Specific Characteristics of Computer Criminal Offenses With Regard to the Law Regulations

Jelena D. Matijasevic[1] and Zaklina S. Spalevic[2]

***Abstract* – There are different categories of perpetrators of computer criminal activity. This paper puts focus on the profile of a hacker – a perpetrator of computer criminal activity who is not motivated by financial gain. It also deals with current classifications of hackers and emphasizes their important characteristics and principles of hacker ethics. The paper also gives a review of judiciary in The Republic of Serbia in this area. It is clear that a society can adequately confront negative phenomenon, only if all of its characteristics and specificities are recognized.**

***Keywords* – Computer criminal activity, Hackers, Computer technology.**

I. INTRODUCTION

Computers represent one of the most important and the most revolutionary achievements of development of technical and technological civilization. There is no single sphere of life, from production, trade and service provision to the national defense and security in the widest sense in which computer does not have practical application. Nowadays we are all aware of the enormous significance of computer use in contemporary societies and of the fact that there is not a single area of human activity in which computers are not being used. However, the conclusion that there has not been a single technical and technological accomplishment that has not been misused in various ways is pretty devastating. Phases of development in which the invention was susceptible to misuse, groupings of persons who committed such actions and different intents of misuse represent specific characteristics.

Growing use of computer technology causes an increase in computer criminal activities, as a new form of criminality in the contemporary society, and a development of its diverse forms. Computer technology is developing very quickly, at the same pace with education and training of persons who intend to misuse it. The press abounds with information about a person (or a group) that had penetrated an important government computer system and had not only acquired specific data, but had also created a possibility for endangering or activation of systems such as nuclear potential of great world forces. This phenomenon is not only a characteristic of the developed western countries – it increasingly becomes typical of the Balkans area [1].

[1]Jelena D. Matijaševic, Faculty of Law, Business Academy, Geri Karolja 1, 21000 Novi Sad, The Republic of Serbia, E-mail: jelena@pravni-fakultet.info

[2]Zaklina S. Spalevic, Faculty of Law, Business Academy, Geri Karolja 1, 21000 Novi Sad, The Republic of Serbia, E-mail: zaklinaspalevic@ymail.com

II. PERPETRATORS OF COMPUTER CRIMINAL ACTS – DIVISION AND BASIC CHARACTERISTICS

There are different categories of perpetrators of computer criminal acts, with respect to a variety of criminal acts that they commit and considering motives which impel them to engage in such activities.

In fact, motive is an important indicator of many classic forms of criminality, and even computer criminal acts. Motive as a clue becomes prominent in setting up versions of suspected persons, regardless of whether it is a case of a single perpetrator or a case of a group of perpetrators, where the method of elimination is used so as to remove suspicion from innocent persons [2].

Obtaining illegal financial gain by committing computer criminal acts is one of the most common motives found in perpetrators of these criminal acts. However, this motivation can be induced by various wishes of the perpetrator, such as unjustified gain, possibility of repaying a debt, an adequate status in society, satisfying certain personal vices and the like. Revenge, inferiority complex, economic competition, the desire for self-approval and achieving a certain success, as well as envy, hatred, jealousy, enthusiasm for one's own knowledge and skills and even political motives in some cases can all be possible motives for committing computer criminal acts [3].

There is a general division of perpetrators of such acts into malicious ones, who commit crime so as to obtain financial gain or just cause damage, and into perpetrators who are not motivated neither by obtaining gain, nor by causing damaging consequences, but simply find pleasure in unauthorized penetration into a well-secured information system.

Malicious perpetrators of computer crimes are mostly motivated by greed. Data from practice indicate a definite set of characteristics that form their criminal profile: about 80% of them are first-time offenders, 70% of them have been working for more than five years for the company which is the damaged party; they belong to the age group below 30; they are mostly male, highly intelligent; they generally have several years of business experience and are considered as conscientious workers that don't cause any problems while fulfilling their work tasks; their degree of technical competence surpasses technical qualifications required for their work position; the perpetrators do not consider themselves thieves or criminals in general, but just borrowers [4].

Computer criminal acts motivated by greed are very common in banking, financial corporations and insurance companies. Statistical data on the perpetrators of computer crime in the area of banking indicates the most common

occupations of the perpetrators: 25% are persons who have special authorization and responsibilities for IT systems; 18% are computer programmers; 18% are empoyees who have access to the terminals; 16% are cashiers, 11% of them are operators – informaticists, and 12% are persons outside the affected corporation, including the service users [4].

The second group of perpetrators of computer criminal acts find deep pleasure in the very act of breaking into multiple security IT systems. The higher the security of the system is, the higher is the challenge to engage in such activities.

Here we are dealing with so-called hackers who break into other people's computer system, using their computer knowledge and a modem [5].

Regarding professional affilation, they are usually computer programmers, operators or highly qualified informaticists, and sometimes they are just people with computers as hobby.

Given the fact that the second group of perpetrators of computer criminal activity raises a lot of attention, causes much contraversy and mixed reactions and that even the computer networks of governments of modern countries were targets of these perpetrators, we will further examine the hacker profile in the following text.

III. Concept of hacker

The word 'hacker' is very often used in a negative context today, without trying to grasp the essence of activities of these persons, or to adequately analyze the reasons and consequences of their activities.

The term 'hacker'is in its original meaning used to denote a person who deals with research of computer potential and its positive application in everyday life. Hackers are highly intelligent people who explore what is hidden in hardware and software. In simpler terms, they locate something hidden from the public or find randomly made mistakes [6].

Hackers still remain a sort of enigma to the world of psychology and sociology. Understanding their development and motivation has become one of the areas of their interest.

Different authors approach hackers in different ways and analyze them from various viewpoints. The dominant attitude nowadays is the one provided in the explanation of the term 'hacker'- namely, that hackers look for errors in programs and then inform the public about it, so that the manufacturer of the given program can rectify the error and that the public can take necessary steps to protect themselves on time.

With the purpose of ensuring a more positive approach to the term 'hacker', data has supplied so as to indicate that more than 10 000 errors have been found so far and that about five new errors are found daily.

IV. Types of hacker

There are several criteria for hacker classification. According to the criterion of respect for ethics, there is a division into the following types of hacker:

- White Hat Hackers – These hackers respect hacker ethics; they deal with computer system and network protection. They try to improve protection of the information system, so as to avoid penetration into it and causing damage. They are typically rented by companies to break into a system and then inform the owner how it was done and how to improve the flaws.

- Black Hat Hackers – These hackers do not hesitate to steal and destroy data in networks and systems they penetrate into. They interpret the hacker ethics in a way they see fit. The principle that all information should be free grants them an excuse to enter into other people's systems. They often destroy a part of the system. Creating and distributing viruses and worms which damage computers belongs to their activities.

- Gray Hat Hackers – are somewhere in between Black and White Hats. They wish to be distinguished from security testers of a company on one hand, and to disassociate themselves from the negative image of Black Caps. These are mostly hackers who initially violated hacker ethics and then used the acquired knowledge according to all the rules of the ethics.

Another more detailed and precise division, where level of computer skills, sphere of interest and ethical rules are taken as a criterion, distinguishes between the following types of hackers:

- *Old school hackers* – Persons who have dealt with computers from their very emergence belong to this group. These hackers could only rely on themselves in terms of learning about computers, because they were the first to engage in research of computers and their possibilities. Copyright protection was unknown to old school hackers. Their favorite activity was to read other people's programs, to modify and expand their possibilities.
- *Phreakers* – They are hackers whose narrow specialty includes theft of dial impulses, conducting international calls at the expense of another person and all activities related to telephone traffic.
- *Crackers* – The major preoccupation of a cracker is the safety of computer systems. Their main activities include breaking into other people's computers. There is a clear difference between crackers and typical hackers – hackers find loopholes in computer systems in order to patch them, whereas crackers use such flaws to cause damage.
- *Warezdoodz* – They specialize in editing programs, finding serial numbers and their illegal distribution to the users. They are at the top of the piracy chain. The activities of Warezdoodz directly violate copyright laws; they contribute to illegal distribution and copying of programs.
- *Hacktivists* – Hacktivists use their hacking skills to promote political ideology, and thus interpret hacker ethics in their own manner, in the sense that hacking for political goals is not contrary to the ethics.

Using computers to achieve political goals was an exception in the past and it did not attract much attention. However, the development of technology enabled the unlimited access of computers to the world of politics and management, which is why the term 'cyber war' has often

been mentioned lately. The latest example of hacktivism is the so-called cyber war between Serbian and Albanian hackers, which started in the August of 2008. Moreover, Serbian and Croatian hackers led a fierce hacking battle during the year 2004, by crashing websites of TV stations, sport clubs and faculties [7].

Each classification of hackers is conditional and by no means final. It is difficult to determine the exact boundaries for some types of hackers; some types are intertwined, while some cannot function alone, without another type. In any case, the existing classifications provide us with a better overview for analysis of specific characteristics of this group of perpetrators of computer criminal acts.

V. PSYCHOLOGY OF HACKERS

If you are a good hacker, everyone knows you; if you are the best, nobody does! Although there are a variety of prejudices against hackers, it is clear that all hackers share the following features (based on different analyses of this specific group of perpetrators of computer crimes): a high IQ, consuming curiosity and the ease of intellectual abstraction. They have an increased ability to absorb knowledge and they pay attention to a variety of details which are irrelevant to the "ordinary people". Hackers are not interested in just one area; on the contrary: they tend to be involved in any subject that stimulates intellectual effort. On the other hand, hackers are afraid of control and do not want to deal with anything binding or authoritative. Similarly, they have no ability of emotional identification with other people, according to many authors. They often tend to be arrogant and impatient with people or things they believe are wasting their time.

Still, there is one thing some of them are exceptionally good that – social engineering. Social engineering denotes the ability of disclosing confidential information by manipulating people. It is most often used by telephone or the Internet and it makes people reveal their confidential information (such as passwords used to access accounts and credit card numbers) or do illegal things [7].

Hackers are often completely disorganized and clumsy when it comes to communicaton with people around them.

During the years 1994 and 1995, ADD (Attention-deficit disorder) was discovered in people who deal with hacking. ADD is characterized by inability of paying attention, combined with hyper-focusing on things they are interested in.

In 1999, AS (Asperger's syndrome) was discovered. This disorder is also known as „high-functioning autism". It is manifested in the inability to understand face and body language of other people, as well as in inability to express empathy with them. On the other hand, people suffering from AS have high intelligence, great analytical skills and an extraordinary ability to solve technical problems [7].

Some authors even advocate the attitude that perpetrators of compter crimes do not have a developed moral maturity.

Hackers believe that many of their illegal acts are justified and ethically correct. The psychologist Lawrence Kohlberg has developed a three-level theory to explain moral development in normal people. The first level deals with avoiding punishment and receiving rewards, the second level comprises social rules and the third one includes moral principles. Each of these level contains two phases. Computer criminals have only evolved through the lowest three phases of the Kohlberg model: two phases of the first level and the first phase of the second level [8].

Hackers have also developed a specific way of communication, which is another important characteristic of them. Due to the fact that they are much more successful in written communication than in face-to-face, interpersonal communication, they have adopted „leet speak". Leet speak is an encrypted form of writing in which letters are represented by numbers, symbols and other signs that resemble the letters. The basic function of this form of communication is to exclude „outsiders" from the communication, i.e. to make a clear difference between the language of this group of people and the language of the the majority. Leet is not to be confused with the so-called AOL language found on the Internet. The primary function of AOL language is to shorten written forms of some words, while the purpose of the leet speak is to make traditional language incomprehensible to people who do not belong to this group.

VI. HACKER ETHICS

There is no definitive and generally accepted definition of the hacker ethics. In a way, every person has their reasons and justifications for the things they are doing. In the same way, hacker ethics does not exist in the form of written, official document anywhere, although several authors have presented its entries.

According to Jargon File, hacker ethics is:

- The belief that the dissemination of information is a powerful, positive characteristic and that it is the ethical duty of hackers to share their knowledge by creating free programs and enabling access to information and computer sources whenever it is possible.
- The belief that breaking into a computer system for fun and research is ethically correct, as long as the hacker commits no theft, vandalism or reveals confidential information [7].

With the development of technology over time, the approach to determining the hacker ethics has changed. Two following approaches particulary stand out: The Original Hacker Ethics and the Hacker Ethic of 90s Hackers.

Steven Levy, the representative of The Original Hacker Ethics singled out six key principles of the hacker ethics in his 1984 book *Hackers: Heroes of the Computer Revolution*. Those principles are: access to computers and anything which might teach us something about the way the world works – needs to be unlimited and total; all information should be free (public); mistrust toward authority – promotion of decentralization; hackers should be judged by their hacking, and not by false criteria such as degree, age, race, sex or position in the society; computers are used to create art and beauty; computers can change life for the better.

On the other hand, The Hacker Ethic of 90s Hackers is essentially contradictory to the Original Hacker Ethics,

because it advocates the opinion that the activity of hackers should be safe, that it should not damage anything, that it should not threaten anyone either physically, or mentally or emotionally, and that it above all should be fun for most people who practice it. All previously stated principles of hacker ethics suggest certain duties, type of conduct, refrainment, attitudes and needs. The extent to which the ethics is accepted and in what way it is interpreted was depicted in the classification of hackers on White, Black and Gray Hackers, which is based on adherence to and compliance with the principles of the hacker ethics.

VII. LEGISLATIVE REGIME

In the area of various types of misuse of computer technology, it is necessary to adopt specific legislative regulations, which settle criminal acts committed within this sphere. It is also necessary to understand technology and individuals who commit computer crimes, so as to achieve effectiveness of legislators.

However, due to poorly developed legal regulations and control in the area of information technology, many countries have become a paradise for hackers. Still, in spite of the cyber crime expansion in the eastern countries, the USA remains by far the leading target on the list of countries attacked by hackers [7]. Difficulties that legal systems face in monitoring new criminal trends of the hackers are a source of embarrassment for governments all around the world. A typical example is that of Canada, because its Criminal Law (law of criminal acts) does not clearly define computer criminal acts. This resulted in prosecutors using metaphors to explain the criminal act, due to lack of knowledge about technology.

Computer criminal acts in the legislation of the Republic of Serbia are regulated by regulations of the Law on Organization and Jurisdiction of Government Authorities in the Suppression of High Technological Crimes [9] and in the Criminal Code of the Republic of Serbia [10].

According to the latest novelty, the criminal acts against the security of computer data have been regulated in the chapter twenty-seven (Articles 298-304a) of the Criminal Code of the Republic of Serbia. The legislator included the following criminal acts in this special group of the Code: damage of computer data and programs, computer sabotage, creation and distribution of computer viruses, computer fraud, unauthorized access to a protected computer, to a computer network and to electronic data procession, preventing and limiting access to a public computer network, unauthorized use of computer or computer network, the criminal act of creating, obtaining and providing the other person with means necessary for execution of criminal acts against the security of computer data. The latest amedmends to the Criminal Code envisage yet another form of misuse of computer and computer networks. Due to the fact that the computer network is often misused so as to commit or to conceal criminal acts against sexual freedom of minors, Article 185b in the Chapter Eighteen of the Criminal Code has regulated the criminal act of using computer network or other technical means of [11] communication to commit criminal offenses against sexual freedom of minors. Introduction of legal provisions on computer criminal acts in the criminal legislation of the Republic of Serbia has contributed to making great progress and to creating new opportunities for prevention of illegal activities and practices in this area. However, given the fact that situations dealt with in practice can be highly unpredictable and that the perpetrators of computer crimes are certainly very inventive, it is necessary to constantly renew these regulations, by adoptinng new legal provisions and making amendments to the existing ones.

VIII. CONCLUSION

It is perfectly clear that the society can adequately confront a certain negative phenomenon only if all of its characteristics and specificities are recognized. Given the fact that the means of the misuse of computer technology are becoming increasingly advanced and more complicated to detect, and that it is very difficult to be step ahead of these criminal activities, it is necessary to keep raising public awareness about this phenomenon and to constantly work on finding the most adequate solution to various criminal activities in this field.

It was our intention to depict the profile of the perpetrator of computer criminal acts as well as possible in this paper and thus to shed light on all of his/her specific characteristics, because effective steps in eliminating negative effects of a certain phenomenon include not only understanding the phenomenon, but also understanding perpetrators of the criminal activities in that field. Transparency and determined opposition to different forms of criminal activities are two important elements of the aim to reduce different forms of crime, including computer crime, to a previously determined framework, which is endurable for that specific community.

REFERENCES

[1] http://www.sk.co.yu/1998/10/skako1.html
[2] B. Banovic, “Providing evidence in the criminal process of economic crimes “, Police College, Belgrade, 2002.
[3] Main problems related to the Cybercrime, 10th United Nations Congress on the Prevention of Crime and the Treatment of Offenders,http://www.justinfo.net/UPLOAD/docs/argentina.htm
[4] Z. Aleksic, M. Skulic, “ Crime tactics, techniques, methods ”, „Official Gazette “, Belgrade, 2007.
[5] G. Goldman, H. J. Stenger, “Die ganze Welt als Tatort, Computer Hacking: Modus operandi und Ermittulungsprobleme”, Kriminalistik, 8-9/89, Kriminalistik Verlag, Heidelberg
[6] http://www.mycity.rs/Zastita/ko-su-hakeri.html
[7] http://www.svethakera.com
[8] The socio-psychological profile of the perpetrator of a computer crime, Faculty of Informatics and Computing, http://www.dir.singidunum.ac.rs/
[9] Law on the organization and responsibilities of state bodies for the fight against cyber crime, „ Official Gazette of the Republic of Serbia “, No. 61/2005.
[10] Kriminal Code, „ Official Gazette of the Republic of Serbia “, No. 85/2005, 88/2005, 107/2005 i 72/2009.