Computer crime, concept and forms

Dr. Srđan Stajić, Dr. Vlado Širić, Dr. Melvedin Jašarević

s.srdjan1987@hotmail.com, wsiric@gmail.com, melvedinjas@hotmail.com
Nevesinje 88280, BiH
Posušje 88240, BiH
Goražde 73000, BiH

Abstract

Computer crime began to develop in the recent past, with the development of computer techniques and technology. Nowadays, there are frequent occurrences of intrusions into the computer systems of large companies, for the purpose of obtaining property benefits. Nowadays, these intrusions into systems can be carried out by almost any person, because it only requires a good knowledge of computer work and adequate speed. The age structure of the perpetrators of these crimes is diverse. These people mostly come from more developed countries, where technique and technology are far more advanced compared to our country. The reasons why they commit these acts are also diverse. It is very often the acquisition of illegal property benefits, the destruction of certain databases, the disabling of some servers that are of great importance or the theft of some data that have no greater material value but are significant for the perpetrator of that act for some other reasons.

Keywords: Crime, Technology, Computer

1. The concept of computer crime

In any case, the computer represents one of the most significant and revolutionary achievements of the development of technical - technological civilization. But, in addition to the many advantages it brings to humanity, the computer quickly became a tool of abuse by individuals, groups or even organizations. This is how computer crime emerges as a special and specific form of modern crime in terms of structure, scope and characteristics. All of this deserves the attention of the state and its organs, as well as the entire international community. Thanks to the enormous power of computers in memorizing and fast processing of a large amount of data, automated information systems are becoming more and more numerous and an almost irreplaceable part of the entire social life of all subjects at all levels. Thus, the computer becomes an everyday and unavoidable part (segment) of all spheres of social life, from production, traffic, provision of services to national defense and security in the broadest sense. The computer becomes a means of performing various forms of illegal, illegal and socially dangerous activities. Of course, computer crime, under the collective name of which all these diverse forms and forms of behavior related to the misuse of computers and information systems are included, does not have a generally accepted definition. Thus, in the criminal justice literature, different terms are used for these diverse forms of computer crime, such as: computer abuse, computer fraud, crimes with the help of computers, computer crime, computer crime, and technocrime. This type of criminality, unlike others, does not yet represent a well-rounded phenomenological category, and it is impossible to define it with a unique and precise conceptual definition. Computer crime is a crime that is

directed against the security of information (computer, computer) systems with the intention of obtaining some kind of benefit for oneself or others or causing some kind of damage to another. According to some, computer crime is defined as computer abuse in the sense of any event related to the use of computer technology in which the victim suffers or could suffer a loss, and the perpetrator acts with the intention of obtaining or could obtain a benefit. Some define computer crime as the commission of criminal acts in which the computer appears as a tool or object of protection, that is, as the use of a computer in committing fraud, evasion or abuse. The basic characteristics or characteristics of the concept of computer crime can be extracted from the above definitions. These are the following features: ⎫ socially dangerous, illegal behaviors for which the law prescribes criminal sanctions, ⎫ specific way and means of committing criminal acts, with the help or through the medium of a computer, ⎫ special object of protection, security of computer data or information system as a whole or an individual part, ⎫ the intention of the perpetrator to obtain some kind of benefit (property or non-property) for himself or another in this way or to cause harm to another. In theory, various forms of illegal, illegal behavior are classified in the field of computer crime, such as: 1. computer fraud, 2. financial theft, fraud and abuse, 3. theft of goods, 4. falsification of data and documents, 5. vandalism, 6. sabotage, 7. hacking and 8. computer espionage. The great possibilities offered by modern computer equipment also bring with them the dangers of the spread and mass use of electronic eavesdropping, the theft of business and other secrets, and the violation of the rights and freedoms of citizens. American research shows that computer crime happens 40 times more often than general crime.

2. Characteristics of computer crime

Computer crime is primarily characterized by its dynamics and large number of forms. This is understandable because it is a new technology with great possibilities as it is applied in almost all areas of social life. There are also new, significantly more dangerous forms of criminal behavior, which were not known in criminal practice until now, and which do not know the borders between countries and even between continents. The harmful consequences of computer crime are extremely large. They can manifest themselves in the occurrence of property damage for a legal or natural person and sometimes for the entire country. The perpetrators of criminal offenses related to computer abuse themselves represent a special, often specific category of people. These are mostly non-delinquent, non-violent, socially adaptable individuals. As a rule, these are persons who nevertheless have to possess special professional and practical knowledge and skills in the domain of high IT, computing and computer technology and to whom such technological means are available. These crimes are committed covertly, often without any visible and close spatial connection between the perpetrator and the victim (damaged). Most often, they are difficult to detect and even more difficult to prove, and remain practically undetected for a long time until the injured party suffers some damage that is visible in the computer information system. It is a crime that rapidly changes its forms and forms of manifestation, the borders between countries, as well as the type of victim. Modern information and computer technology has brought new drastic changes to all spheres of social life. These changes, in addition to positive and useful news, also brought a number of problems related to the emergence and spread of computer crime in various forms, forms and modes of manifestation. All these changes can be reduced to the following: new forms of value, data concentration, new operating environment, new methods and techniques of action, narrowing the time scale of action, expansion of the geographical area of activity, mobility, risk stability.

3. Computer crime in other European countries – legal certainty

Preventivne mjere često nisu dovoljne niti jedine mjere kojima se društvo suprotstavlja nabujalim oblicima i vidovima kompjuterskog kriminaliteta. Zbog toga je logično da savremena krivična zakonodavstva poznaju jedno ili više kompjuterskih krivičnih dijela za koja propisuju različite sankcije. U Njemačkom krivičnom zakonu ne postoje kompjuterska krivična djela, što ne znači da ova ponašanja nisu inkriminisana. U ovoj zemlji je 1986. godine donesen poseban Krivični zakon za suzbijanje privrednog kriminaliteta koji obuhvata niz kompjuterskih krivičnih djela. Krivični zakon Austrije predviđa kompjutersko krivično djelo. Ono se zove oštećenje podataka. U Velikoj Britaniji je 1990. godine donijet poseban Zakon o zloupotrebi kompjutera. Ovaj zakon predviđa niz krivičnih djela vezanih za zloupotrebu kompjutera i drugih informacionih sistema za koju su propisane veoma stroge kazne. Krivični zakon Makedonije poznaje kompjutersko krivično djelo pod nazivom Upad u kompjuterski sistem. U našem Krivičnom zakonu postoji krivično djelo pod nazivom Upad u kompjuterski sistem. Krivični zakon Republike Slovenije poznaje sledeća krivična dela: Protivzakoniti ulaz u zaštićenu računarsku bazu podataka i Upad u računarski sistem. Krivični zakon Republike Hrvatske poznaje krivično delo pod nazivom: Oštećenje i upotreba tuđih podataka (koje se odnosi na automatski obrađene podatke ili računarske programe). Krivični zakon Ruske federacije poznaje više kompjuterskih krivičnih djela u posebnoj glavi koja nosi naziv: Krivična dela u sferi kompjuterske informacije. Ovdje su propisana sledeća krivična dela: Protivpravni pristup kompjuterskoj informaciji, Pravljenje, korišćenje i širenje štetnih računarskih programa i Povreda propisa o eksploataciji računara, računarskih sistema ili njihovih mreža. Krivični zakon SRJ predviđa sledeća krivična dela: oštećenje računarskih podataka i programa, računarska sabotaža, računarska prevara, ometanje funkcionisanja sistema i mreže za elektronsku obradu podataka i neovlašćeni pristup zaštićenom sistemu i mreži za elektronsku obradu podataka. Za onog ko neovlašćeno izbriše, ošteti, izmeni ili prikrije računarski podatak ili program, predviđena je novčana kazna ili zatvor do jedne godine. Ako je ovim delom učinilac prouzrokovao štetu velikih razmjera, kazniće se zatvorom od tri mjeseca do pet godina.

4. Emerging forms of computer crime

Different documents classify forms of computer crime in different ways. At the 10th Congress of the UN, it was stated that there is computer crime in the broader and narrower sense. Computer crime in the narrower sense is considered as any illegal behavior aimed at the electronic security operations of computer systems and the data processed in them. In a broader sense, computer crime is considered as any illegal behavior related to a computer system and network, including the illegal possession, offering and distribution of information through computer systems and networks. In the same document, specific forms of this criminality are listed. These are: unauthorized access to the computer system or network by violating security measures; damage to computer data or programs; computer sabotage; unauthorized interception of communications; and computer espionage. These forms mostly intersect, that is, they do not exist independently. Computer crime in the broad sense most often appears in the following forms: computer forgeries, computer theft, technical manipulation of devices or electronic components of devices, abuse of payment systems such as theft of electronic credit cards or use of false codes in illegal financial activities. The European Convention on Computer Crime foresees four groups of acts. These groups are: acts against the confidentiality, integrity and availability of computer data and systems (illegal access, interception, interference with data, use of devices, programs); acts related to computers (forgery and theft); acts related to content (most often occurs in the form of child pornography and includes the possession, distribution, transmission, storage or making available of these materials); acts related to the violation of copyright and related rights. Computer crime can be political (cyber espionage, hacking, cyber sabotage, cyber terrorism, cyber warfare), economic (cyber fraud, hacking,

theft of internet services and time, piracy of software, microchips and databases, cyber industrial espionage, fraudulent internet auctions), production and distribution of illegal and harmful content (child pornography, pedophilia, religious sects, spread of racist and nationalist ideas and attitudes, abuse of women and children, human manipulation organs, weapons and drugs) and violations of cyber privacy (email monitoring, spam, wiretapping and recording).

4.1. Computer thefts

Thefts occupy an important place in the field of computer crime, and identity theft is the most important. In this way, identity thieves can open bank accounts, make purchases, and in countries where citizen services are automated, they can obtain birth certificates, passports, loans, etc., all in the name of the person whose identity they are using. Thus, an identity thief can burden the victim financially or create a criminal record. What is characteristic of the victim is that she does not know that her identity is being used until the bills arrive.

4.2. Computer fraud

Computer frauds are committed with the intention of obtaining illegal property benefits for themselves or others, with the fact that they do not mislead a person as in ordinary fraud. This fallacy refers to a computer into which incorrect data is entered, or correct data is omitted, or the computer is used in any other way to commit fraud. Computer fraud is the most widespread form of computer crime. The basic characteristic of frauds is their territorial distribution. Computer fraudsters take advantage of the fact that online fraud does not require access to a payment system, as any other type of fraud does. Every 44 seconds, someone becomes a victim of computer crime after deciding to buy a product, the possibilities of which he became familiar with over the Internet. More than 1,400 suspicious websites in the health sector alone were discovered, which resulted in lawsuits against some companies. The most common products are pills that allow their users to drink as much beer as they want without getting fat, liquid that turns fat from tissues into muscles during sleep, magnets against insomnia, etc. In the period from June to August 1994, in eighteen raids, Vladimir Levin from Petrograd withdrew over 10 million dollars from the Citybank system. The following year he was arrested in London, in 1997 he was extradited to the American authorities, and in August 1997. was sentenced to 36 months in prison and a fine of 250,000 dollars. Kevin Mitnik was arrested and convicted in the USA in 1995 for falsifying 20,000 credit card numbers. Even five ladies over the age of 50, employees of the Pensions Institute in France, transferred 6 million francs to their accounts as pensions for people who had already died a long time ago.

4.3. Computer terrorism and sabotage

Computer sabotage consists in destroying or damaging computers and other data processing devices within computer systems, or deleting, changing, or preventing the use of information contained in the memory of computer devices. The most common types are those that have a harmful effect on certain programs that have the function of saving data. In recent times, terrorists are increasingly abandoning classic acts of terrorism and switching to computer terrorism, which is a very effective tool in the hands of terrorists because it enables them to act in ways they never dreamed of before. Until now, terrorists lacked the appropriate talents and skills for computers, but nowadays they use highly developed techniques and technology. They are constantly setting up new websites where they propagate their ideas. It can be said that computer terrorism is constantly developing and that it will appear more and more in the future.

4.4 Intrusion into the system

Nowadays, hackers are mostly motivated by profit. That is why they make numerous intrusions into systems. The final outcome of a typical takeover of a computer by a hacker could be that tens of thousands of messages with advertising or compromising content were sent from your computer or server to various addresses, or a mountain of prohibited products and information was sold through your server. Such criminal acts are quickly discovered today, and the trail of the sender finally leads to - your computer. One domestic company recently experienced the bitterness of such an experience. The attack began on Friday, at the end of the working week. In an attempt to download various tools to the computer to establish comprehensive control over the device, the hacker first ran into an obstacle - antivirus software, which detected and successively deleted from the server a whole series of applications that were inserted, but the attacker realized this and changed the attack strategy. He had the whole weekend at his disposal to transfer several gigabytes of pirated software to the server and allow Internet visitors to download it. The basic omission in this case was that there was no firewall on the company's server to prevent unauthorized access from the network. However, even if you are a serious attacker, he would probably look for weak points elsewhere, and in this case he would find them in bad security procedures, which is why the SQL server patch was not installed. There is a hacker race going on in the world, in which about 30 new opportunities to break into the system are "produced" every day. It is estimated that there are currently more than 4,500 ways of "breaking in", the number of which grows depending on new products that appear on the market. Therefore, there is no 100% safe security system, as it is launched in marketing messages, but it is possible to reduce the risks to a minimum. The key mistake of managers in the West was the excessive haste to follow every new trend in this area, without sufficiently analyzing what their business priorities are in the use of new technologies, and thus their real needs. The consequence is that the IT infrastructure in companies, which often contains several thousand servers, is built from the ground up and with many interventions, which has led to the fact that most managers do not even know what is in the company's networks. That is why they are now forced, if they want to invest more rationally and establish more efficient control of the security system, to approach the audit of the entire network. Individual attacks on websites are quite common, unlike mass attacks which are quite rare. However, last year there was a case of an attack on more than 1,000 websites in Denmark, and unknown attackers left messages protesting against controversial caricatures of the Prophet Muhammad. A similar attack on Chinese websites was recorded in 2001 after fighter jets of the Chinese army forced down a spy plane of the US army.

5. How to protect yourself from this form of crime

In addition to antivirus, it is necessary to have a firewall on the computer. The firewall serves to prevent unauthorized access of users from the Internet to your computer. In other words, anyone who tries to access your data from the Internet will be prevented and thus a higher level of protection will be achieved. Hackers try to access the victim's computer and thus find out more about the victim, to simply insert a virus or to delete some important data. There are viruses, trojans and worms. Viruses are programs that infect computer databases by inserting their own copies into those databases. Copies are usually executed when a database is loaded into memory and allows them to infect other databases which is their goal. Viruses have a harmful effect on the computer. They can cause the system to crash, slow down the operation of the computer, disable the operation of certain programs, etc. Trojans are destructive programs disguised as a game, tool, utility... When started, the Trojan causes damage while appearing as if it is doing something useful. A worm is a program that is transmitted from computer to computer, usually generating copies of itself in memory. It multiplies quickly and very easily leads to a system crash. It is entered into the system secretly with the

intention of making a joke or damaging the databases. The worm was in 1988. destroyed 6,000 computers. An antivirus is a program that prevents the entry of viruses/trojans/worms into your computer as well as their exit. It scans your PC for viruses for greater security. It can be started at the user's request and works in real time, i.e. constantly. It scans your e-mails and in case it finds a virus, it will take the action you give it. There are many antivirus programs. The most famous and best ones are: AVG, KAV (Kaspersky), NOD32, Panda Antivirus, BitDefender, NORTON Antivirus, McAfee, F-Secure and others. In addition to Antivirus and Firewall, it is necessary to have a program that will neutralize spyware. As their name suggests, spy programs are used to spy on your computer. The spy program remembers every move you make, every file you open and every game you start. When you connect to the Internet, the spyware sends information to the Internet. This information is used by unauthorized persons to gain access to your computer. However, there are programs that prevent spyware from entering your PC. They have special bases and special facilities that detect spyware. The most famous of them are AdAware SE Professional, Spybot S&D, Microsoft Antispyware and others. Buying expensive security systems by itself does not solve much, agreed Nemanja Nikitovic, one of the leading experts of the Italian company Hacking Team. Not even NATO is safe from hacker intrusions, as this young Belgrader himself proved during the bombing of Yugoslavia. Having translated his knowledge of flaws in security systems into publications published on the Internet, Nikitovic was hired by several Italian IT companies, becoming very quickly an official hacking expert, but - morally. Ethical hacking is carried out with the approval of the client, who is interested in checking the security of information systems and data protection in his own company in this way. For example, in a large European bank, the data from the server where the client enters the code to the identification server was sent in clear text. As a result of such an omission, it was possible to falsify a payment order, which was used to withdraw money from the account of a very well-known and financially powerful client on several occasions. In the actual check, these amounts were symbolic, but it was shown that huge sums can be robbed in the same way. When asked how it is possible to make such oversights, the young expert explains that it is a consequence of the trend in the IT market, in which "outrunning" the competition and quick realization of profit become much more important than the quality of the products offered. There is a huge number of companies on the Western market that offer a variety of products and solutions for protection, with at least five to ten new products appearing every day.

Conclusion

Although the life and functioning of citizens and the state as a whole is impossible today, without the use of computers and modern information technology, the awareness has matured that these useful and above all necessary means can be used for illegal, illegal purposes, primarily for obtaining illegal property benefits for a person or for causing harm to others. Since our reality has recorded numerous cases of computer abuse for criminal purposes in recent years, it was high time that the state tackled such irresponsible individuals and groups not only with preventive measures but also with a system of criminal sanctions. This was the basic motive for our country to join a large number of countries that in their system of criminal legislation foresee various forms and types of computer crime for which strict criminal sanctions are prescribed. In the system of these incriminations, various cases of illegal, unauthorized intrusion into other people's computers and computer systems of other persons (natural persons, legal persons or state bodies or public services) prevail. Such illegal activities can be different: from modification, destruction, damage to the use and use of data obtained without authorization. Most often, these acts are undertaken with a special psychological element on the part of the perpetrator - with the intention to gain some benefit (property or other) for himself or another, or to cause some damage to another. If such a benefit has been obtained or such damage has been caused, it is a serious, qualified form for which the law provides for stricter punishment. We hope that the application of

these legal solutions will largely suppress and prevent numerous illegal actions in relation to computers or through computers, which will increase the protection of human and social goods and values, security and trust in computer systems, as well as the protection of human freedoms and rights.

References

Mirjana Drakulić, Osnovi kompjuterskog prava, Beograd, 1996. godina
Slobodan Petrović, Kompjuterski kriminal, Beograd, 2000. godina
Milan Škulić, Kompjuterski kriminalitet, 1997. godina
http://www.overklok.net
http://www.computersandlaw.cjb.net
http://www.pctv.co.yu
http://www.grisoft.com
http://www.kaspersky.com
http://www.blic.co.yu
http://www.bos.org.yu