measures and to notify serious incidents to the relevant national authority. Also key digital service providers (search engines, cloud computing services and online marketplaces) will have to comply with the security and notification requirements under the new Directive.

In terms of cooperation:

- At a National level, the CSIRTs, competent NIS authorities and single points of contact should exchange information upon incident occurrence.
- At the EU level, a Cooperation Group is established which is composed of representatives of the Member States, the Commission and ENISA in order to fulfill the aim and scope of the NIS Directive. Since 9 August 2018, and every year thereafter, the single point of contact shall submit a summary report to the Cooperation Group on the notifications received and every two years (after February 9th, 2018) the Cooperation Group shall establish a work program in respect of actions to be undertaken to implement its objectives and tasks, in line with the objectives of NIS Directive.
- At an international level, the EU as long as data are protected adequately, may conclude international agreements with third countries or international organizations, allowing and organizing their participation in certain activities of the Cooperation Group.

Furthermore, as the NIS Directive applies to both the Operators of Essential Services (OESs) and the Digital Service Providers (DSPs) that are established in the EU, the laters in order to be compliant are required to:

- Take ‘appropriate and proportionate technical’ and organizational measures to handle the risks posed to the security of network and information systems;

- Take appropriate measures to hinder and minimize the impact of incidents affecting the security of the network and information systems to ensure service continuity.
- Inform the competent authority or the CSIRT of incidents having an important impact on the continuity of their essential services without undue delay.

More specifically, the DSPs to ensure a level of security of network and information systems appropriate to the risk posed, should take into account the following:

- 'The security of systems and facilities;
- Incident handling;
- Business continuity management;
- Monitoring, auditing and testing;
- Compliance with international standards'.

Finally, the consequences for non-compliance to NIS Directive requirements are based on financial penalties and are to be set by each Member State which will take the necessary measures to ensure that they are implemented[42].

2.4 The EU General Data Protection Regulation (GDPR)

In April 2016, the European Union adopted a more collective and strict approach in order to address the issue of the privacy and the processing of personal data or else, any information relating to an identified or identifiable natural person ("data subject"). This approach realized through the European Parliament and the Council which they introduced the General Data Protection Regulation (GDPR)[43] a law that replaced the EU Directive 95/46/EC. Unlike the 1995 Directive, which had to be passed through each national legislation in order to be implemented, the GDPR regulation in a standardized way applies automatically over all 28 EU member states and supersedes all pre-existing national data protection laws.

[42] Official Journal of the European Union, *Directive (EU) 2016/1148 of the European Parliament and of the Council*, 6 July 2016
[43] Official Journal of the European Union, *Regulation (EU) 2016/679 of the European Parliament and of the Council*, 27 April 2016

The European Union (EU) with this new regulation (GDPR) that came into force on May 25th, 2018 marked a new era in data privacy by setting stricter rules on controlling and processing of personal data. This protection of personal data within the EU is a fundamental right, which organizations not only must respect, but also are accountable for that through a number of obligations and responsibilities. Towards the same direction, the EU introduced new principles and gave certain rights to EU residents that would enable them to take control over their own data.

Some key definitions for a better understanding of the GDPR are the following[44]:

- Personal data, is "any information that is relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person". In other words, any information that could identify an individual, even if it does not contain his/her name, is deemed as personal data.
- Processing of personal data, is "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, storage, alteration, use, disclosure, dissemination or otherwise making available, erasure or destruction, etc."
- Controller, is the entity that "determines the purposes and means of the processing of personal data" where the "purposes and means of such processing are determined by Union or Member State law",
- Processor is the entity that "processes personal data on behalf of the controller". Controllers are responsible for ensuring that their processors provide "sufficient guarantees to implement appropriate technical and organizational measures in such a manner that processing will meet the requirements" of the GDPR.

According to article 3 of th Regulation, the GDPR applies to **controllers** and **processors** in the context of their activities concerning the processing of personal data, whether the latter takes place in the Union or not. Furthermore, the GDPR also applies to the processing of personal data

[44] Ibid. *Regulation (EU) 2016/679,* April 2016

by a controller not established in the Union but the data subject is within the EU and under the EU Law.

The GDPR imposes the following general principles[45] for the processing of personal data:

- Lawfulness, fairness, and transparency. Organizations must make use of lawful, fair, and transparent ways of processing the personal data.
- Purpose limitation. Organizations must collect personal information for legitimate and specific purposes and process it within these limitations.
- Data minimization. Information should be limited only to what is necessary for the process purposes.
- Accuracy. Organizations must take "every reasonable step" to ensure accurate and updated personal data, otherwise erase or rectify it without delay.
- Storage limitation. Personal data must be stored for no longer period than is needed to achieve the stated purposes.
- Integrity and confidentiality. Personal data must be protected against unauthorized access, loss, or destruction via "appropriate technical or organizational measures."

More specifically, the processing of personal data is "lawful" under the following conditions[46]:

- The data subject has provided consent to processing the personal data, via a written declaration which must be in a "clearly distinguishable" form, intelligible, and easily accessible. In the case of children this consent is given by the holder of parental responsibility and in all above cases can be revoked at any time.
- The person is party of a contract for which processing is necessary.
- Processing is necessary for the controller of the data to comply with a legal obligation.
- Processing is necessary to protect "the vital interests of the data subject".
- When performing a task in the public interest or under the data controller's official authority.
- There are legitimate interests of the data controller that comply with the fundamental rights of the data subject.

[45] Article 5, Ibid. *Regulation (EU) 2016/679,* April 2016
[46] Article 6, 7, ibid *Regulation (EU) 2016/679,* April 2016

Moreover, the processing of personal data apart from lawful need to be always "fair". According to this principle, it is meant that those who handle personal data they should have obtained them through a legitimate process and further process them in justifiable ways or how a data subject would reasonably expect under normal, legal and logical conditions.

Furthermore, the processing of personal data must be "transparent". That is, upon request, any company must clearly and intelligibly provide the data subject with information, that would include among others:

- The contact information for the data controller and, if applicable, its data protection officer.
- The purposes for the processing and legal basis of it.
- The recipients or categories of recipients of the personal data.
- The length of time the personal data will be stored.
- The existence of the right to request access to as well as erasure of personal data.
- The existence of the right to withdraw consent[47].

What is more, is that GDPR goes on to impose certain restrictions on the processing of "special categories" of personal information, which defines as data that "reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation"[48]. Such data require the individual's explicit consent for their processing, or if an exception applies.

Finally, the GDPR provides a number of rights to EU residents, that is:

- The 'right to be informed'. That is, the individuals have the right to be notified about the collection and use of their personal information. As we have mentioned above, the data subject can learn the contact information for the data controller and, if applicable, its data protection officer, purposes for the processing, recipients or categories of recipients of the personal data, retention time of data, existence of right to withdraw consent, existence of

[47] Article 13, 14, ibid *Regulation (EU) 2016/679,* April 2016
[48] Article 9, ibid *Regulation (EU) 2016/679,* April 2016

right to request access to as well as erasure of personal data, right to lodge a complaint, the source of the data, etc.

- The right of access. Individuals have the right to access their personal data and they can request it either verbally or in written form. obtain a copy of their personal data as well as other supplementary information. This enables individuals to understand how and why their data are used and if it is done lawfully.
- The right to rectification. Individuals who have inaccurate personal data can make a request for rectification verbally or in written form and this right is closely linked to the controller's obligations under the accuracy principle of the GDPR.
- The right to erasure. Individuals have the right to have personal information deleted. This is also known as the 'right to be forgotten'. The right is not absolute and only applies in certain circumstances, specifically, when personal data is no longer necessary for the purpose which they were originally collected or processed, data subject has withdrawn the consent, data subject objects and the controller fails to demonstrate "compelling legitimate grounds for the processing, personal data was processed unlawfully, personal data was collected from a child under 16, etc.
- The right to restrict processing. Individuals have the right to request the restriction or suppression of their personal data. This means that in lieu of requesting the erasure of the data, an individual can limit the way that an organization uses their data, due to the content of the information reasons or how they have been processed.
- The right to data portability. 'Allows individuals to obtain and reuse their personal data for their own purposes in different services, and also to request that a controller transmits this data directly to another controller (for better processing, etc.)'. This includes the move, copy or transfer of personal data easily and in a safe and secure way, without affecting its usability.
- The right to object. Individuals have the right to refuse the processing of their personal data (especially for marketing reasons). This effectively allows individuals to ask to stop processing their personal data when there is no other legitimate reason.
- Rights in relation to automated decision making and profiling. 'An automated individual decision-making, that is making a decision solely by automated means without any human involvement, and profiling, which is an automated processing of personal data to

evaluate certain things about an individual', can be restricted when the data subject requests that decision-making not to be solely based on automated decisions.

Finally, one significant addition of the GDPR is that, apart from having controllers and processors to "implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk" such as, pseudonymization and encryption of personal data, safeguarding the confidentiality, integrity, availability and resilience of processing systems and services, timely restoration of the availability of personal data, etc., the companies are forced to fulfil the data breach notification requirement. For that reason, in case a company experiences a breach of personal data, the controller must without undue delay, and, if feasible, within seventy-two hours, notify government regulators.

3. Incident Response

In todays wired world, from individual users to organizations, all are reliant upon the well-functioning of the information systems. However, the growing sophistication of the cyber threats pose major challenges not only to the security of these systems, and to economy, but also to national security. Security incidents caused by criminals, non-state actors and state actors who engage in such activity, target these information systems and bring about damages, malfunctions, and financial losses. Thus, it is more than necessary these incidents to be addressed accordingly in order to protect and provide continuity to organizations and critical infrastructure. Towards this effort and due to the fact that it is almost impossible to eliminate the threats or even to prevent incidents from happening, it is critical to develop the capacity to respond fast and effectively in the case of a cyber security incident.

Response capacity usually involves an incident response team and an incident response plan that the aforementioned team would implement throughout the response process. The National Institute of Standards and Technology (NIST)[49] value the importance of having incident response capability because in that way, it helps to respond to incidents in a coordinated and structured manner (i.e. following a consistent incident handling methodology). By doing so, organizations not only have better chances to appropriately act and handle the occurrence of an incidence, but also are able to minimize its effects. For example, in a data breach case by efficiently handling the incident, an organization could minimize not only the loss or theft of information and any system processes disruptions, but also the impact on the organization itself. Moreover, the benefits can be multiplied if we take into consideration the lessons learned from each and every incident that could help improve the whole processes, build stronger protection against future attacks, and also be better prepared to respond to them[50].

[49] Cichonski, P., Millar, T., Grance, T., and Scarfone, K., *Computer Security Incident Handling Guide. Recommendations of the National Institute of Standards and Technology*. NIST Special Publication 800-61 Rev.2, 2012

[50] Van der Kleij R., Kleinhuis G. and Young H., *Computer Security Incident Response Team Effectiveness: A Needs Assessment*, Front. Psychol. 8:2179, 2017

3.1 What Is Incident in Cyber Security?

The term ‘cyber security incident’ has been a troublesome in terms of how it could be defined and more specifically, whether its meaning would be limited to an event that would bring about data breach, loss of information, and/or damage to an information system or it would be broader and include any threat to all the above.

In fact, when we talk about an incident, we automatically mean something that has negative implications if not bad, implies impact and harm or at least, intent to harm. Thus, an incident could be any occurrence that threatens the confidentiality, integrity, or availability of an information system, or the information the system processes, stores, or transmits, jeopardize the normal operations of information systems, and/or the networks[51].

According to the Computer Security Resource Center (CSRC) of the National Institute of Standards and Technology (NIST) an incident is defined as “violation or threat of violation of computer security policies, acceptable use policies, or standard security practices”, whereas an event is “any observable occurrence in a system or network” [52]. Of course, this definition requires an organization to have established a security policy, which as it is commonly known can vary among organizations.

An example of an incident could be an attacker who performs distributed denial-of-service attack (DDoS attack) usually by commanding a botnet(s) or set(s) of hundreds of thousands — or even millions remote-controlled and infected computers (bots), to send high volumes of connection requests to a web server, causing it to crash. Other examples of cyber security incidents might include attacks such as malware ones (malicious software-code like worms and viruses), theft of information, unauthorized or unlawful intrusions-access into computer systems, embezzlement, an insider’s inappropriate use of a computer system against the organization’s rules and policies.

According to the National Cyber Security Center (NCSC) of the UK Government Communications Headquarters (GCHQ), a cyber incident is defined “as a breach of a system's

[51] Leighton R. Johnson III, Com*puter Incident Response and ForensicsTeam Management*, Elsevier Inc., 2014
[52] Cichonski, P., Millar, T., Grance, T., and Scarfone, K., *Computer Security Incident Handling Guide. Recommendations of the National Institute of Standards and Technology*. NIST Special Publication 800-61 Rev.2, 2012.

security policy in order to affect its integrity or availability and/or the unauthorized access or attempted access to a system or systems"[53]. The NCSC notes some common types of activity, that could be recognized as being breaches of a typical security policy, which are:

- 'Attempts to gain unauthorized access to a system and/or to data.
- Unauthorized use of systems for the processing or storing of data.
- Unauthorized changes to a systems firmware, software or hardware.
- Malicious disruption and/or denial of service'[54].

Moreover, the NCSC assumes as a significant cyber security incident one that may have an impact on national security or economic wellbeing or even the potential to cause a serious impact on an organization's operation.

Furthermore, another approach on how to define cyber security incident is by analyzing its characteristics. Although there is no single accepted definition, it is vital to every organization to identify what constitutes a cyber security incident, so that its personnel being responsible to deal with them would be aware of what would consider as such and act accordingly. Generally, such incidents would have the following three characteristics[55]:

- Intent to cause damage
- Performed by a individual
- Involved a computing resource

The first characteristic means that an incident must intent to cause harm even if there are no immediate consequences, such as malicious activity engaging in the performance of vulnerability scan to information systems with the obvious intention to do harm at a later stage. The second characteristic, requires a person's involvement, thus excluding events such as random system failures or natural disasters, etc. For example, a disruption of normal operations due to voltage deficiency could not be an incident, unless a person takes advantage of it and engage in malicious activity. Lastly, a cyber security incident, as the term implies, could not exist without

[53] National Cyber Security Center of UK GCHQ, *What Is a Cyber Incident*, September 19th, 2016, available at https://www.ncsc.gov.uk/articles/what-cyber-incident, accessed on 12/21/2018
[54] National Cyber Security Center of UK GCHQ, *What Is a Cyber Incident*, September 19th, 2016, available at https://www.ncsc.gov.uk/articles/what-cyber-incident, accessed on 12/21/2018
[55] Jason T. Luttgens, Matthew Pepe, *Incident Response & Computer Forensics*, 3rd Edition, Mc Graw Hill, 2014

the involvement of a computing resource. This broad term of computing resources includes any device connected to the internet such as phones, cameras, smart TVs, GPS devices, and many others[56].

3.2 What is Incident Response?

Incident response over the past decade or so, has changed significantly and this is true due to the continuous developments in technology that, in turn, provided the appropriate tools and useful knowledge to bad actors in order to deploy more sophisticated attacks. In fact, nowadays attackers have nothing less, in terms of capabilities, than an IT professional does. On the contrary, they patiently improve their tactics, perform reconnaissance by monitoring the networks and have an advantage to deploy attacks in a time and way they choose. However, as the attack techniques evolve, so the countermeasures and approaches do and today an incident responder need to have the right tools, very good knowledge and appropriate procedures to address such occurrences.

Many organizations in order to face these challenges that the information security attacks and data breaches pose to them, they respond by developing an incident response plan and creating a security incident response team. The primary goal of a security incident response approach is to ameliorate the effects of an incident along with leading the organization to an acceptable security posture being able to return to normal operations as quickly as possible[57].

A Security Incident Response is a "specialized form of incident management" that could go from the 'monitoring and detection of security events on a computer or computer network', to resolution and execution of proper responses to those events[58]. Incident response may include activities such as:

- Confirm of incident occurrence, along with quick detection and containment.
- Determine and document the scope of the incident

[56] Jason T. Luttgens, Matthew Pepe, *Incident Response & Computer Forensics*, 3rd Edition, Mc Graw Hill, 2014
[57] George Grispos, William Bradley Glisson and Tim Storer, *Rethinking Security Incident Response: The Integration of Agile Principles*, 2014
[58] Leighton R. Johnson III, Com*puter Incident Response and ForensicsTeam Management*, Elsevier Inc., 2014

- Prevent a disjointed, non-cohesive response
- Determine and promote facts and actual information
- Reduce disruptions of network processes, damages and losses to the attacked organization
- Recover normal operations
- Control the public perception of the incident
- Initiate or facilitate legal (criminal or civil) actions against the perpetrators
- Report to and educate senior management
- Improve security level of a infected entity against future incidents[59]

However, all the above-mentioned activities that are part of the incident response cannot be the same for each and every incident. That means that the incident response provides flexibility and varies depending on its goals, which in turn they depend on the nature of the incident (how was performed, what targeted, etc.), the senior management guidelines, the degree of the impact on the organization and its network, etc.

Finally, if one wonders why an incident response would be necessary for an organization, then the answer could be simple. And that is because, having an incident response plan and an appropriate incident response team, not only can address the ever evolving threats that affect the private and the public sector as wells as the individuals, but also, as stated in the new GDPR regulation and more specifically in the principles in the article 5 (EU 2016/679, April 2016), an organization should take all necessary measures to be protected from data breaches. That is actually a requirement that all organizations are obliged to meet across Europe.

3.3 The Incident Response Life Cycle

With an ever-growing number of cyber security incidents now happening more often than in the past, even large organizations find it difficult to keep pace with these challenges and face them, usually resulting in significant impact. However, what is needed is nothing more than to build an effective and efficient cyber security incident response capacity, able to deal with cyber security incidents from simple ones to the most sophisticated. That capacity would enable organizations

[59] Jason T. Luttgens, Matthew Pepe, *Incident Response & Computer Forensics*, 3rd Edition, Mc Graw Hill, 2014

of any size to be well-prepared, respond effectively and build upon lessons learned for future attacks.

There are quite a few approaches in terms of how to respond to a cyber security incident, which although they differ in the number of stages followed throughout the incident response process, however they all have a common denominator in terms of what elements they engage-include and in what sequence. In our approach, we adopt a four-stage one, that is the Preparation stage, Detection, Identification & Analysis, Containment, Eradication & Recovery, and lastly the Follow-up Actions one[60].

3.3.1 Preparation Stage

Being properly prepared is one of the most important actions in order to deal with a cyber security incident. However, there are many cases in which organizations skip this stage and go directly to detection & analysis and then containment, eradication, etc., due to support and resources deficiencies or/and lack of cybersecurity awareness, having almost always devastating results.

In this crucial first stage all actions that are taken will then help the organization to reduce the impact of the attack, recover its ICT systems faster, maintain its credibility in the market and, of course, save money in the long run. The most significant steps that have to be followed are first to create an incident response plan and then to establish an incident response team.

3.3.1.1 Incident Response Plan

In order to get prepared for the "inevitable cyber incident"[61] an organization needs to be ready not only to react after the incident occurs, but also needs to respond effectively and efficiently.

[60] Additional information on how to respond to cyber security incidents can be found at: First Responder's Guide – Policy and Principles from the UK's Center for the Protection of National infrastructure (CPNI), GovCertUK incident response guidelines, The Good Practice Guide for Incident Management from the European Network and Information Security Agency (ENISA), NIST Computer Security Handling Guide (Special Publication 800-61), Responding to targeted cyberattacks from ISACA (collaborating with E&Y), and many other.

[61] Deloitte, *Incident Response Brochure*, Deloitte LLP and affiliated entities, reached on December 28th, 2018 available at: https://www2.deloitte.com/content/dam/Deloitte/ca/Documents/risk/ca-en-deloitte-crisis-incident-response.pdf, accessed on 12/26/2018

That means to “plan proactively”, defend the information systems and other assets, try to get ahead of the evolving threats, and finally, return to prior the attack condition.

In order to do so, it is imperative to know how to handle certain situations ahead of time in lieu of encountering them when they occur. And the only way to know in advance is, to have a well written plan which will be kept updated regularly to integrate latest developments, new processes, etc. and, of course, one that will define all steps and specific operation procedures to be followed in case of an incident. In that way, it would help to limit the damage, reduce costs for the organization as well as the recovery time.

The key elements of an incident response plan are, for example, what needs to be protected, who is responsible in case of an incident, what incident means for the organization and what are possible categories of incidents, who is included and what are the roles for each one in the response team, and what are the external resources, such as experts that would support[62].

As for the content of the incident response plan, it should, first of all, include the identification of all organization’s assets as well as the potential threats. That is really crucial because in case of an incident, what we will ask first is, what was attacked and what is at risk.

These questions, though, create other considerations that we have to pay attention to, such as which assets are vital, secondary, or of minor importance. That means, the response plan apart from the identification, requires documentation and categorization of the assets so that during the incident management process, we will be able to make quick decisions on what to protect first, which of those are vital-needed for the business continuity and also minimize the total damage to the organization[63].

Some of these assets that could be characterized as vital are the following: management, organization, intellectual property (technical knowledge-expertise), personnel, data-information, processes, applications, infrastructure (systems and/ or network connections), financial capital (bank accounts).

[62] Cyber Security Coalition, *Cyber Security: Incident Management Guide*, Cyber Security Center, Belgium
[63] Cyber Security Coalition, *Cyber Security: Incident Management Guide*, Cyber Security Center, Belgium

Finally, the way to identify, document and categorize is, first, to determine which are the core activities that enable the organization to achieve its goals and moreover, which ICT systems (hardware, software, data) and network connections are involved in these procedures, their physical location and how the flow of information is realized with third parties. Secondly, to determine the sequence of the above procedures in which they will be handled in case of an incident, that is prioritize the vital procedures to be addressed first. Thirdly, to document all the procedures of the ICT systems such as, the Network Scheme (network architecture with internal network segmentation and external gateways), Equipment and Services inventory (servers and network components and what services are running), Accounts and Access lists from those who are authorized to access[64].

What is of equal importance is, to identify the vulnerabilities and potential threats of the organization. A vulnerability could be defined as a weak spot or lack of capacity to withstand to a hostile activity that could or might be exploited by a security threat to breach security and damage the organization. The existence of unaddressed vulnerabilities creates risks which in turn implies minor or major impacts in the organization.

Vulnerabilities can be identified via a vulnerability assessment and analysis that involve the use of vulnerability scanning tools (i.e. Microsoft Baseline Security Analyzer, Wireshark, Nmap, etc.), via audit reports, the NIST vulnerability database, etc. Similarly, the threats and risks can be identified by performing a risk and threat assessment[65]. Some possible vulnerabilities could be associated with patrons that access the staff network, not secured servers (exposed to the Internet), not updated OS, no physical security, no backed up data, weak passwords, no security policies, no cybersecurity awareness means no understanding of social engineering risks, etc.

3.3.1.2 Incident Response Team

Should an incident occur, an organization must have a stand by and ready to act response team. This team should be composed by personnel with a number of skills and ideally have more than

[64] Cyber Security Coalition, *Cyber Security: Incident Management Guide*, Cyber Security Center, Belgium
[65] For more information on Risk and Threat Assessment, read Mark Ryan M. Talabis and Jason L. Martin, *Information Security Risk Assessment Toolkit*, Syngress Elsevier, 2013, or/and online at Isaca.org, https://www.isaca.org/Journal/archives/2010/Volume-1/Pages/Performing-a-Security-Risk-Assessment1.aspx

one person in each skill area. In that way, not only would ensure that more than one individual would be available at any time, but also it could help prevent collusion[66].

However, what is really important, is to assign responsibilities and roles to each person of the team with the right skills. Thus, while creating the cyber security incident response team we need to assign roles, such as:

- Incident Response Manager, that will manage the whole incident from its detection to the end (until it is contained and remediated).
- Management, that will have to make decisions for the organization after assessing the impact (how to proceed, when to stop and set from the start, file a report/complaint, etc)
- Technical ICT staff, that will provide the knowledge on the networks (firewall, proxies, routers, etc.). Will analyze and control the ICT systems (i.e. block or restrict the data flow, control software, hardware-workstations-servers). And will provide with forensic expertise to gather and maintain the collected evidence to be accepted in the court of law.
- Legal Advisor/Lawyer, that will provide with legal advice, asses the incident and assure the incident response activities would be within organization's policies, laws and regulations' framework.
- Security Officer, that will take care of the physical access, physical protection of the ICT systems and networks.
- Communication-PR, that will handle the information of involved stakeholders, etc.
- Crisis Manager, that will manage the crisis should this happen[67].

However, the aforementioned roles and responsibilities are not exclusive, and they always depend on the number of people that compose the incident response team, which number in turn depends on the size of the organization as well as the services that provides. For example, in small organizations, an Incident Response Manager and ICT staff or even just a First Responder might make up the whole response team. In such a case, external experts, especially forensic expert, legal advisor, and others with specific skills that the organization cannon accommodate,

[66] Pete Finnigan, *Oracle Incident Response and Forensics: Preparing for and Responding to Data Breaches*, Apress, 2018
[67] Cyber Security Coalition, *Cyber Security: Incident Management Guide*, Cyber Security Center, Belgium

might assist during the incident response process[68]. In a nutshell, the larger the organization, the bigger the response team and the more roles to be assigned to them.

3.3.2 Detection, Identification & Analysis

The next step in the process of handling a cyber security incident effectively is to detect, identify and then analyze the cyber security incidents. This step is also crucial for the whole process and challenging at the same time, because in this step is confirmed whether an incident occurred or not and in which type/category belongs to. In other words, which of those incidents would threaten and also might have an adverse impact on the organization's operations, so that it would have to respond accordingly.

However, in order to be able to detect and identify cyber security incidents, we need to have a clue about what would most likely attack the organization and perhaps know somehow what the consequences would be[69]. In that way, the organization can make decisions on how to proceed and response team act accordingly.

Moreover, the detection of some incidents might be easy due to their nature, but others could go for a long time in a stealthy mode doing reconnaissance and/or waiting the right time to hit the systems and networks and might be undetectable or difficult to detect. This might be the case of malware attacks and specifically Trojans who steal credentials and other data while they remain undetected for a long time.

In order to detect and identify an incident there are many ways, including but not limited to, monitoring systems, such as Antivirus software (although not sufficient against advanced attacks, they can still prevent widely recognized threats), Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS) with Data Loss Prevention (DLP) systems, and Log Analyzers[70]. Moreover, detection and identification, as we have mentioned above, could also be done through regular Audits, and Threat Assessment, and Investigations by specialized personnel (forensic experts) as well.

[68] Cyber Security Coalition, *Cyber Security: Incident Management Guide*, Cyber Security Center, Belgium
[69] Cyber Security Coalition, *Cyber Security: Incident Management Guide*, Cyber Security Center, Belgium
[70] Jason Crasey and Ian Glover, *Cyber Security Incident Response Guide*, CREST, 2013

Furthermore, the personnel and other legitimate users could also be potential detectors in case they notice something suspicious or abnormal and thus, they report it to the IT staff center/department or to the incident response team directly. Finally, apart from the aforementioned measures that should be taken from a network or a host viewpoint in the organization, it is also important to take into account the endpoint protection, that is to ensure that any device that would be connected to the organization's network, such as laptops, tablets, smartphones, etc., they would be sufficiently protected because they could be a potential entry point for cybercriminals[71].

Lastly, the final step that needs to be taken while putting into practical use the set of proactive capabilities of the organization is the analysis of the incident(s) that occurred. Analyzing involves the gathering of information as well as and the prioritization of what happened and how to respond to. It also comprises the whole forensic investigation process and analysis of the data in order to determine the extent and impact of the incident[72]. Among the elements that should be analyzed are, (but not limited to) event logs from IDS and IPS, network data (cloud service providers), date/time of the events, internal or external Internet Protocol (IP) addresses, source and destination Ports, Domain and File (exe, dll, etc.), System, such as hardware vendor, OS, applications, purpose[73].

3.3.3 Containment, Eradication & Recovery

Once the incident is detected and identified, then a set of actions has to be taken in order to regain control of the ICT systems and networks and return back to normal operations. That whole process will require to contain the incident, then to eradicate it, and finally to recover from it.

Containing a cyber security incident means that we are restricting the damage while we are putting an end to the attack. This procedure is really crucial because at this stage we need both to

[71] Cyber Security Coalition, *Cyber Security: Incident Management Guide*, Cyber Security Center, Belgium
[72] Deloitte, *Incident Response Brochure*, Deloitte LLP and affiliated entities, reached on December 28th, 2018 available at: https://www2.deloitte.com/content/dam/Deloitte/ca/Documents/risk/ca-en-deloitte-crisis-incident-response.pdf
[73] Jason Crasey and Ian Glover, *Cyber Security Incident Response Guide*, CREST, 2013

hinder the damage from spreading to other devices and networks within our organization and beyond, and at the same time keep the systems running.

However, the goal of containment is not always to recover right away, but sometimes it is vital to take some time to analyze first the incident, preserve and gather the evidence during the investigation process for potential future use in the court of law and plan longer term remediation. In that way, the incident response team instead of shutting down the systems and disconnect the networks in order to restore operations faster, they might monitor the malicious activity so as to better analyze and gather as much evidence as possible that could lead to the perpetrators. It is also possible, as mentioned earlier, that external assistance from experts on the field might be of need to assist towards that direction, especially in highly sophisticated attacks.

Some of the ways in which a cyber security incident could be contained, are:

- 'Blocking (and logging) of unauthorized access
- Blocking malware sources (eg email addresses and websites)
- Closing particular ports and mail servers
- Isolating systems
- Changing system administrator passwords where compromise is suspected
- Firewall filtering
- Relocating website home pages'[74]

The next step at this stage is eradication, in which, actually, the response team eliminates the causes of the incident and any compromised component of the systems (malware, breached user accounts, etc.) and it does it as fast and cautiously as possible, in order to leave no chances to attackers to respond again. Thus, after the incident's containment, eradication hits the root causes of the incident and also helps to identify and alleviate any vulnerabilities that were exploited, by performing actions, such as deleting malware, disabling breached accounts or changing its passwords, updating signatures, identifying security gaps and fixing them, raising cybersecurity awareness among employees to avoid such events in the future, waiting and checking whether there was any response from the attacker to eradication actions, etc[75].

[74] Jason Crasey and Ian Glover, *Cyber Security Incident Response Guide*, CREST, 2013
[75] Cyber Security Coalition, *Cyber Security: Incident Management Guide*, Cyber Security Center, Belgium

The final step, as part of the responsive capabilities against a cyber security incident is to recover, that is to restore systems to normal operations and remediate vulnerabilities to deter similar future attacks. Recovering from a cyber security incident involves actions, such as:

- 'Rebuilding infected systems from scratch
- Replacing compromised files with clean versions
- Removing temporary constraints imposed during the containment period
- Resetting passwords on compromised accounts
- Installing patches, changing passwords and tightening network perimeter security (firewalls)
- Testing systems thoroughly – including security controls
- Confirming the integrity of business systems and controls'[76].

Once all systems have been recovered and controls have been tested, stakeholders should also then be informed about what happened and any other significant findings.

3.3.4 Post-Incident Activity - Follow-Up Actions

When the incident response process reaches to its closure, each incident should be reviewed via a "lessons-learned" process. The follow-up process of the incident response is really essential to continuously improve the whole incident response procedure and it should take place right after the incident response completion, in order to identify any issue areas and process adjustments[77].

The lessons-learned could be reviewed, documented and then included at the early stage of the incidence response, and specifically during the preparation stage, for training reasons and also to ensure that the latest updates and changes are incorporated to the incident response plan and associated procedures. The new knowledge that would be obtained, it would help tackle similar incidents in the future that might necessitate the same handling procedures, or even address a smaller incident that could be part of a future bigger one. It is in fact, an on-going process through which we can collaborate and learn from previous mistakes, incidents and experiences,

[76] Jason Crasey and Ian Glover, *Cyber Security Incident Response Guide*, CREST, 2013
[77] CyberDefences, Inc., *Guide To Developing An Incident Response Program*, Version 2018 0406, 2018

build strong knowledge based on ideas and expertise sharing and thus, be better prepared for anything that may come[78].

Furthermore, apart from documenting and resolving the incident, it is also crucial to report the incident to relevant stakeholders (both internal and external), and of course, to the organization's top management, where a documented report would contribute on what happened, what actions were taken to recover, what did well/wrong, what is needed and how we could improve it for future incidents, etc.

What is also important to note, is that when an incident occurs, organizations and, of course, government departments have a responsibility to report it to particular authorities depending on the case and extend. Such authorities, include but not limited to:

- Law enforcement agencies
- Computer Emergency Response Teams (CERTs)
- Specialized international bodies, such as NIST or ENISA
- Collaborative partners (see Part 8 The Way Forward for more details)

This greater and broader collaboration could bring results that could benefit the victims by stopping and deterring future criminal cyber operations, reducing the impact of the incidents, and incriminating and prosecuting the offenders[79].

[78] Jason Crasey and Ian Glover, *Cyber Security Incident Response Guide*, CREST, 2013
[79] Jason Crasey and Ian Glover, *Cyber Security Incident Response Guide*, CREST, 2013

4. Investigating Cybercrime. What The Challenges Are?

In the previous chapter we described and analyzed the incident response process that involves an incident response plan and an incidence response team ready to implement it. However, these cyber security incidents (cyber-attacks, data breaches, etc.) usually have legal implications. That means an investigation by law enforcement agencies might follow in order to examine all the digital evidence (and not only) and try to identify the attacker(s) behind the cyber security incident.

This chapter focuses on investigating cybercrime[80] committed against any organization or even individual by describing the goals investigators want to achieve, the steps they need to follow, and the challenges they face or will face while investigating such crimes. It then briefly discusses the different forensic methods and tools investigators use when investigating cybercrimes.

Cybercrimes as mentioned in chapter 2, are generally crimes or else, any illegal activities that involve a computer(s) and a network(s) and are committed over the Internet or by using the Internet[81]. Due to this exactly special nature, cybercrimes pose a number of challenges for law enforcement (also, judicial authorities, etc.), the greatest of which we will discuss later on this chapter.

4.1 Investigating Cybercrime

Due to the fact that cybercrimes of today are committed with high sophistication, their investigation has become even more demanding. More specifically, law enforcement agencies are going after these perpetrators of such crimes and find it challenging to trace and identify them, to seize the evidence and successfully investigate and solve the case. Similar, or even the same challenges, face the attorneys, judges, forensic examiners, and corporate security professionals, because cyber criminals use cutting-edge technology to deploy their attacks, avoid detection and escape apprehension.

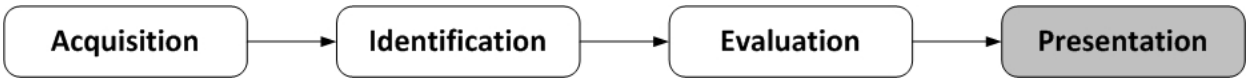
[80] Course Technology/Cengage Learning Staff, *Investigating Network Intrusions and Cybercrime*, EC-Council | Press, 2010

[81] The different categories and types of cybercrimes were mentioned in chapter 2.

On the other hand, the use of technology by cybercriminals, and more specifically the use of computer(s) and/or network to commit their crimes, has also a positive aspect. That is, investigators have a plethora of digital evidence to seize, examine, analyze and then apprehend and prosecute the offenders[82]. By digital evidence we mean any digital information that is transmitted or stored with the use of a computer or other electronic medium and is crucial for either the support or refute of the offense allegations.

In order to extract digital evidence from electronic devices that were involved in any way in the crime, investigators use forensics and more specifically digital forensics. Forensics could be defined as the "use of scientific or technological techniques to conduct an investigation or establish facts (evidence) in a criminal case", whereas digital forensics is a field of forensics which include the recovery and investigation of evidence found in digital devices, often in relation to computer crime[83].

Digital forensics plays a critical role in the investigation process and typically includes four steps which is acquisition, identification, evaluation, and presentation[84].



Although the scope of this dissertation is not to go deep into the forensic processes, we could just mention a couple of the computer forensic tools that are widely used in digital investigations and are: the FTK and EnCase.

The AccessData Forensic Toolkit (FTK) and the EnCase Forensic Tool contain a full suite of tools, making them capable of conducting large-scale investigations and generating reports that include, among others, listing of all files and folders in a case, detailed listing of all URLs and corresponding dates and times of visited websites, hash lists, password lists, and detailed hard drive information about physical and logical partitions[85].

[82] Eoghan Casey, *Digital Evidence and Computer Crime*, Elsevier, 2004
[83] Computer forensics is defined as the application of computer investigation and analysis techniques in the interests of determining potential evidence, according to computer crime investigator Judd Robbins, quoted in Computer Forensic Legal Standards and Equipment on the SANS Institute Web site at http://rr.sans.org/incident/legal_standards.php, accessed on 12/19/2018
[84] Ibrahim Baggili, *Digital Forensics and Cyber Crime*, Springer, 2010
[85] Ibrahim Baggili, *Digital Forensics and Cyber Crime*, Springer, 2010

Among the Goals of the Digital Investigation is[86]:

• To gather and ensure that all evidence is preserved and is enough to incriminate the suspect

• To understand how the attack was perpetrated

• To obtain information that may narrow the list of suspects

• To document the damage caused by the intruder

4.2 Challenges in Investigating Cybercrime

However, and although identifying, preserving and reporting digital evidence is only a part of the criminal investigation lifecycle and a challenge itself, building robust capabilities as a whole to respond effectively and efficiently to investigative needs adds even more challenges. From acquiring technical skills and infrastructure to legal framework, cooperation and coordination with law enforcement, prosecutors, defense attorneys and judges, the investigation of a cybercrime followed by a successful prosecution, face even more challenges. In the following section we shall provide a brief overview of the major challenges in the fight against cybercrime.

4.2.1 Transnational Legal Jurisdictions

When malicious actors commit a cybercrime, deploy cyberattacks, etc., many of the electronic traces and data transfer processes affect and pass through more than one country. Even in domestic transfer processes within a country, data may go outside of the borders of the originated country, be transmitted over routers and go back again to their destination.

That creates challenges because apart from the legislation at a national level which is totally necessary in order to incriminate and prosecute cybercrime offenders, international laws and regulations are needed to cover and facilitate such cases. Besides, acts on the internet that are legal in the source country, may be illegal in the destination and other involved countries.

Moreover, jurisdiction problems might also rise due to the difficulty in interpreting and defining what jurisdiction in cybercrime means; is it the place of the act, the location of the effect, the

[86] Course Technology/Cengage LearningStaff, *Computer Forensics, Investigating Network Intrusions and Cybercrime*, EC-Council Press, 2010

country of residence of the perpetrator, or the nationality of the owner of the computer that was attacked? Or, all of these at once?[87].

4.2.2 International Cooperation

Unlike traditional crime, which is usually perpetrated in one geographic location, cybercrime has global dimensions because is realized online and there is no linkage to any geographic location. Therefore, a coordinated global response is required, that in turn poses big challenges to law-enforcement agencies in all countries involved, when it comes to work close together in order to uncover the attackers of a cybercrime.

Cybercrime investigations need international cooperation of law-enforcement agencies in all countries affected[88]. Because sovereign countries do not allow investigations within their territory conducted by different countries without the permission of local authorities, cooperation based on the principles of mutual legal assistance is necessary. However, the requirements and time needed to collaborate with foreign law-enforcement agencies, especially when digital evidence and other electronic traces vital to the investigation are in danger of being lost or deleted, hinder the whole investigation procedure.

What is sure is, that cybercriminals know about that and almost always choose to attack through multiple countries with inadequate or even differences in cybercrime legislation, so that to cause delays and loss of evidence before the investigation reaches to an outcome or identification of the perpetrator(s). Thus, towards that direction, the harmonization of cybercrime-related laws and international cooperation would improve the investigation procedure (as the scope of the Convention on Cybercrime)[89].

[87] Marco Gercke, *Understanding Cybercrime: Phenomena, Challenges and Legal Response*, ITU, 2012
[88] Sofaer/Goodman, *Transnational Dimension of Cyber Crime and Terrorism*, 2001, in Tonya L. Putnam David D. Elliott, International Responses to Cyber Crime, available at: http://media.hoover.org/documents/0817999825_35.pdf, accessed on 12/19/2018
[89] Marco Gercke, *Understanding Cybercrime: Phenomena, Challenges and Legal Response*, ITU, 2012

4.2.3 Encryption

Another factor that can complicate the investigation of cybercrime is the use of encryption technology by the offender. Usually, the malicious actor has all of the stored suspicious/incriminating data encrypted. With so many encrypting tools/software available, every individual can quite easily implement a robust encryption to his/her data, thus preventing anyone else from unauthorized access to them.

Encryption tools/software uses various algorithms to encode a message or information in such a way that only authorized parties can access it. It is important, though, to note that encryption does not itself prevent interference, but only makes the content unintelligible to a potential interceptor. Moreover, current encryption software goes even further from encrypting only single files and entire hard disks to using tools to encrypt communications, such as e-mails and phone calls through encrypted VoIP technology against interceptors[90].

Although encryption could protect privacy of personal and other sensitive data, it also makes it more difficult for law-enforcement and other investigators to monitor communications and recover digital evidence in case of a cybercrime. Many experts have not only characterized it as a challenge, but also highlighted that encryption could be a threat to the investigation of a cybercrime[91.]

The most used and secure encryption algorithms are: Advanced Encryption Standard (AES), which is a symmetric encryption algorithm with 128-bit and 256-bit long keys and the RSA asymmetric algorithm which was named after Ron Rivest, Adi Shamir and Len Adelman. The latter algorithm uses public-key cryptography with one public and one private key and the length of keys can be 1024-bits and 2048-bits which increases security. With the use of such algorithms, "brute-force attacks" (testing every possible combination) or other processes of identifying the code might take long time or even decades to decode, depending on the encryption technique and key size.

---

[90] Matthew Simon and Jill Slay, *Voice over IP: Forensic Computing Implications*, 2006, available at: http://scissec.scis.ecu.edu.au/wordpress/conference_proceedings/2006/forensics/Simon%20Slay%20-%20Voice%20over%20IP-%20Forensic%20Computing%20Implications.pdf, accessed on 12/20/2018

[91] Denning and Baugh, *Encryption and Evolving Technologies as Tolls of Organized Crime and Terrorism*, 1997, available at: www.cs.georgetown.edu/~denning/crypto/oc-rpt.txt, accessed on 12/20/2018

4.2.4 Anonymization

A key role to the identification of the perpetrators plays the information that comes from the communication of the offenders. The nature of the Internet as a distributed system and the services that offers makes it possible to pose uncertainty on the origin of the communication. More technically savvy cyber offenders tend to conceal their identity by taking advantage of available online services that offer such capability. Among such services are:

- ‘Public Internet terminals (e.g. at airport terminals or Internet cafés);
- Network Address Translation (NAT) devices and virtual private networks (VPN);
- Wireless Networks;
- Prepaid mobile services that do not need registration;
- Storage capacities for homepages offered without registration;
- Anonymous communication servers;
- Anonymous remailers’[92]

An example of an attacker using the anonymous remailer could be the case in which an email is sent by having removed the identifying information from the email header before sending the message to the recipient. Although law enforcement might seek after the logs of the actual email address, most of the remailers do not keep them or it is difficult to disclose them, since their job is to protect the identity of their users.

Other practices that offer anonymity to users and are a challenge at the same time to law enforcement agencies, are the use of fake e-mail addresses from providers that do not require any kind of identity verification. Additionally, the use of unprotected private wireless networks or SIM-cards from foreign countries not requiring registration can bring the same result.

Towards the same direction, some support that users should act more freely under the principle of anonymous use of Internet email services. This principle is expressed, for example, in the

[92] Marco Gercke, *Understanding Cybercrime: Phenomena, Challenges and Legal Response*, ITU, 2012

European Union Directive on Privacy and Electronic Communications in Article 37 of the European Union Regulation on Data Protection[93].

Nevertheless, some countries due to investigative reasons, are dealing with the challenges of anonymous communications by implementing legal restrictions. For instance, "Italy requires public Internet access providers to identify users before they start using the service"[94].

4.2.5 Legal Challenges

As mentioned earlier, the existence of national legislation for cybercrime is a prerequisite for the investigation and prosecution of its perpetrators. The challenge here that lawmakers face is, that Internet technologies are changing fast and there is a need to continuously monitor and "adapt" laws to new technological capabilities that might be taken advantage by criminals for their new advanced schemes.

However, it takes time to update national criminal law to prosecute new forms of online cybercrime, not to mention how much will take for the international law that is needed to harmonize domestic legislation in different countries. Every delay in law adjustments even from one country, may have disastrous consequences for the investigation process with law enforcement agencies being unable to proceed further in their examination of the case.

Offences that have been criminalized under national criminal law need to be reviewed and updated to include their new forms. For example, an offence that could be perpetrated by making use of a forged traditional signature on a paper, now a law adjustment is needed to include in its new form of the offence the use of a forged digital signature.

[93] Article 37 – Traffic and billing data "1. Without prejudice to the provisions of paragraphs 2, 3 and 4, traffic data relating to users which are processed and stored to establish calls and other connections over the telecommunications network shall be erased or made anonymous upon termination of the call or other connection". – Regulation (EC) no 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, in Marco Gercke, *Understanding Cybercrime: Phenomena, Challenges and Legal Response*, ITU, 2012

[94] Marco Gercke, *Understanding Cybercrime: Phenomena, Challenges and Legal Response*, ITU, 2012

There is no question that many countries are working on adjusting their legislation to new forms of offences, however the main challenge is how fast they can do it before it is too late. In general, we could say that the whole adjustment process has three basic steps, that is, the recognition that a new form of offence has appeared due to and making use of latest technological developments that consequently creates the need of specific legislation, secondly, the identification of gaps in the law (e.g. penal code) that do not cover the details of the new variety of offence, and thirdly, the drafting-writing of the new legislation [95].

[95] Marco Gercke, *Understanding Cybercrime: Phenomena, Challenges and Legal Response*, ITU, 2012

Conclusions, Observations and Recommendations

If we would ask ourselves whether and who should care about cyber crimes the answer involves way more than one can imagine. In an interconnected world where each and every state is networked to one another, cyber threats committed on the network infrastructure of one country can easily cross the borders of other sovereign countries around the world thus, engaging multiple jurisdictions.

However, by engaging multiple jurisdictions, cybercrime automatically creates challenges to all the involved parties especially when todays criminals take advantage of highly technological improvements. Besides, it is obvious that the more technologically advanced the countries are today the more vulnerable against evolving cyber threats are and the greater impact will have as a result of their inadequacy to respond effectively and efficiently.

In the same context, and as we mentioned above, the fast growth of the Internet has generated unprecedented new opportunities for criminals to offend. These improvements present serious challenges for law and criminal justice, as they struggle to adapt to new form of offenses that in contrast to traditional ones, they know no borders, they might engage multiple criminals and victims, they evolve fast, and they are realized in or through the cyberspace.

Thus, a more collective approach in dealing with the cybercrime including not only governmental forces, but also the industry as well as each and every user, is necessary to deal with the continuously evolving cybercrime. This is essential especially when organized crime of today is less constrained by national boundaries, has become international in its scope, and with the use of information and communication technology (computer systems, information) and networks, not only can cooperate with other similar groups, but also can expand their targets geographically to almost everywhere.

Moreover, while there are cybercriminals that operate independently, the vast majority of them cooperate and share knowledge and practices posing further challenges to those who fight against. For example, there are known international “syndicates” of malicious computer hackers who collaborate and commit cybercrimes ranging from unauthorized access to information systems of critical infrastructure to malware attacks, phishing attacks, and online frauds against

both the public and private sector. Examples of such groups are, "Cult of the Dead Cow," "G-Force," and the "Chaos Computer Club" who have coordinated attacks on an international scale by communicating through the Internet[96].

Such growing evolution of the cybercrime has given rise to challenges that are connected with its global nature. When investigating a cybercrime, it is almost always the case that the perpetrators, in an attempt to remain elusive, have committed their activities by using computers and networks in countries other than the one from which he/she initiates the attack. In such cases, law enforcement investigators and all other involved parties, need to consider the laws and regulations of the rest involved nations throughout the investigation process until the arrest and prosecution of the suspect(s).

However, the biggest challenge is not to become aware of the other countries' cyber related legislation, but how to deal with a cybercrime when admittedly the lack of a universal definition of the term cybercrime makes matters worse. In fact, existing legislation might provide different interpretation to specific crimes and thus, dealing with them in different ways, or there might not be national laws at all to address certain cybercrimes or if they do exist, they may deal with specific crimes as non-cybercrime activities.

Furthermore, an outdated and rigid legislation not only creates difficulties in interpretation but essentially, prevents improvements and appropriate course of action taken by competent authorities to deal with contemporary threats. All the above create the need for establishing international laws with obligatory standards that would harmonize national ones in order to cover all cyber malicious activities and facilitate the investigative procedures across the involved nations.

Moreover, it is important to note that, according to a study conducted by the Center for Strategic and International Studies (CSIS) along with McAfee, cybercrime costs $600bn to the businesses annually, equating to 0.8% of global GDP[97]. McAfee also attributes this growth to the highly

[96] Sumit Ghosh and Elliot Turrini, *Cybercrimes: A Multidisciplinary Analysis*, Springer, 2010
[97] Center for Strategic and International Studies (CSIS) and McAfee report, *The Economic Impact of Cybercrime—No Slowing Down*, February 2018

sophisticated attacks, with cyber criminals continuing to adopt new technologies that are able to overcome traditional and stagnant cybersecurity frameworks.

Since cybercrime has become a profitable "criminal affair"[98], which is a very strong motivation for cybercriminals, it is also important for organizations, companies, and critical infrastructure in both the private and public sector, to establish appropriate cybersecurity policies, continuously keep them up-to-date and also keep its users aware of the current threats and risks.

Moreover, many organizations and companies have already taken substantial steps towards their preparation for the unexpected, that is a cyber incident, by issuing an incident response scheme-program for their ICT systems and networks involving both a response plan and a response team to implement it. Furthermore, what is equally significant, is the cooperation and collaboration with external experts as well as the support of other stakeholders such as law enforcement, forensic examiners, and the Computer Emergency Response Team (CERT) where necessary, in the fight against cybercrime.

Last but not least, and towards the same direction in addressing cybercrime, although there are national laws that criminalize certain types of cybercrime, and international laws, such as the Convention on Cybercrime that harmonizes national laws, there are still legislative differences that can impede law enforcement from being effective. For that reason, legislation in different countries should be as harmonized as possible, and cooperation between state institutions and between state and private ones should be facilitated. Although, the Budapest Convention on Cybercrime offers such provisions to countries to respond effectively, the problems arise when other directives and legislations offer harmonization in laws with sort of flexibility. A case in point could be the data retention period in which an Internet Service Provider has to maintain the user's data and personal information, etc. Even though all countries were obliged to introduce national data retention laws for their ISPs, however, the specific time could vary from 6 months up to 24 months. For example, in Greece the ISPs according to national law are obliged to retain user's data and information for 12 months, whereas in the Netherlands its national law says for 6 months, or in some other countries just different time periods. It is obvious how disastrous could be for law enforcement investigations when both of these countries could be involved in the

[98] Igor Bernik, *Cybercrime and Cyberwarfare*, Wiley, 2014

same case. Evidence cannot always be acquired due to legislative discrepancies and thus, a more harmonized legislation needs to be established.

Finally, as we have mentioned earlier, international cooperation is not only of great importance between only law enforcement agencies, but also between them and other involved stakeholders during the investigation process of a cybercrime. However, international cooperation even though is so vital, the well-established methods on how different agencies deal with that, needs modernization.

The current processes in international cooperation are facilitated through various ways, such as via Europol and Interpol when the involved countries are located either in the European Union or elsewhere in the world, and via diplomatic channels, that is through communication between the Ministries of Justice following the process based on the Mutual Legal Assistance Treaty (MLAT) or Letter of Rogatory (LOR). These processes allow governments to enlist directly the assistance of other governments in cybercrime investigations and collection of digital evidence. The challenge here is the time needed from the beginning to the end of this MLAT process that usually takes between eight to twelve and even more months. Again, this might be disastrous for the whole cybercrime investigation when evidence after so long time might be lost taking into consideration the previous mentioned different data retention periods.

Bibliography

Anthony Reyes, Kevin O'Shea, Jim Steele, Jon R. Hansen, Captain Benjamin R. Jean, Thomas Ralph, *Cyber Crime Investigations, Bridging the Gaps Between Security Professionals, Law Enforcement and Prosecutors*, Syngress, 2007

Abraham David Sofaer and Seymour E. Goodman, *Transnational Dimension of Cyber Crime and Terrorism*, 2001, in Tonya L. Putnam David D. Elliott, International Responses to Cyber Crime, available at: http://media.hoover.org/documents/0817999825_35.pdf

Barack Obama, President USA, Remarks at Release of White House Cyberspace Policy Review (May 29, 2009), available at http://www.whitehouse.gov/the_press_office/Remarksby-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/ accessed at 12/20/2018.

Cichonski, P., Millar, T., Grance, T., and Scarfone, K., *Computer Security Incident Handling Guide*. *Recommendations of the National Institute of Standards and Technology*. NIST Special Publication 800-61 Rev.2, 2012

Cyber Security Coalition, *Cyber Security: Incident Management Guide*, Cyber Security Center, Belgium

Cyber Defenses, Inc., *Guide to Developing An Incident Response Program*, Version 2018 0406, CyberDefenses, Inc., 2018

Center for Strategic and International Studies (CSIS) and McAfee report, *The Economic Impact of Cybercrime— No Slowing Down*, February 2018

Council of Europe, *Convention on Cybercrime***,** European Treaty Series-No.185, Budapest, 23.XI.2001

Course Technology/Cengage Learning Staff, *Computer Forensics, Investigating Network Intrusions and Cybercrime*, EC-Council Press, 2010

David S. Wall, *Cybercrime, The Transformation of Crime in the Information Age*, Polity Press, 2007

David S. Wall, *'The Internet as a Conduit for Criminal Activity'*, pp. 77-98, 2005 (chapter rev. 2015) in April Pattavina (editor) *Information Technology and the Criminal Justice System*, Sage Publications, 2005

Debra Littlejohn Shinder and Ed Tittel, *Scene of the Cybercrime: Computer Forensics Handbook*, Syngress Publishing, Inc., 2002

Deloitte, *Incident Response Brochure*, Deloitte LLP and affiliated entities, reached on December 28th, 2018 available at: https://www2.deloitte.com/content/dam/Deloitte/ca/Documents/risk/ca-en-deloitte-crisis-incident-response.pdf

Denning and Baugh, *Encryption and Evolving Technologies as Tolls of Organized Crime and Terrorism*, 1997, available at: www.cs.georgetown.edu/~denning/crypto/oc-rpt.txt

Donn B. Parker, *Crime by Computer*, 1976

Eoghan Casey, *Digital Evidence and Computer Crime*, Elsevier, 2004

Encyclopedia Britannica, *Cybercrime*, https://www.britannica.com/topic/cybercrime

European Commission, High Representative of the European Union for Foreign Affairs and Security Policy, *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, 2013

George Grispos, William Bradley Glisson and Tim Storer, *Rethinking Security Incident Response: The Integration of Agile Principles*, 2014

George Curtis, *The Law of Cybercrimes and Their Investigations*, CRC Press, 2012

Hamid Jahankhani, Ameer Al-Nemrat, Amin Hosseinian-Far, *Cybercrime Classification and Characteristics*, (chapter 12) in Babak Akhgar, Andrew Staniforth, Francesca Bosco, *Cyber Crime and Cyber Terrorism Investigator's Handbook*, Elsevier, 2014

Ibrahim Baggili, *Digital Forensics and Cyber Crime*, Springer, 2010

Igor Bernik, *Cybercrime and Cyberwarfare*, Wiley, 2014

Jason T. Luttgens, Matthew Pepe, *Incident Response & Computer Forensics*, 3rd Edition, Mc Graw Hill, 2014

Jason Crasey and Ian Glover, *Cyber Security Incident Response Guide*, CREST, 2013

Jessica Bregant and Robert Bregant II, Cybercrime and Computer Crime, The Encyclopedia of Criminology and Criminal Justice, First Edition, Edited by Jay S. Albanese, John Wiley & Sons, Inc. 2014

Jonathan Clough, *Principles Of Cybercrime*, Cambridge University, 2010

Judd Robbins, quoted in Computer Forensic Legal Standards and Equipment on the SANS Institute Web site at http://rr.sans.org/incident/legal_standards.php

Leighton R. Johnson III, Com*puter Incident Response and ForensicsTeam Management*, Elsevier Inc., 2014

Majid Yar, *Cybercrime and Society*, Sage Publications, 2006

Marco Gercke, *Understanding Cybercrime: Phenomena, Challenges and Legal Response*, ITU, 2012

Mark Ryan M. Talabis and Jason L. Martin, *Information Security Risk Assessment Toolkit*, Syngress Elsevier, 2013

Matthew Simon and Jill Slay, *Voice over IP: Forensic Computing Implications*, 2006, available at:http://scissec.scis.ecu.edu.au/wordpress/conference_proceedings/2006/forensics/Simon%20Slay%20-%20Voice%20over%20IP-%20Forensic%20Computing%20Implications.pdf

Mohamed Chawki, Ashraf Darwish, Mohammad Ayoub Khan, Sapna Tyagi, *Cybercrime, Digital Forensics and Jurisdiction*, Springer, 2015

NCA Strategic Cyber IndustryGroup, *Cyber Crime Assessment 2016*, Version 1.2, July 7th, 2016

National Cyber Security Center of UK GCHQ, *What Is a Cyber Incident*, September 19th, 2016, available at https://www.ncsc.gov.uk/articles/what-cyber-inciden,

Nir Kshetri, The Global Cybercrime Industry, Springer, 2010

Official Journal of the European Union, *Regulation (EU) 2016/679 of the European Parliament and of the Council*, 27 April 2016

Pete Finnigan, *Oracle Incident Response and Forensics: Preparing for and Responding to Data Breaches*, Apress, 2018

Regulation (EC) no 45/2001 of the European Parliament and of the Council of 18 December 2000

Robert Taylor, Eric J. Fritsch, John Liederbach, *Digital Crime and Digital Terrorism*, Pearson, 2015

Robert Taylor, Eric J. Fritsch, John Liederbach, *Digital Crime and Digital Terrorism*, Pearson, in Anthony Reyes, Kevin O'Shea, Jim Steele, Jon R. Hansen, Captain Benjamin R. Jean, Thomas Ralph, *Cyber Crime Investigations, Bridging the Gaps Between Security Professionals, Law Enforcement and Prosecutors*, Syngress, 2007

R. G. Smith, M. N. Holmes and P. Kaufmann, *Nigerian Advance fee Fraud, Trends and Issues in Criminal Justice*, AIC, 1996

Russell G. Smith, Ray Chak-Chung Cheung, Laurie Yiu-Chung Lau, *Cybercrime Risks and Responses: Eastern and Western Perspectives*, Palgrave Mcmillan, 2015

Sumit Ghosh and Elliot Turrini, *Cybercrimes: A Multidisciplinary Analysis*, Springer, 2010

Susan W. Brenner, *Cybercrime, Criminal Threats from Cyberspace*, Praeger, 2010

The European Parliament and The Council of the European Union, *concerning measures for a high common level of security of network and information systems across the Union*, Official Journal of the European Union, 6 July 2016

Thomas and Loader, *Cybercrime: Law Enforcement, Security and Surveillance in the Information Age*, Routledge, 2000

Van der Kleij R., Kleinhuis G. and Young H., *Computer Security Incident Response Team Effectiveness: A Needs Assessment*, Front. Psychol. 8:2179, 2017

Websites

Isaca.org, https://www.isaca.org/Journal/archives/2010/Volume-1/Pages/Performing-a-Security-Risk-Assessment1.aspx

http://conventions.coe.int

www.antiphishing.org/word phish.html

https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime