COMPUTER CRIME (CYBERCRIME), AS A GLOBAL RISK FACING STATES IN TRANSITION, AND WIDER

Afrim OSMANI, PhD

Abstract

Using computers also brought a new kind of crime. This new type of crime is related directly to the use of the computer to perform criminal activities. Today, the virtual world imposed itself as "normal" life. In such a world, man satisfies personal needs and develops his forces through a comprehensive communication "indirect" and from a distance.

Humanity today is facing an unimaginable of technical and technological development, followed by a revolution of information systems and willful misuse of these scientific achievements and informative.

Leading position takes computer crime, whose perpetrators operate from the comfortable seats of their homes, using, or rather abusing phone or personal computer. They can easily penetrate the information systems of different countries, such as government bodies, state administration, insurance companies, banks, etc.., In order to harm them or benefit for themselves or goods other benefits.

Given the power of the computer, as well as their grandiose role in society, we are not surprised that all the attention of contemporary society is oriented computer crime, even though we are dealing essentially with traditional crime committed by men, the not the computer itself.

Computer-related criminality is not only a single type of crime, it is the general form of all crimes. In the last line, this form of criminality would become the dominant type of crime, so that in the near future would be illogical and impossible to make difference between computer crime and uncomputer crime.

Keywords: crime, computer, organized crime, international convention, fighting crime, etc.

1. Definition

It is impossible to give a comprehensive definition of what is computer crime. Various authors give different definitions, criminal legislature is also not comprehensive, or hold another computer the same offense in different ways.

A definition of cybercrime means that computer crime is any act in which the computer is the means or purpose of committing a criminal offense[1].

According to another author with computer crime refers to a type of criminal activity in which the use of computer technology and information systems emerge as a means of committing a criminal offense, or used as a computer or purpose of committing, which is realized in view relevant legal and criminal consequences[2].

Another definition which gives the U.S. Justice Department, would say that computer crime is any criminal law violation in itself include knowledge of computer technology for their preparation and execution[3].

Computer crime is not any legal action, where various data of a computer are available without someone else's permission. This access to information not necessarily mean that these data be lost or modified. Perhaps the most serious computer crime occurs when there is no indication that the data have been available to the contractor[4].

Is a collection of computer crime offenses, made in a certain area at a certain time, which enables the use of unauthorized access, integrity and availability of technical bases, program or computer system data or privacy of digital data[5].

Definitions that limit cybercrime offenses only which can be done only with possession of specialized knowledge or offenses which are impossible to be carried out without the necessary computer equipment, would be too narrow. Few computer offenses committed by persons informatics professional areas. The use of computers is very easy and does not require any preparation, because the light we found another different computer programs specialized for this work, and the computer can be used directly but also indirectly for committing criminal acts.

Another group of definitions can rightfully say that definitions provide very separate things that summarize a large number of activities and situations that only the definition of charge and do not give a clear picture.

So difficulties as complete definition of computer crime come from these factors:

- computer crime is a relatively new type of criminal activity, which is not yet fully differentiated from other types of crime;
- different views of theorists associated with this phenomenon;
- computer crime has a very rich and diverse fenomenology, which makes it very difficult summary of all in a single definition;
- these days are not rare legislation that recognize computer offenses as separate crimes, but science cannot rely on them to define, given the fact that the criminal law has a little more access and systematization of different from science;
- the speed with which spreads.

The most of theorists escaping defining cybercrime, due to circumstances that were mentioned above, therefore they see fit classification and annotation of computer offenses separately.

Defined more broadly, the term "computer crime" can encompass a wide repertoire of criminal offenses, activities and topics. Giving it the importance computer in everyday life, including the lives of those who have not seen a computer, almost always there is some inevitable and unbreakable connection between the computer and crime. This is especially the case when the computer is used in large-scale records, administration, police records, insurance, bank accounts and the like.

The term "computer crime" is targeted at defining the very institutions world. For example, according to FBI National Computer Crime Squad's (NCCS), in Cybercrime includes:

[1] Sulejmanov.Z.: "Kriminologija" pg.634

[2] Stevan LILIÇ i Dragan PRLJA : "Pravna informatika veština"- Beograd 2010

[3] http://ecommerce.hostip.info/pages/237/Computer-Crime-DEFINITIONS.html

[4] http://www.mariosalexandrou.com/definition/computer-crime.asp

[5] Drazhen DRAGIÇEVIÇ: "Kompjuterski kriminalitet i informacijski sustavi". Zagreb 2004, f. 113

• Illegal entries in the networks of telephone companies;
• Illegal entries into a larger network of prominent companies;
• Compromising the integrity of computer networks;
• Compromising Privacy;
• Industrial espionage;
• Pirated Computer Software; and
• Any criminal activity where a computer is a major factor criminal offense.

Apart from the above mentioned actions, the "computer crime" includes many traditional crimes such as theft, fraud, etc., but of course in this case the difference is that the computer is turned on and if the tool of criminal activity. Under "computer crime" includes viruses, trojan horses, or "worms" that are used to destroy entire computer systems or computer espionage.

Illegal entry into a computer system or computer penetration in network is a duty and work of hackers. Although these people have a great knowledge of computers, in most cases these are people who do not think what damage they can do with their actions. Because there are systems such protection of types intruders and will be elaborated below. Illegal copying of computer software, a fearsome economic impact of the legitimate owners of the software.

Computer crime is not "rounded phenomenological category" and therefore it is impossible to completely and only acceptable definition of the term. Computer crime is a general form which is manifested through various criminal forms and shapes in the future should have a dominant character for most crimes, particularly in the area of economic crime.

The scientific and technical literature on the concept of cyber crime is found and the name SYBER crime and cybernetic crime. The term SYBER crimes should be classified only crimes where the use of computer or computer network is essential to being a crime, and not all crimes in which a way as a means of execution appears the computer and its natural equipment. This are untypical computer crimes, but in providing the evidence procedure is implemented to provide electronic evidence or, in general, this process in criminalistic is increasingly seen as a computer investigation for securing electronic evidence.

2. Evolution and development of computer crime

To determine the exact period of submission of cybercrime, should be determined in advance when making misuse of money or by a computer. It is almost impossible to determine exactly when the abuses were made before and which methods. In the academic literature as the first example of abuse i.e. automation computer work mainly in the manufacturing industry, noting the invention of Joseph-Marie Jacquard. Joseph-Marie Jacquard was a French inventor who in 1801 publicly promoted to use automatic tool with elements of a revolutionary technology for the time. This device operated with the help of Drilling tiles that shape the fabric. This invention enabled the automation of work in this area. The workers fear that this way of producing fabric, will reduce the need for human labor, began to seek methods for sabotaging production work and in this way, in order to discourage Jacquardin in further automation of the production process. These are considered as acts of sabotage before the penalized in the area of cybercrime. With that in this case it was about goods and private property, the legislature of that time has not been difficult to determine appropriate sanctions. This situation canot be compared with today[6].

Other authors, beginnings of computer crime in the view of the early years of the twentieth century, with the introduction of the so called crime of "white collars".

The white collar crimes counted in professional crime, which is conducted by members of the upper class, the ruling circles and business, who use their influence and connections in society for committing offenses. These actions were bringing great material wealth, and great harm society. Besides this characteristic, white collars crime characterized by the fact that the perpetrator of criminal activities related to use (misuse) of their workplace. Fabrications "white collar crimes" for the first time will be used in the U.S. in 1939 by E. H. Sutherland them to stress that this type of crime is categorized as different expressions of abuse of people with high social status within their profession, which, inter alia characterized by the appearance in the sphere of economic relations, security, Burse, works banking, railways, state institutions, inspection and service tax, customs, police etc.[7].

Most of the authors are of the opinion that computer crime, presented by the development of digital electronic computers and their widespread use in the work and functioning of many enterprises comprehensive in the sixties. The first recorded case, in which the computer has been the main vehicle for the commission of theft, has happened in the U.S. in 1966, when the computer is used as a tool for Minnesota bank robberies[8]. In Europe, Deutsche Bank robbery "Herastatt"[9] can be considered the first case of cybercrime, which aroused interest for deeper study of this phenomenon. An important characteristic of this period is the fact that increasingly appear when computer crime, its perpetrators were employees of the organization or enterprise damaged, or someone who had easy access to the computers of those organizations. Accountants were regularly different companies that finance companies led cybercrime victims. This is because the modems to connect to remote computer systems began to be used in the late sixties.

Empirical studies cybercrime appear anywhere from the seventies years, as the inaugural use of criminal methods known for the research of this kind of criminality. At that time these types of crime researchers come to the conclusion that the number of undetected cases is denounced or not much higher[10].

[6] http://library.thinkquest.org/C0126120/jacquard.htm
[7] Zoran SULEJMANOV: "Kriminologija"- Skopje 2003, f. 554
[8] Drazhen DRAGIÇEVIÇ: "Kompjuterski kriminalitet i informacijski sustavi". Zagreb 2004, f. 115
[9] Vladica BABIÇ: "Kompjuterski kriminal"- Sarajevo 2009, f. 70
[10] Drazhen DRAGIÇEVIÇ: "Kompjuterski kriminalitet i informacijski sustavi". Zagreb 2004, f. 115

Calculating the characteristics, etiology and phenomenology of cybercrime, can we conclude that the real crime computer starts at the moment when the computer telecommunications networks makes. Presentation of fears, first as criminals technically educated, later filing these delinquent personal computers further refined and have the appearance of hackers, who will do this type of crime is widespread and frequent.Computer crime is seen as forbidden activity which directly relates to the use of computer systems in the eighties will pass from the sphere of economic relations (which mainly operated in the beginning) in all other spheres of human life. At this time more frequently made when ordinary people that own a personal computer, began to use the same unauthorized collection of personal information to various people from various institutions, and then become the common case computer surveillance, hacking, unauthorized copying of commercial software. In the eighties the national law of various countries strengthen the criminal-legal protection of copyright, since precisely in these years will be seen drastic increase in software piracy, which brings enormous losses to software manufacturers. Then the introduction of the internet and further development of telecommunication systems, computer crime increasingly goes beyond national boundaries of countries. Today there are almost no territorial restrictions cybercrime[11].

With the proliferation of computer crime, the extent to which cross territorial aspects, regional and global scale have today, certainly increased the interest in politics, science, law, especially criminal criminology, research and recognition of this phenomenon. Today most of the world recognizes and criminalizes cybercrime activities. Before legislative reforms and regulations establishing criminal law, justice had to make their decisions regarding these actions, directed towards existing offenses, such as theft, fraud, intellectual property protection, etc.. But the following question: are the digital data owned by someone, whether their part which should be given legal protection, to what extent and in which cases. Failure to give correct answers to these and many other questions related fraud types, the most developed countries of the world began to undertake various activities in the national plan for changing the current legislation. So, in most developed countries of the world too soon it became clear that existing legislation is inadequate and that that should be done urgently amendment of existing laws with new criminal offenses that address cybercrime. Also is making efforts to reach consensus about defining the meaning of this crime, in one hand, and about his determination of the species in other hand[12].

3. Nontraditional types of computer crime

Today there are different types of computer crime. Some computer crimes carried out simply by curiosity of some individuals, as personal skills to test. On the other hand we have also very dangerous types of cybercrime; these species in some cases are threatened even for national security. As an illustration we will consider the case of NASA, which has discovered illegal entry into its computers, and are often damaged data even more important. Not infrequently happened that the suspects are just some teenagers who possessed a personal computer and software built partly for having access to NASA systems. A certain number of people who come to the aid of computers to obtain passwords (passwords), which then enables you to enter easily on the computer systems of different companies. This information posts the specific locations of the web pages by the range of people, in order that other hobbyists can use this data for purposes which they appear necessary.

Which measures are taken by the various authorities to prevent and combat this phenomenon who are also the most varied? For example giant Microsoft company act their lawsuit against two persons who will develop their own domains but with commercial purposes, which occurs extensions to Microsoft, says it is only the beginning of the war against the widespread practice of registering domains that are attractive to large companies. We all know the fame and success of the company Microsoft, so everyone who encounters this name is convinced it has to do with the quality of the services offered by this company, so you can easily fall prey to fraud or misuse or say good use of the name of the company for personal gain. Another way of protection from violent penetration of computer systems is the use of passwords, even though in some cases their use is not enough. Given that the legislation on protection of computer crime is very poor, only a few developed countries in the world, can feel safe from cybercrime attacks. Such are regularly developed countries are more dependent on economic security of computer systems, and thus strengthen legislation on this type of crime.

A widespread form of cybercrime in all countries of the world is software piracy. With that is more than software-s easy to be recorded on disks, CDs and other media. The latter can be found everywhere in the market, and said material benefits from this kind of piracy is very large, on the other hand the damage caused to elsewhere are even greater. The entry of several individuals in personal computers to other people in order to misuse of their personal data, are not uncommon. On the contrary, nowadays have become so frequent that any person who in one way or another gives his personal data for x reasons is endangered. As information technology and electronics developed quickly, at any moment we innovations on various computer, as well as hackers known actors Cybercrime, every day and perfect themselves in the areas of concrete action. Another form of widespread computer crime, especially nowadays when even our lands, especially those of Albania, has become more widespread trend that creation and distribution of television programs via satellite networks, is also decode these satellite programs without legal purchase cards for their encryption. Not only decode done through the Internet network, but also create different modem form-s Box Dreem which

[11] Phrikers- janë persona që përdorin metoda dhe mjete të ndryshme për arritjen e qëllimeve të caktuara. Qëllim i tyre është vjedhja e impulseve telefonike, gjegjësisht shfrytëzimi i papaguar i shërbimeve telefonike.

[12] Drazhen DRAGIÇEVIÇ: "Kompjuterski kriminalitet i informacijski sustavi". Zagreb 2004, f. 118

serve for domestic use. The value of these devices is very high if we take into account the fact that the programs offered are very high quality, and purchase legal decode without decoding cards is prohibited and criminal offenses.
The new kind of crime is also illegal operation of automotive services will be supplied with equipment for computer diagnostific. In today's automotive industry production has moved to a new stage of its development. Modern technology, or electronics which is increasingly present in the composition of new vehicles, forcing service outlets of these vehicles to be educated or educated in this area. To be on the cutting edge, they must learn to work with computers to be able to repair the car and remove the fault. Since different companies producing modern vehicles have also their authorized service outlets, it is clear why we say that there are illegal repairmen. Again it should be emphasized that these multiple crimes committed with the use of modern technologies in them have an infinite diversity. Some of them have become associated with criminal codes, but a significant number of them still have not found the right place in the codes, so it is very difficult to classify penalized and sanctioned appropriately.

3.1. Computer pedophilia and pornography

The traditional division of cybercrime, contains offenses which have in their composition elements of works that we know well in advance (theft, fraud, sabotage, etc..). However, with the further development of technology, especially the development of the global information network (Internet) these works may consider neotradicionale, since their performance is presented in a new method which does the same work even more dangerous is also difficult to classify. In addition to the offenses mentioned above, in this section we will discuss some specific offenses, the danger of which is very large.
In recent years great momentum in its development, takes the pornography industry. If not enough, another phenomenon takes the stage-pedophilia. These works not only seriously affect a country's legislation, but rather undermine the integrity and human dignity of the child respectively. Much is said about pornography as well as pedophilia. But what actually is and what the other one. Pornography is a form of literature, drawings or pictures with sexual motives, whose placement can be made with different purposes, whether for material benefits (most often), retaliation, humiliation, etc. Pornography is as old as human civilization itself. But today it is so cruel and unscrupulous enough that even the strongest legislation in many cases may fail. More dangerous phenomenon is pedophilia. According to medical science pedophile considered people who feel sexual attraction to children before puberty (12 or 13 y.). In most cases people with low education or middle income with which in some cases even fail to fulfill their fantasies associated with this category of minors. Besides, a number of these people psychologically and morally misguided they succeed, but the worst is that only a small fraction of them arrested and punished.
That what is important about this work is pedophilia and pornography on the internet. Although at first glance can say that it is the same, with a slightly deeper analysis will see that in fact there are differences. Internet as a media type, in recent years has achieved an exceptionally great popularity. Major benefits achieved by placing material of various contents. So even this sphere of human activity finds its place in the global network. Very little can be done to control this type of content on the Internet. First we should start from the fundamental changes in the national legislation of all countries to control these systems security and networking performance if adequate protective measures at the institutional state, either at the level of organizations, associations and within the family. With regard to pedophilia on the Internet must first classify Internet pedophiles into two groups: Internet pedophiles and Internet listener. The first are classic pedophiles who find potential victims through the Internet, while the latter are something more specific. They are people who deal with the collection of photographs of children in provocative poses, then distribute these files via the Internet or share with each other. This means that they do not pull the child's body, but the fact that they do something. This transaction enters the realm of abuse or exploitation of children, and should be punished equally and with no mercy.
As known, the application of the different products on the market, followed by large offer of products is the same; we can conclude that the Internet has porn productions wholesale or surplus. From all this pile of pornographic content that can be found on the Internet, must distinguish what is legal and what is illegal. A large number of websites on the Internet place a legally pornographic content, which means that different protocols have stated previously, it is regulated sphere of action. But the placing of pornographic content that will satisfy the desires pedophile is certainly in no way stop and there can be no other law or any rule that would allow such a thing. Differentiation of pornographic content on the Internet in legal and illegal is best suited to ensure a double protection of children from this negative phenomenon. First you have to protect children from becoming victims of pedophiles and pedophilia phenomenon in general and secondly to protect children from the use or access to content such negative and immoral.
Child pornography is one of the worst abuses on the internet, so most of the countries which have signed the Convention for the protection of children's rights, has applied these choices in national legislation, and based on them makes prosecution and punishment of such persons. From the legislative point of view, pornography is not prohibited, but not infantile pornography. However there are some prohibitions or restrictions on the production and distribution of pornographic content. In most of the world considered legislation as an offense any activity which enables the production, distribution and availability of various pornographic content[13]. The basic feature of this offense lies the essential elements of the offense and passive entity to which it is a minor[14]. In the classification of this offense in computer crime group has mostly contributed website development.

[13] magazines, photographs, films, etc.
[14] under the age of 14 y

According to the UN Convention on the protection of children's rights, the perpetrator of this crime can be any person. Completion of the criminal act can be done with actions such as recording of children or minors for pornographic materials processing, sale of pornographic materials in the content, or whose children are minors and encouraging children to participate in pornographic performance[15].

In the field of computer crime, computer pornography offenders may include: owners, creators and editors of websites. Since these people are almost impossible to arrest the reasons mentioned earlier, in practice it is considered that the work completed at the beginning of any activity by which completed the crime figures. This would mean that in case of computer pornography fact of writing or forming such a website is considered a criminal offense. But the latter is applied in practice is a big question. As mentioned in the introduction that this paper has educational character, it is time to give some information about how pedophiles operate online.

Pedophiles initially contact potential victims through various links where you can communicate online (MSN, Facebook, Netlog etc..), then invite them to continue communicating in a unique space to chat. After that creates a level of trust with potential victims, begins our research phase, in which case such as data collected who is next to him/ her, where is the computer at home, have someone check the computer, and the like. Once pedophilia finds that the circumstances are not safe to continue the conversation, immediately discontent and continue the conversation with any other potential victim. On the contrary, provided the ground is better than free, encourages the child to these kinds of conversations remain confidential and the child learns where to hide things that they share each other's. After this begins the so-called grooming process, which in fact is to gain maximum confidence that the child left the meeting and the final stages of indecent act, i.e further recording and distribution of that act[16].

In this regard, the protection of spiritual and bodily integrity of the child has a primary role adequate education of children and control of child labor occasional online. But since children today are more educated in terms of information than parents efficient variant is gaining the confidence of the child and extraction of relevant information from them before they get hurt. More dangerous than the infantile pornography is a lack of awareness of the existence and availability of such contents on the Internet. Large number of people still thinks it is hard to find infantile pornography on the Internet, it is available for a small number of people and it is very expensive. In fact it is quite the opposite: it is enough to correct some words clicked and activated properly search for the right material. Since the industry is booming and is available to those who are willing to use, shows the fact of organizing tourist groups in Thailand in different locations where sexual services are provided to children and minors of both sexes. But not only that, enable the recording and distribution of these contents[17].

With the UN convention on the protection of children's rights, in an effort to expand the area of maximum action against such authorities computer crime[18], and maximum space narrowing action pedophiles and beneficiaries of this kind of activity. How effective? Infantile pornography is one of the offenses for which there is a complete consensus for its unlawful character of the moral aspect as well as from a legal perspective. This kind of pornography is the most dangerous show on the Internet. Need to take concrete steps to combat this phenomenon by educating judges, lawyers, prosecutors, but also the wider public as to what is what and what is not allowed[19].

3.2. Cyber terrorism

With the phenomenon of terrorism are all familiar. Its features and features those are most popular. Mode of operation, the ideology and activities of terrorist organizations from around the world are doing our almost daily. For every day through the media informed about various terrorist attacks of terrorism that have the primary purpose of the authorities and the population of a country, who then pass on their real requirements. Even terrorism has recently started to work mainly with the help of the global information network. The emergence of the Internet has certainly provided a major contribution to the organization, development and rapid spread of various terrorist networks. These organizations mainly use the internet to spread their ideology, propaganda of their activities, to recruit new members and to raise money to achieve their goals. As cyber terrorism is a growing problem in all societies, it is important to know what is and how does this phenomenon neotradicional.

The criminal act of terrorism enters the criminal group to which the object is the joint defense of the constitutional order any country. In criminal law generally positive as terrorist acts allegedly committed by activation of explosives, lighting fires or other actions that endanger the security of the wide masses of the population. Classic weapons that terrorists use are: biological, chemical, nuclear, radiological and similar. But terrorists could use the missile attacks on aircraft, ships and other means of transport. Then there are many well known bombs placed in cars, various outposts which contain similar chemical substances. With the use of the computer cannot become the active actions on the ground, but in combination they deal with cyber terrorism threatening the maximum dimensions of this phenomenon. In cases of cyber terrorism, the computer will be used for other purposes such as recruitment of new members, various fundraising, push or any other necessary support for the preparatory phase of concrete attack. But this form of activity recently, it tends to change the way of concrete action.

The more you increase the importance of information systems for the company, the more same system becomes

[15] Konventa e OKB për të drejtat e fëmijëve e vitit 1989. n. 34

[16] Nga gjuha angleze që do të thotë ujdisur

[17] http://www.vachss.com/av_articles/rtcl_chxp.html

[18] sanctioned by the fact that the possession of some photos that can be stored automatically by the computer

[19] Vladica BABIÇ: "Kompjuterski kriminal"- Sarajevo 2009, f. 156

more attractive or appealing to the different activities of terrorist organizations or terrorist attacks precisely for these systems. Cannot imagine that state institutions, large multinational companies, various companies whether large or small, normal function without a functioning computer network. It's vital that computer technology which nowadays imposed as a necessity, does that also change the appearance of terrorism, as well as everything else changes. The goals remain the same, but different ways of acting. Today terrorist acts can be performed by different countries which also may be miles away from where they have been the consequences of this action. The worst of all this is that tactics, procedures and systems of intelligence prepared, which were supposed to be effective against terrorism, are now weak and ineffective against this new form of terrorist actions. Terrorists do not attack the already modern trucks with explosives or chemical means, much less suicide attacks, but the seats comfortable home with sophisticated, with smaller costs and especially with less human casualties. It is in this way can cause much greater damage. Terrorists are increasingly becoming aware that cyber space allows better conditions to fight for their ideals, ranging from tools, methods, minimum risk and the ability to hide in cyber space where practicable impossible to find. In other words terrorist cyber space provides opportunities for greater safety, greater efficiency and operational flexibility.

Often corrupt practice to IT professionals and purchased from them information about the vulnerabilities of information systems to large corporations and institutions. Then the processing of viruses, trojans and other malicious manipulations with the aim of establishing logical bombs, worm which will enable the system collapse. Greater risk hackers pose introduction of these information systems terrorists in civil aviation, water supply, electrification networks, telephone companies, etc.., dealing directly with the civilian population. Cyber terrorists today are available, in addition to classic weapons mentioned above, a number of new weapons that are even more efficient, such as mass media and technology. The main element of terrorism is just terror, or sows panic and fear that so quickly will be placed with the help of mass media and electronic media. Basically terrorism is an act of communication, and is highly dependent on its publicity. Media terrorists serve as catalysts for the spread of this phenomenon and an essential factor for the choice of tactics, which means that the effect itself depends on the attitude of the media which can discourage or give courage to potential perpetrators[20]. This means that without the support of the mass media, terrorism cannot be sowed so much fear among the masses of the population. Internet as a public media, terrorists use to a significant extent. Given that the Internet offers easy access, legal regulations for its use is more or less weak, feels the lack of censorship, the rapid flow of data and information, all these make clear why cyber space today is quite important for terrorist activities. Terrorists use the Internet for the following purposes: psychological warfare, publicity and propaganda, finding data, fundraising, recruitment and mobilization, building relationships, sharing information, planning and coordination, etc.[21].

Organizations most developed and most powerful al-Qaida terrorist, IRA, ETA, etc., have already proved that information networks are attacking their targets future. They have already proven that they have the opportunity to use high-tech tools and know how to use them. For example IRA in 1997 that shocked the British public opinion than bombs, explosives, and other tools classical attacks of terror will begin to use the electronic attacks on government and administrative computer systems. Al-Qaida uses highly sophisticated tools to ensure their communication channels on the Internet, changing the locations of its websites. In recent times, during the discovery of numerous cells of al- Qaida around the world, to its members found computers with encrypted databases that IT professionals were causing great hardships for their decoding[22].

4. Preventing and combating of cybercrime

4.1. Cybercrime as a global problem

A law, systems of criminal justice and international cooperation does not maintain the speed at which technology is changing. Only a few countries have adequate laws to address this problem, and none of them failed to resolve all legal, regulatory and preventive issues. When the issue is evaluated on the international stage, problems are apparent inadequacies. Cybercrime is a new form of international crime and to be considered effective, international cooperation is necessary. This can happen only if there is a basis for understanding who and what the problem could be resolved. Some of the problems of international cooperation in cybercrime and criminal law can be:

1. a lack of global consensus on what types of behavior will enter

Within the computer crime;

2. a lack of global consensus on definitions of criminal behavior;

3. a lack of expertise in the areas of police, prosecutors and the court in this field;

4. a lack of agreement between different national procedural laws connection with the investigation of cybercrime;

5. trans character of cybercrime;

6. a lack of extradition and mutual assistance and synchronized mechanisms for enforcement of international field.

5. Need for local action

These issues have already been addressed, to some degree, the international and local levels. In particular, the Organization for Economic Cooperation and Development (OECD) and the Council of Europe has made initial instructions for bringing law.

[20] http://www.strassmann.com/pubs/cyberterrorism.html

[21] Vladica BABIÇ: "Kompjuterski kriminal"- Sarajevo 2009, f. 171

[22] Vladica BABIÇ: "Kompjuterski kriminal"- Sarajevo 2009, f. 164

In 1983, the OECD published a study about the possibility of an international application and consent of criminal laws to address the problem of cybercrime. In 1986, it published the report "Computer Crime: Analysis of legal policy," the report examine existing laws and proposed reforms in many Member States, set a list of abuses to be persecuted by law, for example, computer fraud, amendment computer programs and data and copyrights. Many members of the Committee for Information Protection and recommended by other types of crime, theft of trade secrets and unauthorized access to computer systems.

6. Need for global action

Regardless of international efforts, much work needs to be achieved international cooperation. Although most of this cooperation takes place in Western Europe and the OECD countries, the potential effect of cybercrime is spreading just as in the case of operation of international telecommunication systems. All regions of the world must be involved to prevent this form of crime. Ensuring the integrity of computer systems is a challenge for both developed countries and developing countries. It is predicted that in the next decade, it will be necessary for developing countries to experience significant technological development to become economically viable as competitors in the world market. It is important to plan security and protection from crime at the same time even implements computer technology.

The first activities for the prevention and combating computer crime, within the developed countries, are taken in the Sixties, when the date of the first misuse of information systems. In parallel with the development of new technologies and wider public awareness of the importance of information systems, develop measures to ensure information systems. With the development of measures for the protection of these systems, so preventive influence of computer crime prevention. Activities such as within national deal[23] and within international[24]. These activities primarily undertaken in those areas of life where information systems play a significant role, such as in the sphere of protection of personal secrets, computer crime, economy, intellectual property protection, etc.. Every country in one way or another is faced with cybercrime, regardless of the consequences. Activities are undertaken mainly in the field of combating this crime, whether through criminal legislation, either within various state institutions. As will be very little done in terms of prevention of this phenomenon. In its efforts to prevent and combat cybercrime, the Council of Europe in 2001 will bring the Convention on cybercrime, according to which all the Member States but also from the acceding countries are required to comply with this convention under the national legislation minimum determined to prosecute and punish the perpetrators of these crimes. An innovation in this area is the legal persecution of the circle which have emerged abuses of this kind.

Efficient prevention, detection and initiation of criminal proceedings against the perpetrators of these crimes have worsened its situation transnational dimensions that come as a result of globalization. The Internet as a global information network still more aggravates the whole situation. All measures that can be taken, as we have noted above, can be divided into preventive and repressive. Emphasize once again that in the context of national legislation much more repressive measures[25] than that given to preventive aspect. This entire situation is more characteristic of less developed countries where computer crime thrives more. Developed countries approach this issue slightly differently. They largely devoted to the discovery and application of different methods to protect information systems before they can be the target of a criminal attack. One of the most common criminal activities of this nature is the spread of viruses, trojans, worms, logic bombs etc. In their fight against various antiviral programs developed, which in most cases the catch viruses and other malicious programs. But the market every day presented new types of malicious programs, so it is necessary to be on the cutting edge, i.e. in step with the compiler of viruses, Trojans, logic bombs etc.., which is not easy for people who are not professionally deal with this. With that in some way we stated how could defend by similar viruses, we would like to mention some widespread methods for protection from other forms of cybercrime, ranging from physical protection system, access control, cryptography, digital certificates, digital signature, etc. Although it is established that profit Cybercrime nowadays exceeds the profitability of illegal narcotics traffic, no country is immune to this type of criminal activity, especially cyber crime.

7. Strategies to prevent cyber crime

General worldwide protection of computer crime to pull from chase cybercriminals, though it must be implemented, but much more pays attention the protection of computer systems before the any criminal activity. So continue to give more emphasis on the protection of computer systems from any criminal activity. One of perhaps the most widespread crimes is the spread of viruses, Trojan horses, worms and logic bombs. The most common is probably because they are transmitted in different ways. By transferring data through various media, e-mail, FTP, etc.. every day various types of viruses. Some of them probably innocuous but viruses are created and how that can "shatter" any unprotected computer system. Solution in most cases these problems are anti-virus programs that in most cases the "catch" viruses, Trojan horses, worms and logic bombs and deleted. Because the daily emergence of new should more often to take the latest virus definitions from the web sites of virus programs.

7.1. IT (Information Technology) method of protecting computer systems

[23] with relevant legislation interference

[24] with advice and guidance

[25] with radical policies to combat cybercrime

In order not to compromise a system at risk of various types of threats, criminal actions or intruders[26], it is better that system well in advance to protect. Here are some of the most widespread types of procedures and methods for protecting a computer system or network within an organization:

• Classification of information – it is essential to classified information under the appropriate level of accessibility. For example, "reading", "confidential", "secret". This classification is needed and only then can lay the best and most effective measures to protect the information. Classification should be made by the owner of the information.

• Rules of Documentation – all systems, especially the system of identification and authentication, system classification of information and application systems must be documented and recorded. The organizations under the security rules and regulations, any trespassing incident and would commensurate to document. In addition, the organization should make manual containing guidelines for activities and measures to be taken in the event of an incident.

• Administration and staff – the successful protection of information is important to gain a good basic work habits and to establish procedures for maintenance work habits. Also important to create a working environment and establish disciplined approach to work. The need to work with confidential information, it is important to choose people who are completely adequate and reliable for the job. They should be sensitive to the same level of confidentiality of information with which they work. Access to information should be limited only to the extent that the employee is required to complete its work. Particularly sensitive matter should be divided into several parts, which will be given to different employees, so that none of them will not have access to the entire content. Furthermore, security measures will be effective only when employees are properly trained. It is very important that they understand and work to understand the problem. This can be achieved by training in the workplace. Each employee must be trained how to use the network, how to deal with confidential information, making back-up, etc.. The employees need to be told what to do to confront certain threats, that should not make, who can call in case of illegal entry into the system and from whom to seek help. It is also very important to train employees to report every incident to be able to take steps to protect and prevent future unwanted penetrations in the system.

8. Convention on Cybercrime

Convention on Cybercrime was adopted by the council of Europe on November 23 in Budapest on 2001 in order to make country signatories of this document, a common policy aimed at the protection of society against computer crime, among other, through the adoption of appropriate legislation and fostering international cooperation. The necessity of making this conventional is caused by fundamental changes that occur with digitalization, convergence and continuing globalization of computer networks, but also because of the risk computer networks and electronic information can be used to commit crimes and that evidence related to the enforcement of such works can be preserved and transmitted through these networks. The contribution of the Convention should be seen efficiency combat cybercrime and protect the legitimate interests of development and use of information technologies.

The Convention defines the terms "computer system", "computer data", "provider", and "portable data". Thus, the term computer system means any device or group of interconnected devices which one or more of them perform automatic processing of the data according to a certain program. The term computer data means presenting the facts, information or concepts in a form suitable for processing by a computer system, including calibrating program suitable computer system put into operation. The term provider means a public or private entity that allows users to communicate through a computer system and another person who processes or keeps a computer data on behalf of such communication service or services on behalf of users of such services. While the term portable data indicate data related to communication which is achieved through computer systems, which are part of the chain of communication, while keeping the label-origin communication, destination path, the time the flag, date, size, duration or type of communication services.

Convention gives recommendations for measures to be re-taken at national level in the field of substantive criminal to great, and the separate groups of offenses for:

- Offenses against the confidentiality, integrity and availability of computer systems and data to incriminate, relationship-but anticipate such offenses when committed intentionally, such as: actions of illegally accessing the whole or part of a computer system, the actions of illegal junction using technical means to transmit computer data that no public interest to, from or within certain computer system, including electromagnetic emissions from a computer system that supports such computer data; acts of unlawful damage, deletion , deterioration, alteration or concealment of computer data - breaking into the data; acts of unlawful and seriously disrupting the functioning of a computer system input or suppressing computer data - intrusion system, production line, sales, procurement for use, import, distribution or otherwise make available device, including computer program developed or adapted primarily for the purpose of performing any of the aforementioned crimes, computer password, access code, or similar data by which the whole or part of the computer system is trained to Prix-blunt intended to be used to commit any of the previously mentioned works.
- Acts whose performance is linked to a computer or criminalization of specific crimes, such as: forging connected to a computer - act of committing the crime is entering, changing, deleting or suppressing computer data, which results in getting something false data with a view to legal transactions to consider or be employed as reliable, regardless of whether they are data may be directly loaded or virtual; fraud relating to a computer - criminal actions

[26] internal or external

which causes a decrease in property to another person by entering, modifying, deleting or suppressing computer data and intrusion in the functioning of a computer system, with fraudulent or other dishonest intent to obtain unlawful material benefit for himself or for another.

- Offences related to child pornography - incrimination or prediction as criminal offenses the following crimes: producing child pornography so its distribution through a computer system, offered or otherwise making available child pornography through a computer system, distributed or transmit child pornography through a computer system for oneself or for another is purchased child pornography through a computer system for oneself or for another person or possess child pornography in a computer system or medium used for storing computer data. The term "child pornography" means pornographic material that visually displays obvious sexual act with a minor, obvious sexual act with a person who appears as a minor and real images showing apparent sexual act with a minor.
- Offences related to infringement of copyright and other related rights - which are recommended for national legislation to criminalize or to forecast how crimes surfaces Water Administration of copyright, as these violations are determined by the law of a Party, and accordance with the commitments undertaken by signing the Paris Act of 24 July 1971, which revised Berne Convention for the Protection of Literary and Artistic Works, the Agreement on Trade Related Aspects of Intellectual Property and the WIPO Treaty copyrights, with the exception of moral rights recognized in the conventional CO, when such acts of copyright infringement carried out intentionally, in a commercial context and using a computer system. Cybercrime Convention provides for the aforementioned incrimination liability for legal persons in cases where most work is done on their behalf by an individual, regardless of whether the person acted as an individual or as a member of the collegial body of the legal person, while to a managerial position, based on the power of representation of the legal person authorized to make decisions on behalf of the legal entity or authority to exercise control within the legal person.

9. Additional Protocol to the Convention on the Prevention of cybercrime, concerning the punishment of acts of racism and xenophobia committed through computer systems

An additional Protocol to the Convention on the prevention of cybercrime concerning the punishment of acts of racism and xenophobia committed through computer system was adopted in Strasbourg on 28 January 2003 with the aim of highlighting and enhancing the freedoms of citizens regardless of their nationality, religion, affiliation, etc.. It emphasizes the need to ensure full and effective implementation of all human rights without any discrimination or distinction as it is guaranteed by European and other international documents, convinced that acts of racism and xenophobic nature constitute a violation of human rights and threat the rule of law and democratic stability. It is believed that the national and international law must provide appropriate legal responses to propaganda of a racist and xenophobic nature committed through computer systems, while taking into account technical and communication incentives for transferring information across countries ball short period. The specified protocol is made definition of "racist and xenophobic moraine material" which is any written material, any image or any other presentation of ideas or theories that help promotion or incites hatred, discrimination or violence.

10. Areas and instruments of cooperation

Under conditions in which the previously flat assembly, regional cooperation in fighting of crime is presumed clear strategy on each subsection of the states in the region, like their adjusting the framework of the activities of the Council of Europe and the EU. It may be that divided several key term territory on such an been coordinated strategy: compliance to material, procedurals and execution criminal legislation and the Creation of an independent and stable institutions of the system on the penalty justice: the police, other government bodies responsible `neither the detection of crime, as it's Customs Administration and his financial police units for prevention of laundering money etc., the public prosecutor, and the court.

In all these areas[27], necessarily reforms either at the beginning or away from that. In the state in transition, started reforms of criminal legislation and reform of the judicial system, but there is a still lacks of the willingness to change deeply demanding constitutional reform in the direction of empowerment of the independent position of the public prosecutor and the courts. Rising and stabilization of the capacity of the system of criminal justice cannot be performed without the necessity investments[28] and without elimination on Corruption in the mentioned sectors in the fight against the crime. Integral part of the legal framework institutional develops of instruments on mutual cooperation of states in the region in the suppression of criminal activities.

Thus, for example, the Republic of Macedonia there is mutual agreements for certain parts predominantly forms of cooperation with the Republic of Slovenia and the Republic of Croatia, while most problematic cooperation with Kosovo is not regulated with no arrangements with the UN and UNMIK. Due to this, especially is important a second type of survey multilateral arrangements, especially tie adopted by the Council of Europe[29]. New quality in cooperation should bring ratification of the site state in the region, the UN Convention on the suppression of organized crime since 2000[30] with additional protocols[31]. But of course that the application of all mentioned multilateral instruments remains only on formal grounds, if the obligations taken over with their ratification of and are resulting not with the

[27] with the exception of the Republic of Slovenia and Republic of Bulgaria
[28] material, personnel
[29] European conventions for extradition, is mutual assistance in criminal matters, recognition and enforcement whatsoever on the criminal conviction, transfer the convicted person, launder pairs and corruption
[30] the Convention of Palermo
[31] in our country is still on the process for the ratification

"internal preparation" of the national legislation and the criminal justice systems of their application.

11. Conclusions

Authentic crime computer crime is the last stage of the development of human society, which was unknown to the early development of humanity. So, computer crime is kind of contemporary crime, which goes hand in hand with the development of modern humanity, which means goes hand in hand with the development of modern technology. The emergence of electronic age was associated with various abuses, but these abuses have intensified and became more dangerous with the introduction of the possibility to access these networks remotely, with the help of computer and communication technology. Since the introduction of the first forms of criminality telecommunications, it has become clear that technology development will follow the increase of misuse of these scientific achievements. Indeed, this prediction was actually done. From frickers (fiction) hackers appeared to misuse computer systems and global information network. How would you try to act in a unified manner and comply with advice, guidance or standards of international organizations, national interests will do its work and will continue to be a constant barrier to the operation of interstate or intercontinental joint?

Computer crime is indeed a major challenge of any modern state. The first problem faced by these countries, is planting the awareness of all stakeholders that computer crime is dangerous not only for the individual, institution, region or state, it is dangerous for the whole world. This very high risk of social requires a harmonization of legislation that would permanently fight this phenomenon and efficient. This harmonization of legislation required for practical reasons. With that we have said several times that transnational computer crime is immediately striking work collision laws. What does this mean? The question is: if detected and arrested a dangerous hacker, whose activity is conducted in the comfort of his home, and the results has come at a more remote location, as would a criminal procedure? In which country will be judged? Which law will apply? National legislation of the vast majority of countries adhering to conventions World, advice or instructions above organizations, somehow has incriminated a number of computer offenses. Computer offenses are in large numbers. In the national legislation of different countries also happen to be appointed in various ways, be listed in different countries, but the characteristics of these offenses are almost identical.

Analyzing the legislation of different countries of the world, positive criminal law, criminological approach to this phenomenon can conclude that the presentation format of cybercrime can be different, but all they can to classify: theft of services, crime intelligence, crime and criminality rather than property ownership. Phenomenology of cybercrime can be presented in the following forms: illegal use of services, making unauthorized information, computer theft, computer fraud, computer sabotage, terrorism and criminality associated with computer networking. While, in terms of theory criminal case, computer offenses most commonly encountered are: hacking, computer fraud, computer theft, computer sabotage, spying software, falsification of documents and data theft etc. system timing.

If we make a summary of the contents of this paper we would conclude that the objective factors of occurrence of cybercrime are many, among them the most important are the specificity of information technology and computer technology, the speed with which this technology develops and spreads, supporting the largest ever of the whole society in this technology and its achievements in all spheres of human activity. There are separate subjective factors that lead contractor to deal with this kind of activity as frustration, motivation, attitudes and outlooks, inward, mental illness, etc.., these moments that affect the type of computer crime and the harm that can cause. That technological development has facilitated largely functioning of human society in all its aspects. Certainly affected the system of human values. Can unequivocally state that modern man is evaluated based on how many languages you know and how technology has particular knowledge of computing. But this does not mean that people are estimated to misuse the technology achievements. If any person was educated informaticly and it was a high human value will not be misused, perhaps it would not be necessary to take repressive measures. Maybe then humanity will be able to return to the future and the changes that it brings without fear. But, while there are people who their skills in the field of technological knowledge of abuse to criminal activities that endanger the fundamental human values will be in constant danger, the danger from which will not protect us nor legislation on strict.

Literature

Convention on Cybercrime was adopted by the council of Europe on November 23 in Budapest on 2001.
Additional Protocol to the Convention on the prevention of cybercrime concerning the punishment of acts of racism and xenophobia committed through computer system, adopted in Strasbourg on 28 January on 2003.
Konventa e OKB për të drejtat e fëmijëve e miratuar në vitin 1989.
Babiç, Vladica: “Kompjuterski kriminal”- Sarajevo 2009.
Dragiçeviç, Drazhen: “Kompjuterski kriminalitet i informacijski sustavi”. Zagreb 2004.
Sulejmanov, Zoran: “Kriminologija”- Skopje 2003.
Filiç, Stevan i Prlja, Dragan: “Pravna informatika veština”- Beograd 2010.
http://ecommerce.hostip.info/pages/237/Computer-Crime-DEFINITIONS.html
http://www.mariosalexandrou.com/definition/computer-crime.asp
http://www.vachss.com/av_articles/rtcl_chxp.html
http://www.strassmann.com/pubs/cyberterrorism.html
http://library.thinkquest.org/C0126120/jacquard.htm