343.9:004-042.3

COMPUTER CRIME AS A FORM OF THREAT CAUSED BY THE PROGRESS IN INFORMATION TECHNOLOGY

Svetlana Nikoloska, PhD
Faculty of Security
E-mail: Svetlana.nikoloska@uklo.edu.mk

Abstract

In the history of mankind there is no other technological invention with a wider range of application or of greater influence on changing human lives as it is the invention of computers and the corresponding development of computer systems and networks. The benefits of the rapid development of the information technology, which are pretty obvious, can be viewed in the area of collecting, storing, processing and presenting of information, making the information a strategic resource which, in a post-industrial era, can be proved as valuable and influential to a extent that is considered as capital in the industrial era. Thanks to this, the contemporary information and communication system, if used in a proper manner, can increase the efficiency of a large variety of activities.[187] The increase of efficiency and improved communication are actually the greatest benefits of the information technology, both in the business sector and in communication and exchange of information among state authorities and bodies, by means of which large amounts of information are exchanged within a very short period of time with the furthermost parts of the globe. The revolution is in the fact that computer systems and networks enabled fast and efficient exchange of information – data at disposal on the most widely used network, the Internet, which is used by all age groups on the Planet. Beside all the advantages and benefits, the computer and the computer networks and systems, become a means and an object of attacking with elements of abuse by unprincipled individuals, groups or even criminal organizations. The unlawful, illegal use, or better, misuse of computer technology is more and more of

an incriminated character and the criminals are more and more directed towards execution of computer crimes and involve minimal knowledge and resources for achieving higher crime proceeds, at the same time causing enormous damage, deriving from a variety of motives. Fighting the crime imposes the need for permanent following and analyzing the cases involving the computer, the networks and the systems as a means or as an object of crime attack by individuals and organized groups. Based on this is the incrimination of certain computer-related crimes in the national legislation upon which builds on the prosecution of perpetrators and, further on, the international cooperation in this field as the computer crime is, naturally, not performed only within the borders of a single state. It is usually a crime of international character and fighting it requires a wider, international reaction involving application of modern methods and instruments, collaboration and coordination among the corresponding institutions worldwide. This paper is aiming at analysis of the conditions related to the evident shapes and forms of computer crime as they are incriminated in the Macedonian national legislation, as well as the situation related to discovering, revealing, evidencing and preventing this type of crime in the Republic of Macedonia.

Key words: information technology, computer systems and networks, computer crime, incrimination, prevention.

INTRODUCTION

The progress in technology and innovations is the key to the development in society and every period in the past is marked by corresponding technological benefits achieved on the basis of scientific and technical research and whose application improves and modernizes the production, the transport, the trade and the communications. Yet, the largest benefit produced through the technical research is the discovery and the application of information technology. The development of IT has largely contributed to the improvement and modernization of society and humanity and particularly great advancement has been achieved with fast data processing and fast and efficient communication. Thus, on the other hand, an uninterrupted communication among people is conditioned, involving visual getting in touch and exchange of contents involving photographs, instead of simple audio communication that was only made

possible by applying telephone. The development of the communication information technology has largely improved the world, on one hand, but has also on the other, laid the grounds for criminal behaviors unknown from before, but damaging the citizens, their property, identity, renome, even endangering the security on every social layer. Based on what has been going on and the tendencies, there are no suspicions about the information technology influencing every aspect of our lives, both now and in the future. Having the individuals, groups and nations faced with the challenge of adapting, innovating and reacting to circumstances and possibilities made available via the IT, the necessary transformation is made known as information revolution, from industrial into information society, announcing a new digital period with ones and zeros representing knowledge and skills, tools and weapons, currency and goods, science and art, fun and sport. Such a courageous ascertation has been deduced on the basis of facts that can be described in the following manner: everything that functions is in automation; everything that's worthy is digitalized. Furthermore, in almost every single undertaking, the application of a computer is to be included and there will be transformations of various social values, either small or big, into the so-called cyber-goods. This is all going on in a huge newly-created virtual space, bearing the prefix cyber, leading to the English word cybernetics (or the science of communications and automatic control systems) and tending to point at the technological complexity, interdependence and problematic, that are present in this new, but yet not defined informatics ambience different from the common, physical world of matter and energy which is governed by knowledge, electronic impulses and digital numbers. This new parallel world becomes gradually an arena where various activities and processes, including criminal ones with warning and worrying potential, permanently creates and develops them affected by the tumultuous progress and the ever-growing application of information technology facing its rapid revolution and expansion (Ачкоски Ј. : 2012).

The advantages of information systems and computer networks in the overall human living do not remain out of the area of misuse by organized groups or individuals, who make use of their informatics knowledge for illegitimate criminal purposes, regardless whether they produce illicit crime proceeds or endanger in other ways the rights and freedoms of citizens or their property, further widened to jeopardize the overall security involving national, religious, social and economic rights of citizens all over the globe. Criminals in the world seldom choose ways for criminal acting and the computer is a perfect tool for reaching certain criminal goals with

minimum possibility for being revealed as the cause might be located at one point of the globe and the consequences can be felt at a number of locations, in various parts of the world. Even the participants in the criminal network may be unknown to each other – they are simply connected by the skills and the power they share through their knowledge of computer technology and of course, by the criminal goal. The computer is growingly becoming the tool for performing various forms of illicit, unlawful and socially dangerous activities. Computer crime becomes a synonym of all forms of criminal behaviors and plays an important role in the criminal behavior itself, regardless whether it is about misuse of computers as means of executing criminal activities or simply being the object of criminal attack.

The computers and the Internet, undoubtedly opened up the possibilities for increasing the social benefits, so numbers of individuals and groups, even whole countries have become completely dependent on the services that the cyber space provides. The Internet communication has provided distance education and scientific research, electronic trading, online entertainment, publicity of state matters, whereas the email has turned into a medium for doing business and for personal communicating, giving an opportunity for its users to get in touch, to send texts, pictures, musical files to individuals or groups, to buy and/or sell a product or service, in a quick and affordable way. At the same time, the access to scientific-research data bases, that were previously available only to those who had the time, the money and the energy for physical access, has now become available to all citizens. The Internet, just like many other new technologies, represents an instrument of neutral value. Just as it can be useful in gaining social benefits, it can also be used in socially deviant behaviors, in as much as creating new forms of socially harmful behaviors and facilitating the execution of traditional forms of crime (Тупанчевски Н. и Кипријановска Д.: 2008).

The connection between crime and Internet has produced two types of computer crime: network attacks and using the network as a means and location for execution of other forms of crime. The international cooperation of criminals, thanks to the Internet, has been made very easy. Expanding its boundaries and introducing new forms, the computer crime today sets new challenges that threaten the citizens, the collective security, as well as the economic stability of many countries (Urošević and Uljanov, 2010: 13).

The computer crime has been listed among the most significant groups of crimes which stands out from classical economic crimes with reference to its characteristics, such as tools used (instrumentum operandi), the manner (modus operandi), the time of the crime (tempus operandi), the space span of the crime (radius operandi), the location of the crime (locus operandi), the object of criminal attack and the personality of the perpetrator. The rapid growth and expansion of the forms of computer crime are provided by the extended possibilities the computer offers in terms of storage and processing of data, in combination with transfer of the data, on the grounds of information communicating and networking via computer systems and networks (Николоска С. : 2013).

Computer crime represents a realistic phenomenon that security and persecution authorities are facing in the course of their common legal purpose of finding means, methods and techniques for discovering, unveiling, proving and preventing in the process of criminal investigation and providing the judicial authorities to lead a successful criminal procedure and adopting corresponding convictions and verdicts.

Computer crime has also an international character which imposes the need for harmonization of national legislation and penal law for the purpose of providing unimpeded international cooperation in the exchange of data and information, extradition of perpetrators and taking up joint actions for criminal investigations and conviction of perpetrators, confiscating of unlawfully accumulated criminal proceeds. Analyzing the most frequently perpetrated computer crimes, indicators of whether and to what extent are these crimes performed for the purpose of gaining illicit property or performing other acts of crime driven by various motives. A period of five years (2011-2015 inclusive) has been analyzed involving the Macedonian criminalist practice related to characteristic criminal events with elements of organized computer crime.

1. FORMS OF COMPUTER CRIMES

Computer crime represents a common formulation including various forms of criminal behavior. Namely, it is a crime directed against the safety of computer (information) systems as whole, or to segments of it, involving a number of manners and instruments, for the purpose of gaining illicit proceeds for the involved or for third parties, causing damages of various scales (Јовашевиќ Д.: 2002).

The defining of computer crime, depending on the forms of criminal behavior, has been the subject of study of Kaiser (Кајзер Г.:1996), who differentiates among three major computer abuses, based on the major goods of interest:

1. Computer violating of the personal right, particularly in the civil sphere,
2. Computer delicts against and over individual or social legal goods, and
3. Computer property-related crime.

There are certain notions shared among the criminologists that computer crime represents a part of the economic financial crime, but also ideas that it is about property crime and that computer abuse, in its nature, is the closest kin of property crime (Konstantinović - Vilić S. and Nikolić – Ristanović V.: 2003).

The computer crime is a crime related to information and computer systems and it encompasses every criminal behavior, regardless whether it is about threatening personal human rights and freedoms, about abuse of personal data, violation of morality, but also violation of property rights and interests of legal entities, which is considered an element of importance in categorizing this type of crime as an economic one. Namely, the recent automation of the working process and the overall functioning of the legal entities, applying computer technology, create possibilities for financial and accountancy abuses and computer frauds, producing at the same huge criminal proceeds for the perpetrators in position and possessing the knowledge for executing the act of crime. Based on the analysis of statistical data about the computer crime in the world, the financial consequences are pretty serious which leads to the conclusion that the aim and the motives of the perpetrators to gain financial proceeds at the expense of natural and legal entities that keep their money in financial institutions – banks. The crime that makes vulnerable the financial institutions involve payment card frauds congregating perpetrators from around the globe, even not knowing each other, just using the facilities of electronic communication for criminal activity and making use of financial data downloaded from databases of financial institutions and put for sale electronically, too. Also, other criminal forms have their positive financial implications on perpetrators, involving violations of rights, freedoms and morality of victims. For example: the child pornography via computers means financial gain through online selling of child pornographic materials, causing serious violation of the abused children's feelings, causing psychological pain and great deal of insecurity. "The acts

qualified as computer crime are, by their nature and objective essence, close to the acts of damaging other people objects and fraud, also related by the identical intention to unlawfully gaining property or causing damage to others" (Камбовски, 2003: 117).

The computer is increasingly considered as an instrument of execution of crime activities and this crime is more and more involving the application of computer systems and networks, as well thus leading to possibilities for tangible computer crimes resulting in illicit crime proceeds or causing property, financial or any other kind of damage, or even damaging the computer systems and the data stored in them. Thus, computer crime covers several various forms of criminal activities mentioned in a number of definitions of the term computer crime, in line with the following related terms: computer abuse, computer fraud, computer crime, information or technical crime. (Николоска С. : 2013).

The computer becomes an object of criminal attack when the computer or the computer systems and networks, as well as the data they contain, are the actual and final target of the criminal attack, or the aim of the perpetrators. The purpose of the crime attack is to destroy the computer system or the computer network or partially or completely damaging the data stored at a specific computer system. Besides, the criminal attack can be directed towards obtaining information from a given computer system due to a variety of motives, like, economic, political or intelligence, or for the purpose of planning and executing computer terrorist act. However, there are certain situations when the target of the criminal attack are actually the data and information related to bank accounts of natural and legal entities for the purpose of revealing them and using them in producing specific software for withdrawal of money from these accounts and transferring them to another, created just for the purpose of criminal gain. The target of a criminal attack may be also the process of collecting data and information and the computer system of strategic state bodies and institutions, like security bodies collecting data on criminal structures, aiming at abusing and "selling" these data to foreign intelligence services or using them for planning and performing terrorist attacks (Бановиќ Б.: 2001). The computer becomes an object of criminal attack after certain preparations have been completed ahead of time, again involving the computer as an instrument for conducting the criminal act. In order to create and apply a computer virus, first and foremost, one needs a computer to "produce" that virus. Then, the virus is to be directed towards its target system or network, by using

that same or some other computer, for the purpose of destroying computer data, partially or completely, and making them unavailable to the users.

Computer crime involves a great deal of intellectual engagement on the part of the perpetrator, that it acquires the attributes of a "perfect crime" (Цуклески Г.: 2000).

The computer crime does not represent a "rounded phenomenological category" and due to this, it is impossible to offer full and uniquely acceptable definition of the term. It is basically a common form of crime manifested through the various forms it acquires, which are to be granted a character of predominance in the majority of crimes, particularly the ones in the area of economy. The development of computer crime ranks from the very first abuses of computer technology in financial institutions, via some forms known as white collar crimes, to the contemporary forms of electronic piracy, hacking, violating of privacy and sabotaging including creation and sending of computer viruses and worms, but very often computer crime combines elements of child abuse in terms of production and distribution of child pornography and alluring children into contacts and sexual exploitation of minors under the age of 14. The computer crime is further spread to endangering the integrity and security of states involving computer espionage, computer sabotage, cyber terrorism, as forms of crime involving creation and using of hate speech.

2. HARMONIZATION OF MACEDONIAN PENAL LEGISLATION

The international community encounters the computer crime as early as the 1980s when the mass computerization of almost of areas of social living throughout the globe. The miracle of the 20th century, the instigator of the third revolution of information technology and the privilege of the ingenious minds, becomes, beside its immeasurable values for the overall human progress, a potential danger threatening the overall security in the modern world. The ingenious minds of information technology are also a potential threat misusing the knowledge and skills they possess in manipulating the exchange of data for the purpose of accumulating unlawful property gains, spreading racial and religious intolerance, as well as a sort of competition among skilled computer users in the role of criminal perpetrators involved in crimes that are difficult to be revealed. In the direction of improving the national legislations and provision of penal legal protection, the international community adopts a series of

international acts regulating the issues of increasing security against computer abuses and improving the safety of information systems and databases of both legal and natural entities.

The most important document in the domain of fighting computer crime is of course the Convention on computer crime adopted by the Council of Europe, in Budapest, on November 23, 2001 and whose main purpose is joint policy directed towards protecting the society against computer crime, among other things, by adopting corresponding legislature and fostering international cooperation in this area among the states signees of this document. The need for this Document stems from the thorough changes introduced through digitalization, convergence and continuous globalization of computer networks, but also from the risk that computer networks and electronic information could be used for criminal activity and that evidence relating to this type of crime could be saved and transferred via these networks. The Convention is expected to contribute to the more efficient fight against computer crime and to protect the legitimate interests for using and further developing of information technologies. Also, it is considered significant tool for re-directing from acts against secrecy, integrity and availability of computer systems and networks and computer data, as well as against their abuse through criminalization of acts described in this Conventions and introducing authorizations needed for efficient fight against such crimes that would facilitate the process of discovery, trial and conviction on national and international levels on the basis of secure international cooperation.

The cited Convention provides recommendations for redefining the national material legislations for the purpose of incriminating behaviors that underline the abuse of information technologies with criminal aims, as well as recommendations for redefining the process procedure and foreseeing appropriate measure and activities for securing and saving computer data and their adjusting to a form of proof acceptable for the judiciary. Also, the recommendations are partly directed towards improving the international cooperation as it is indispensable because of the very nature, the spreading and the international relations of perpetrators of this kind of crime. The international cooperation is also required for provision of proofs of the crimes conducted, identification of perpetrators and following the illicit proceeds gained through such criminal activity.

The Republic of Macedonia has implemented the recommendations of the Convention through redefining the criminal acts in the Penal Code in 2004, 2008 and

2009 with reference to typical computer crimes that can be performed by simply using the computer and the information technology and to classical and economic crimes, making provisions related to the grounds for their realization by means of using the computer as an instrument or the information systems as targets of the criminal attack.

The Convention foresees 4 groups of computer crimes that are to be incorporated within the national legislations (Penal Code of the Republic of Macedonia, 2008, 2009) as follows:

1. **Acts against the secrecy, integrity and availability of computer systems and data.**
2. **Acts, for the realization of which is linked to using computers (computer frauds, computer forgeries etc.).**
3. **Acts related to child pornography.**
4. **Acts related to violation of copywriters' and other similar acts.**

The Convention gives recommendations with regards to criminal liability of legal entities in cases when the act is done to their benefit, by a natural entity, regardless whether taken by an individual or a member of a collective body of the legal entity, a person heading a unit of the legal entity and entrusted the authority to represent the legal entity, to take decisions and to perform controlling on behalf of the legal entity. The Convention foresees confiscating measures regarding the criminally gained proceeds through computer crime, as well.

3. COMPUTER CRIMES IN THE MACEDONIAN PENAL LEGISLATION

Computer crime in the Republic of Macedonia has been for the first time designated as crime in the Penal Code of 1996 and the list of computer crime types is permanently enlarged based on the acceptance of recommendations and international legal acts that incriminate such activities involving forms of criminal abuse of computers and other machines for automatic data processing and crimes involving computer systems and networks as objects of attacks. However, there is no single chapter in the Macedonian Code that systematizes all computer crime forms, but there are several chapters dealing with forms of crime that include the term *computer* as a

determinant in their titles, referring even to classical economic crimes and criminal behaviors with information systems and networks as objects of criminal attacks and the computer as an instrument of the crime performed. The Penal Code of the Republic of Macedonia takes into consideration the following crimes in several of its chapters:

Chapter XV – Crimes against human and civil rights and freedoms
Chapter XVIII – Crimes against personal dignity and integrity
Chapter XIX – Crimes against sexual freedom and morality
Chapter XXIII – Crimes against property
Chapter XXV – Crimes against public finances, payment system and economy
Chapter XXXII – Crimes against legal traffic and
Chapter XXXIII – Crimes against public order.

The Macedonian criminal and legal-penal practice in the studied period between 2011 and 2015 notifies the execution of only a part of incriminated computer crimes for which there are reported, indicted and convicted perpetrators, based on relevant proofs, determined by the court. The process of providing electronic proof is a complex procedure of selecting, collecting and storing of electronic evidence and the forensics of computer crime is an area that permanently develops and improves, just like the information technology and the possibilities it offers.

This paper analyzes the incriminated computer crimes in accordance with the chapters of the Penal Code of the Republic of Macedonia. For crimes that have been identified, revealed and for which there are evidence and trial has been conducted, here follows the presentation of the number of reported, indicted and convicted perpetrators per given acts of crime.

3.1 Crimes against human and civil rights and freedoms

Respecting human and civil rights and freedoms is constitutionally guaranteed right of citizens, that, supported by the information technology, are becoming more and more the object of abuse of perpetrators, who by applying their knowledge in information technologies for criminal purposes, abuse the rights and freedoms of other people in different ways. Macedonian legislation, by incriminating a set of criminal behaviors involving computer systems and networks, has laid the foundations of the

basic penal-legal protection against this kind of abuse. The following ones are defined as crimes: Safety threats – Art. 144 p.4; Violation of secrecy of mail and shipments – Art. 147; Personal data abuse – Art. 149; Denial of access to public information system – Art. 149-a; Unauthorized wiretapping and recording – Art. 151; Unauthorized videotaping – Art. 152; Violation of copyrights and similar rights – Art. 157; Violation of distributor right to technically protected satellite signal – Art. 157-a; Piracy of audio-visual works – Art. 157-b and Phonograph piracy – Art. 157-c.

The practice in the Republic of Macedonia has notified crimes against human and civil rights and freedoms, as either individual crime deeds or as an organized way of perpetrating criminal deeds, and in particular, crime deeds that provide the perpetrators high crime proceeds, but also, those violating the victims' privacy.

Table 1: Reported, indicted and convicted perpetrators of computer crimes against human and civil rights and freedoms in the Republic of Macedonia in the period between 2011 and 2015

Year	Art. 149			Art. 157			Art. 157 – a			Art. 157 – b			Art. 157 – c			Total		
	R	I	C	R	I	C	R	I	C	R	I	C	R	I	C	R	I	C
2011	/	/	/	/	/	/	2	4	4	12	15	15	/	1	1	14	20	19
2012	/	/	/	/	/	/	5	4	1	1	14	13	/	2	2	6	20	16
2013	/	/	/	/	1	1	12	4	4	1	3	3	/	/	/	13	8	8
2014	23	9	7	8	6	6	/	8	7	/	1	1	/	/	/	31	24	21
2015	/	/	/	9	12	9	3	3	3	/	1	1	/	/	/	12	16	13
Total	23	9	7	17	19	16	22	23	19	14	34	33	/	3	3	76	88	77

Based on the above data it can be stated that perpetrators in the Republic of Macedonia have used their knowledge and the capacity of information technology for criminal purposes and abused personal data of other people, but also the copyrights for piracy of audio-visual works. The analysis of figures of reported, confirms continuous perpetration in the period of interest and the crime varies in structure for each year, whereas from the aspect of re-qualification of deeds based on the available evidence, it can be deduced that the re-qualification in the process of trial is in the direction from reported classical crime to computer crime. This can be viewed in the light of the ratio

of convicted to reported perpetrators, but also due to the development of procedure upon filing criminal report during the trial based on evidence provided. When it comes to the figures of convicted, the percentage of conviction is rather high – 87.5% and implies high quality of performance and respecting the procedures of providing, storing and presenting the official electronic evidence.

3.2 Computer crimes against sexual freedoms and morality

Crimes against sexual freedoms and morality cover the criminal behaviors related to sexual delicts (delicta carnis), and the legislation protects the individual, his/her freedom to sexual intercourse, but on the other hand, regulates and protects the morality, the ethical views and understanding of acceptable and unacceptable in the realm of sexual interacting. Sexual delicts are also an aspect of the group of violent crime, as this is about criminal behaviors involving violation of sexual freedoms of the victims and their choices, orientation, decisions etc. Based on the object of protection or the victims of sexual crimes, from the aspect of computer crime, we can be speak only about a few criminal instances of protecting the minors against the dangers deriving from using computer technology and computer systems.

Child pornography, as a safety issue is not only confined to national, but it is becoming a huge international problem that attracts growing attention due to the frequently occurring cases of international trafficking of minors for the criminal purpose of selling organs and accumulating high criminal proceeds and human trafficking of minors for the criminal purposes of sexual exploitation. Beside physical sexual exploitation of minors, with the emergence of high-tech cameras, this form involves taking pictures and video-recording of children with sexual connotation (naked photos, sexual acts etc.) and these recordings are further multiplied and distributed on the pornography market. However, the international community makes great efforts and takes actions in the direction of getting on the way of this issue and protecting the young population in the "twisted world of adults", who, are becoming more and ruthless in their constant race for profit, and do not care about the methods and ways involved in enticing children and their abuse and exploitation via taking photographs and recordings that are sold on the pornography market, which, based data obtained from relevant institutions, is rather profitable.

The introduction of computers and computer networks and the expansion of Internet particularly, provided grounds for rapid development of computer pornography on global level. This encouraged the scientific and professional public to take up defining this kind of safety issue and to initiate methods for prevention. The Council of Europe defines the child pornography as incorporating "all audio-visual materials involving children in sexual connotation" (Council of Europe, Recommendation R(91)11 and Report of the European Committee on Crime Problems: 1993).

Child pornography is displayed through photographs and filmed materials containing sexually explicit activities involving children (minors under the age of 14). Child abuse includes forcing and enticing children in order to perform certain sexual activities that are going to be photographed or filmed and they are also considered child pornography. These contents are made easily accessible by the perpetrators and even for certain money compensation if used via certain web-sites. According to the sociologists, this is a pervert abuse of minors and it is about sexual exploitation that provides high profits for the perpetrators. Or, to put it in other words, child pornography is not produced for the purpose of satisfying low instincts, but it is produced and distributed for lucrative purposes. Computer child pornography is among the most profitable criminal businesses conducted by means of computer networks and according to some researches and data published on the Internet, it is about achieving over 25 mln dollar income per year (http://www.popcenter.org/problems/child_pornography).

Computer child pornography represents a criminal activity manifested mainly in three ways, such as: enticing children and their abuse in pornography footage, then, downloading of porn contents from Internet or reaching certain hidden or limited access contents by hacking and porn contents with children as actors. According to the findings of research carried out in the European continent, a categorization of criminal activities containing the term computer child pornography has been made. Namely, taking into account the statistics from the Missing Children Europe from the text titled EU more severely against child pornography, published in October, 2008, (http://it.com.mk/IT-EU-Protiv-detska-pornografija-mono/):

- 39% of pornographic pictures involve children between the age of 3 and 5, 19% - children under the age of 3
- In 2003, the pedophilia contents doubled online
- In 2007 there 16% more pornography pictures online

- Telefono Azzurro (Italy) worked on 192 cases, 45% of which involving children between 0 and 5 years of age
- Child Focus (Belgium) notified 2562 cases in 2007.

The penal – legal definition of child pornography in the Penal Code of the Republic of Macedonia (2008) states that: "Child pornography involves pornographic material that visually shows conspicuous sex acts with minors, or obvious sex activities with a person that seems as under age, or realistic pictures of conspicuous sex activities with minors".

Computer child pornography involves enticing and abusing of minors under 14 for the purpose of photographing and/or filming sexual contents – sex positions, intercourses, advertizing of products for producing pleasurable sex/erotic stimulation, multiplying them and electronically distributing them.

Child pornography is becoming a burning, acute security issue that has been dealt with in the Convention of Child Rights, with a particular emphasis in this era of global communication via the Internet, when possibilities for abuses of minors are really enormous. The world has been shocked in the last several years by the cases of huge, organized pedophilic networks in several Western European countries, but also the organized one functioning in Australia. What is even more scandalous is the involvement of Catholic priests in the pedophilic networks. Large number of states in the world has amended their criminal codes in order to further protect the sexual freedom and morality of children, and children understands minors under 14, according to the Penal Code of our country. 94 out of the total number of 187 Interpol member states have already adopted corresponding legal provisions for protecting against computer child pornography and some of them have criminalized the possession of child pornography, regardless of their purpose.

The globalization and criminalization of computer child pornography are aiming at taking up broad action for preventing child abuse and sexual and financial exploitation of children, as, with the installation and functioning of computer networks globally, a corresponding global prevention action is needed in order to stop this evil. Child pornography has existed very long before the computerization era, but its mass circulation is made possible through the computerization and the Internet communication.

The material criminal legislation in the Republic of Macedonia incriminates the following: Showing child pornography materials – Art. 193; Production and distribution of child pornography – Art. 193-a and Enticing and seducing a minor under 14 to sexual activity – Art. 193-b.

Table 2: Reported, indicted and convicted perpetrators of computer crimes against sexual freedoms and morality in the Republic of Macedonia in the period between 2011 and 2015

Year	Art. 193			Art. 193 – a			Total		
	R	I	C	R	I	C	R	I	C
2011	2	/	/	1	1	1	3	1	1
2012	6	1	1	2	/	/	8	1	1
2013	3	1	1	/	/	/	3	1	1
2014	/	/	1	/	/	/	/	/	1
2015	/	/	/	/	/	/	/	/	/
Total	11	2	3	3	1	1	14	3	4

Computer child pornography as a crime has been noted in the Macedonian legal penal practice over the investigated period, with reported 14 offenders, 4 of which were convicted, which implies difficulties in providing appropriate evidence, required for taking up an indictment process and reaching court verdict. For cases with provided evidence in the trial stage involving expert evidencing as well and charges, the courts have managed to adopt corresponding verdicts for all indicted.

3.3 Computer crimes against property

In the sphere of computer crime, beside the forms of endangering human rights and freedoms, increases the threat of using computers and computer systems for the purpose of gaining material goods or causing damages of direct or indirect nature. Thus, the former case can involve gains or damages caused by means of using the data and information or their deleting from the system and/or destroying, whereas in the latter case, the system is used for entering or changing data that provide further harmful managing the property of third parties (for instance, increasing the deposit of

the perpetrators bank account!). In its nature and its objective essence, the deeds qualified as computer crime are close to damaging other people's possessions and to fraud, to which they are also related by the identical purpose of illicitly gaining property or causing damage (Камбовски В. : 2003). The computer crime, just as any other forms of crime, understands tangible crime deeds that are contained in the criminal and any other special laws, and which are manifested in that exact form, regardless of the fact that they are performed by means of a computer as an instrument, or as an object of the criminal attack, so they display certain specific characteristics in relation to the instrument and the manner of executing the criminal attack.

Computer crime offenders could not be matched with those of classical forms of crime, because of a series of specifics that makes them different. They have to possess certain knowledge and skills in the area of computer technology and criminalist informatics. It is mainly about people involved in technical intelligence and whose criminal activity could not be easily made visible, and according to that, even more difficult to be proved. Computer technology provides grounds for criminal activity at large distances; the perpetrator does not necessarily need to be in the same location with the consequence of the performed crime. This type of crime shows certain specifics and based on them, the legislation tries to classify several incriminations contained in the Penal Code that represent the grounds for taking up criminal-legal charges against perpetrators of computer crimes.

Computer crimes against property involve: Damaging and unauthorized entering a computer system – Art. 251; Computer viruses – Art. 251-a and Computer frauds – Art. 251-b.

Table 3: Reported, indicted and convicted perpetrators of computer crimes against property in the Republic of Macedonia in the period between 2011 and 2015

Year	Art. 251			Art. 251 – b			Total		
	R	I	C	R	I	C	R	I	C
2011	45	9	9	/	/	/	45	9	9
2012	23	25	21	/	/	/	23	25	21
2013	41	33	27	5	3	3	46	36	30
2014	30	14	14	/	/	/	30	14	14
2015	50	20	20	2	/	/	52	20	20
Total	189	101	91	7	3	3	196	104	94

In the Republic of Macedonia, the most frequently executed crime, with the largest number of indicted, is Damaging and unauthorized entering a computer system, regulated in Art. 251, with a number of 189 indicted out of the total number of 196 reported computer crime perpetrators against property. Out of the total number of reported 104 are indicted and 94 convicted. The percentage of conviction is 47.6% in relation to reporting and 90.4 in relation to indictment which refers to application of computer forensics in expert evidencing of electronic evidence and indictment only on the basis of provided unbeatable evidence.

3.4 Computer crimes against public finance, payment system and economy

Electronic payments by means of electronic money represent an exchange of material means via telecommunicating infrastructure, such as the Intranet banking systems or the Internet. Basically, it is about virtual (electronic) money that exists in the numerical system of the computer memory and as such knows no geographical boundaries. They can be easily transferred at great distances instantly. The most frequently used term is "electronic money" although "digital money" is a terminologically more accurate one, as the former can also be used in analogous communications. Electronic money provides purchasing products and services by means of computer in the frames of commercial computer networks, like Internet for instance, or via banking networks such as SWIFT. In a practical manner, the electronic money today replaces cash and payment checks. On the other hand, business entities are given

direct opportunity for working by using computer networks. This way of payment is also very subject to various abuses, both inside and outside the system, by persons who obtain the information of interest in a process of misuse of their position and authorities, of applying various technical means or simply intersecting the communication channels and later on using them in re-directing them to their bank accounts, or accounts of their accomplices, helpers etc.

All over the world, the criminals dealing with abuse of payment cards in the frames of organized criminal groups perform their deeds via Internet, most often hoping to achieve significant property gains in an illicit manner. In order to easily get in touch with "collaborators" for their crimes, these people join Internet services that have already formed groups with similar interests or create new forums for attracting others interested in similar topics to join with others and communicate. Beside the economic, cultural or technical reasons, there are lots of other motives that these people might have in common for joining such virtual groups.

In addition to the really large number of unemployed individuals that possess skills and competences for using the computer, are the corruption and the bad economic conditions that influence the increase of criminal deeds in the area of high-tech crime. Some of the traditional, already existing criminal groups begin to attract individuals with such skills, having in mind that a large number of computer viruses have originally, and among other reasons, been created for the purpose of stealing financial and other data contained in the payment cards and further abuses. At that time a number of Internet forums have been created in servers on the Russian territory, but also in other countries of what was once known as the Eastern Bloc. These forums used to offer a variety of data, among the best selling ones being the malicious softwares intended for stealing computer data (computer viruses), as well as data related to payment cards, user names and passwords for various servers. Such servers are known as carder services as within their frames, the perpetrators of criminal deeds offer, sell and/or exchange data from payment cards, and find their accomplices.

In the course of the 1990s, while numerous highly educated people were trying to get employed, some of the programmers, who wanted to do something, and not for little money, started making programs known as computer viruses. The term "virus factories" is used to describe the job of these intellectuals, but having no employers to offer them legal jobs, they did not receive any payment in this period. Most often, they created these viruses to express their dissatisfaction. In March 2001, the Russian

hacker, Igor Kovaliev stated in an interview: "Hacking is an excellent job, one of the few that are left". This criminal way has provided many experts with a way out of poverty and increased the chances for mobility of experts on the Russian market. The skilled engineers capable of developing new technologies, were very much interested about Internet, particularly in the area of economic works. Even today programmers in Russia are willing to work for criminal organizations, of course for good money. In this country, which is even now overburdened with violent crimes, certain organizations dealing with high-tech crime are perceived as the major force and potential of this country in the digital era. The criminals in this area are viewed as modern "Robin Hood" figures that can adequately support the organization members and their families by stealing money from the rich people from the West, who, "possess large sums of money on their accounts and cards, without any justification". In Chine for instance, according to a study carried out in 2005 by the Academy of Social Sciences in Shanghai, it is clear that hackers and rock stars enjoy the most of respect and glorification, whereas 43% of the primary school students stated they appreciate the hackers (Urošević V. and Uljanov S.).

The wide spread usage of payment cards, the coverage and availability of information technologies, have all contributed to making them very attractive to a large number of individual or groups of criminals throughout the world. Particularly vulnerable are the markets that have introduced the cards into the payment system, but lack experience in electronic finances and there is no system for preventing abuses of this kind, as well as in countries with high living standard and developed system of online trade and banking. Today the cards can be used for cash withdrawal from ATM, from the banks, for payment of goods and services, for purchases at points equipped with POS terminals, for payments in the electronic trading system and for payments related to ordered via phone or mail. The cards are used for payments on the Internet, avoiding going to the bank or to the store, from your home, both in our country and abroad. And it is the Internet that creates the largest danger related to the possibility of abuse of credit card data while making transactions via the Internet. The most frequent Internet frauds are the frauds related to selling the payment card data by organized criminal groups that obtain previously agreed sums of money as compensations on special bank accounts opened exclusively for this purpose. Also, the fast money transfer systems like Western Union etc. are used for this purpose.

The Penal Code of the Republic of Macedonia incriminates the following computer crime against public finance, payment system and economy: Production,

purchasing or alienating instruments for forging – Art. 271, p. 2 and p. 3; Preparation and using of fraudulent credit cards – Art. 274-b and Violating the rights to published or protected patent and topography of integrated circuits – Art. 286.

Table 4: Reported, indicted and convicted perpetrators of computer crimes against public finance, payment system and economy in the Republic of Macedonia in the period between 2011 and 2015

Year	Art. 274 – b			Total		
	R	I	C	R	I	C
2011	8	7	3	8	7	3
2012	11	5	1	11	5	1
2013	16	8	4	16	8	4
2014	/	/	/	/	/	/
2015	13	26	26	13	26	26
Total	48	46	34	48	46	34

The fraudulent payment card manufacturing as a crime is present in the Republic of Macedonia, but it also has an organized and international character as well. With regards to the analysis of reporting, all through to the conviction, by means of providing firm and relevant evidence, the conviction participates with 70.8% in relation to reporting, and 73.9% in relation to indictment of perpetrators.

CONCLUSIONS

The Republic of Macedonia has accepted the recommendations of the international community that refer to the incriminating of computer crime deeds and incorporated this in the Penal Code of the Republic of Macedonia. The Code foresees the incrimination of several typical computer crimes, and part of them involve the possibility for executing the crime by application of information technology and of the computer as an instrument of execution, as well as the computer systems and networks as objects of the criminal attack. This means that the criminals make use of the information technology for criminal purposes and driven by criminal motives, including

elements of abuse of personal data that causes damage to the victims, then, taking the opportunity for producing computer child pornography thus seriously damaging the morality of the minors as victims. Accumulating property and financial gains is the most frequent motive of the perpetrators which can be deduced from the deeds of crime against property executed and their number outgrows that of other forms of financial crimes.

The prosecution authorities keep pace with the contemporary trends in the forms of computer crimes and are permanently trained in the area of discovering and disclosing of these crimes and providing relevant electronic evidence, which is of key importance for the judiciary.

BIBLIOGRAPHY

1. Ачкоски Ј., (2012), Сигурност на компјутерските системи, компјутерски криминал и компјутерски тероризам, Скопје. http://eprints.ugd.edu.mk/10870/1/Skripta%20za%20Sigurnost%20na%20kompjuterski%20sistemi%2Ckompjuterski%20kriminal%20i%20terorizam_revJA_2.pdf, преземено на 15.03.2017.
2. Бановић Б. (2001), *Обезбеђење доказа у криминалистичкој обради кривичних дела привредног криминалитета,* Београд.
3. Тупанчевски Н. и Кипријановска Д. (2008), *Основи на македонското информатичко казнено право*, МРКПК бр. 2 - 3, Скопје.
4. Urošević V. i Uljanov S., (2010), *Uticaj karderskih foruma na ekspanyiji i globalizaciji zloupotreba platnih kartica na Internetu",* NBP Žurnal za kriminalistiku i pravo, Kriminalističko – policijska akademija, Beograd.
5. Јовашевић Д. , (2002), *Лексикон кривичног права*, ЈП Службени лист СРЈ, Београд.
6. Кајзер Г. , (1996), *Криминологија*, Александрија, Скопје 1996.
7. Камбовски В. (2003) *Казнено право, посебен дел"*, Просветно дело АД Скопје.
8. Konstantinović - Vilić S. i Nikolić – Ristanović V., (2003) , *Kriminologija*, Niš.
9. Николоска С., (2013), Методика на истражување на компјутерски криминалитет, Ван Гог, Скопје.

10. Petrović S., „*Kompjuterski criminal*“, drugo izdanje, Ministarstvo unutrašnjih poslova Republike Srbije, Beograd, 2001.
11. Petrović S. (2004) , Kompjuterski kriminal, Vojnoizdavački zavod, Beograd 2004, III izdanje.
12. Цуклески Г. , *Најчести облици на извршување на компјутерски криминал во САД*, Годишник на Факултетот за безбедност, бр. 1/2000, Скопје, стр. 70.
13. Council of Europe, Recommendation R(91)11 and Report of the European Committee on Crime Problems (1993).
14. http://www.popcenter.org/problems/child_pornography/преземено 01.08.2016.
15. [1] http://it.com.mk/IT-EU-Protiv-detska-pornografija-mono/преземено 31.07.2016.
16. Child Pornography and Sexual Exploitation: European Forum for Child Welfare Position Statement, 3 (Nov. 1993).
17. Кривичен законик на Република Македонија, Сл. весник на РМ бр. 07/08 и 114/09.