

## **1. COMPUTER CRIME – NOTION AND DEFINITION**

The computer is one of the most important revolutionary discoveries in the development of the technical-technological civilization. Informatics, although a young science, is developing much faster than any other science. In only 50 years' time many devices for storage and processing of massive data have been discovered and enhanced (improved). By comparison, other scientific branches took decades to reach the same level of knowledge and experience.

But apart from all advantages and benefits that the computer has brought about very soon it has also become a device for misuse in the hands of individuals, groups or even organizations. That's how the computer crime appeared as a specific model of present-day crime in regard of its structure, scope and characteristics. If we take into account the danger and damage to the society that can be caused by this crime, this ultramodern crime needs special attention to be paid both by state governing organs and the international community as well.

Because of the great possibilities for memorizing data and fast processing of huge data bases in very short time the number of automatic information systems goes up every day as they become an indispensable part of the work of all social subjects, both physical and legal, at all levels. So the computer has become an indispensable 'gadget' of modern living, its purpose ranging from private use, manufacturing use, traffic, services to national security and defense.

But this various and far stretching use of computers was recognized by irresponsible individuals who stop at nothing to get material benefit in illegal ways. To put it briefly the term computer crime refers to all forms and modalities of crime connected with abuse of computers and informatics systems in general. The characteristics of the computer crime are:

- socially dangerous illegal behavior that is punishable by the law
- specific way and device for committing crime using computer
- special object for protection, security of stored data of information systems in segments, or globally (entirely)
- the aim of the perpetrator to gain benefit (material or immaterial) and cause damage to other person

The frequency of this crime is 40 times greater when compared with classical crime, and even 90 % of computer crime remains practically undiscovered that is to say in the dark crime, because the detection and producing evidence for this crime is exceptionally difficult. This criminal spreads with great dynamics and variety of forms because we deal with a technology with enormous possibilities and applications

in every day life. Moreover, criminals who perpetrate classic crimes realize the power and advantage of computers and they start using them as helping device when committing classic crimes.

## **2. LEGAL REGULATION OF THE COMPUTER CRIME IN THE REPUBLIC OF MACEDONIA**

Article 251 of the Criminal Law of RM (entering into computer system) Official Gazette no 37/1996.

In Macedonia this criminal act was added to the Criminal Law in 1996 and since then takes effect. It is included in chapter 23, criminal acts against property of CL of RM.

In position 1 of this article it is stated (quotation): He who without authorization will input changes, will announce, conceal (hide), delete or destroy computer data or programs or in any other way will enter into a computer system with the aim to gain (get) material benefit for himself or to injure someone else, will be punished with fine or imprisonment up to 3 years

Position 2 (quotation): If with the crime committed in proposition 2 a substantial material benefit was gained (acquired) or caused greater property injury, the perpetrator will be punished with imprisonment of 1 up to 5 years.

In regard of the way in which these crimes were committed we could say that there was unauthorized entering and free of charge use of the services of several Internet providers. Also there were cases of unauthorized entering into the computer systems of the Macedonian Telecommunications with the aim of free use of telephone services by the perpetrators (crime doers) through false voucher cards with unlimited duration of calls.

Ministry of the Interior of RM has also indicted several officials in charge in bank institutions and private firms who breached their duty by deleting data and feeding the computers with false data in order to acquire material benefit for them or people close to them. For instance, by inputting false data a bank clerk employed in one of our prominent banks transferred over 9 milion denars to her husband's saving account.

One of the latest cases was the one in 2003 when there was unauthorized entering into the computer systems of Commercial Bank and Economic Bank through use of VISA, MASTERCARD, etc. credit cards that were not issued to the perpetrators (crime doers). In this way, by withdrawing cash from cash point (auto bank / cash dispenser) they illegally gained over 1 million denars. Through well-

developed international hacker network they continually received codes of valid credit cards and misused them.

Upon reporting our Ministry took prompt measures and arrested the violators. At the same time in cooperation with Interpol persons from other countries were arrested.

### **3. MANIFESTATION FORMS AND WAYS OF COMMITTING COMPUTER CRIMES**

- computer trickery
- financial theft and misuse
- forgery of data and documents
- making and use of computer viruses
- computer sabotage and espionage
- hackership

**Computer trickery** is crime committed by a person through inputting certain false data or by *not* inputting certain important data with the aim of changing the result of the electronic processing or data transfer and in such way the perpetrator (doer of the crime) can get material benefit for him/her or can cause damage to another person.

**Financial theft and misuse** committed with use of computers are most frequent crimes and they refer to the misuse of credit cards which represent one of the most common and most modern ways of payment (circulation media) as well as entering into the protection systems and making unauthorized financial transactions.

Today's level of computer development allows digitalization and changing of the contents of various paperwork and documents which are used in the legal traffic and forgery of data in electronic form. Moreover, there are frequent attempts to forge banknotes with usage of computer, scanner and printer whose performance possibilities reach a very high level nowadays.

**Computer viruses** are software programs which are made by irresponsible individuals to cause damage to many computers connected in network, for example the Internet, and are considered one of the most powerful weapons of cyber criminals. Basic characteristic of these programs are:

- They copy themselves into each computer they came in contact with
- They are not noticeable i.e. users often do not know about them especially if a program for virus scanning is not installed
- They automatically do some commands like deleting useful data out of the victim's computer, or sending data to other location in the network about which the owner of the computer does not know.

Apart from hackers and the groups they organize to enter into protection systems illegally today there are secret specialized governmental services which enter into the computer systems of other states to espionage (spy). So the term **computer espionage** means a very modern form of intelligence, but there is industrial espionage too used only for commercial purposes.

We talk about **computer sabotage** when somebody destroys, deletes, changes, hides or in some other way makes a datum or program useless or damages the computer which is important for a state organ, institution or public service.

Cyber criminals or hackers as they are popularly called are as a rule are persons with special expert and practical knowledge and are very skillful in the domain (field) of high information technology and who use their knowledge to damage some protection systems. **Hackership** as a modern phenomenon is a result of the challenge to decode and break the protection of a certain information system and finally to enter it. These crimes are done secretly without any space connection between their doer and the victim. As a rule they are difficult to prove and stay in the dark crime. Very often even the administrators of the network systems cannot identify unauthorized entering in a system by a hacker until the system shows damage (starts not to function / starts to malfunction).

#### **4. WAYS OF DETECTING, MEASURES FOR FINDING OF THE PERPETRATORS AND PRODUCING EVIDENCE FOR COMPUTER CRIME**

- injured party reports damage
- administrators of information systems find out
- the investigation and producing evidence must be done by experts that have practical knowledge
- computer forensic

One of the most frequent ways to discover any crime is receiving a report about it by the injured party. This is true for computer crimes too. In this sense an injured party can be both physical and legal subjects, state organs and institutions.

For example when people who administrate and maintain information systems notice that there was unauthorized entering into the system by unknown user(s) and that there was loss of data or system failure they should report the incident to the competent state organ that will find out, determine the damage done and undertake legal sanctions against the crime doer.

Investigators of this type of crime sometimes use the original application program and sometimes use special software for analysis and tools for investigation. Investigators have found ways to collect traces from a remote computer which is out of their physical reach through telephone line or network connection. Moreover it is possible to follow the work of the computer network using the Internet.

These procedures are part of what is called *computer forensic* so some people use this term to talk about (to refer to) analysis of complex data (for example investigating connections among individuals by investigating telephone logging and/or bank transactions. The other use of the term *computer forensic* is to talk about events when computers are used in court in the form of computer graphics in order to illustrate complex situation or as a replacement for a great number of pages based on investigation and states.

What is *computer forensic* actually?

*Computer forensic* is evidence produced by a computer which is supported, conclusive (convincing), and sufficient to be accepted by the court.

#### Forensic Information Procedures

No matter how much people are careful when stealing electronic information they leave behind traces of their activities. Also when perpetrators try to destroy the evidence (proof) in the computer they leave traces behind. In both cases the traces are detectible and can be presented before the court. Computer forensic specialists do more than turning on of the computer to list folders or browse files. They should be able to run complex *evidence recovery procedures* with ability and expertise that will support the credibility of the expert witnessing in question. They should be able to do these services:

- Copying of data
- Search of evidence in electronic mail and other Internet communication
- Recalling of data
- Browsing of documents and other data
- Filing and presenting of computer traces

## **5. PREVENTION OF THE COMPUTER CRIME**

- information education
- administering of the information systems by trained persons
- use of protection from unauthorized entering (both hardware and software security systems)
- punishing of the computer crimes

The term information education here refers to education of each computer user on the dangers of the computer crimes, especially the young generation which are the most numerous users. Through this education each individual user will learn how to protect from himself from cyber intruders or computer viruses before injuries happen.

When choosing administrators who will take care of the security of the information systems special attention should be paid to their proper education and experience so that they are one step ahead of the computer criminals and so that they apply proper protection of the systems they administrate, according to regulations.

When choosing security systems modern tested technologies in this field should be used so that you minimize risks from the so-called security holes in the systems which are skillfully used by hackers to enter them.

Having in mind the dangers of the computer crime the state should pass proper sanctions against perpetrators of such crime that will impose serious threat to many potential hackers who will not run the risk of entering into protected systems.

### **1. CONCLUSION**

- The computer crime is a great social danger
- Each individual who is a computer user in a network should be aware of the possibilities of external intruding and attack
- Protection in time (Due protection)
- Punishing and re-socialization of the perpetrators

This type of crime easily passes state borders and is international in nature. Also the amount of the injury when they are done is increasing every day. Moreover, international terrorist groups use computers and the global network more and more to fulfill their goals.

Every modern state should undertake proper due measures to prevent and sanctify this crime. Also selecting teams within Interpol will contribute greatly to successful handling of this ultramodern crime of the present and of the future.

Each individual that is a computer user for private or duty purposes should be aware of the danger and should use specialized original software for protection from computer attacks and viruses so that risks of injury are minimized.

Finally the perpetrators of these crimes should be re-socialized through their involvement in the constructive streams of informatics, and in such their knowledge of computers is made useful.