Available online at www.ijournalse.org

Emerging Science Journal

Vol. 4, Special Issue "IoT, IoV, and Blockchain", 2020

Cybercrime is Very Dangerous Form of Criminal Behavior and Cybersecurity

Siniša Franjić [a*]

[a] *Faculty of Law, International University of Brcko District, Brcko, Bosnia and Herzegovina*

Abstract

Computer crime is a form of criminal behavior in which the use of computer technology and information systems is manifested as a mode of crime or the computer is used as a means or purpose of perpetration with which is producing some relevant criminal consequence. Computer crime is also an unlawful violation of property in which computer data is intentionally altered (manipulated by a computer), destroyed (computer sabotaged) or used in conjunction with hardware (theft of time). Objective of this paper is consideration of using new computer technology in everyday life. Unfortunately, some users using new technology for criminal acts. For Analysis, author use official resources from books, scientific papers and online resources. Even though it is a new technology, police and justice successfully deal with different types of computercrimes.

Keywords:

Cybersecurity; Crime;

Threats; Hacking.

Article History:

Received:	31	October	2019
Accepted:	10	June	2020
Published:	30	September	2020

1- Introduction

New times bring new crimes. Humanity today is experiencing a time that is obsolete tomorrow in the technological-scientific sense. Revolutionary information achievements and at the same time their imaginative misuse pervade almost every sphere of human life and work. It is common knowledge that all developed countries in the world are primarily concerned with knowledge and capital, and only afterwards, labor, capital and other physically tangible benefits are the primary factors of their development and well-being. We are today witnessing a historical turning point that transformed the globalization division of the world into rich and poor into the same globalization division of those who possess knowledge and information and those who do not possess that knowledge or information without completely losing geographical position of state. People have become aware of the fact that information alone is a prerequisite for the dissemination of knowledge, and that knowledge is a major factor, that is, a prerequisite for any further development and prosperity of every developed society or state. The visible interest of all or even more developed countries in investing in "acquiring" and updating their IT staff should not be surprising. It is also not surprising that a large number of studies and specialized schools have been opened with a view to achieving IT literacy, and its standardization and even development within the borders of individual geographical regions, whether it is only in the territory of a particular country or in an area covering more than one country (such as European Union). It is important to note that investments in this direction are not small. The funds invested are very profitable, especially in the area of IT innovations that bring about changes in communication and social information, which is reflected in new knowledge and products that are being marketed on the world market every day.

Among these economic and social abuses, abuse from the domain covered by cybercrime is the most prevalent today. The hidden privacy of the perpetrators, who can easily reach the outermost places with the help of phones and PCs, and entry into the computer systems of economic and governmental organizations and institutions for the purpose of harm or obtaining benefits are the greatest obstacle to all bodies and organizations concerned with preventing this new types of crime whose development can be compared with the development of information technology. In this

[*] **CONTACT**: Sinisa.franjic@gmail.com

DOI: http://dx.doi.org/10.28991/esj-2020-SP1-02

way, computer crime has globalized. With the development of information technologies and their application in the criminal milieu, as well as modifications and adaptations of this technology (by the perpetrators), cybercrime is subject to daily changes, extending to those areas where it was not present yesterday. Analogous to that, cybercrime methods and techniques also become obsolete with the obsolescence of information technology equipment. Sophisticated tools require less user knowledge, and with the development of each newcomer to information technology, new methods and techniques, more sophisticated tools and a more sophisticated approach to computer crime are emerging. The effects of cybercrime are becoming more and more dangerous every day, especially when the goals are the privacy of individuals, entire branches of management and even the national security of countries [1].

Information And Communications Technology (ICT) is an integral part of our daily lives. Whether people have a computer at home, use online banking services or simply receive electricity supplies, the community's reliance on technology is increasing. A safe and secure online environment enhances trust and confidence and contributes to a stable and productive community.

Government and business also take advantage of opportunities for economic development through increased use of information technology.

The AFP sees the increasing use and dependence on technology as one of the major influences on the domestic and international law enforcement operating environment.

In Australia, the term 'cybercrime' is used to describe both:

- Crimes directed at computers or other information communications technologies (ICTs) (such as computer intrusions and denial of service attacks), and
- Crimes where computers or ICTs are an integral part of an offence (such as online fraud.

Just as the internet and other new technologies are opening up tremendous possibilities, they also provide opportunities for criminals to commit new crimes and to carry out old crimes in new ways. On the evidence available, it is clear that the number, sophistication and impact of cybercrimes continues to grow and poses a serious and evolving threat to Australian individuals, businesses and governments.

Online, criminals can commit crimes across multiple borders in an instant and can target a large number of victims simultaneously. Tools that have many legitimate uses, like high speed internet, peer to peer file-sharing and sophisticated encryption methods, can also help criminals to carry out and conceal their activities.

The AFP is responsible for detecting, preventing, disrupting, responding to and enforcing cybercrime offences impacting the whole of the Australian economy. It focuses on investigating cybercrime threats against Commonwealth Government departments, critical infrastructure and information systems of national significance, with a key element being the banking and financial sector. The AFP is guided by Commonwealth priorities for combatting cybercrime.

In general, the investigation of fraud against an individual is a state police responsibility. However, where there is a crossover between the investigation of a fraud against an individual and the investigation of an organised attack against critical banking systems, the AFP will work together with the local jurisdiction and the banking and finance industry.

The AFP also works closely with State and Territory Police and international policing agencies in the fight against all types of cybercrime [2].

While the benefits of the Internet and other forms of computer networks are streamlining financial institutions, the same institutions are often among the first institutions to be affected by Cybercrime and Cybersecurity issues due to the financial incentives as well as their strategic place in each nation’s infrastructure and economy. We must look not only at the efficiency, but also at the negative aspects of the use of technology by financial institutions. Consumers as well as businesses must be well informed about conducting transactions in the safest manner possible. The nature of the Internet is cross-border, and thus Cybercrime and Internet Security issues involving financial institutions should be made known by international organizations, regional organizations, and when there have been cross-border law enforcement collaborations in investigations, extraditions, and so forth. At present, due to the fact that law is generally written at the national (or even state level, as is the case of Identity Theft law in the U.S.), there is a need for reporting of cross-border cases in the literature if such data can be obtained from law enforcement officials by scholars [3].

There are two reasons to label criminal conduct a computer crime. First, an individual might use a computer to engage in criminal activity. Second, the evidence needed to prove a criminal case might be stored in computerized form. The law governing use of a computer to commit a crime is substantive computer crime law, because it concerns the scope of substantive conduct that has been criminalized. The law governing the collection of computerized evidence is procedural computer crime law, because it concerns the legal procedures investigators can use to collect digital evidence in criminal investigations.

Substantive computer crime law divides into two basic categories: computer misuse crimes and traditional crimes. Computer misuse crimes are a new type of criminal offense involving intentional interference with the proper functioning of computers. Examples include hacking offenses, virus crimes, and denial-of-service attacks. These offenses punish interference with the intended operation of computers, either by exceeding a user's privileges (as in the case of a hacking crime) or by denying privileges to others (as in the case of a denial-of-service attack).

The second area of procedural computer crime law is statutory privacy law. Traditional criminal procedure is primarily constitutional law, but much of the law regulating digital evidence collection derives from three privacy statutes: the Wiretap Act, the Pen Register statute, and the Stored Communications Act. As a practical matter, the divide between statutory and constitutional law often tracks the divide between evidence collection from stand-alone computers and computer networks. The law governing computer network surveillance is primarily statutory, and the law regulating retrieval of evidence from stand-alone computers is predominantly constitutional.

Jurisdictional disputes provide the third area of inquiry in computer crime cases. Traditional crimes usually are local. The defendant, the victim, and the evidence often are in the same place, and the charges tend to be brought under state criminal codes wherever the offense occurred. Computer crimes present a very different dynamic. A defendant in one place may connect to a computer in a second place and launch an attack against a computer located in a third place. The victim, the defendant, and the evidence are located in different places—maybe different states, or even different countries. As a result, the law must define for each sovereign what kinds of conduct outside its borders can and should be criminalized, as well as what procedures regulate extraterritorial evidence collection. The global nature of Internet surveillance and terrorism investigations also creates jurisdictional friction between two competing legal regimes, the law of criminal investigations and the law of national security investigations [4].

2- Crime

The development of cybercrime should be viewed through the prism of the development and economic exploitation of computers. Namely, the first computers were used exclusively for military and scientific purposes. After that, computers started to be used by large companies. Since these were closed centralized systems, their access was restricted to authorized users only. Therefore, it was not possible to have a computer crime perpetrator who is not an employee of the organization. This population of users has had the privilege of becoming the first people to try their computer system abuses. The development of modems in the late 1970s, developed other forms of cybercrime and spawned new categories of perpetrators. The widespread use of modems with the rapid development of personal computers, which were increasingly accessible to a growing number of people due to their lower cost, has increasingly strengthened the "digital underground" during the 1980s. In those years, another form of computer crime intensified, namely software piracy. Even then, many saw the simplicity of media multiplication and the disembodied form of software as their main source of income. It should be noted that even today, this type of cybercrime is present in almost every country in the world. The development of computer networks and their integration into the network of all networks or the Internet, enables the unrestricted movement of computer crime beyond national borders and enables it to scale globally. In addition to cybercrime, other forms of crime (especially organized crime) that have been able to use the Internet as a medium of transmission are transcending national boundaries [1].

Computer crime describes a very broad category of offenses. Some of them are the same as non-computer offenses, such as larceny or fraud, except that a computer or the Internet is used in the commission of the crime. Others, like hacking, are uniquely related to computers. Read on to find out what kinds of activities are considered computer crimes and how to protect yourself from them. Computer crime laws in many states prohibit a person from performing certain acts without authorization, including:

- Improperly accessing a computer, system, or network;
- Modifying, damaging, using, disclosing, copying, or taking programs or data;
- Introducing a virus or other contaminant into a computer system;
- Using a computer in a scheme to defraud;
- Interfering with someone else's computer access or use;
- Using encryption in aid of a crime;
- Falsifying email source information; and
- Stealing an information service from a provider [5].

3- Threats

In the context of industrial information technology, the Internet and World Wide Web increasingly are seen as a solution to the problem of providing “anywhere, anytime” services. In the classical view of an Internet security-enabled IT infrastructure, services are requested and consumed by a user (a human requesting plant production dana from his or her desktop); and, data are provided by an origin server (a Web server located in a plant that can authenticate users, implement encryption, serve data, and source multimedia streams). This rather simplistic view works well if the number of users is small, the complexity of services required is modest, and the real-time response requirements are lax. However, it fails to scale when one accounts for the complexities of modern networking: many simultaneous users, potentially operating in multiple languages; many complex data types, including incompatible display formats; many differing schemes for implementing privacy and Internet security through many combinations of authentication and encryption [6].

The world has become ever more reliant on computers for critical infrastructure, communications, and commercial operations. The security of computer systems now affects billions of lives, yet architectural and legacy decisions and consequent vulnerabilities allow malicious actors to compromise sensitive information and deny access to legitimate users. In addition, intrusions by dedicated actor groups appear to have become more persistent, threatening, and global.

Many organizations approach computer security strictly as a business requirement, best handled by an internal department or outsourced to third-party service providers. Network defenders attempt to forestall break-ins by using traditional perimeter defense technologies such as firewalls and guards, mandatory and discretionary access controls, and intrusion detection and prevention technologies. Such perimeter defenses are insufficient, and the size and complexity of the attack surfaces in modern computer systems present too many vulnerabilities. Further, perimeter defenses do not allow the computer network defense (CND) community to assess damage on the basis of the information stolen, or to understand the attacker’s intent, as defenders have no access to most of the communication between the attacker and the compromised system. Malicious actors take advantage of social engineering and client-side exploits to evade perimeter defenses, while proprietary file formats and perpetually vulnerable code allow compromise of machines on the order of millions. Access controls fail because an adversary can take over an insider’s credentials and privileges. Intrusion detection technology generates too many false positives—that is, alarms resulting from the legitimate activities of authorized users—to be deemed effective.

While traditional tools are important components of a defensive posture, they are not sufficient to stop dedicated adversaries such as the advanced persistent threat (APT) and those who launch zero-day attacks (attacks that exploit a previously unknown vulnerability). To combat these extant threats, the CND community should augment detection and response with the capability to carefully monitor and study adversaries. Research in evolutionary biology shows that deceptive creatures have an evolutionary advantage over their competitors—which could extend into the virtual world. Physical combatants use denial and deception (D&D) to enhance their ability to exploit their opponent in order to fight and survive— network defenders should do the same [7].

In online environments, offenders can target thousands of victims at a time, worldwide, within seconds. For example, individuals regularly send out unsolicited emails, called spam, to thousands of victims using addresses harvested from information posted on public websites. For instance, public universities often post the addresses of professors, faculty, and staff on their websites. In turn, individuals can copy and collate these addresses into lists and use them to send a variety of different spam messages. In fact, one of the most common forms of spam message appears to originate in part from Nigeria, where the sender claims to be foreign royalty, bankers, or attorneys who need assistance in moving large sums of money. They request information from the email recipients like names, addresses, phone numbers, and bank account details so that they can reuse the information to commit identity theft or bank fraud. Since few people fall for this sort of scheme, sending out thousands of messages increases the likelihood that a victim may respond. Thus, fraudsters increase the likelihood of success by targeting thousands of victims simultaneously [8].

The greatest threats to the security, privacy, and reliability of computer networks and other related information systems in general are cyber crimes committed by cyber criminals, but most importantly hackers. Judging by the damage caused by past cyber criminal and hacker attacks to computer networks in businesses, governments, and individuals, resulting in inconvenience and loss of productivity and credibility, one cannot fail to see that there is a growing community demand to software and hardware companies to create more secure products that can be used to identify threats and vulnerabilities, to fix problems, and to deliver security solutions.

The rise of the hacker factor, the unprecedented and phenomenal growth of the Internet, the latest developments in globalization, hardware miniaturization, wireless and mobile technology, the mushrooming of connected computer networks, and society’s ever growing appetite for and dependency on computers, have all greatly increased the threats both the hacker and cybercrimes pose to the global communication and computer networks. Both these factors are creating serious social, ethical, legal, political, and cultural problems. These problems involve, among others, identity theft, hacking, electronic fraud, intellectual property theft, and national critical infrastructure attacks and are generating heated debates on finding effective ways to deal with them, if not stop them [9].

Theft of hardware has increased from warehouses and manufacturing facilities due to the growing demand for high-tech products such as microprocessors, computer memory, microcomputers/PCs, Laptop/notebook, palmtop, hard disk drivers and cellular phone that are valuable, compact and easy to transport. For example, a suitcase of microprocessors is worth more than an equivalent volume of cocaine.

Approximately, 4 percent of the hardware theft accounted for over 60 percent of total company losses. While the average high-tech hardware theft is probably in the low thousands of dollars, it is the high-value thefts that dominate overall company losses. Hardware theft has created different levels of cost. In addition of the direct cost of replacing stolen equipment from manufacturers, there are other indirect costs [10].

The hacker threat is often perceived as being one of the major ones of the Digital Age; certainly it is the endless number of hack attacks that grabs the media headlines. However, hackers are just one of the groups that threaten you. One of the key differences with hackers is that the majority of attacks are carried out not for financial gain, but to prove that such an attack can be successful – and thus inherently demonstrate the severe security flaws in the Web site or system being attacked. The term hacker has now gathered a certain amount of controversy in that ‘ethical’ hackers consider that the term does not apply to cyber criminals who access systems and databases for monetary gain – these should be described as crackers. Moreover one of the key factors in the apparent fear of hackers is that they have a vibrant subculture which is perceived as being alternative to, and at variance with, the ‘mainstream’. Like any formal or informal group they share experiences, backgrounds – and values. They have their own heroes, villains, myths, ‘in’ jokes and ‘no go’ areas [11].

4- Cryptography

There are many aspects of computer and information security. Encryption, the process of scrambling a message or other information so that it cannot be easily read, is one of the most critical parts to the security puzzle. If you have the best firewall, very tight security policies, hardened operating systems, virus scanners, intrusion-detection software, antispyware, and every other computer security angle covered but send your data in raw, plain text, then you simply are not secure.

The aim of cryptography is not to hide the existence of a message, but rather to hide its meaning—the process known as encryption. To make a message unintelligible, it is scrambled according to a particular algorithm, which is agreed upon beforehand between the sender and the intended recipient. Thus, the recipient can reverse the scrambling protocol and make the message comprehensible. This reversal of the scrambling is referred to as decryption. The advantage of using encryption/decryption is that, without knowing the scrambling protocol, the message is difficult to re-create [12].

5- Computer Viruses

A computer virus is a piece of software that can “infect” other programs, or indeed any type of executable content, by modifying them. The modification includes injecting the original code with a routine to make copies of the virus code, which can then go on to infect other content.

Biological viruses are tiny scraps of genetic code—DNA or RNA—that can take over the machinery of a living cell and trick it into making thousands of flawless replicas of the original virus. Like its biological counterpart, a computer virus carries in its instructional code the recipe for making perfect copies of itself. The typical virus becomes embedded in a program, or carrier of executable content, on a computer. Then, whenever the infected computer comes into contact with an uninfected piece of code, a fresh copy of the virus passes into the new location. Thus, the infection can spread from computer to computer, aided by unsuspecting users, who exchange these programs or carrier files on disk or USB stick; or who send them to one another over a network. In a network environment, the ability to access documents, applications, and system services on other computers provides a perfect culture for the spread of such viral code.

A virus that attaches to an executable program can do anything that the program is permitted to do. It executes secretly when the host program is run. Once the virus code is executing, it can perform any function, such as erasing files and programs, which is allowed by the privileges of the current user. One reason viruses dominated the malware scene in earlier years was the lack of user authentication and access controls on personal computer systems at that time. This enabled a virus to infect any executable content on the system. The inclusion of tighter access controls on modern operating systems significantly hinders the ease of infection of such traditional, machine executable code, viruses. This resulted in the development of macro viruses that exploit the active content supported by some documents types, such as Microsoft Word or Excel files, or Adobe PDF documents. Such documents are easily modified and shared by users as part of their normal system use, and are not protected by the same access controls as programs. Currently, a viral mode of infection is typically one of several propagation mechanisms used by contemporary malware, which may also include worm and Trojan capabilities [13].

6- Identity Theft

With identity theft, victims suddenly find that someone has stolen their identities, cleaned out their bank accounts, “maxed out” their credit cards, and left them with a huge debt. Worse, sometimes the impostor has committed a serious crime under the victim’s identity, leaving him or her with an undeserved criminal record. And although identity theft is often viewed as a high-tech crime perpetrated by crackers, the thief is often a real-life family member, a trusted friend, or a coworker who has knowledge of the target’s personal information, including passwords to bank accounts.

Cyberthieves glean the information needed to steal someone’s identity—name, social security number, driver’s license number, mother’s maiden name, and bank information— through electronic methods. Atarget’s good credit history is then used by the thief to secure a line of credit that is then used up to the limit—and the Black Hat cracker then disappears.

Targets have reported spending significant amounts of time trying to resolve the harm resulting from identity theft—bounced checks, loan denials, credit card application rejections, and debt collection harassment. Some targets even experience criminal investigation, false arrest, or conviction [14].

There are various ways for criminals to get the personal information they need. First, they may watch the victims or listen to them provide their Social Security number, credit card, or bank account number to someone in person or over the phone. Second, if the victim throws away credit company letters with preapproved credit cards, criminals could activate these cards, as not all companies have adopted sufficient security measures. Third, criminals may simply steal mail from an open mailbox or out of the trash. Finally, the Internet provides ample opportunities to steal someone’s personal information. Weak passwords or the use of the same password for several accounts makes it easy to steal the victim’s information. The most common passwords are “12345” and “password.” Also, Internet dating sites and chat rooms are popular venues to obtain personal information. In response to this growing criminal activity, in 1998 Congress passed the Identity Theft and Assumption Deterrence Act, making identity theft a federal crime. Offenders may be punished with up to 15 years in prison, a fine, and criminal forfeiture. Unfortunately, victims rarely get compensated for the damages incurred [15].

7- Hacking

Many in the general public conceive of hackers as skilled technological wizards who break into the Department of Defense, financial institutions, and other protected networks with the intent to do harm. The notion of a hacker may also conjure up images of various characters from television and movies, such as Neo from the Matrix Trilogy, who had the ability to “see” in programming language code and bend “virtual” reality. These stories and representations have become the dominant model for hackers in popular media and news organizations. Although there are a number of hackers who engage in malicious activities, and some who are amazingly sophisticated technology users, they do not accurately represent the entire population of hackers. Instead, hackers also operate to defend computer networks and expand the utility of technology. In addition, an increasing proportion of the hacker community has a relatively low level of technological sophistication; only a small group has expert-level knowledge of computer hardware and software. The global hacker community is also driven by a wide range of motivations which leads them to engage in both legal and illegal hacks.

Hacks that modify programs and subvert security protocols, however, are illegal and may be used to obtain information or gain access to computer systems and protected resources in furtherance of illegal acts, ranging from stealing credit cards to acts of terror. In many cases, hackers use very basic non-technical strategies rather than sophisticated attacks to obtain information. For instance, individuals can steal someone’s passwords for email accounts or access to a system by looking over the victim’s shoulder and watching their keystrokes. This act, called shoulder surfing, is simple, and can be performed by anyone in order to obtain sensitive information. Similarly, hackers can employ social engineering tactics to try to fool or convince people to provide them with information that may be used to access different resources. These attacks often involve making simple requests and acting clueless in order to prey upon people’s willingness to help others. These sorts of nontechnical attacks are invaluable to attackers because it is extremely difficult to protect individuals from being compromised, unlike computer systems and physical buildings. Often the most easily exploited vulnerability for a person, organization, or a business is not a flaw in hardware or software, but rather the individuals themselves. In fact, more than half of all investigated data breaches in a sample of businesses and universities were completed through the use of techniques that required little or no skill [8].

8- Forensics

Since the 1990s, few fields have progressed as rapidly as computer technology. Computers are no longer a luxury, nor are they in the hands of just a select few. Technology and electronic data are a part of everyday life and permeate all aspects of society. Consequently, computers have become increasingly important as sources of evidence in an ever-widening spectrum of criminal activities.

Police investigators frequently encounter computers and other digital devices in all types of cases. As homicide investigators sift for clues, they may inquire, for example, whether the method for a murder was researched on the Internet, whether signs of an extramarital affair can be found in e-mails or remnants of instant messages (which may provide a motive for a spouse killing or murder for hire), or whether threats were communicated to the victim before a murder by an obsessed stalker. Arson investigators may want to know whether financial records on a computer show a motive for an arson-for-profit fire. A burglary investigation would certainly be aided if law enforcement could show that the proceeds from a theft were being sold online— perhaps through eBay or a similar online auction site.

In addition, the use of computers poses some threats of its own. The accessibility of computers to children and the perception of anonymity in online interactions has given sexual predators a way to seek out child victims online. The vulnerability of computers to hacker attacks is a constant reminder of security issues surrounding digitally stored data. Finally, the fact that computers control most of our critical infrastructure makes technology an appetizing target for would-be terrorists.

Computer forensics involves the preservation, acquisition, extraction, analysis, and interpretation of computer data. Although this is a simple definition, it gets a bit more complicated. Part of this complication arises from technology itself. More and more devices are capable of storing electronic data: cell phones, personal digital assistants (PDAs), iPods, digital cameras, flash memory cards, smart cards, jump drives, and many others. Further complicating matters is the cross-pollination of devices. Cell phones now have the same capabilities of personal computers, and personal computers are often used to facilitate communications. Methods for extracting data from these devices each present unique challenges. However, sound forensic practices apply to all of these devices. The most logical place to start to examine these practices is with the most common source of electronic data: the personal computer [16].

Data changes can occur directly, through direct access to data, using some of the database management programs. This can be done on the system itself, accessed from another workstation within a computer network, or remotely accessed via telephone, satellite and other communication channels. After accessed to the computer system, manipulations are performed on the input or output data. Input data can be changed directly, added new or deleted existing during input or before processing. It is similar to the output data, in that the data is manipulated after the processing is completed and before the data and information are printed or distributed. This can be done by people within the system, such as the experts who created the program and/or the people responsible for maintaining it. Furthermore, manipulation can also occur due to the operation of programs such as Trojan horse - a program that, in addition to its visible purpose, has other functions, ie hidden and unknown functions to the user, in this case changing, deleting existing or adding new data. Very often, such programs also contain an order for self-destruction, ie deletion after the act of manipulation, and their activation is possible only after a certain period of time, which can further complicate the detection of such illegal activities [17].

9- Evidence

In approaching the study of evidence logically and progressively, one starting point is to consider the task of producing evidence with which to prove the truth of a given proposition. No attorney takes a civil or criminal case to court unless there is a good chance that the ultimate proposition can be established by the proper level of proof. In a criminal case, the state has the burden of proving the guilt of the accused beyond a reasonable doubt. Therefore, the “burden of proof” is on the prosecution throughout the trial and this burden never shifts. The term denotes the duty of establishing the truth of the charge against the accused. Ascertaining the truth then becomes an important, if not the most important, objective of the court and jury.

In the criminal justice process, it is necessary that those involved understand the considerations and obligations of the parties in presenting sufficient evidence and the consequences of failing to do so. Failure on the part of the prosecution to introduce sufficient evidence, or failure to properly explain the evidence, will make it impossible for the jury (or judge, when the case is tried without a jury) to determine the truth and thus will result in a miscarriage of justice. Therefore, a thorough knowledge of the concept of burden of proof is an essential starting point on which to build an understanding of the rules of evidence.

Burden of proof could be defined as “[a] party’s duty to prove a disputed assertion or charge.” The burden of proof may also be defined as the duty upon one party to establish the truth of an issue that is important to the case by the quantum of evidence demanded by law. Black’s Law Dictionary notes that the burden of proof also “includes both the burden of persuasion and the burden of production.” The burden of persuasion means that one party must convince the judge or jury to see the facts in a manner that favors the party who introduced the evidence, while the burden of production means that the party has a duty to introduce evidence to attempt to prove a particular point or issue. In a criminal case, the burden of proof means that the prosecution has the duty of proving the guilt of the accused beyond a reasonable doubt. This duty or burden never shifts during the course of the trial, but remains with the prosecution throughout the trial. The emphasis is on the ultimate result rather than on individual issues or questions within the case [18].

To prove a criminal case, it is not absolutely essential that the prosecution actually present to the jury or judge each fact or bit of knowledge in the form of direct evidence. To save time and to avoid placing an unnecessary burden on the parties, the judge may take judicial notice of certain facts and may advise the jury that they may make certain presumptions and inferences. The factfinders may also consider facts stipulated by the parties. Therefore, the jury or other factfinders may make a decision from: (1) facts presented in the form of evidence; (2) information judicially noticed by the judge; (3) legal presumptions; (4) judicially approved inferences; and (5) accepted stipulations [18].

10- Police

The modern police officer will be expected to deal with an increasing number of instances where technology is involved, and will need to deal with each one in the correct manner. He/ she will need to know what actions to take (and why) as these may differ depending on the type of technology that is encountered. Younger officers will be more familiar with day-to-day use of technology, but still will be required to deal with it in a manner that will ensure the integrity of any evidence that may be derived from digital devices. The temptation to 'take a quick look' at a computer or cell phone has to be resisted.

The fact that technology may be involved in the commission of a crime should not in itself make the offence in question or its investigation more difficult. The vast majority of technology related crimes fall under traditional laws, and only those at the more serious end of the scale are covered by specific legislation such as the Computer Misuse Act 1990. Some offences (such as grooming) may be committed online or offline, and are likely to be covered under other legislation such as the Protection of Children Act 1978. This was initially used most often where indecent analogue photographs of children were taken, exchanged, and distributed, but it is now a key piece of legislation in combating the presence and distribution of such images on the Internet. Today's police officer requires the ability to consider crime in new environments and take appropriate actions.

Technological change will continue to increase exponentially and this will place extra requirements on police officers to keep up to date with potential new uses of technology on criminal behaviour. It is only a few years ago that a conversation about the cloud would be about the weather, but in 2016 it is more likely to be about data storage, a topic of increasing interest and relevance to investigators. New ways of abusing technology for criminal purposes will always develop, and present a challenge for policing [19].

Computer crime is a kind of inevitable active participant in the exponential development of information or computer technology especially in the digitized electronic networks in all areas of life. It differs from the known forms of crime because of his common facility incorporeal digitized data, computer main tool of unlawful activity or purpose of his execution, and the invisible computer to do a specific area of action at a distance that in earlier periods was virtually unthinkable. With the development of information society, computer crime takes on more complex forms and expands to the other, "traditional" areas of crime. Computer crime today is not a unique phenomenon with clearly visible manifestations through which it manifests itself, a specific profile of the perpetrator and the ways in which it is executed. This gives it a new dimension, makes it much more dangerous, and its consequences more harmful and farreaching. Therefore, it is modern society must oppose with all available methods and means, including legal protection is certainly one of the most important [20].

11- Conclusion

Computer crime is a crime which is directed against the security of computer systems in order to gain some benefit or harm to others. In order to secure your computer, the information contained in it and all that is done using the Internet, it is necessary to take some precautionary measures against possible cyber-intrusion into your computer or attempts to download data or control the device by various types of specialized and well-trained cyber - criminals. On this occasion, criminals use certain harmful programs to gain access to computers unnoticed. Malicious software is a common name for harmful or malicious programs used by cybercriminals to access someone else's computers. Such programs are usually hidden in attachments or in free content. They are used for a variety of unlawful activities, such as identity theft, deleting or damaging data, creating botnet networks (networks of infected computers) and bypassing security programs. There are a number of different malwares, and most commonly used viruses, trojans, spyware, adware, scareware, etc.

12- Funding and Acknowledgments

Authors of the present research acknowledge the management of the Universidad Autónoma de Nayarit and the Universidad Politécnica de Madrid. This work was supported and funded by the Mobility Program offered by the

National Council of Science and Technology (CONACYT, by its acronym in Spanish) to carry out academic stays at the Universidad Politécnica de Madrid as part of postgraduate studies or to conclude research projects.

13- Conflict of Interest

The author declares that there is no conflict of interests regarding the publication of this manuscript. In addition, the ethical issues, including plagiarism, informed consent, misconduct, data fabrication and/or falsification, double publication and/or submission, and redundancies have been completely observed by the authors.

14- References

[1] Bača, M. Uvod u računalnu sigurnost", Narodne novine, Zagreb, Hrvatska, (2004): 1. – 2.; 25.

[2] Australian Federal Police, AFP, Cyber crime", (2019.). Available online: https://www.afp.gov.au/what-we-do/crime-types/cyber-crime.

[3] Reich, Pauline C. "Cybercrime, Cybersecurity, and Financial Institutions Worldwide." Advances in E-Business Research (2008): 1–33. doi:10.4018/978-1-59904-828-4.ch001.

[4] Kerr, O. S. Computer Crime Law", West Academic Publishing, St. Paul, USA, (2018):1.

[5] FindLaw, Computer Crime", (2019), Available online: https://criminal.findlaw.com/criminal-charges/computer-crime.html

[6] Vacca, John R. "Practical Internet Security" (2007). doi:10.1007/978-0-387-29844-3.

[7] Heckman, Kristin E., Frank J. Stech, Roshan K. Thomas, Ben Schmoker, and Alexander W. Tsow. "Cyber Denial, Deception and Counter Deception." Advances in Information Security (2015). doi:10.1007/978-3-319-25133-2.

[8] Holt, Thomas J., Adam M. Bossler, and Kathryn C. Seigfried-Spellar. "Cybercrime and digital forensics: An introduction." Routledge, Taylor & Francis Group, Abingdon, USA (2015): 83-85.

[9] Kizza, Joseph Migga. "Guide to Computer Network Security." Texts in Computer Science (2020). doi:10.1007/978-3-030-38141-7.

[10] WikiBooks, The Computer Revolution/Security/Computer Crime", (2019.), Available online: https://en.wikibooks.org/wiki/The_Computer_Revolution/Security/Computer_Crime

[11] Lilley, Peter. "Hacked, attacked & abused: Digital crime exposed." Kogan Page Publishers, (2002).

[12] Easttom, Chuck. "Computer security fundamentals." Pearson IT Certification, (2019).

[13] Stallings, William, Lawrie Brown, Michael D. Bauer, and Arup Kumar Bhattacharjee. "Computer security: principles and practice." Upper Saddle River, NJ, USA: Pearson Education, (2012).

[14] Schell, Bernadette Hlubik, and Clemens Martin. "Cybercrime: A reference handbook." ABC-CLIO, (2004).

[15] Kremling, Janine, and Amanda M. Sharp Parker. "Cyberspace, cybersecurity, and cybercrime." SAGE Publications, (2017).

[16]Donofrio, A. W., Computer Forensics"in Saferstein, R.: Criminalistics - An Introduction to Forensic Science, Twelfth Edition", Pearson, New York, USA, (2018).

[17] Pavišić, B., D. Modly, and P. Veić. "Kriminalistika–Knjiga 2 (Criminalistics–Book 2)—." Dušević&Kršovnik, Rijeka, Croatia 218 (2012).

[18] Ingram, J. L. "Criminal Evidence, Tenth Edition", Anderson Publishing, LexisNexis Group, (2009).

[19] Bryant, Robin, and Sarah Bryant. "Blackstone's Handbook for Policing Students." Oxford University Press, (2014).

[20] Franjić, S.; Silaev, S., "Criminal law aspects of computer crime." The International Journal of FORENSIC COMPUTER SCIENCE (2017): 36-41.