Bachelor's Thesis

HACKERS: CYBERCRIMINALS OR NOT?

Submitted by:

Denisa Maria Medovarschi

Tutor:

Manuel Mollar Villanueva

Bachelor's Degree in Criminology and Security

Year 2018/19

INDEX:

Abstract: The development and constant evolution of new technologies (ICTs) has originated a society that is constantly connected to the Internet. Obviously, this offers advantages, but it also creates important problems. There is always a fraction of people in all societies who act inappropriately, break the law or use illicit means to take advantage of others. The Internet provides a place for cybercriminals and allows them to exist and flourish. These recent years, issues concerning cyber security have received significant attention and have become a priority for many governments, organizations, and industries. Today, the technological advance is continuous and this brings crime new opportunities. One of this is the unauthorized access to computer networks. The current study focuses on this cybercrime, the hackers and the image that society has about them. In particular, a view of hackers that it is intended to distinguish them from cybercriminals and to assist law enforcement in understanding the way hackers think. The paper starts with the definition and history about hackers to continue with computer crimes from a criminology perspective and the way hackers are seen among people. Hacktivism, which is a new way of protest using the Internet, is addressed as well. Also, the paper presents laws, applicable to the computer crime, and highlights the issues about tracking and tracing these types of crimes by comparing United States and Spain.

Keywords: hacker, hacking, computer security, cybercrime, criminology.

1. Introduction: what is a hacker?

Computer hackers are an important social phenomenon today that has emerged in rapidly lately. Yet, when someone hear the word *hacker*, most of them had a wrong idea about what it means. There is a popular consensus that hackers are bad people who do bad things, but one thing is clear: there is no real consensus for the meaning of the word *hacker*. This may be because hackers engage in a variety of different activities (Taylor, Fritsch, Liederbach, Saylor and Tafoya, 2017).

During the 1960s, the term *hacking* was first introduced and used to describe a person with particular developed skills in programs and algorithms. Over the years, this has shifted and became negative in some way. Today, the hacker population represents individuals with a broad range of computer knowledge who differ in their motivations, skills, and usage of that computer knowledge. For example, the Jargon File text document, which defines and translates hacker slang, provides eight different definitions for a hacker, including those who “enjoy exploring the details of programmable systems and how to stretch their capabilities, as opposed to most users, who prefer to learn only the minimum necessary” (Bachmann, 2010; Taylor et al., 2017, p. 78).

Hackers can break into government and military systems and electronically steal money from banks, however, not all hackers engage in illegal activities. Also, not all illegal online activities are hacking. It must be noted that hacking can be legitimate and legal (Taylor et al., 2017).

In order to understand it better, the usual hacker term needs to be broken down into different categories. Hackers can mostly fall into two groups, “white hat” and “black hat” hackers. There is also a third major group, “gray hat “hackers. The term white hat describes an ethical hacker. This term was needed because the computer security field started to search and hire former hackers. They generally work for corporations or governments and avoid breaking laws. A gray hat hacker is someone who may occasionally be engaged in illicit activity. Usually, gray hat hackers behave in an ethical manner, but sometimes may violate the hacker ethic. A black hat hacker is typically more malicious or out for profit or exploitation of others. Individuals within the hacker community think that a black hacker is essentially a cracker or malicious hacker. But this term does not apply to all computer criminals (Taylor et al., 2017).

On the other hand, we have crackers and script kiddies too. A cracker is a malicious hacker, a person who breaks into other people's computer systems with the intention of causing harm. While script kiddies are unskilled individuals who use scripts or programs developed by others to attack computer systems and networks, often with simple exploits of vulnerabilities. They can be described as a scourge or pestilence on the Internet. Both can easily be identified because their actions are malicious (Taylor et al., 2017).

In addition, there has been an increase in the political activity of self-identify hacker. Recently, hacktivists emerged as a new type of hacker who use their skills to transmit a political message.

1.1. Hacker profile.

One thing that is clear is that there is no generic profile of a hacker. Usually, hackers are young males, but the percentage of women today is clearly higher and are generally respected and treated equally.

According to Adam Tyler, who was interviewed at the South by Southwest festival in Austin, Texas in March 2017, the profile of the new hackers is a common young man – usually, under 18 years old– keen on videogames, accustomed to Internet and social networks, who learns hacking as a personal challenge, in the same way that tries to overcome a complicated videogame. This new generation of hackers use the hacking as fun and to obtain visibility in the community, online or in the physical world. Their

motivation is not financial, but in some cases, what begins as a game ends up being a business (The Christian Science Monitor, 2017).

In the same interview, Adam affirms that it all starts experimenting with video games, tinkering with mods, cheats, and other programs that serve to modify elements of a game. It all about hacking a game like a game in itself. He points out that at an early age they are not aware of the moral implication of actions like these. As he says “These kids aren’t doing it to be malicious, these kids are doing it to have fun. These kids are doing it because to them it seems like a game, like an expansion of Call of Duty. Young individuals see this as a game, and don’t understand the consequences” (The Christian Science Monitor, 2017).

2. The origins and history of hacking.

Now it is important to consider how these various groups came to be. As there is no agreement on the meaning of the term *hacker*, its origins have problems too. The term hacker probably first emerged from the Massachusetts Institute for Technology (MIT). MIT students traditionally used the word hack to describe the college pranks. A hack was “a project undertaken or a product built not solely to fulfill some constructive goal, but with some wild pleasure taken in mere involvement”. These hacks intended to exhibit specialized aptitude and astuteness, or to recognize mainstream culture and historical topics. But not all computing or anybody at MIT was qualified as hacking or hacker. “To qualify as a hack, the feat must be imbued with innovation, style and technical virtuosity”. This creative problem solving became necessary due to the limitations of the hardware available at that time, because computers only existed in universities. This is why hacking was associated with creative, unorthodox problem solving (Levy, 2010, p. 10; Wark, 2006; Taylor et al., 2017).

Hacking emerged in an academic environment which contributed enormously to the ethic of collaboration on shared objectives through the challenge for acknowledgment and recognition, yet the recognition of one's peers was what made a difference (Wark, 2006).

In the early 1960s, this consideration of hackers continued but it changed due to the turbulent social climate and the hacker culture came under pressure from administrative and commercial necessities. In 1969, the ARPANET (see Figure 1) was created by the United States Department of Defense as an experiment on digital communications, but it was growing to connect hundreds of universities, research laboratories and arm industries. It allowed researchers from all over the world exchange information at a speed

and unprecedented flexibility. But ARPANET did something else; it put in contact all hackers (Gradín, 2004).

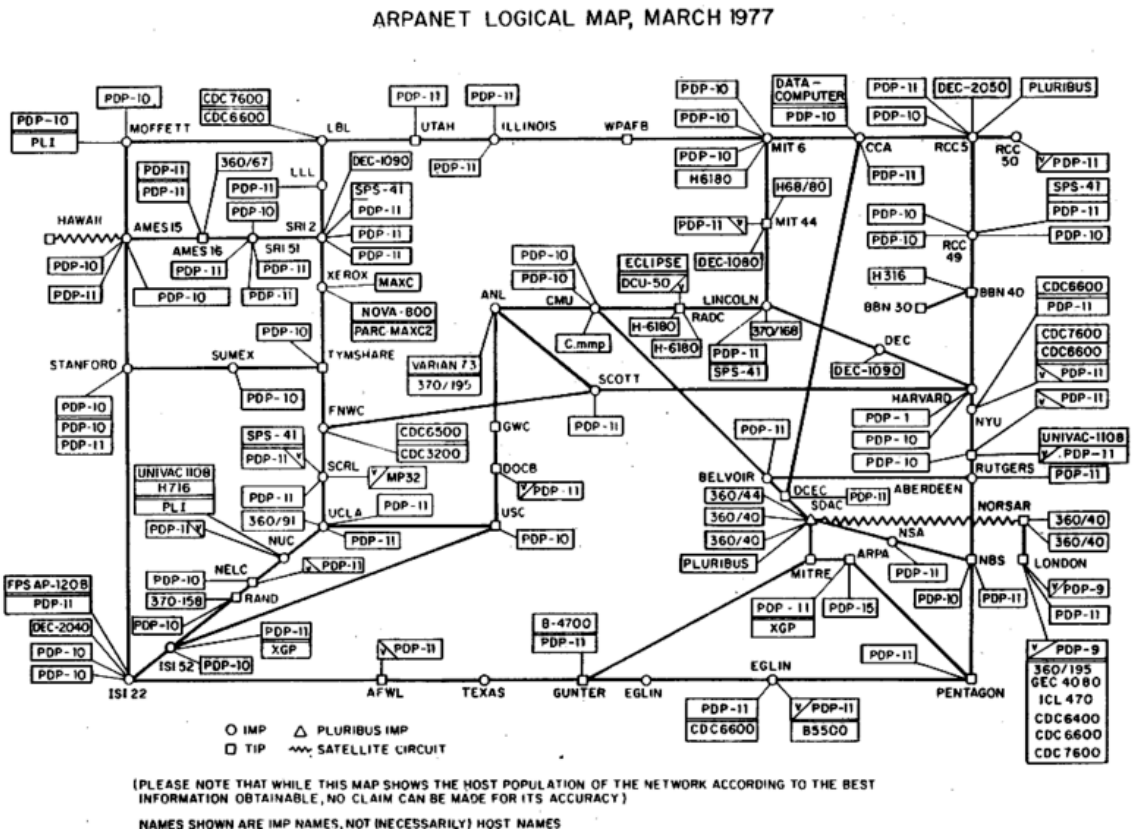


Figure 1. ARPANET logical map of 1977 (ARPANET, 1977).

The ideals of the core hacker culture of this period was that the information should be free to all to understand how things work and can be improved. This resulted in a series of ideas that forms the hacker ethic which is documented in the book *Hackers: Heroes of the Computer Revolution* by Levy (2010, pp. 28-31):

- "Access to computers –and anything that might teach you something about the way the world works– should be unlimited and total. Always yield to the Hands-On Imperative!
- All information should be free
- Mistrust Authority – Promote Decentralization.
- Hackers should be judged by their hacking, not bogus criteria such as degrees, age, race, or position.
- You can create art and beauty on a computer.
- Computers can change your life for the better".

At this time hackers believe that fundamental lessons can be mastered about the systems from dismantling things, perceiving how they work, and utilizing this information to make new and considerably more interesting things (Levy, 2010).

From here, this ethic was present in hacker's actions and conformed the roots of the actual hacker culture. Here the hackers were viewed as skilled computer users, but this shifted early in the 1970s with the development of *phone phreaking* which is the tampering of telecommunication systems to see how it works. This new generation that appropriated for themselves the word hacker was defined by crime (Taylor et al., 2017).

During the 1980s, the computer users increased and the hacker ethic was challenged. The technology started to change and more individuals had access to computer technology which allowed them to connect to other dedicated computer users and explore the computer networks. With all of this, Bulletin Board Systems[1] (BBS) dedicated to hacking appeared. The BBS were created by Warez d00dz as a way to share files with others they trusted in because they were breaking the law by sharing and breaking copyright protections (Taylor et al., 2017).

In 1983, a film called *War Games* appeared and had a significance influence on a new generation of computer users. This and *The Hacker Manifesto* from 1986, changed the hacker community. It caused a rift between hackers. On one side there were hackers with malicious intent and on the other side hackers with interest in exploring networks without breaking the law. Because of this, malicious hackers became the focus of law enforcement during the mid-to-late 1980s and criminal hacking started to emerge. By mid 1990s, the access to the Internet and mote powerful computers facilitated the growth of unskilled hackers and script kiddies. With the new millennium, Internet allow the interconnection of most computers around the world and, as a consequence, the nature of hacking changed and the computer security industry grew up. Today, the hacker community is divided into individuals engaging in legal and illegal activities for different reasons (Taylor et al., 2017).

2.1. The hacker subculture.

Researchers have explored hacker subculture to understand the nature of norms, values, and beliefs of hackers. They suggest that computer hackers' social world is formed by five social norms: technology, knowledge, commitment, categorization, and law. These are important for our understanding of the hacker community. They use these

[1] Computer or application dedicated to the sharing or exchange of messages or other files on a network.

norms to generate justifications for behavior and attitudes toward hacking (Holt, 2007; Taylor et al., 2017).

2.1.1. Technology.

One of the most significant norms in the hacker subculture is technology. Hackers and technology have an evident relationship, a profound association to computers and technology. This has an essential role in their hobbies and activities. When a hacker approached and accessed to a computer, they invest their energy diving into it ending up more skilled. To increase their skill level, the extra time they go through technology, the more the level increase. They also developed interests in the many different aspects of computer technology. For example, many hackers developed an interest in technology before or during adolescence (Holt, 2007; Taylor et al., 2017).

Hackers also discuss the need to understand computer technology, recurring to online sources for help. They used to use BBSs and web forums in the past. Today, the use of blogs, forums or tweets is common. These resources can increase a hackers' connection to computer technology (Holt, 2007; Taylor et al., 2017).

In addition, hackers created their own language in the 1970s and 1980s based in the technology. The dialect is called eleet ('leet) speek or k-rad and involves components like symbols and characters of computer programs. This reflects the importance of technology in their communications. It is a common component of the hacker subculture, which is still used by individuals in hacker communities around the world (Taylor et al., 2017).

2.1.2. Knowledge.

Other essential norm in the hacker culture is knowledge. The hacker identification is built at the devotion to learn about and comprehend technology. To be called a hacker was an obvious indication of the understand and skills of and individual. This is the reason why hackers need to invest a lot of energy to learn and apply their knowledge on- and off-line. Of course, the learning procedure starts with the essential parts of the computer technology. To appreciate the interrelated nature of computer systems, it is necessary to understand the rudimentary functions of computers. The develop of an extensive knowledge of equipment, hardware, programming, and systems administration is critical in light of the fact that it impact hacker's capacity to hack (Holt, 2007; Taylor et al., 2017).

Notwithstanding, hackers in the actual subculture do not instruct others in hacking abilities. “Hackers learned on their own through *trial and error*, and individual effort”. Evidence suggests that hackers have almost none real-world relationships with other hackers and therefore, they must establish online relationships to learn. Additionally, forums provided information to hackers in order to remain connected and ask questions of other hackers (Holt, 2007; Taylor et al., 2017).

Besides, knowledge is determining in the development of hacker conferences or *cons*. The goal of this conferences is to spread knowledge and share information around all over the world. In some of them, hackers show their comprehension of technology through difficulties and rivalries (Taylor et al., 2017).

2.1.3. Commitment.

Commitment is significant on the grounds that individuals should always learn and work on hacking procedures so as to improve and advance. Those who does not invest time in this often end up as script kiddies, who are limited and unskilled individuals. A continued study and practice and an individual attitude on- and off-line with regards to hacking techniques express commitment. In addition, consistent changes and enhancements in technology makes commitment fundamental. Hackers must be focused on the constant acquirement of new data. A hacker named Mack Diesel said “the minute you feel you’ve learned everything is the minute you’re out. There’s always something new to learn”. That’s why constant learning is so important (Holt, 2007; Taylor et al., 2017).

The effort implemented to study the tradecraft of hacking represents commitment as well. The amount of time and dedication demonstrate the importance of understanding how hacks actually works. Moreover, it significantly affects the interests and activities of hackers (Holt, 2007; Taylor et al., 2017).

2.1.4. Categorization.

Categorization, the fourth norm of the hacker subculture, refers to the ways individuals create and define the hacker identity. Technology, knowledge and commitment obviously affected how individuals assembled their definition of the word hacker. But there are significant discussions in the forums over how to characterize hackers and their motivations. Many users of forums argued that once they played out a specific assignment or comprehended a specific procedure, they could see themselves as a hacker. In the meantime, numerous individuals proposed that there were attitudinal

segments of their meaning of hacker which incorporates a specific perspective or essence (Holt, 2007; Taylor et al., 2017).

Consequently, closely-held conviction impacts the discussion in forums and the conception of the term hacker. Singular conception likewise fomented exchange about various sorts of hackers, what they do, and how this identifies with their label or title. This is particularly true for the belief or practices related with each kind of hacker previously mentioned. In summary, individual experience influence how hackers characterized themselves in respect to other ones (Holt, 2007; Taylor et al., 2017).

2.1.5. Law.

The final norm in the hacker subculture is law. Hackers regularly examine the lawfulness of hacking and data shared in the Internet and in the real world. With the time, hackers have turned out to be more conscious of the law in regards to computer networks because they are interested in knowing if their hacker are legal or illegal and should not be accomplished. Hacker conferences also addresses legal matters of hacking (Holt, 2007; Taylor et al., 2017).

As seen before, there is a division between hackers who feel there is no compelling reason to do unlawful hacks and those who viewed hacking in as admissible. Regardless, attention over potential law infringement seemed to have little efficacy on hacker attitude towards hacking. Hackers can offer data that could be utilized to execute an illegal action which caused a discrepancy regarding the process of information sharing. In the event that a hacker imparts data that can be used illegally, they legitimize its need, usually saying they provided information to educate others (Holt, 2007; Taylor et al., 2017).

Although some hacker actively encourages the exchange of illegal information, there are others that do not approve this type of exchange. Law enforcement attention may be attracted by the division of information sharing that exists in the hacker subculture. Limiting the amount of illegal information traded in the forums reduced the risk of law enforcement intervention. Despite the fact that hackers take measures to not be under the law enforcement radar, the way hackers relate to others impacts on law enforcement interests in them (Holt, 2007; Taylor et al., 2017).

2.2. Motivations.

Motivation is the most significant qualities of human behavior. It might change crosswise over time and spot since what is a main force in one place might be ostensible in another.

In 1999, Rogers categorized hackers into seven types based in his findings about hacker's motivations from his work and research. The taxonomy is based on hacker's skill level and motivations. It uses the following categories: "Tool kit/Newbies (NT), cyberpunks (CP), internals (IT), coders (CD), old guard hackers (OG), professional criminals (PC) and cyber- terrorists (CT) (Van Bereven, 2001, p. 2; Rogers, 2005, pp 2-5):

1. **Newbies** (NT): Their essential motivation depends on new emotions and the satisfaction of their ego.
2. **Cyberpunks** (CP): Their motivation is the desire for media consideration and sometimes financial gain.
3. **Internals** (IT): Their motivation is revenge.
4. **Coders** (CD): Their motivations change from acknowledgment from peers and experimentation, advancing to revenge and social reputation.
5. **Old guard hackers** (OG): Their motivations are mostly knowledge and intellectual challenges.
6. **Professional criminals** (PC): Their motivation is primely monetary profit.
7. **Cyber-terrorists** (CT): Their motivation is patriotism.

When hackers are interviewed, it is often reported that while hacking they experience full engagement in the task and think about no prizes. This is a significant allusion of the hackers' supposed motivation. According to Voiskounsky and Smyslova's (2003) self-reports, intrinsic motivation is distinctive in hackers. "Intrinsic motivation is the tendency to engage tasks for their own sake; one finds these tasks interesting or challenging" (p. 173).

Currently, the most elaborated concept of intrinsic motivation is the flow theory or paradigm originated by Csikszentmihalyi (1975). "Flow means that an action freely follows the previous action, and the process is in a way unconscious; flow is accompanied by positive emotions and is self-rewarding". An exact coordinating of somebody's aptitudes and challenges is the principle predecessor of flow. Expanding aptitudes need an expansion of difficulties, and high challenges prompts an update of abilities (Voiskounsky and Smyslova, 2003, p. 173).

After their research, Voiskounsky and Smyslova (2003) present a motivational model of hackers' development, based on the flow/non-flow ratio (see Figure 2).

The model depends on a harmony between the dimension of computer and IT skills and the dimension of difficulties in hacking. A hacker may advance in the following way: An inexperienced hacker may discover a mix of difficulties and aptitudes and begin to encounter flow. At that point, the hacker may remain at this phase for a considerable length of time or advance in three different ways: (1) step- by-step advancement both in difficulties and abilities, (2) the hacker increases new aptitudes but comes up short on the correspondence of new aptitudes to non-updated difficulties, and (3) the hacker takes high difficulties and discovers he/she needs non- updated aptitudes. Regardless, a zigzag of the flow motivation development is because of the advancement in hackers' skills and challenges (Voiskounsky and Smyslova, 2003).

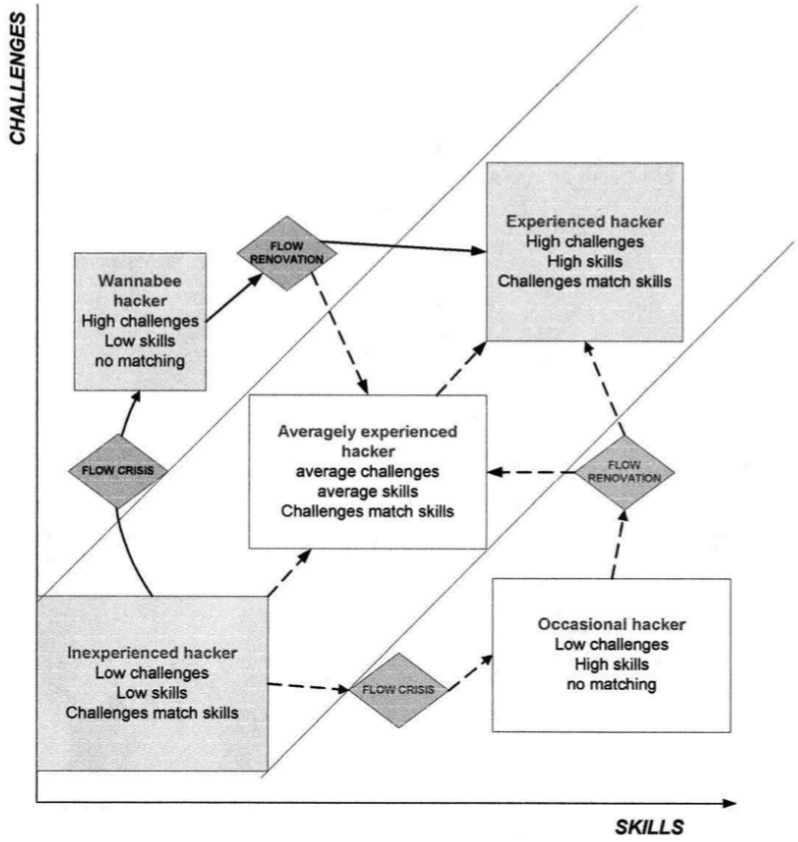


Figure 2. Flow-based model of computer hackers' motivation (Voiskounsky and Smyslova, 2003, p. 177)

Today, the majority of the research suggests that there are six key motives among hackers: entertainment, ego, status, entrance to a social group, money, and cause (Holt and Kilger, 2012).

Since the emergence of computer technology, *entertainment* is a motivation that has stayed steady in the hacker subculture. Hackers have an intense desire to understand technology, as seen earlier, which implies that they will play around with technology so as to figure out how these functions, and distinguish their cutoff points. Likewise, entertainment can be connected to the motivation of *ego* dependent on (1) the mental and passionate lift an individual may feel after the fruitful finish of a hack and (2) the status collected from hacking. Hacking abilities can also be helpful so as to *gain entrance to various groups*. A hacker, might be incorporated into a group to extend the individual general limit. Lastly, the motives of *money* and *cause* are progressively present in these days. The increase of the financial and individual data now accessible online has made that the information gained through various types of attacks is sold through open markets to produce a benefit for hackers. Money has turned into a significant motivation for criminal hackers in the course of the most decades. In this way, there has been an increment in the quantity of cause-driven hacks because of the development of the Internet and its use in communicating political, nationalistic, and religious convictions (Holt and Kilger, 2012).

3. The criminology of computer crime.

Cyberspace presents a new challenge for criminologists, being a perfect place for new sorts of deviance and crime. Over the years, several theories have been postulated to explain crime. Some researches try to explain cybercrimes applying traditional concepts. It is important to note that these theories were developed to explain crime in general, not cybercrime specifically. Although these theoretical explanations were observed to be insufficient, some can apply to this phenomenon (Schmalleger and Pittaro, 2009; Taylor et al., 2017).

3.1. Rational choice theory.

Rational choice theory explains how a few people deliberately and reasonably choose to carry out criminal acts. An individual commits crime since the person in question settles on a balanced decision to do as such by gauging the hazard and advantages of it. The attention ought to be on the offense submitted, not the offender. This is because the wrongdoer has settled on a rational decision to submit an offense (Lanier, Henry and Anastasia, 2018; Taylor et al., 2017).

The central basis of this theory is that individuals are rational creatures whose behavior can be controlled or altered by a dread of penalty. Therefore, in order to control

wrongdoing, cybercrime too, offenders need to fear the punishment implicit in the crime and, in that way, be deterred from carrying it out. Endeavors should be put on making the dangers of perpetrating cybercrimes higher than any benefit got from perpetrating the offenses (Lanier et al., 2018; Taylor et al., 2017).

3.2. Routine activities theory.

Routine activities theory is derived of rational choice theory. The main idea of routine activity is the study of crime as a circumstance which relates in space and time. It was first formulated by Lawrence Cohen and Marcus Felson in 1979. Crime is the result of decisions made inside a setting of situational requirements and opportunities. According to this, crime happens when there is a confluence in reality of three variables: (1) a motivated offender (e.g. a hacker), (2) a suitable target (e.g. a vulnerable computer system), and (3) the absence of a capable guardian (e.g. inadequate software protection). Each of these three components must be available all together for a crime to happen (Lanier et al., 2018; Schmalleger and Pittaro, 2009; Taylor et al., 2017).

The increase of the number of available targets, due to the quick development of the use of computers and the Internet, made this theory applicable to cybercrime. All the computers online at any time made potential objectives for hackers. Likewise, the nature of the Internet allows to hack into computers hundred miles away without leaving home. The opportunity for crime is multiplied by the fact the criminal is no longer “place-bound”. In addition, there is an absence of capable guardians to defend individuals from cybercrime without and adequate software protection like antivirus software, firewalls, and similar programs (Schmalleger and Pittaro, 2009; Taylor et al., 2017).

3.3. Deterrence theory.

Deterrence theory is related with rational choice theory. Choosing to obey or violate the law is subsequent to ascertaining the results of their behavior. This is applicable to all offenders, including cybercriminals. When the risks exceed the benefits, the individual will not carry out the crime because the person in question will be deterred from the criminal act due to the dread of punishment. There are two basic types of deterrence: general and specific. General deterrence is intended to avoid crime in the all the society. Specific deterrence is intended to dissuade just the individual offender from carrying out that crime in the future (Taylor et al., 2017).

“As it applies to cybercrime, it can be argued that many cybercriminals are rational actors, making rational choices to commit computer crime. As it applies to computer

crime, it is argued that many computer criminals do not know the potential penalties they face for particular crimes" (Taylor et al., 2017, p. 52).

Offenders must view the risks as unpleasant in order to make deterrence work. If a computer criminal does not think about incarcerations as unpleasant or does not believe he will be caught, then the cybercriminal is not deterred. Also, to be effective, the sanction needs to be swift, certain, and severe. Most computer crimes remain unsolved which makes the probability of arrest low, making deterrence unlikely (Taylor et al., 2017).

3.4. Strain theory.

Strain theory is one major type of social structure theories. Overall, the theory describes the interchange among social structures, social setting, and individual activity. The most prominent is Robert Merton's strain theory (Taylor et al., 2017).

In capitalist societies, the approved methods of obtaining success are the institutionalized means used for accomplishing society's goals. Yet, not every person has equivalent access to institutionalized means to obtain economic success (goal). People are hindered in their capacity to get to the methods, which causes strain because there is a gap between a person's desire and their ability to do so. Merton emphasized that the differential opportunity structure is the cause of strain rather than the goals (Lanier et al., 2018; Taylor et al., 2017).

Merton identified five ways in which individuals respond or adapt to selective blockage of access to opportunities. These five adaptations (see Table 1) are all based on an individual's attitudes toward means and goals. The first mode of adaptation is *conformity*. The conformist accepts both the goals of society and the legitimate means of acquiring them. It is the most widely recognized method of adjustment and it is very improbable to carry out criminal acts. The second mode of adaptation is *innovation*. Innovators acknowledge the goals, however altogether dismiss or modify the methods to obtain them. They try to advance and find other way to progress, but it is frequently illegitimate. This mode of adaptation is well on the way to prompt crime, including computer criminals. The third mode is *ritualism*. Ritualists dismiss the societal goals, however acknowledge the means. These individuals perceive that they will never accomplish the goals because of individual failure or different variables, so they lower their aspirations. It is unlikely that these individuals will commit a crime. The fourth mode is *retreatism*. The individual rejects both the goals of society just as the way to acquire them. Examples would include chronic alcoholism, drug abuse, and vagrancy, who may commit crimes in order to maintain their drug use. The fifth mode of adaptation is *rebellion*. Rebels dismiss the

goals and means as well as supplant them with new ones. Crime is probably going to happen with this mode of adaptation and can be represented by some gangs, militias or cults (Lanier et al., 2018; Taylor et al., 2017).

Adaptation	Cultural Goals	Institutionalized Means
I. Conformity	+	+
II. Innovation	+	-
III. Ritualism	-	+
IV. Retreatism	-	-
V. Rebellion	-/+	-/+

Table 1. Merton's individual modes of adaptation (Lanier et al., 2018, p. 221)

Note: (+) signifies acceptance, (-) signifies rejection, and (-/+) signifies rejection and substitution of new goals and standards.

3.5. Neutralization theory.

Sykes and Matza's neutralization theory is one type of learning theories. According to them, most criminals holds conventional values, norms, and beliefs. When they violate social norms, they legitimize their conduct by methods for a particular arrangement of legitimizations, called neutralization techniques, which empower them to shortly neutralize those values, norms and beliefs (Schmalleger and Pittaro, 2009; Taylor et al., 2017).

Sykes and Matza (1957) argue that the techniques of neutralization are learned and precede the criminal act. There are five techniques of neutralization (Schmalleger and Pittaro, 2009; Taylor et al., 2017):

1. *Denial of responsibility*. The individuals claim that their acts are because of powers outside their ability to control.
2. *Denial of injury*. Individuals perceive their behavior as harmless. They deny the wrongfulness of their actions. This can be applied to the majority of computer crime where the computer criminal does not feel that anyone is really harmed.
3. *Denial of victim*. The individuals view their behavior as revenge, the victim deserved it. Computer crimes like malicious attacks are an example of it.
4. *Condemnation of the condemner*s. Individuals blame lawmakers and law-enforcement, shifting the culpability to others who dislike their activities.
5. *Appeal to higher loyalties*. The individuals claim that their actions were necessitated by loyalty to others. The peer group becomes a priority over the guidelines of society.

Taken as a whole, these techniques of neutralization may be significant to account for cybercrimes. Specially, hackers use most of the neutralization techniques to justify three types of computer offences: (1) software piracy, (2) hacking, and (3) phreaking (Schmalleger and Pittaro, 2009).

3.5.1. Denial of injury.

Although hacker's behavior deviates from the norm, they try to prove that it does not hurt anybody or even if it hurts someone, the harm is insignificant. For example, Schmalleger and Pittaro (2009) interviewed individuals who used this technique to report copying, cracking, and distributing protected software by using other's people Internet accounts and credit cards, programming and sending viruses, and browsing through other's people files. Here, hackers claimed that they had not malicious purposes. One of the interviewees said that developed viruses "for the challenge in it, and to see how it works".

Hacking is an offense in which the hacker may not feel that the damage has been done due to the fact that the offense is not physically tangible. The virtual space is the domain where computer hacking occurs. According to hacker, downloading information is copying, not stealing. In the same way, to neutralize their guilt about unauthorized browsing, hackers claim that people are not harmed as long as they are not aware (Schmalleger and Pittaro, 2009).

3.5.2. Denial of victim.

"Hackers who committed offenses such as spreading viruses, crashing computer systems, removing other users from the network, or deleting content from other people's computers justify their actions by revenge". For them, to employ malicious practices is the easiest way. Also, in this way they can cause intentional harm to anyone who is "the enemy". Microsoft is often perceived by hackers as a remote enemy and an offense against it is justified (Schmalleger and Pittaro, 2009, p. 326).

3.5.3. Condemnation of the condemners.

Today, hackers mistrust the authorities and promote decentralization due to an ethic question: freedom of information. Hackers express their disdain against big corporations that control the media and the sources of data by encroaching on software copyrights, distributing passwords, and unlawful logging and browsing. From their point of view,

these are not deviant behaviors. “Hackers often divert attention from their acts to what they define as tyrannical and overpowering bureaucracies that, in their eyes, are the real criminals of the computer world” (Schmalleger and Pittaro, 2009, p. 327).

In addition, they often show an objection to pay the prices charged by the companies and blame the company owners and information security experts for their violations because they failed to protect their computer systems. An interviewee of Schmalleger and Pittaro (2009) said “If I succeeded in doing it, it must be legitimate. If I got in there, it was open. I don’t enter closed places”.

3.5.4. Appeal to higher loyalties.

Hacker’s ethic of freedom information it is very important. Their curiosity generates a desire to learn and know as much as possible and to explore all the options and limits. Knowledge is regarded as a venerate value. That’s why hackers content that their actions were a result of craving for information (Schmalleger and Pittaro, 2009).

3.6. Hackers versus cybercriminals.

For many people, hacking is the archetypal cybercrime, and the hacker is the archetypal cybercriminal. But this is not a reasonable conception. Hackers themselves occasionally utilize various terms to make distinctions dependent on their motivations and actions. This can be valuable to an investigation because it may allow the investigator to include or exclude a specific suspect from an investigation. There are determined activities that a hacker would not perform, for instance, a malicious attack that serves just to back up an extorsion. For the hacker, access to a computer system is essentially a technological challenge that improves the system (Miró Llinares, 2012; Taylor et al., 2017).

There is little analysis support to distinguish hackers from computer criminals. Many articles equivocate hacking with computer crime. Some computer criminals deny that there is a difference while others admit illicitness of the activities, yet assume different motivations. Nevertheless, in the hacker media the distinction is important (Taylor et al., 2017).

In one of the interviews of Discovery News (2009), Darren Kitchen talks about hackers and cybercriminals. He says “I have a malicious curiosity and I do things in the lab that might get me arrested if I actually try them on the streets, but that’s not to say that I’m evil. Is, you know, having fun with tools”. Besides, when talking about hackers and computer security professionals, for him, the only difference is a paycheck.

Most of online activities are legitimate. The difference among hackers and computer criminals lay on the attitudes toward they approach the activity. The problem is that the hacker subculture accepts as hacking some actions that are illegal and considered computer crime by law enforcement. These actions can be called criminal hacking. Figure 4 shows these three concepts (Taylor et al., 2017).

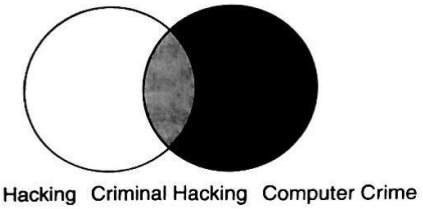


Figure 4. The relationship between hacking, criminal hacking, and computer crime (Taylor et al., 2017, p. 84)

Besides, apparently, to people in love with the "old school" of hackers, like Steven Levy, there is a big difference between old hackers and new hackers. According to Levy (2010), the differences between the old and new hackers huge and clear. Table 2 shows Levy's differences (as cited in Gradín, 2004, pp. 128-129).

Old hackers	New hackers
They strove to create.	They strive to destroy and tamper.
They loved control over their computers.	They love the power computers gives them over people.
There were always seeking to improve and simplify.	They only exploit and manipulate.
They did what they did because of a feeling of truth and beauty in their activities.	They hack for profit and status.
They were communal and closely knit, always sharing openly their new hacks and discoveries.	They are paranoid, isolated, and secretive.
They were computer wizards.	They are computer terrorists, always searching for new forms of electronic vandalism or maliciousness without thought of the consequences.

Table 2. Differences between old hackers and new hackers (as cited in Gradín, 2004, pp. 128-129)

4. The hacker as a threat.

Since the primary public familiarity with hackers, an important number of sensational news stories has obscured the line among hackers and computer criminals. Part of this ambiguity surrounding the perceptions of hackers has to do with the changing attitude toward hackers over the years and the many types of hackers –discussed earlier– and hacking activities (Schmalleger and Pittaro, 2009).

The way hackers are characterized by the media is important. Investigators offer their opinions on hacker behavior and depending on how these are shifted through the media, different images of normalcy and deviance are produced (Halbert, 1997; Taylor et al., 2017).

Naming and labeling is a crucial step in creating an enemy. In the 1980s and 1990s, hackers' control of computer systems and the *Operation Sundevil*[2] supposed the starting point for identifying hackers as a serious threat. They turned into the focal point of fear for a society struggling with the new information age and the media started to apply the word hacker to electronic trespassers and vandals (Halbert, 1997; Taylor et al., 2017).

As people became more familiar with the Internet and more depended on computer technology, it was easier to use the hacker as a threatening figure. This has continued through today, as media frequently centers on publishing the worst aspects of crimes, including hacker crimes. Currently, the label hacker is still used negatively to refer to electronic criminals or vandals and an exertion is made to connect hacking to crime. It seems that the attitude toward hackers conforms an unstable equilibrium in societal reaction to deviance (Halbert, 1997; Schmalleger and Pittaro, 2009; Taylor et al., 2017).

The development of Internet and ICT and the emergence of a whole generation that has already lived in the use of these technologies has led, on one hand, to a relativisation of the meaning of the hacker, and on the other hand, to a greater concern for safety of computer systems. This, joined to the impact of the globalization of cybercrime and the fact that many mafia organizations use hackers to gain access to computer systems with harmful purposes, can explain why the image of the hacker has broken down (Miró Llinares, 2012).

However, even if the hacker label may suggest people who are a threat to national security or the intellectual property of others, the term still retains its original connotation of someone who have mastered the computer technology at very high levels. Contrary to what most of people may think, hackers are involved not only in deviant activities, but

[2] *Operation Sundevil* was a 1990 nationwide United States Secret Service crackdown on illegal computer hacking activities.

have also developed the computer, the Internet, computer programs, etc. (Schmalleger and Pittaro, 2009).

As Adam Tyler says in one interview at the South by Southwest festival in Austin, Texas in March 2017, hackers are now been seen as a new attractive subset of the world and hacking is now seen as an attractive trait. With this we can see that the perception of the hacker as a threat varies among the population (The Christian Science Monitor, 2017).

4.1. Dynamics of hacking.

Hacking can be done in different ways, although usually the way of proceeding can consist in the following steps (see Figure 5):

1. **Inspection**. Obtaining the information from the potential victim using different Internet resources. Some of the techniques used include social engineering, dumpster riving, or sniffing.
2. **Scanning**. Using the information obtained before, the next step is to obtain information relative to IP addresses, hosts, and authentication data. Tools that can be use are network mappers, port mappers, network scanners, port scanners, and vulnerability scanners.
3. **Obtaining access**. Consists of the search for vulnerabilities in the targeted system that can be derived from an insufficient programming, a technological change that makes it obsolete, or the search and use of backdoors that unwittingly the owner or any of the subjects who have access to the system or the computer may leave open. Some of the techniques used can be buffer overflow, Denial-of-Service (DoS), Distributed Denial-of-Service (DDos), password filtering and hijacking.
4. **Maintaining access**. When the entrance to the system is achieved, the intruder will seek to implement tools that allow him or her to access in the future from any location with Internet access. For this reason, the use of backdoors, rootkits and trojans is common.
5. **Deleting traces**. To avoid being discovered by the security professional or the network administrators, the intruder need to delete his or her traces eliminating the log files for example.

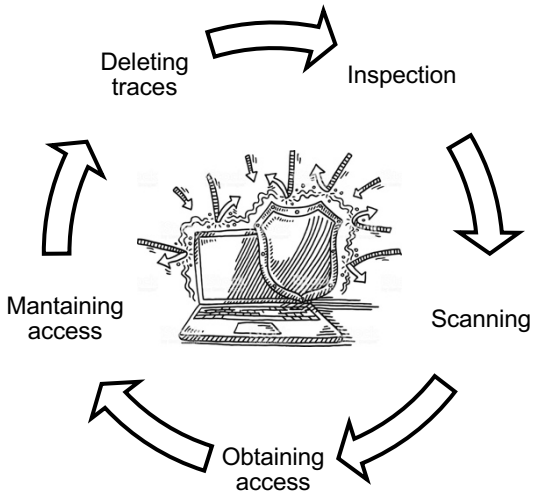


Figure 5. Steps of cyberattacks (own photo)

5. Hacktivism: the new way of protest.

Recently, there has been an increase in the general level of understanding about hacking among the population which is paralleled to a desire to expose governments for their undercover activities. This sentiment has generated the *hacktivist*, a way of protest on the Internet usually aimed against agencies or States which, according to the communities of Internet users, put at risk the idea of open cyberspace that hackers defend. Hacktivists often define themselves as hackers with political consciences. "Hackers come together to challenge the treatment of their peer by the government". Their shared characteristic is the use of hacker skills to communicate a political message (Gold, 2014; Miró Llinares, 2012; Taylor et al., 2017, p. 88).

The term hacktivism has been characterized as the pacifist use for political finishes of "illegal or legally ambiguous digital tools" like website defacements, information theft, website parodies, DoS attacks, virtual sit-ins, and virtual sabotage. It can be delivered by taking forward the breakdown of a technological-social distinction in computers and systems and applying it to governmental issues outside the data space originated by computers and systems. This is, in summary, the ideology of the hacktivism; the defense of the liberty in Internet and the fight against any barrier imposed in the cyberspace. This ideology has made hacktivists act against (1) the attempt of governments to control the Internet, and (2) public and private organisms that try to block the free dissemination of data and information in the cyberspace (Hampson, 2012; Jordan, 2008; Miró Llinares, 2012; Taylor et al., 2017).

To analyze hacktivism as a form of protest, there is a need to consider five methods used by hacktivists that have existed in the recent past. As technology develops, so too

will the types of hacktivism, which implies that the techniques could be altogether different sooner rather than later (Hampson, 2012).

5.1. Denial-of-Service Attacks.

Denial-of-Service (DoS) attacks “involve attempts to block access to websites by any of several means”. It is an attack intended to closed down a machine or system, making it out of reach to its proposed users. A DoS attack exploits an innate vulnerability in the manner computer systems convey, which means that, it does not rely upon a special program to run. Generally, it uses a single computer and a single IP address to attack its target, making it easier to defend against (Hampson, 2012; Taylor et al., 2017).

DoS attacks by and large take one of two structures. They either (1) flood web seervices or (2) crash them. Flooding is the more typical type of DoS sttack. It happens when the assaulted system is overpowered by a lot of traffic that the server is unfit to deal with and the system in the end stops. In other words, the attack sends fake solicitations to the server, over-burdening it and counteracting legitimate traffic. Crash attacks happen less frequently, when cybercriminals transmit bugs that take advantage of defects in the focused system. Subsequently, the system crashes (Taylor et al., 2017).

A distributed Denial-of-Service (DDoS) attack might be differentiated from a DoS attack by its utilization for a network to develop a multiple attack. It is a way of disturbing the Internet. Here, “the initiating party activates a network of computers under its control, called a botnet, to multiply the power of the attack, thereby directing an exponentially increased volume of information requests to the target server”. For instance, multiple computers can be instructed to shell the objective site with nonsense information. This makes the servers come up short on memory making it lethargic (Hampson, 2012, p. 518; Taylor et al., 2017).

5.2. Site defacements.

Site defacements include acquiring unauthorized access to a web server and supplanting or changing a web page with new elements that send a specific message. They are usually utilized not just as a way to convey a message, yet additionally to exhibit the specialized ability of the defacer. This is why the majority of the times, the defacement is harmless, however, it can sometimes be used as a distraction to cover up other actions (Hampson, 2012).

For instance, sites representing the Indian parliament, television networks, newspapers, and academic institutions have been defaced with anti-India images and

slogans, with some redirecting web traffic to pro-Pakistani sites. Also, the White House and the FBI web sites have both been attacked with this method by Earth Liberation (Taylor et al., 2017).

5.3. Site redirects.

By this method, the hacktivist reconduct users to a website that is not the same as the one shown by the web address. The perpetrator causes users to reach an alternative site by increasing unauthorized access to a web server and altering the settings. They basically hijack access to the targeted web site and allege authority over the elements showed on the site (Hampson, 2012).

5.4. Virtual Sit-Ins.

Virtual sit-ins include individual protestors reloading web pages. It very well may be practiced basically by users manually and over and over reloading the targeted site or enable members to download exceptional code that automatically and more than once reloads the targeted website (Hampson, 2012).

5.5. Information theft.

Information theft involves “gaining unauthorized access to a computer or network and stealing private data” (Hampson, 2012, p. 521).

Besides, there are other methods used by hacktivists like site parodies, virtual sabotage, or software development.

5.6. Anonymous.

Anonymous has become the most widely recognized source of hacktivism. The group originated in 2003 from the 4chan.org message board, a simple image-based bulletin board where anyone can post comments and share images without registering. Before Wikileaks, Anonymous was best known for Operation Payback in which it attacked the Recording Industry Association of America (RIAA) and other organizations connected with copyright protection and music and software anti-piracy efforts. Shortly afterwards, Anonymous acted in Spain resulting in the closure of the websites of the SGAE, Promusicae and the Ministry of Culture, as a protest against the Law of Sustainable

Economy (Ley de Economía Sostenible), producing a shut down for forty hours. After this, they became known for its attacks on the Church of Scientology with *Project Chanology*[3] (Mansfield-Devine, 2011; Miró Llinares, 2012; Taylor et al., 2017).

Amid this period, Anonymous spread out politically. The name Anonymous was progressively being utilized to proclaim activist actions, regularly in manners that challenged expectations. Its members, called Anos, are easily identified by the mask from the film *V for Vendetta*. It is an open and indefinite group of persons with computer skills that may be hackers or mere initiated, united by ideological convictions. Unlike WikiLeaks, Anonymous has no salaries to dole out or rent to pay. The group's activities are organized via Internet Relay Chat (IRC), Twitter, and Facebook. (Coleman, 2013; Mansfield-Devine, 2011; Miró Llinares, 2012; Taylor et al., 2017).

Anonymous' favorite tool is the Low Orbit Ion Cannon (LOIC), a renew version and retrofitted with a rough direction and control ability of the supposedly network stress-testing tool developed by Praetox Technologies (see Figure 6). In short is a DDoS tool. "LOIC comes in two main forms: (1) a Windows executable that Anons download and run from their own machines, and (2) a Javascript-based version (JS-LOIC) (see Figure 7) designed to be integrated into a web page and therefore usable by anyone who visits the site" (Mansfield-Devine, 2011).

LOIC tool empowered even beginner users to participate in the DDoS attacks in two different ways: directly, by entering the objective IP address and clicking "fire"; or, on the other hand, by volunteering their computer or system to the "LOIC Hivemind", and in this manner enabling different users to coordinate attacks from the surrendered system (Hampson, 2012).

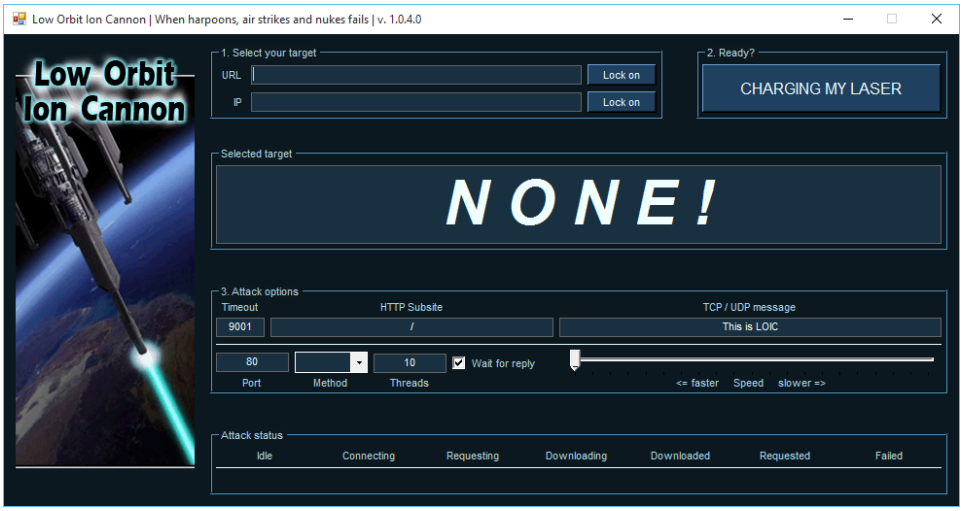


Figure 6. LOIC-0 screenshot in Windows 10 (FockeWulf FW 190, 2015)

[3] *Project Chanology* is a series of dissent movements that began because of the Church of Scientology's endeavors to remove video clips from a highly publicized interview with Scientologist Tom Cruise from the Internet in January 2008.

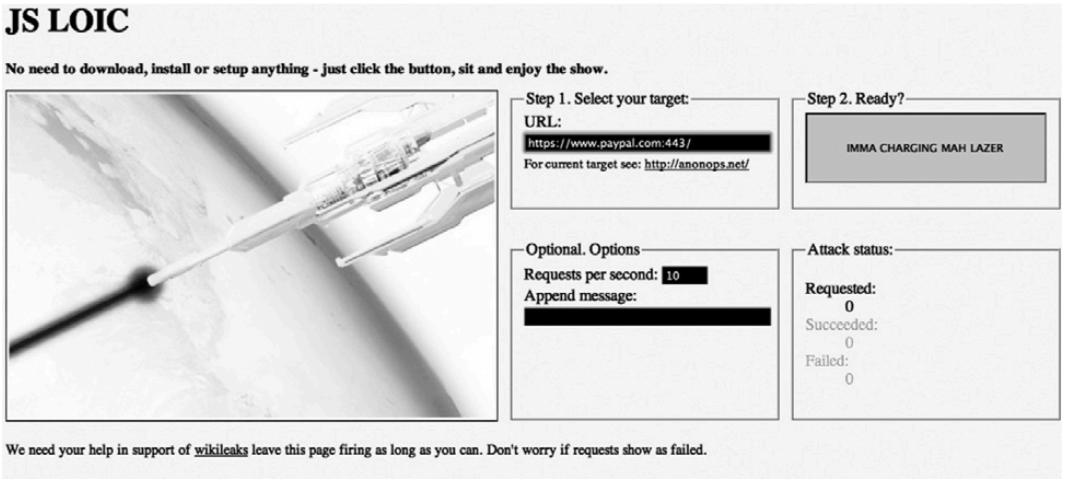


Figure 7. JS-LOIC, the Javascript version of the LOIC DDoS tool (Mansfield-Devine, 2011)

5.7. WikiLeaks.

The WikiLeaks phenomenon caused a firestorm of controversy in 2010 when they started to release a trove of leaked classified diplomatic cables – roughly 250,000 cables sent by 274 U.S. embassies to the government– stolen from the U.S. government, and after publishing confidential information and disclose Abu Graib' tortures. By 2011, both Anonymous and WikiLeaks were perceived as staunch promoters for free speech (Coleman, 2013; Hampson, 2012; Miró Llinares, 2012).

WikiLeaks acts on the basis of the liberal idea that transparency can be used in the service of limiting state power. It is the result of many years of collective work by individuals engaged with applying computer hacking to political causes and associated, almost entirely, with one figure, Julian Assange (Coleman, 2011; Ludlow, 2010).

Operation Payback of Anonymous contributed to raise awareness of the actions of WikiLeaks' opponents too. They proclaimed that their fight is the same: transparency (in copyright in Anonymous case) (Mansfield-Devine, 2011).

6. How hacker phenomena affect law enforcement?

The emergence of computer technologies and the growing threats created have originated a huge variety of challenges for law enforcement. With the continued growth of computer crimes there is a need to focus on new priorities and strategies to fight it (Taylor et al., 2017).

Hackers explore computers. It is not a crime when the computer is owned by the hacker or the hacker has licit access to that computer. In contrast, there is a system intrusion when the hacker does not have consent to utilize the computer, which is

considered illegal. During the interruption, information might be deliberately or accidentally changed, and depending on the effects of such data alteration, others crimes may be committed. For hackers, the essential difference between simple interruption and information change is the intent. The problem of this is that for law enforcement is regularly difficult to mark off the intent of an intruder. Malicious intent is not constantly vital for a crime to happen, yet straightforward carelessness or guiltless oversights can cause harm (Taylor et al., 2017).

Basically, understanding and anticipating hacker actions is hard for law enforcement in light of the fact that the law does not perceive a hacker's right to explore systems, data, and computer of others. Plus, when law enforcement deal with hackers who use their computer skills to commit cybercrimes there is a frequent issue that arises: perpetrators are in a foreign country (Brenner, 2010; Taylor et al., 2017).

6.1. Tracking and tracing cyberattacks: issues.

For an appropriate investigation on hackers, cyberattacks or computer crime it is necessary a good understanding of the roles and skills needed by the personal involved. According to Brown (2001) criminal investigation is "the process of legally gathering evidence of a crime that has been or is being committed" (as cited in Schmalleger and Pittaro, 2009, p. 439; Taylor et al., 2017).

To have different perspectives on how investigations are done, this section provides how both United States and Spain track and trace cyberattacks that can be done by hackers or cybercriminals. The process is the common for computer crimes in general.

6.1.1. United States vs. Spain.

For the most part, Unites States federal agencies are in charge of the fight against computer crimes. This is because the United States is a federal system in which "sovereignty is constitutionally divided between a central governing authority and constituent political units" product of the U.S. Constitution (Brenner, 2010). The resources at the national level are the following (Taylor et al., 2017):

1. *The Department of Justice* (DOJ). The mechanism within this agency that deals with computer crimes is The Computer Crime and Intellectual Property Section (CCIPS).
2. *The Federal Bureau of Investigation* (FBI). Protects the United States from cyber-based attacks and high-technology crimes.

3. *The National Security Agency* (NSA). Is in charge of planning and keeping up computerized coding systems intended to ensure the integrity of the U.S. data systems. It basically combats cyber threats.
4. *The Federal Trade Commission* (FTC). It is the federal government's primary mechanism for protecting consumers and to promote competition. The mechanism to combat computer crimes that exist with the agency is the Identify Theft Program.
5. *The Postal Service* (USPS). The part of the agency that helps deal with computer crimes is the Computer Crimes Unit.
6. *The Department of Energy* (DOE). The mechanisms that exist with the DOE to combat cybercrime are the Cybersecurity Division and the Cyber Incident Response and Recovery (CIRR).
7. *The Department of Homeland Security.* Installed the National Cybersecurity and Communications Integration Center (NCCIC) to protect critical infrastructure against computer crimes.
8. *U.S. Immigration and Customs Enforcement* (ICE). It has a Cyber Crime Unit, Child Exploitation Investigations Unit, Computer Forensics Unit, and an Information Technology and Administrations Unit.
9. *U.S. Secret Service*. It has a Crime Division and an Electronic Crime Brand to deal with computer crimes.

Hence, the dangers identified with computer crimes have turned into a developing concern to law enforcement at the state and local levels as well.

For the most part, the roles and responsibility of police in electronic investigations is equivalent to the physical crime investigations. The following roles exists (Schmalleger and Pittaro, 2009; Taylor et al., 2017):

- *First responders*. Usually they are patrol officers who are not dedicated electronic crime investigators. If they have basic training, may be able to safeguard a potential electronic crime scene for investigators. Nevertheless, they are prepared to abstain from contaminating a crime scene or destroying physical proof.
- *Investigators*. They are trained law enforcement officers who must have enough expertise to accumulate evidence, appreciate the crime, and discuss adequately with technical experts.
- *Digital analysts*. They are in charge of the complex analysis of evidence through computer forensic techniques.

- *Corporate security*. They are part of a corporation to secure the data assets of it and always consider the good of the corporation. They often cooperate with law enforcement.
- *Subject matter experts*. They are individuals with detailed knowledge on a highly specialized or uncommon topic. Investigators can turn to them to provide the necessary guidance.

With the roles of law enforcement clear, the preliminary investigation methods related with computer crimes ought to be executed as some other sort of crime. First of all, a warrant is needed. Once the warrant is obtained, the details of the search may be finalized. During a search there are some considerations to take (Taylor et al., 2017):

- *Priority concerns*. Investigators must assess the potential danger to themselves and then the particular dangers of working with electronic equipment.
- *Securing the scene*. This typically includes removing everyone away from computers and electronic devices.
- *Handling ongoing activity*. "The one certain rule is: if it off, leave it off". If the device is not off, there are different methodology to manage computers that are running. The learning and experience of the investigator have a great deal to do with how to continue.
- *Examining the crime scene*. Safety is always the first concern, followed by not alter the evidence. Then, once the scene is documented, the process of collecting and preserving evidence can begin.
- *Collection and preservation of evidence*. The National Institute of Justice[4] provides a procedure to follow in these cases.
- *Packing and transportation of evidence*. Computers are delicate gadgets that are touchy to temperature, humidity, static electricity, magnetic sources and physical shock, therefore, the moves made should not include, alter, or destroy information. It is likewise imperative to keep up the chain custody.
- *Storage of seized evidence*. The evidence must remain unaltered until it is analyzed. The National Institute of Justice[5] suggest a procedure too.

The following figure provides a flow chart detailing the process of collecting digital evidence discussed above.

[4] National Institute of Justice - Technical Working Group for Electronic Crime Scene Investigation, 2008. *Electronic Crime Scene Investigation: A Guide for First Responders*, 2nd ed.
[5] Ibíd.

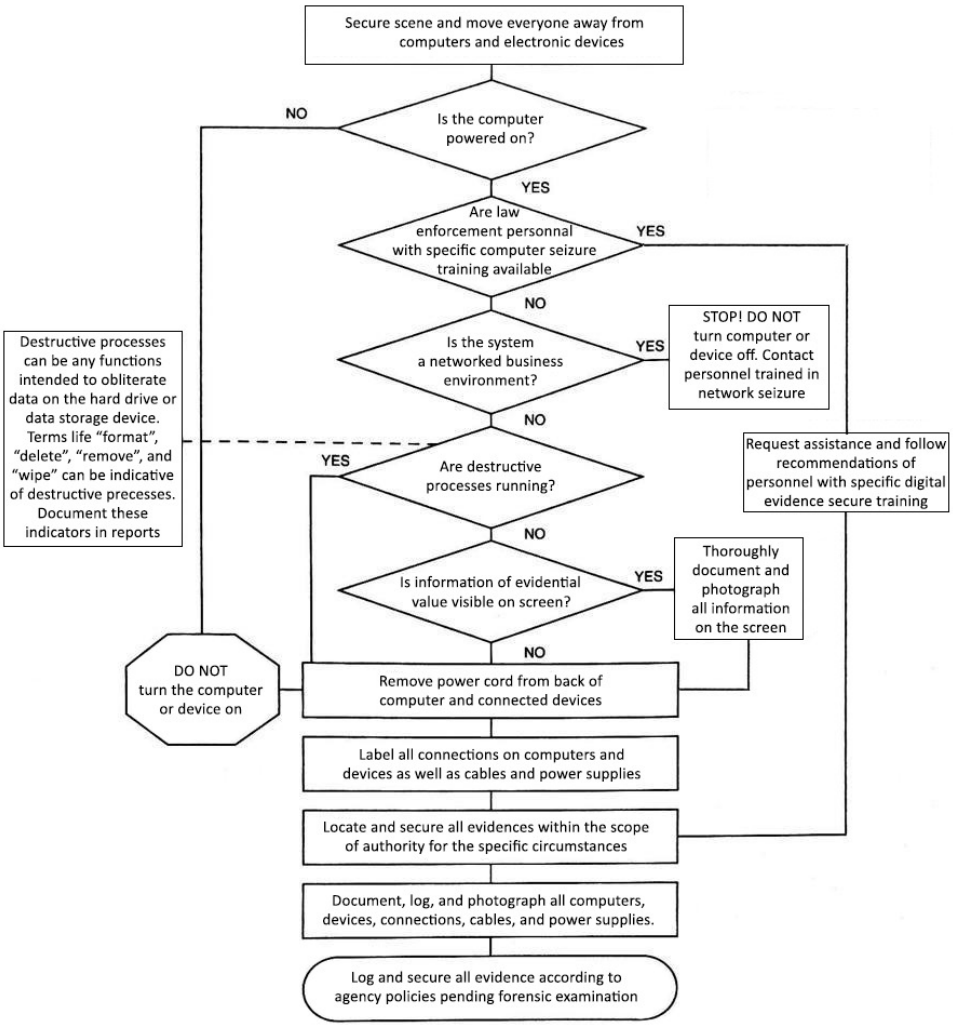


Figure 8. Collecting digital evidence flow chart (Taylor et al., 2017, p. 315)

Once all of this is done, the digital analyst examines the devices through computer forensic techniques. The field of digital forensics covers the examination of information stored on a physical medium. According to the National Institute of Standards and Technology (NIST), there are four phases of the digital forensics process or analysis:

1. **Collection**. Data is identified, labeled, recorded and acquired from all relevant sources.
2. **Examination**. Examining and extracting the data using automated and manual methods.
3. **Analysis**. Analyzing the extracted data using well documented standards.
4. **Reporting**. Describing the process and the conclusions reached after the analysis.

When the data is examined, it is made by creating a bit stream copy, also called a mirror or image. It reproduces every bit of information found in any device, including both active file and latent data. Figure 10 shows the complete process.

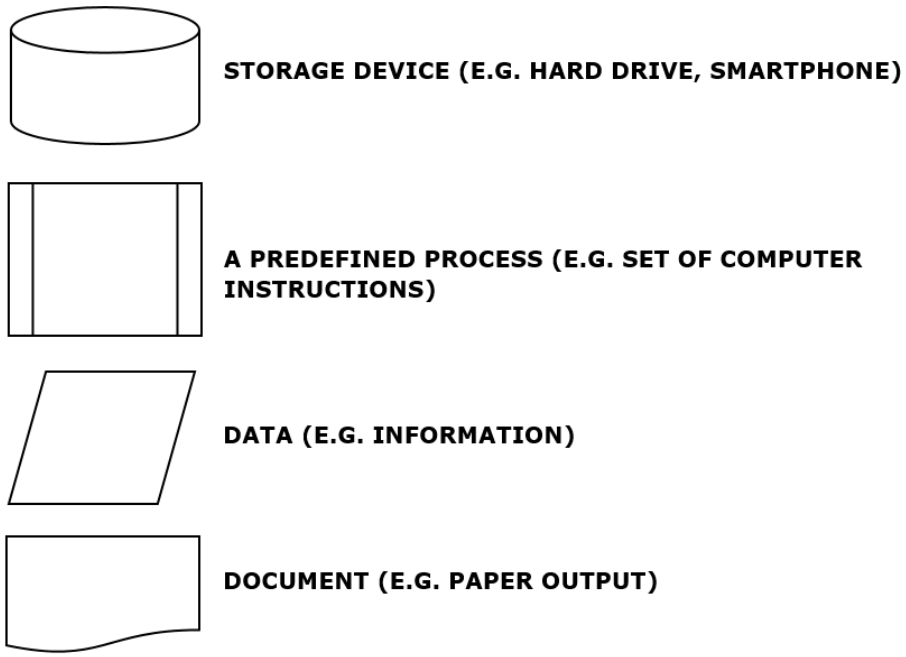
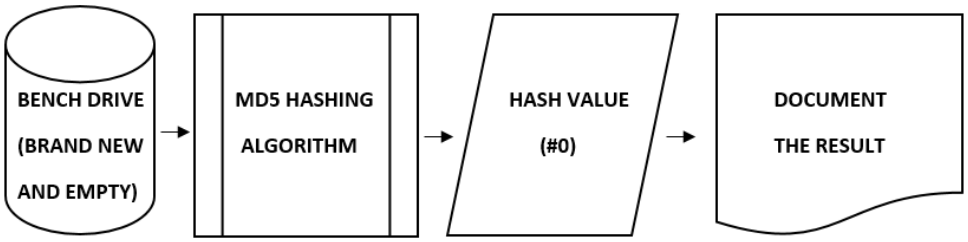
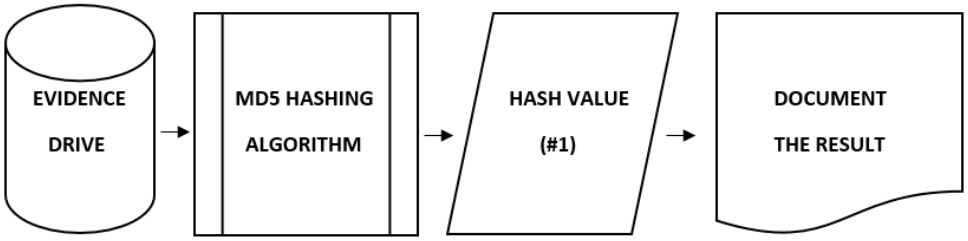


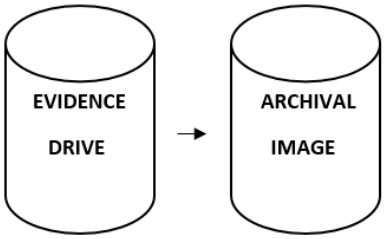
Figure 9. Flow chart symbols and definitions used for Figure 10 (Taylor et al., 2017, p. 334)



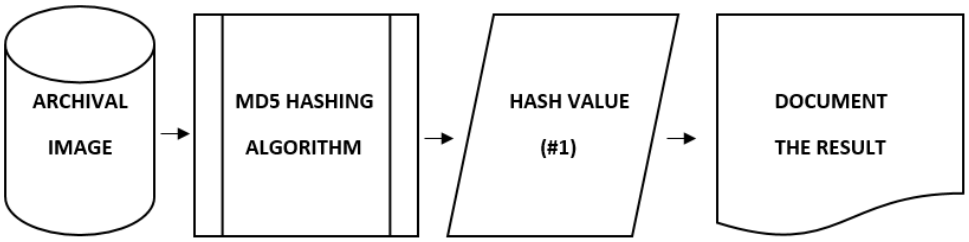
Step 1 is to verify mathematically the contents of the evidence drive. This value will prove that any future copies match the original exactly.



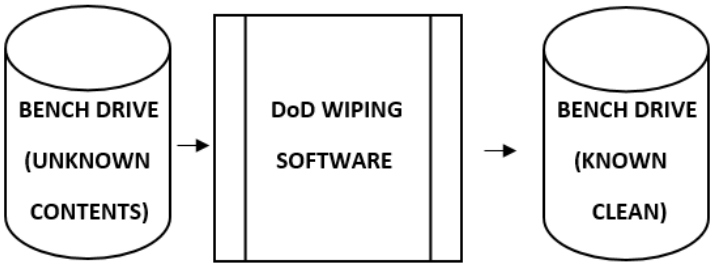
Step 2 is to create an exact “image” or bit-stream copy, of the evidence drive.



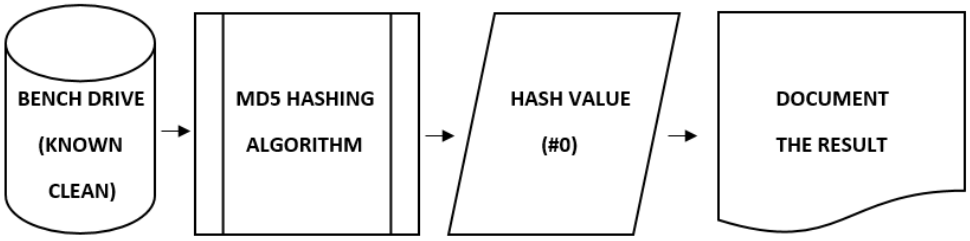
Step 3 is to verify that the image of the evidence drive is a true copy of the evidence drive. Note that the hash value produced (#1) is the same as the hash from the evidence drive.



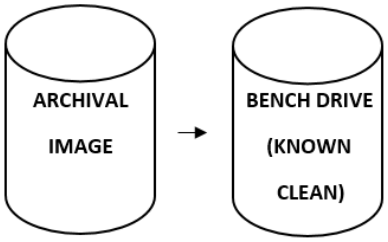
Step 4 is to wipe the bench drive to be used when analyzing the archival image



Step 5 is to create a hash of the clean bench drive and compare the value to the value of the drive when it was last known to be blank. Note that the hash value produced (#0) is the same as the hash from the blank bench drive.



Step 6 is to restore the archival copy (from Step 3) of the evidence drive to a blank bench drive (from Step 5).



Step 7 is to authenticate the restored image by calculating an MD5 hash and comparing that hash value to the hash of the evidence drive. Note that the hash value produced (#1) is the same as the hash from the evidence drive (#1).

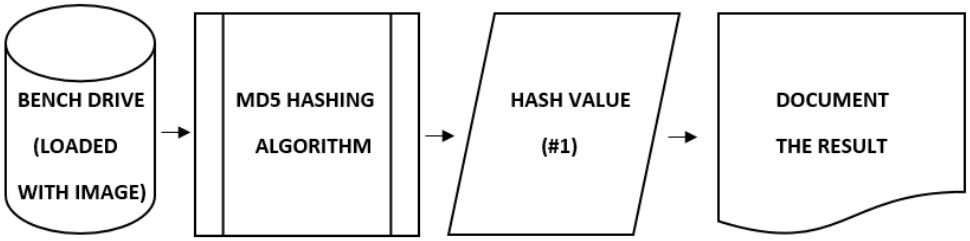


Figure 10. Summary of the process of imaging (Taylor et al., 2017, pp. 341-342)

The MD5 (Message-Digest Algorithm 5) hash that appears in the process of Figure 10 is the most commonly used hashing algorithm which is the key to authenticate digital evidence. “A hash is a unique numerical value calculated from the data in a digital data set (file, hard drive, software application, etc.)”. Essentially, it is like a “fingerprint” because two files cannot have the same hash value. By comparing hash values, the forensic analyst can check that the digital file being analysed is an authentic copy of the digital evidence and the data is unaltered (Taylor et al., 2017, p. 336).

In addition, if the investigator does not have a physical storage, like a computer, to analyze, the latent signs of the actions are extremely important for investigating purposes. The investigator has to realize how to follow an activity through the system and recognize the sources where the evidence can be found (Taylor et al., 2017).

In general, all networks can be described with the Open Systems Interface (OSI) model. It is a reference model for the protocols of a network made of seven layers that define the different phases through data must cross to travel from one device to another over a communication network. The model proceeds from the most concrete (layer 1) to

the most abstract (layer 7), but there are another two abstract layers (layers 8 and 9), each with a specific function (Table 3). The layers 8 and 9 are not part of the worldwide standard, just accentuate the role of human users and the policies that govern the investigations (Taylor et al., 2017).

9. Policies	Human	The rules, policies, and management controls that govern the actions of users.
8. User		The human being using the computer and network.
7. Application		Provides direct interaction with the user.
6. Presentation	Application services	Standardizes data transmission formats.
5. Session		Provides checkpoint, fall back, and encryption services.
4. Transport		Allows multiple simultaneous operations across a single network connection.
3. Network	Network services	Provides unique addressing for transmission across different networks.
2. Data link		Assembles bits into packets, provides error correction, and flow control.
1. Physical		Provides a path for the transmission of bits

Table 3. Layers of the investigation from the OSI model (Taylor et al., 2017, p. 322)

Specific types of logs are useful too. A log file is a sequential recording in a file or in a database of all the events (events or actions) that occur in an operating system or other software. It is an evidence of the performance of the system, this is why many operating systems, software frameworks and programs include a logging system. These logs, use identifiers to match networks transactions with the machines involved, which are often associated with a level of the OSI model. Some of them, useful to trace network evidence, are the following (Taylor et al., 2017):

- *Mac address*. The media access control (MAC) address is a 48-bit identifier reported in hexadecimal couplets that corresponds uniquely to a network card or network device. It also known as physical address. Within the OSI model, MAC addresses are used in the medium access control protocol sublayer of the data link layer (layer 2).
- *IP address*. The IP address is a logical number that identifies any device, that is part of a TCP/IP-based network, connected to a computer network that uses the

Internet Protocol. Is a binary number made up of bits. Within the OSI model, the IP is associated with transactions at the network layer (layer 3).

- *DNS*. The domain name system (DNS) is a protocol that allows converting alphabetic names into numeric IP addresses. It is a helper service for the network layer (layer 3) in the TCP/IP systems.
- *PPP*. The Point-to-Point Protocol (PPP) is a data link layer (layer 2) used to establish a direct connection between two nodes. Figure 11 below shows the PPP.

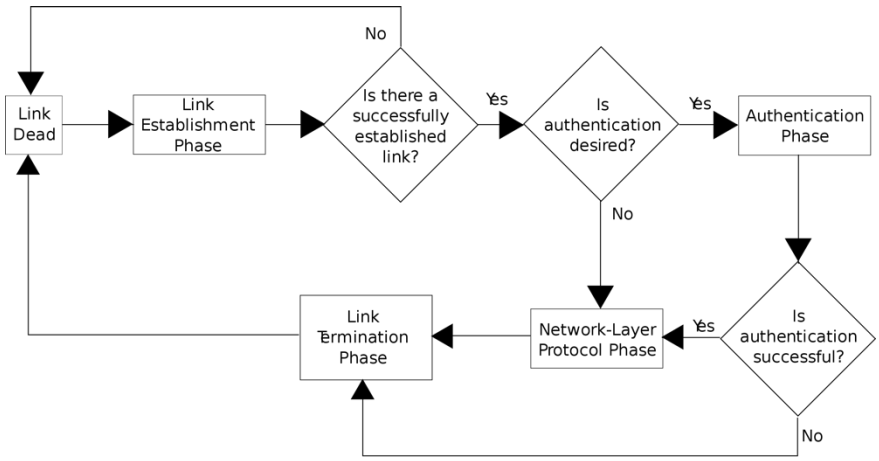


Figure 11. PPP protocol (Viviano, 2008)

On the other side, Spain does not count with as many entities as United States to combat cybercrimes. Cybercrime encompasses a broad spectrum of behaviors related to computing and communications. As set out in the Convention on Cybercrime signed in Budapest (Hungary) in 2001, it is possible to group cybercrime in four major areas: the dissemination of child pornography, intellectual property-related offences, and frauds and scams; naming these three categories as cybercrime itself. Additionally, it recognizes a fourth category called criminal offences related to computer systems intrusion and the theft or destruction of data, understanding as such what is commonly called “hacking” (Lorenzana González, n.d.).

To combat all of them, there are two basic organisms: (1) the *Grupo de Delitos Telemáticos* (GDT) which is part of the *Unidad Central Operativa* (UCO) of *Guardia Civil*, and (2) the *Brigada de Investigación Tecnológica* (BIT) which is part of the *Policía Judicial* of the *Cuerpo Nacional de Policía* (CNP).

The GDT is an agency specialized in the investigation of those crimes that use the new technologies or Internet for its commitment. Its main functions are the identification and detection of computer-related crime on the Internet, as well as the research related to cybercrimes. Also, it promotes the safe use of new technologies in order to, in the near

future, help to minimize the impact of this type of crime. The GDT has *Equipos de Investigación Tecnológica* (EDITEs) in each of the provinces of Spain (Guardia Civil – Grupo de Delitos Telemáticos, 2011).

The BIT is the police unit designed to respond to the challenges posed by new forms of crime. Their mission is to obtain the evidence, prosecute offenders and bring them to justice. Their main functions are: (a) the realization of particularly complex investigations, (b) the coordination of operations involving different higher headquarters, (c) the training of the personnel of the national police and other foreign police, and (d) international representation and coordination of investigations that originate in other countries.it is formed by seven specialized squads (Cuerpo Nacional de Policía – Brigada Central de Investigación Tecnológica, 2019):

- Two groups of child protection dealing with offences related to child pornography.
- A group of fraud in the use of telecommunications, which investigates threats, slanders and false accusations committed through the Internet.
- Two groups of fraud on the Internet, one of them specialized in phishing and the other specialized in fraudulent sales and Internet auctions.
- A group of intellectual property that investigates piracy crimes.
- A group of logic security that investigates intrusions, hacking and data theft.

In addition to the BIT, the CNP count with specialized groups in technological crime which are developed by higher headquarters (CNP – Brigada Central de Investigación Tecnológica, 2019).

Computer research in Spain starts with the knowledge of an offence and ends with the submission of incriminating evidence of the criminal act to the judge. Based on the computer crime, the circumstances surrounding it, and the technologies employed, law enforcement can proceed in various ways. However, it is possible to establish a set of common principles that are applicable to all those investigative processes and guidelines. We can distinguish four stages (Lorenzana González, n.d.):

1. *Prosecution*. Assuring the evidence from the crime scene and the data that can provide the victims to the research.
2. *Investigation*. Aimed at trying to find electronic evidence related to the computer crime. The investigator has to reconstruct the criminal process of the offender and has to understand the overall process of the computer crime.
3. *Securing the evidence*. This includes the seizure of the technological devices of the suspect, using technical computing devices that guarantee this process.
4. *Construction of incriminating evidence*. The investigator, supported by forensic tools, brings together all the electronic evidence, giving rise to a technical report.

Based on these four basic stages, when the GDT or the BIT collect digital evidence during a search and seizure, data is examined later by creating a bit stream copy, also called a mirror or image, which produce a unique hash as explained earlier. According to one expert of GDT from Castellón, Spain, they use a cloner to create the image, but they can use specific software too. The image is made of the hard drive if it can be removed from the device. If not, the image would be of all the device. When there is no physical device to analyze, they need to use other techniques and tools in order to found digital evidence. It is usual to use the following (Lorenzana González, n.d.):

- *Money transactions*. They often track and trace the money transactions of the suspects to found evidence that match with the timeline of the computer crime. Also, it is useful to look into the bank account and the payment terminal too. The problem comes when they have to deal with cryptocurrency because of the value of it.
- *IP address*. To trace an IP which is not hidden, the ISP need to be identified and then the customer data requested which can help to locate the physical point of connection to the Internet. This is useful but it is not always reliable.
- *Domains and websites*. In cases where information is accessible, it is just necessary to perform a simple request and obtain contact and payment data given in the registration process. This data is stored in the ISPs but if they do not have a logging system there is no way to identify the devices linked to the crime.
- *E-mails and social networks*. It is necessary to resort to the e-mail service providers, since they store the identification data of the account. The data of the connection (IP, date and time) is stored in the registration process too.

7. Cyber-Laws.

7.1. United States.

As computers have become the new tools that are used to commit both computer-based crimes and computer-focused crimes, new laws are necessary to deal with it. Due to the fact that the United States has had a lot of involvement with cybercrime, it has the most extensively developed set of cybercrime laws in the world. Made out of 52 jurisdictions, each U.S. state in addition to the District of Columbia has its own cybercrime law in relation to hacking, unauthorized access, computer trespass, viruses, malware, Denial of Service attacks, ransomware and computer extorsion, as does the U.S. federal system (Brenner, 2010).

From a legal perspective, hacking is practically equivalent to the crime of trespass; the offender violates use restrictions on property. This notion shaped how U.S. law deal with this type of activity (Brenner, 2010).

Most computer hacking charges are prosecuted under the Computer Fraud and Abuse Act (CFAA) (18 U.S.C. §1030), which covers a wide range of sorts of computer crimes and lately has been used in all respects forcefully by the government. Example of this is the case of Aaron Swartz[6], the golden boy of the Internet. His prosecution was based on the premise that he downloaded a huge number of pages of academic journal articles from JSTOR by getting unauthorized access to the computer network at the MIT, even when the supposed victim does not consider the use unauthorized. Swartz's actions were expected to create a statement and the Government refused to let the matter, since they wanted to make an example with him and the trial date was set, but before that could be done, Aaron committed suicide at the age of 26 on January 11, 2013 (Ludlow, 2013).

The CFAA initially was established by Congress in 1986 as a reaction to the developing utilization of computers, especially by the federal government, and the developing risk of computer crimes. Yet, as computer crimes kept on developing in modernity and as prosecutors picked up involvement with the CFAA, the CFAA required further amending, which Congress did in 1988, 1989, 1990, 1994, 1996, 2001, 2002, and 2008 (Office of Legal Education Executive Office for United States Attorneys, 2010).

Today, under the statute, seven types of criminal activity (outlined in Table 4 below) are prohibited as they relate to “protected computers”, which are defined as (Computer Fraud and Abuse Act 1984, s.1030(e)(2)):

> “a computer–
>
> (A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or
>
> (B) which is used in or affecting interstate or foreign commerce or communication of the United States”.

Offense	Section	Sentence*
Obtaining national security information.	(a)(1)	10 (20) years

[6] Aaron Hillel Swartz (November 8, 1986 – January 11, 2013) was an American computer programmer, entrepreneur, writer, political organizer, and Internet hacktivist.

Accessing a computer and obtaining information.	(a)(2)	1 or 5 (10)
Trespassing in a government computer.	(a)(3)	1 (10)
Accessing a computer to defraud and obtain value.	(a)(4)	5 (10)
Intentionally damaging by knowing transmission.	(a)(5)(A)	1 or 10 (20)
Recklessly damaging by intentional access.	(a)(5)(B)	1 or 5 (20)
Negligently causing damage and loss by intentional access.	(a)(5)(C)	1 (10)
Trafficking in passwords.	(a)(6)	1 (10)
Extortion involving computers.	(a)(7)	5 (10)

Table 4. Summary of CFAA penalties (Office of Legal Education Executive Office for United States Attorneys, 2010, p. 3)

*Note *The maximum prison sentences for second convictions are noted in parentheses.*

In addition to the CFAA, there are other laws that deal with computer hacking offenses. (1) The Electronic Communications Privacy Act protects stored messages. Under the ECPA, accessing computer messages without authorization constitutes a federal crime. (2) Unlawfull access to stored communications (18 U.S.C. §2701), which punishes the utilization of a computer to get to someone else's "electronic communication service" where the individual has their email or voicemail saved. It is a felony when the unauthorized access to an individual's voice message or email is accomplished for benefit or monetary profit. And (3) the CAN-SPAM Act (18 U.S.C. §1037) is expected to arraign individuals who distribute a lot of unsolicited commercial email (spam) (Pate and Johnson, 2018).

Besides, there are other federal statutes that deal with criminal activity involving computers like: The Pen/Trap Statute, the Wiretap Statute (Title III), the USA PATRIOT Act/USA FREEDOM Act, the Communication Assistance of Law Enforcement Act (CALEA), the Economic Espionage Act, the Copyright Act and the Family Entertainment and Copyright Act (Taylor et al., 2017).

7.2. Spain.

When it comes to Spain's law, computer-related crime is not referred to as a special type of crime, but there are several legislations related to this type of behavior:

- Ley Orgánica de Protección de Datos de Carácter Personal.
- Ley de Servicios de la Sociedad de la Información y Comercio Electrónico.

- Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal.
- Ley General de Telecomunicaciones.
- Ley de Propiedad Intelectual.
- Ley de Firma Electrónica.

Further to these legislations, the Spanish Criminal Code include plenty of illicit conduct related to cybercrime. The next table sums them.

Offense	Article(s)	Sentence
Threats.	169	1 to 5 years of prison
Sexual exploitation and corruption of minors.	189	1 to 5 years of prison
Discovery and disclosure of secrets.	197	1 to 4 years of prison and 12 to 24 months of fine
Computer intrusion.	197 bis 1	6 months to 2 years of prison
Interception of transmissions of computer data.	197 bis 2	3 months to 2 years or 3 to 12 months of fine
Production or facilitation to third parties for the realization of the above offences	197 ter	6 months to 2 years or 3 to 18 months of fine
Computer fraud.	248	6 months to 3 years of prison
Improper use of any telecommunications without the consent of its holder terminal.	256	3 to 12 months of fine
Computer sabotage.	264	6 months to 3 years of prison
Against intellectual property.	270-272	6 months to 4 years of prison and 12 to 24 months of fine
Against industrial property.	273-277	6 months to 2 years of prison and 12 to 24 months of fine
Misleading advertising.	282	6 months to 1 year of prison or 12 to 24 months of fine

Table 5. Summary of Spanish Criminal Code penalties (Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, Reforma 2015)

8. Hackers today: statistics.

What is clear is that cybercrime today and, in the future, will continue to escalate and become more virulent than it is. In the same way, hackers, through the years, have experimented a change since today. The hyperevolution of technology and networking has contributed to fuel the figure of the hacker but also the cybercrime. The short history of computer crime has demonstrated that offenders are quicker and more versatile than law enforcement when it comes to technology.

According to the Internet Crime Complaint Center (IC3) of the Federal Bureau of Investigation (FBI), in the United States there are approximately 284,000 complaints each year with 4,063,933 complaints about cybercrime reported since inception (2013-2017). In 2017 there were a total amount of 383,473 victims. On the other hand, according to the *Ministerio del Interior* and the *Sistema Estadístico de Criminalidad*, in Spain there were 257,982 complaints about cybercrime reported between 2014 and 2017. The following figures show it.

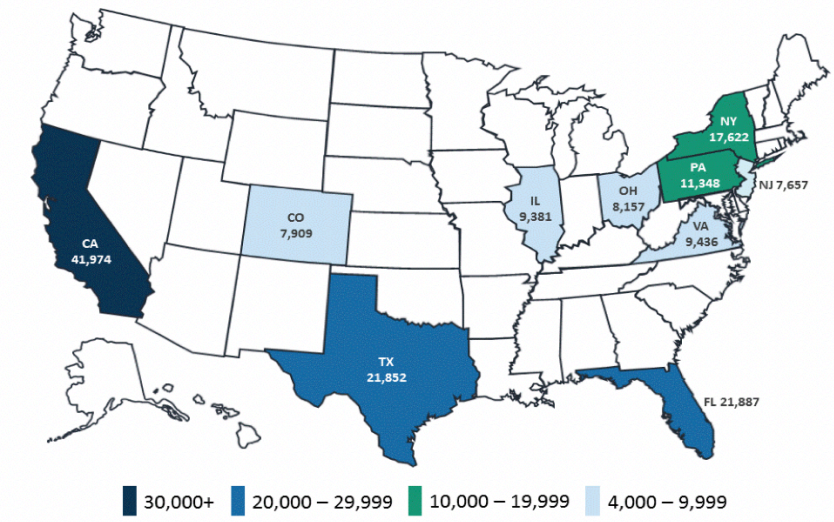


Figure 12. Top 10 states in cybercrime by victim loss (FBI – IC3, 2017, p. 19)

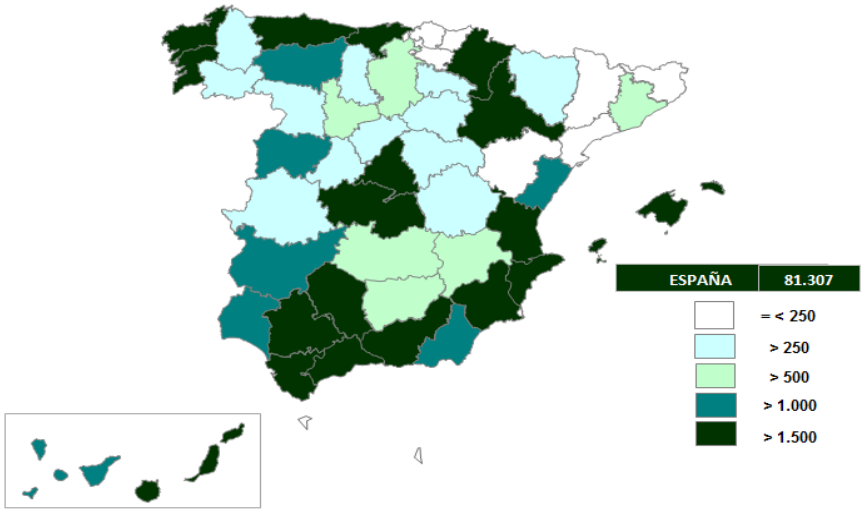


Figure 13. Cybercrimes reported by province (Ministerio del Interior, 2017, p. 38)

As it is obvious, there is a category for hacker attacks in the crime types that are reported each year to both the IC3 and the *Ministerio del Interior*. This is because, as explained earlier, hacker attacks are considered cybercrime by law enforcement and therefore liable to prosecution. Still, compared to another type of cybercrimes, there is a low percentage, at least in Spain, of hacker attacks –data and system interference– (see Figure 14).

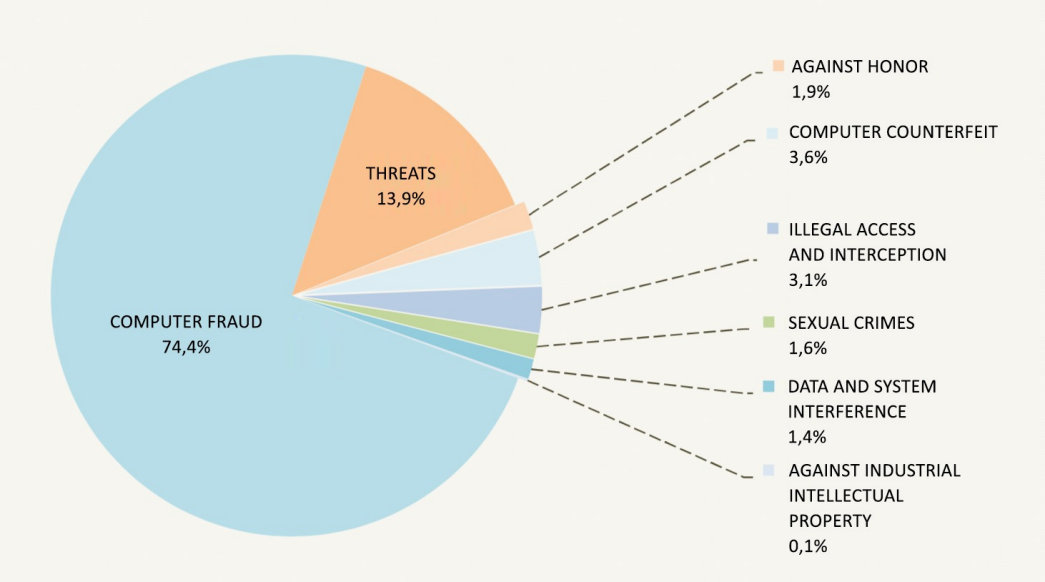


Figure 14. Percentage of cybercrimes reported in 2017 (Ministerio del Interior, 2017, p. 37)

9. Conclusions.

Finally, after gather together all the information available about the subject what we are concerned about and made a specific research, we can reach some conclusions:

FIRST: Despite the fact that everyone thinks that hackers are bad people who do bad things, they are not cybercriminals or computer criminals. The word is used wrongly. There is a difference between hackers and cybercriminals. Yet there is not a universal definition about the hacker. We can consider a hacker a person with developed skills in programs and algorithms who possess a desire to learn new things to overcome a technological challenge.

SECOND: Although people can think that hackers and cybercriminals can have similar motivations, they are very different. The basic difference between them is that hackers hack into things because they have an intense desire to understand how technology works and to identify their limits. Cybercriminals, on the other side, are often motivated by monetary benefit and they are not keen on technology or knowledge.

THIRD: The Internet has turned into an incredible power in this day and age. The access to the Internet has transformed numerous parts of life and some changes have originated new crimes in recent years, due to the manner in which Internet users handle themselves. Cyberspace allows cybercriminals to exist and flourish, which at the same time presents a new challenge for criminologists. This is why now researchers try to apply to cybercrimes the several theories that have been proposed to explain crime in the course of recent years.

FOURTH: Hacktivism emerged in the mid 1990s in the context of the emerging anti-globalization movement. Today, it is the popular way of protest on the Internet, delivered by taking forward the breakdown a technological-social distinction in computer and network technologies and applying it to politics.

FIFTH: As we saw in this paper, it is often difficult to track and trace cybercrimes because of the crime itself and the absence of resources and training. Besides, cybercriminals in one country can target victims in a different country. This complicates law enforcement job because (1) they are territorially based, and (2) they cannot rely on techniques they ordinarily use. This is why this type of crime creates two challenges: (1) collecting evidence from abroad, and (2) obtaining custody of a suspect who is abroad. This is why it is usually very hard or even impossible for them to apprehend cybercriminals who are located in a place different to the place where they are investigating.

SIXTH: After all, there is still a dichotomy in our society regarding hackers and hacking. This is unlikely to change in the near future due to the perception of hackers in the actual

society and the existing laws against this behavior. Lately, governments have demonstrated their position in relation to this topic by making laws that has been used very aggressively despite the fact that hacking represents a very low percentage of cybercrime as a whole. And still, this type of behavior is not going down. Since technology exists and changes every day, hackers will too.

10. References.

ARPANET, 1977. *ARPANET logical map, March 1977*. [electronic print] Available at: https://en.wikipedia.org/wiki/File:Arpanet_logical_map,_march_1977.png [Accessed 8 April 2019].

Bachmann, M., 2010. The Risk Propensity and Rationality of Computer Hackers. *International Journal of Cyber Criminology*, [e-journal] 4 (1&2), pp. 643–656. Available through: http://www.cybercrimejournal.com/michaelbacchmaan2010ijcc.pdf [Accessed 8 April 2019].

Brenner, S. W., 2010. *Cybercrime: Criminal threats from cyberspace*. Westport, Connecticut: Praeger.

Coleman, G., 2013. Anonymous in Context: The Politics and Power behind the Mask. [pdf] Waterloo, Ontario, Canada: Centre for International Governance Innovation. Available at: https://www.cigionline.org/publications/anonymous-context-politics-and-power-behind-mask

Computer Fraud and Abuse Act (18 U.S.C. §1030) 1984. Washington D.C.: United States.

Cuerpo Nacional de Policía – Brigada Central de Investigación Tecnológica, 2019. *B.C.I.T. - ¿Quiénes somos?* [online] Available at: https://www.policia.es/org_central/judicial/udef/bit_quienes_somos.html [Accessed 9 April 2019].

Cuerpo Nacional de Policía – Brigada Central de Investigación Tecnológica, 2019. *B.C.I.T. – Actuaciones* [online] Available at: https://www.policia.es/org_central/judicial/udef/bit_funciones.html [Accessed 9 April 2019].

Cuerpo Nacional de Policía – Brigada Central de Investigación Tecnológica, 2019. *B.C.I.T. - Funciones* [online] Available at: https://www.policia.es/org_central/judicial/udef/bit_funciones.html [Accessed 9 April 2019].

Discovery, 2009. Hackers Versus Cyber Criminals [video online] Available at: https://www.youtube.com/watch?v=w0u_7DHuuNg [Accessed 8 April 2019].

FBI & Internet Crime Complaint Center, 2017. *2017 internet crime report*. [online] Available at: https://pdf.ic3.gov/2017_IC3Report.pdf [Accessed 9 April 2019].

FockeWulf FW 190, 2015. *LOIC-0 screenshot in Windows 10*. [electronic print] Available at: https://commons.wikimedia.org/wiki/File:LOIC-0.png [Accessed 8 April 2019].

Gold, S., 2014. *Get your head around hacker psychology*. *Engineering & Technology*, [e-journal] 9 (1), pp. 76-80. http://dx.doi.org/10.1049/et.2014.0111

Gradín, C. (compiler), 2004. *:(){ :|:& };: Internet, hackers y software libre*. Buenos Aires: Editora Fantasma.

Guardia Civil – Grupo de Delitos Telemáticos, 2011. *La unidad*. [online] Available at: https://www.gdt.guardiacivil.es/webgdt/la_unidad.php [Accessed 9 April 2019].

Halbert, D., 1997. Discourses of Danger and the Computer Hacker. *The Information Society*, [e-journal] 13 (4), pp. 361-374. https://doi.org/10.1080/019722497129061

Hampson, N. C. N., 2012. Hacktivism: A New Breed of Protest in a Networked World. *Boston College International and Comparative Law Review*, [e-journal] 35 (2), pp. 511-542. Available through: https://lawdigitalcommons.bc.edu/cgi/viewcontent.cgi?article=1685&context=iclr [Accessed 8 April 2019].

Holt, T. J., 2007. subcultural evolution? examining the influence of on- and off-line experiences on deviant subcultures. *Deviant Behavior*, [e-journal] 28 (2), pp. 171-198. https://doi.org/10.1080/01639620601131065

Holt, T. J. and Kilger, M., 2012. *Know Your Enemy: The Social Dynamics of Hacking*. [pdf] Available at: https://www.honeynet.org/sites/default/files/files/Holt%20and%20Kilger%20-%20KYE%20-%20The%20Social%20Dynamics%20of%20Hacking.pdf

Jordan, T., 2008. *Hacking: Digital media and society series*. Cambridge: Polity Press.

Lanier, M. M., Henry, S., and Anastasia, D., 2018. *Essential Criminology.* 4th ed. New York, NY: Routledge.

Levy, S., 2010. *Hackers: Heroes of the computer revolution*. 1st ed. Sebastopol: O'Reilly.

Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.

Lorenzana González, C., n.d. La investigación de delitos telemáticos por la guardia civil, y sus capacidades al servicio del Ministerio Fiscal. [pdf] Available at: https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/ponencia%20escrita%20Sr%20Lorenzana.pdf?idFile=e14972b0-5d5a-40d6-8940-f1ef8152c3f9 [Accessed 8 April 2019].

Ludlow, P., 2013. Hacktivist witch hunt. *The Nation*, [e-journal] 2013, pp. 23-26. Available through: https://www.thenation.com/issue/december-2330-2013/ [Accessed 8 April 2019].

Mansfield-Devine, S., 2011. Anonymous: serious threat or mere annoyance? *Network Security,* [e-journal] 2011 (1), pp. 4-10. https://doi.org/10.1016/S1353-4858(11)70004-6

Mansfield-Devine, S., 2011. Hacktivism: assessing the damage. *Network Security,* [e-journal] 2011 (8), pp. 5-13. https://doi.org/10.1016/S1353-4858(11)70084-8

Ministerio del Interior, 2017. *Estudio sobre la cibercriminalidad en España*. [online] Available at: http://www.interior.gob.es/documents/10180/8859844/Informe+2017+sobre+Cibercriminalidad+en+España.pdf/a9f61ddb-3fcf-4722-b9d8-802a424a1a70 [Accessed 9 April 2019].

Miró Llinares, F., 2012. *El cibercrimen: Fenomenología y criminología de la delincuencia en el ciberespacio*. Madrid: Marcial Pons.

Office of Legal Education Executive Office for United States Attorneys, 2010. *Prosecuting Computer Crimes*. [pdf] United States: Department of Justice. Available at: https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf [Accessed 9 April 2019].

Pate and Johnson, 2018. *Computer hacking laws*. [online] Available at: https://www.pagepate.com/experience/criminal-defense/federal-crimes/federal-computer-crimes/ [Accessed 25 April 2019].

Rogers, M. K., 2005. *The Development of a Meaningful Hacker Taxonomy: A Two Dimensional Approach*. [pdf] West Lafayette, IN: Center for Education and Research in Information Assurance and Security, Purdue University. Available at: https://www.cerias.purdue.edu/assets/pdf/bibtex_archive/2005-43.pdf

Schmalleger, F. & Pittaro, M., 2009. *Crimes of the internet*. Upper Saddle River, NJ: Prentice Hall.

Sykes, G. M., and Matza, D., 1957. Techniques of Neutralization: A Theory of Delinquency. *American Sociological Review*, [e-journal] 22 (6), pp. 664-670.

Taylor, R. W., Fritsch, E. J., Liederbach, J., Saylor, M. R., and Tafoya, W. L., 2017. *Cyber crime and cyber terrorism.* 4h ed. Hoboken, NJ: Pearson.

The Christian Science Monitor, 2017. Hacking's next generation [video online] Available at: https://www.youtube.com/watch?v=f9_95pKzts0 [Accessed 8 April 2019].

Van Beveren, J., 2001. A conceptual model of hacker development and motivations. *Journal of E-Business*, [e-journal] 1 (2), pp. 1-9. Available through: https://pdfs.semanticscholar.org/d087/07b80bbd035ea81a95bf50beab60a5226a65.pdf?_ga=2.187732648.125749872.1558548570-575363398.1558548570 [Accessed 8 April 2019].

Viviano, J., 2008. *PPP protocol.* [electronic print] Available at: https://commons.wikimedia.org/w/index.php?curid=3530407#file [Accessed 8 April 2019].

Voiskounsky, A. E. and Smyslova, O. V., 2003. Flow-Based Model of Computer Hackers' Motivation. *CyberPsychology & Behavior*, [e-journal] 6 (2), pp. 171-180. Available through: https://www.researchgate.net/publication/6993559_Flow-Based_Model_of_Computer_Hackers'_Motivation [Accessed 8 April 2019].

Wark, M., 2006. Hackers. *Theory, Culture & Society*, [e-journal] 23 (2–3), pp. 320-322. https://doi.org/10.1177/0263276406065779