Psychology of the Perpetrators of Computer Criminal Acts and Review of Legal and Economic Consequences for the Community

Zaklina Spalevic, Jelena Matijasevic, Dejan Rancic

Abstract - **There are different categories of perpetrators of computer criminal acts. In this paper, we have devoted attention to motivational analysis of perpetrators of computer crimes, and to analysis of the psychological profile of hackers, given that a motive is significant circumstantial fact. We have highlighted the features of hacker culture and hacker ethics, with review of legal and economic consequences of committing these offenses. Because, it is clear that society may adequately oppose to a certain phenomenon, only if consider all of its properties and if come in all aspects of its specificity.**

Keywords - **Computer crime, The motives of performing criminal acts, Hackers, Hacker culture, The Hacker ethic**

I INTRODUCTION

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 [1].

At the beginning of implementation of computer technology, computers were not be eligible for great abuse, because their application were not be mass, so it was focus of interest of a very small number of users - IT professionals. What opened the door to expanding opportunities to misuse of computer technology in various applications, is its rapid development, simplifying its use and availability to wide range of users [2, p. 852].

Computer technology has very rapidly development. Also, such level of development has education and training those people who would abuse it. Lately, in the media, very often appears some information that an individual (or group) illegally accessed to a computer system, and came up with some data, or created the ability to threaten or triggers such systems like nuclear potentials with great powers. This phenomenon is not characteristic only for developed Western world. It is becoming characteristic of our - Balkan region. In this paper, we have devoted attention to motivational analysis of perpetrators of computer criminal acts, and the analysis of the psychological profile of hackers.

[1]Zaklina Spalevic is with the Faculty of Law for Economy end Justice at University Business Academy, Geri Karolja 1, Novi Sad 21000, Serbia, E-mail: zaklinaspalevic@ymail.com.

[2]Jelena Matijasevic is with the Faculty of Law for Economy end Justice at University Business Academy, Geri Karolja 1, Novi Sad 21000, Serbia.

[3]Dejan Rancic is with the Faculty of Electronics at University of Nis, Aleksandra Medvedeva 14, Nis 18000, Serbia.

II THE MOTIVES OF PERPETRATORS OF COMPUTER CRIMINAL ACTS IN THE FIELD OF CYBERCRIME

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. Individuals who illegally access to another computer or network without further criminal motives are significantly different from an employed in a financial institution or bank, who with abuse of information technologies accessed to other computers and make substantial damage.

The emotional mood, needs, interests and attitudes are an integral part of the mental processes that we call motives. Motivated behavior involves all aware of the elements that occur under the influence of needs, goals, aspirations and interests of people in general. The motive is the current psychological phenomenon. The motive is the incentive for crime. It means incentive as internal cause, and also reason as external category, which affect the character, instincts, feelings, perceptions of people. Because of the treatment an appropriate incentives and cause to the personality of the offender, he sets to himself a goal he wants to accomplish making a criminal act. The needs, interests, customs, beliefs, traditions, instincts, passions, desires and feelings lead to motive for the crimes [3,4].

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 [5, p. 323].

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 [6].

In this context we may emphasize the parallels with organized crime. Bearing in mind that "the desire for profit is the main motive of most criminal offenses committed in the field of organized crime", we can notice a certain similarity of some activities in the field of cyber crime and activities in the field of organized crime.

So, when it comes to computer offenses, we note that a heterogeneous array of motives beyond, in scope and variety, most of the motivational systems of other groups of criminal offenses. Motivational factors of computer crime perpetrators that appear most frequently as dominant [6,7,8] are: intellectual challenge, curiosity and adventurousness, fun, a sense of omnipotence, the need to triumph, dizziness own knowledge and skills, compensation and personal sense of social inferiority, elitist, revenge, internal pressure (hacking) rules, prestige (reputation). The *offender sharing computer crimes based on the structure* motivational.

III TYPES OF THE COMPUTER CRIMES OFFENDERS BASED ON THE MOTIVATIONAL STRUCTURE

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 [2, p. 388].

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 employees who have access to the terminals; 16% are cashiers, 11% of them are operators – IT Specialist, and 12% are persons outside the affected corporation, including the service users [2, p. 388].

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. 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.

IV PSYCHOLOGICAL PROFILE OF HACKERS

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, but not breaking into a computer. This method is based on the assumption that man is the weakest link in the chain of security. 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.

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 [7].

Sarah Gordon, an expert on the psychology of computer criminals, conducted a survey of the Dark Avengers, notorious creator of the virus. He consistently refused to acknowledge responsibility for his creations and, like traditional computer criminals, blamed the victims. Dark Avenger said that human stupidity, but not a computer, spreading the virus. Trying to justify the creation of destructive viruses, he said that most of the computers that were attacked did not contain any important information, and therefore his malicious program has not made any real damage. At the hearing, said that he hates when people have more computers than him, especially

when those resources are not used to what he considered constructive [9].

Hackers have their own specific culture in which they are recognizable. Although they do not need to have a prejudices, it is clear that every culture, including the hacker culture, has its own distinctive characteristics in terms of key characteristics, mode of communication, relations among members, behavior, habits, etc. The hacker culture began to develop in early 60s of last century. After the 1969th was merged with the technological culture which included the founders of the Internet. Over time, it assimilated all cultures associated with technology and computers, and by the 1990s hacker culture is almost equal to what is called "Open Source Movement." The central pillars of the hacker culture in which it develops are: Internet, World Wide Web, the GNU project, Linux operating system and all the hacker creations. From the 1990s until today, the hacker culture gets some recognizable symbols: Tux, the Linux penguin, the BSD Daemon, Perl Camel, and the hacker emblem.

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.

V ABOUT 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: a.) 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; b.) 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 [10].

Both beliefs are widespread among hackers, and most of the hacker population, among other things, engaged in writing free software. Also, many hackers breaking into computer systems for fun, and many even going so far that have unauthorized access to system and send by e-mails free advice and guidance on how to improve the irregularities and imperfections to system-operators.

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. All of these principles suggest that hackers obligation is to remove the border, decentralize power, to evaluate people based on their capabilities and to improve lives through computers.

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, refraining, 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.

VI CONCLUSION

In this paper we tried to present the most important segments related to the personality and actions of the perpetrators of computer crimes. Explaining the motivational structure and psychological aspects of personality, as well as aspects of the basic division with an essential overview of the principles of the hacker ethic and specificity of the hacker culture, we are closer to their most important characteristics. Successful steps in elimination the negative effects of certain phenomenon include not only an understanding of the phenomenon but also understanding the offenders of the crime and other illegal behavior in the computer crime field. Relevant fact is that this area includes both, the legal and economic standpoint. It is necessary to establish an adequate legal framework related to the abuse of computer technology, considering that the financial effects of these abuses can significantly damage the quality of economic operation of a state. On the other side, besides the economic effects on the economy in many countries, also is very important moral aspect of the use of computer technology. Certain principles in this area must be respected for the effective use of ICT sector. An important guarantee for quality legal aspect are adopted legislative provisions, which in a very efficient way representing the state's attitude towards the communication

culture with computer technology, and also include efforts to protect economy in countries from variety abuses in this area. Also it includes punishment of such behavior with adequate sanctions.

It should be noted that in addition to criminal acts which are directed against the security of computer technology and information system elements, there are a number of traditional criminal offenses which, with the help of using computers and computer components, offenders made faster, easier, it is more difficult to enter the track of them, and the consequences are far serious [1].

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.

REFERENCES:

[1] J. Matijasevic, Z. Spalevic, "Specific characteristics of computer criminal offenses with regard to the law regulations", ICEST 2010, Conference Proceedings, Vol. 2., PO VII.1, pp.643-646, ISBN: 978-9989-786-58-7, Ohrid, Macedonia, 2010.

[2] Z. Aleksic, M. Skulic, *Criminalistics*, Faculty of Law, University in Belgrade and Public Enterprise „Official Gazette", Belgrade, 2010.

[3] D. Modly, N. Korajlic, *Crime glossary*, Center for Culture and Education, Tesanj, 2002.

[4] S. Petrovic, *Computer Crime*, Ministry of the Interior of the Republic of Serbia, Belgrade, 2002.

[5] B. Banovic, *Providing evidence in the criminal process of economic crimes*, Police Academy , Belgrade, 2009.

[6] *The socio-psychological profile of the perpetrator of a computer crime*, Faculty of Informatics and Computing, p. 5, http://www.dir.singidunum.ac.rs/ (2012, March 05).

[7] 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 (2011, November 29).

[8] The World of the Hackers; http://www.svethakera.com (2011, November 10).

[9] J. Matijasević, S. Ignjatijevic, "Cybercrime in legal theory, the concept, characteristics, consequenses", INFOTEH®-JAHORINA 2010, Conference Proceedings, Vol. 9, Ref. E-VI-8, p. 852-856, ISBN-99938-624-2-8, East Sarajevo, Serbian Republic, Bosnia and Hertzegovina, 2010.

[10] J. Matijasevic, M. Petkovic, "Criminal offenses against the security of computer data - the analysis of Criminal Law provisions and the importance in the context of combating cyber crime", International Scientific and Professional Conferences „Criminological and forensic research" 2011, Conference Proceedings, pp: 598-609,Vol. 4, No 1, ISBN 978-99955-691-1-2, Banja Luka, Serbian Republic Bosnia and Hertzegovina, 2011.