CYBERCRIMES – CURRENT STATE AND CHALLENGES – THE CASE OF THE REPUBLIC OF MACEDONIA

Nikola Mickovski, PhD,
Assistant professor at Faculty of Law, International Relations and Diplomacy, MIT University, Skopje, R. of Macedonia; e-mail: nmickovski@gmail.com
RistoReckoski PhD,
Associate professor at Faculty of tourism and hospitality, University "Sv. KlimentOhridski", Bitola, R. of Macedonia; e-mail: reckoice@t-home.mk

Abstract

Today we live in a world of global digital connections. In a simple and inexpensive way, with help of modern digital technologies, we can make an ordinary conversation or multimillion monetary transactions with people who are on the other side of the world. The way we spend our leisure time and the way we conduct business relations is changed by the easy access to the computer systems and the internet as well as from the up growing market of new communication devices.

In parallel with these global transformations, the way criminals commit their criminal acts have changed too. The universal digital access opens new opportunities for the modern, computer savvy delinquents, who can use this technology and knowledge to cause harm not only to business users but to ordinary users, as well. More worse is the fact that, the computers and networks may be even used for coordination and completion of terroristic attacks, which endanger us all. Unfortunately, in many cases, security services lag behind all those delinquents in terms of technical- technological sense, as well as in the personnel training for suppression of this new and up growing threat called computer or cybercrime.

Thus, for the Republic of Macedonia and the rest of the countries as an imperative comes the need to make a legal base for sanctioning the computer crimes and then to facilitate adequate capacities that will effectuate the strategy for suppression of this type of crimes. Macedonian experiences in manner of creating and constantly innovating the legal framework, as well as in practical dealings with this type of crimes, may be used as a positive example for successful suppression of cybercrimes.

Key words: computer, cybercrimes, reforms, suppression, Republic of Macedonia

INTRODUCTION

Starting from an orthodox approach in which when writing paper for an international conference,the author would attempt (successfully or not) in the introduction of the work to explain the relevance of the issue which he writes about. To accomplish this, almost as axiomatic approach is when authors join the evolutionary description of the problem with the basic definitions of phenomena in elaborated topic.Hence, the elaboration and presentation of the problem with proliferation of the computer crime, especially the best known and most commonlyexisting type, the cybercrime and the current situation and challenges for its prevention in the Republic of Macedonia, we begin in this standard manner: with historical - evolutionary overview and definition of basic conceptsand notions.

How old is the phenomenon of cybercrime? It is safe to say that soon after the first computer networks were built, some people were looking for ways to exploit them for their own illegal purposes. By analogy, just as much as an idea of theft is as old as the concept of privately owned property, and an element of almost all societies is dedicated to taking as much as possible of what isn't theirs—by whatever means they can. In that way as soon as it was widely recognized that computers store something of value (information), criminals saw an opportunity. But just as it is more difficult to target a robbery victim who stays locked up in his own home every day, the data on closed, standalone systems has been difficult to steal. However, when that data began to move from one computer to another over networks, like the robbery victim who travels from place to place, this data became more vulnerable. Networks provided another advantage: an entry point. Even if the informationthat was of value was never sent across the wire, the comings and goings of other bits of data opened up a way for intruders to sneak inside the computer, like a robber taking advantage of the victim's housemates who leave the doors unlocked on their way out.[1]

In July 1961, Leonard Kleinrock from Massachusetts Institute of Technology (MIT) in the application of his doctoral thesis writes for the flow of information in large communication networks. It was the first article that theories packet commutation (packet-switching theory) - a concept in which the information is divided into packets of data, each packet is addressed to the recipient, and is transmitted from point-to-point over a computer network to the receiver where the original message isformed from the received packets. What follows from then is a piece of history.

However, cybercrime did not spring up as a full-blown problem overnight. Inthe early days of computing and networking, the average criminal did not possesseither the necessary hardware or the technical expertise to seize the digitalopportunity of the day. Computers were million-dollar mainframe monstrosities,and only a few of them were in existence.An aspiring cybercriminal could hardlygo out and buy (or steal) a computer, and even if he did, it is unlikely that hewould have known what to do with it.There were no "user-friendly" applications;working with early systems required the ability to "speak" machinelanguage—that is, to communicate in the 1s and 0s of binary calculation thatcomputers understood.

The cybercrime problem emerged and grew as computing became easier andless expensive. Today almost everyone has access tocomputer technology; children learn to use PCs and tablets in day care, and peoplewho cannot afford computers of their own can use PCs in public libraries, or they can rent computer time at business centres orInternet cafés. Applications are "point and click" or even touch and voice-activated; it nolonger requires a computer science degree to perform once-complex tasks suchas sending e-mail or downloading files from another machine across the Internet.Furthermore, with the advance of the cell phone technology and the smartphones and tablets, almost every each one of us carries a second ready computer, 24/7 connected to internet in our pockets that are more powerful than the most advanced pc's just a few years ago. Some of today's cybercriminals are talented programmers (the hacker elite), butmost are not.Advanced technical abilities make it easier for cybercriminals to"do their thing" and cover their tracks, but these abilities are by no means ajob requirement.

Unfortunately this negative global trend did not bypass Republic of Macedonia. With the widespread ingress of digital technologies in the daily life of the average Macedonian, unfortunately also came true the opportunity for easy penetration of criminal use of exactly these digital technologies. What only a few years ago was almost science fiction and distant phenomenon that occured there, in western developed countries, unfortunately on a daily basis are filling police reports in daily newspapers and are becomingconstantconcernfor the security apparatus in attempts to prevent it.And it is them, the security apparatus and members of judiciary on all levels who necessarily need appropriate education, quality legal framework and adequate ways and methods in conjunction with up-to-date technical means for effective detection, clarification and proving computer crimes.

---

[1]Schnider L. D., Scene of the cybercrime,Syngress Publishing, 2002, p. 29.

TOWARDS WORKING DEFINITION OF COMPUTER CRIME

Considering what (in principle) should be the easiest task in the preparation of a scientific paper, the definition of basic concepts that actually outlines the overall covered issues in the article, when it comes to computer related crimes, actually appears as one of the top challenges. The conceptual definition of the computer crime or which criminal behaviourssshould be framed into this generic term shall condition and further shape the overall approach on this issue, including ways to combat computer related crimes, as well as the actors involved in the process.

To be fair, much of the problem with the definition of computer crime lies in the different approaches about its terminological determination, dilemma encountered by the authors themselves in the preparation of this text. Although the term cybercrime is most widely used and recognized, as exotic because of the name and from the powerful Hollywood film industry propaganda, however, that the right terminology for naming of this type of illegal activity would be computer crime. This approach is endorsed primarily because of the limitations of term cybercrime as a category of computer crime which is done by/with the network connection between computer systems.

Hence, having decided terminology dilemma it remains for us to focus on conceptual definition of computer crime. With relative peaceful conscience we can move cybercrime in the group of events that even closely involved actors do not know the exact and complete definition, but even the uninitiated believe that they will recognize once they see. But is it that simple and what complicates the process of extraction of precise and comprehensive definition of cybercrime?

One of the reasons lies in the phenomenological features of this group of crimes - namely the computer and the network may be involved in crime in several ways:[2]

1. A computer or network may be a means for committing the crime, or used to commit the crime
2. The computer or network may be the target of the crime ("victim")
3. The computer or network may be otherwise associated with crime (e.g. storage of illegal drug trafficking data).

On the other hand, in many cases, a series of crimes are conditionally categorised as computer crimes, basicallyrepresent a form of so-called classic crimesonly now, in their execution is included computer systems and networks. This is the case when one uses the Internet forexample - pyramid scam (Ponzi scheme), orto find customers for illegal activities associated with prostitution, illegal betting etc. All these actions are illegal in most national legislations and can be executed without the use of computer systems and networks. In this context the term "computer" is not a necessary element of the substantial definition of the crime, it is only one way to carry out the illegal activities. In fact, computer systems and networks give criminals new ways to carry out the classic forms of crimes, therefore, in these cases the same legal provisions can be used to sanction such cases when a crime is committed with or without a computer. However, some crimes are necessarily connected with the invention of the computer and establishment of the Internet as a global network, and thereforebring up the need for a clear definition of computer crimes as a necessary condition for the creation of legal provisions that penalize such behaviour.

Hence the only possible solution is that the definition for the computer crimes should be based on four main pillars:[3]

1. Unlawful conduct that constitute a breach or violation of important individual and social goods that the law provides criminal sanction for
2. Specific manner, means and purpose of the crime - the use of computer systems and networks
3. The special object of protection - the safety of computer systems and networks, streaming of stored computer data as a whole or a particular section,
4. The objective the perpetrator to obtain unlawful gain (tangible or intangible), or causing harm to others.

Given this, we define computer crimes as any illegal conduct which violates important individual and social goods; executed or in connection with the computer system or networks, and directed against the security of computer systems and the data processed by them including such crimes as illegal possession, offering and/or distribution of information through a computer system or network, committed in order for the perpetrator himself or for others to obtain unlawful gains or to cause someone harm.

COUNCIL OF EUROPE

[2] Ibid, p. 45
[3] I. Marcella, Albert J. II. Greenfield, Robert, Cyber Forensics, CRC Press, 2005, p. 48

Although this kind of comprehensive definition of computer crime we believe meets the basic theoretical and practical needs related to the efficient suppression of computer crimes, still, due to the rapid evolution of emergent forms of crimes that belong in this group we consider that is necessary as a correction to use an approach based on enumeration list of groups of similar and homogeneous crimes that fit in the group of computer crimes.

On the other hand, primarily due to the phenomenological picture of computer crimes as a group of crimes due to its inherent features almost necessarily incorporate international element, there is unquestionably a need for complementaryexistence of international instruments which will appear as a kind of focal point of international efforts to prevent this type of crimes.The result of such efforts to internationalize the effort to prevent computer crime was the adoption of the Council of Europe, Convention on cybercrime.[4]

The Convention on Cybercrime is an international treaty that seeks to harmonize national laws on cybercrime, improve national capabilities for investigating such crimes, and increase cooperation on investigations. The Convention was drafted by the Council of Europe (COE) in Strasbourg, France. In addition to COE Member states, Canada, Japan, South Africa, and the United States participated in the negotiation of the Convention as observers5 and later, signed and ratified the Convention, raising the total number of 53countries that signed and 44 countries that have ratified the Convention.[6]

The origins of the Convention date back to November 1996, when the European Committee on Crime Problems (CDPC) recommended that the COE set up an experts committee on cybercrime.[7]From the beginning, the CDPC recognized that "the trans-border character of cyber-space offences, e.g. when committed through the Internet, is in conflict with the territoriality of national law enforcement authorities."[8]Accordingly, the CDPC opined then, "a concerted international effort is needed to deal with such crimes", and "only a binding international instrument can ensure the necessary efficiency in the fight against these new phenomena."[9]

Following the CDPC's advice, the COE Committee of Ministers, in February 1997, established "the Committee of Experts on Crime in Cyber-space." The Committee of Experts' role was to examine the following subjects and to draft a "binding legal instrument" addressing them[10]:

- cyber-space offences, in particular those committed through the use of telecommunication networks, e.g. the Internet, such as illegal money transactions, offering illegal services, violation of copyright, as well as those which violate human dignity and the protection of minors;
- other substantive criminal law issues where a common approach may be necessary for the purposes of international co-operation such as definitions, sanctions and responsibility of the actors in cyber-space, including Internet service providers;
- the use, including the possibility of transborder use, and the applicability of coercive powers in atechnological environment, e.g. interception of telecommunications and electronic surveillance of informationnetworks, e.g. via the Internet, search and seizure in information-processing systems (includingInternet sites), rendering illegal material inaccessible and requiring service providers to comply withspecial obligations, taking into account the problems caused by particular measures of informationsecurity, e.g. encryption;
- the question of jurisdiction in relation to information technology offences, e.g. to determine theplace where the offence was committed (locus delicti) and which law should accordingly apply, includingthe problem of nonbis in idem in the case of multiple jurisdictions and the question how to solve positivejurisdiction conflicts and how to avoid negative jurisdiction conflicts; and
- Questions of international co-operation in the investigation of cyber-space offences.

The Committee of Experts negotiated and drafted the text of the Convention (and its Explanatory Report) over the next four years, culminating in the final draft that was approved by the CDPC in June 2001 and then adopted by the COE's Committee of Ministers on November 8, 2001, and after ratification of 5 countries, including 3 COE member states, it came into force in July 2004. On November 7, 2002, the Committee of Ministers adopted the Additional Protocol to the Convention on Cybercrime. The Additional Protocol requires ratifying Member States to pass laws criminalizing "acts of racist or xenophobic nature committed through computer networks." This includes the dissemination of racist or xenophobic material, the making of racist or

---

[4]The adequacy of the Convention of the Council of Europe as a global instrument and the need and the possibility of adopting a "global" Convention see more in Harley, B., A Global Convention on Cybercrime?, The Columbia Science and law Review, 2010

[5]Vatis, M.A., The Council of Europe Convention on Cybercrime, Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for U.S. Policy http://www.nap.edu/catalog/12997.html

[6] Status as of: 12/2/2015, http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG

[7] See Convention on Cybercrime, Explanatory Report, ¶ 7.

[8] See Convention on Cybercrime, Explanatory Report, ¶ 8.

[9]Ibid, ¶ 9.

[10]Ibid., ¶10

xenophobic threats or insults, and the denial of the Holocaust and other genocides. It also commits ratifying nations to extend to these crimes the investigative capabilities and procedures created pursuant to the main Convention.

Provisionally, the Convention can be viewed as a document consisting of three parts and Preamble. The first part upholds the substantive definitions of cybercrime offences that member countries are supposed to adopt; the second part is reserved for the investigative procedures that are required and the third part is dedicated for mechanisms aimed at bolstering international cooperation at fighting cybercrimes.

In the Preamble, the Convention states its goals that arise from the need to pursue, as a matter of priority, a common criminal policy aimed at the protection of society against cybercrime, inter alia, by adopting appropriate legislation and fostering international co-operation. In it, member states, conscious of the profound changes brought about by the digitalisation, convergence and continuing globalisation of computer networks and concerned by the risk that computer networks and electronic information may also be used for committing criminal offences and that evidence relating to such offences may be stored and transferred by these networks, state their determinations to resolve this situationby facilitating detection, investigation and prosecution of computer related crimes at both the domestic and international levels by adoption of powers sufficient for effectively suppressing such criminal offences and by providing arrangements for fast and reliable international co-operation.

In the first part, as previously mentioned, the Convention stipulates the substantive definitions of criminal offences that form the generic term computer crime. In this direction, the Convention, at first differentiates four major groups of computer crimes, comprised of:

- Offences against the confidentiality, integrity and availability of computer data and systems
- Computer-related offences
- Content-related offences
- Offences related to infringements of copyright and related rights

The first group of offencesincorporates the following types of crimes:

- Illegal access (to the whole or any part of a computer system)
- Illegal interception (made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data)
- Data interference (damaging, deletion, deterioration, alteration or suppression of computer data)
- System interference (serious hindering of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data)
- Missuses of device which incorporates the production, sale, procurement for use, import, distribution or otherwise making available of a device or a item, including a computer program, designed or adapted primarily for the purpose of committing any of the offences mentioned before; a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the mentioned crimes.

The second group of offences consist of the computer-related forgery and computer-related fraud, where the third group of offences, the content-related offences, are consisted of the crimes related to child pornography (producing, offering or making available, distributing or transmitting, procuring and possessing).

The fourth group of computer of offences is connected with the protection of copyright and related rights and is consisted of crimes committed by infringement of the afore mentioned rights.

Also in the first part of the Convention provisions are found aimed at answering the open questions about substantive criminal law institutes like, attempt and aiding or abetting and corporate liability and provisions concerningsanctions and measures as may be necessary to ensure that the criminal offences are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty.

The second part of the Convention turns its focus on establishing such investigative procedures that are adequate for accomplishingthe purpose of specific criminal investigations or proceedings in the case ofcriminal offences established in accordance this Convention, other criminal offences committed by means of a computer system and the collection of any evidence in electronic form of a criminal offence. In this part, the Convention also provides safeguards when the usage of such investigative procedures is in collision with the adequate protection of human rights and liberties, including rights arising pursuant to obligations undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments. The safeguards provide,inter alia, for principle of proportionality in provisioning of investigative procedures, judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.

Having in mind this restrictions, the Convention stipulates the following investigative procedures and powers:

- Expedited preservation of stored computer data
- Expedited preservation and partial disclosure of traffic data
- Production order to submit specified computer data which is stored in a computer system or a computer-data storage medium and a subscriber information in service provider's possession or control
- Search and seizure of stored computer data
- Real-time collection of traffic data
- Interception of content data

Concerning the last part, international co-operation, the Convention, in accordance with the provisions of relevant international instruments on international co-operation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws, to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence, regulates the extradition and mutual assistance as a form of international cooperation.[11] The Convention is predominantly specific about regulating mutual assistance and its emerging forms and applicable procedures like sharing spontaneous information, mutual assistance regarding provisional measures, Mutual assistance regarding investigative powers, procedures pertaining to mutual assistance requests, confidentiality and limitation on use, etc.

When it comes to the Additional Protocol to the Convention on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, the purpose of this amendment was to expand the scope of the Convention to cover the criminalisation of the dissemination of racist and xenophobic material through computer networks. Hence the Convention discerns four types of such crimes: offences (directed against computer systems and their content); computer-related crimes (computer system is instrument); intellectual property crimes; and content-related crimes (computer system is the environment of the crime), then dissemination of racist and xenophobic expressions fits in the latter category.[12]

The Protocol concentrates on conduct that relates to the electronic environment of computer systems and networks. The protocol defines four independent offences, but the Articles are preceded by a definition of what is called 'racist and xenophobic material'. In the next articles either this material is the object of the criminalised conduct or elements of the definition are used to qualify conduct or circumstances.Thus, art. 3 criminalises the distributing or otherwise making available to the public through a computer system of material as defined by the additional Protocol. Art. 4 deals with racist and xenophobic motivated threats against individuals or groups of individuals. The threat must involve the commission of a serious crime and it is left to the implementing Party to define a serious crime.

Art. 5 deals with racist and xenophobic motivated insults through a computer system. In the frame of the article insulting means causing prejudice to the honour or dignity of a person. The expression therefore needs to be offensive, contemptuous or invective.

Art. 6 deals with the denial or gross minimisation of acts of genocide or crimes against humanity as defined in the relevant UN-instruments. This behaviour is assumed to be deeply insulting to victims, their relatives or other survivors of such crimes. State Parties that included such a provision in their law do not yet refer to the general notions of genocide or crimes against humanity but to the holocaust. Given the fact that genocide and crimes against humanity motivated by racism and xenophobia have and are being committed after W.W. II, the provision therefore was given a more general structure.

As a last remark on the Protocol: according to Article 7 of the Protocol, State Parties can include the intentional aiding and abetting to the crimes defined in article 3-6; namely, individual member states may determine that attempts to commit one of the offences is also punishable, thus, service providers may be liable for the hosting of criminal content if they would intentionally aid or abet the crime.[13]

THE CASE OF THE REPUBLIC OF MACEDONIA

Having in mind the threat to national security and to the security of everyday life of ordinary people and their numerous interactions and transactions, and influenced by international obligation accepted and accumulated by accession to international instruments whose field of regulation are the efforts to combat

---

[11] More about newest trends in international cooperation in criminal mater, especially concerning republic of Macedonia, see BuzarovskaL. G., Mickovski N., International cooperation in criminal matters in the Republic of Macedonia, Proceedings of International Conference Rule of Law and Democracy, Law faculty, State University of Tetovo

[12].Kaspersen, Henrik W.K, Cyber Racism and the Council of Europe's reply, Computer/Law Institute, VrijeUniversiteit Amsterdam the Netherlands, p.7

[13] Ibid, p. 9

computer related crimes, Republic of Macedonia in its Criminal Code[14](CC) starting from its original form has a numerous provisions concerning sanctioning of computer crimes. Also, the Law on Criminal Procedure[15](LCP) holds a number of provisions concerning handling a digital evidences and special investigative techniques and procedures when a computer crime is involved.

The interesting thing about both legislations is that there is a clear evolutionary line in the prospect of achieving more comprehensive coverage of the different phenomenological forms in which computer related crimes can be manifested and to answer the ever evolving structure of this type of offences.

What as a general assessment can be drawn on the legal scope of computer crimes in the Macedonian criminal law is that it is an approach which for now means a maximum legal provisions for the possible forms of this type of criminal behaviour, but also relatively timely adjustment of the provisions to match the rapidly evolving and fluctuating phenomenological picture of computer related offences.

To say simply, the legislator in the Criminal Code, at least for now, provides a wide range of provisions intended to legally cover current forms of computer crime. On the other hand there is visible tendency of the legislator through relatively frequent changes of existing and prediction of new provisions to keep up with rapid changes in the emergent forms of computer crime, thus offering an effective legal framework what is certainly a necessary condition in effective suppression of this type of offences.

This situation can be easily illustrated with the fact that the original legal solution in terms of provisions for computer offences was only limited to unauthorized access and damage to the computer system, and later through continuous renewal and introduction of new legislation in effort to reach the present situation of almost maximum coverage of all possible aspects of computer crime. In this way, we can classify the Macedonian CC as a modern, appropriate and effective legal basis which adequately meets the challenges of the preventive and repressive suppression of cybercrime.

In it, even in Article 122, which contains the meaning of the terms used in the text, with the primary goal of a clear definition of certain terms in order to avoid certain vagueness and ambiguity about their exact meaning, computer system is defined as any device or group of interconnected devices that one or more of them performs automatic data processing according to a program; while computer data is defined as presentation of facts, information or concepts in a form suitable for processing by a computer system, including programs such as operating systems that put computer system into operation.

As basic forms of computer crime Code envisages three offences: Article 251 - Damage and unauthorized access into computer system, Article 251a - creating and infiltrating computer viruses and Article 251b - computer fraud.

The Article 251 - Damage and unauthorized access into computer system, represents “classical” form of computer offence which is found in criminal codes of almost all countries in the world. From the substantial definition of the crime becomes clearly visible the intention of the legislator to sanction the unauthorised maliciousintrusions in someone else’s computers, i.e. those unauthorized intrusions aimed to damage and/or use of the data or programs to which access is gained with the purpose of making illegal profit.

With this legal approach of the normative determination of the scope of the crime unfortunately remains uncovered part of the so-called "benign" unauthorized intrusions into computer systems and networks, i.e. the situation when offenders attempt or carry out unlawful access in order to demonstrate their ability to perform this intrusion, for fun, boredom and curiosity. Unfortunately this youthful “games” often occur as a starting point for much heavier similar offenses, hence one can only regret the lost opportunity for potential preventive effect of sanctioning this type of unauthorized intrusion into a computer system/network.

However, it must be admitted that this legal definition of unauthorized intrusion and attack on a computer system/network is a legal provision that the relatively adequately sanction common (in frequency and damages) intrusions and attacks, and by using of extensive descriptions legislator attempts to cover most of the existing and possible future forms of unauthorized intrusion and damage to computer systems and networks.

In this sense the legislator further continues and as a severe form of the offenceenvisages unauthorized intrusion and damage to the computer system, data or programs that are protected by special measures of protection or used in the operation of state entities, public enterprises and public institutions or international communications or participation in an organized group created to perform such acts, but as a separate form of this offence sanctions unauthorized manufacture, acquisition, sale, possession or making available other special devices, tools, computer programs or computer data intended or suitable for damaging or gaining unauthorized access into another computer system.

Correspondingly, Article 149, starting primarily from the significance and the impact of IT infrastructure in contemporary social trends, stipulates sanctioning of unauthorized access into a computer

[14]Official gazette of Republic of Macedonia, No. 37/96, 80/99, 4/2002, 43/2003, 19/2004, 81/2005, 60/2006, 73/2006, 7/2008, 139/2008, 114/2009, 51/11, 135/11, 185/11, 142/12, 166/12, 55/13, 82/13, 14/14, 27/14, 28/14, 115/14, 132/14 and 160/14)

[15] Official gazette of Republic of Macedonia, No. 150/2010 и 100/2012

information system containing personal data, in orderperpetrator, using the accessed data for himself or for others, to achieve a benefit or to inflict some damage.

Similar motivational background rests behind the legal solution inArticle 251 – a, creation and infiltration ofcomputer viruses. But in this case, unlike in the case of unauthorized intrusion and damage, legislator's normative scope moves ahead by sanctioning event the creation of computer virus with the intention of infiltratinginto another's computer or computer network (paragraph 1), not only the use of a computer virus that will cause actual damage to someone else's computer system, data or program (paragraph 2). With this normative approach is clearly demonstrated the intention of the legislator to legally cover real life situation in which the ordinary user has the largest "chance" to appear in the role of victims of computer crime - the missuses of malicious computer programs specifically designed to damage the program and/or mechanical part of computer systems or their regular functioning.

Although the legislator in the legal definition uses only the term "computer virus" that in real life situations is manly used for only a portion of malicious computer programs, hence, legally the term should be interpreted in the broadest sense, or as a term that in despite of the importance of the viruses covers and other types of malicious computer programs such as worms and Trojan horses (Trojans).

The legislator in paragraph 3 of this Article as an aggravated form outlaws the case when the use of malicious computer program caused severe damage and in the last paragraph of this Article is criminalised the attempted use of a computer virus.

Third primary crime cybercrime Macedonian Criminal Code criminalizes is the offense under Article 251-B Computer fraud. In the substantial definition of this offence the act of committing this crime is defined as act of the perpetrator who, with intent to obtain unlawful gains for himself or for others by entering into a computersystem untrue information data, not registering the factual data, changing, deleting or concealing the computer data, falsification of electronic signature or otherwise causing false results from the electronic processing and transmission of data.

From the chosen way of defining the substantial definition of this offence is evident the attempt by the legislature to incriminate a wide range of ways of committing this crime, which of course is aimed as an adequate response to a potentially rich modus operandi of the perpetrators of this crime.

On this occasion must be emphasized the separate legal provision that sanction the unauthorized manufacture, acquisition, sale, possession or making available of special devices, tools, computer programs or computer data intended for perpetrating computer fraud, for which the legislator provides fine or imprisonment up to one year.

Also in the group of basic forms of computer crimes that Macedonian CC has provisions for is the offence from Article 149-a, Preventing access to public information system. Defined as unauthorized action preventing or limiting other access to public information system, the offence is directed primarily to legally sanction so called DoS attacks, which mainly represent automated indirect attacks aimed at overloading the victim's network servers with requests and as a result of that servers actually become unusable for legitimate users.

Besides these basic forms of computer offences, Macedonian legislator imposes a series of computer crimes that are directly related to computer systems and networks, whether their role is limited to instrumentum operandi or the target of the criminal act.

Thus, in Article 147, which penalizes the violation of the secrecy of correspondence and other consignments, as a guarantee of confidentiality of communication, in paragraph 1, in the ways of carrying out this offence, the Code provides for the violation of the confidentiality of the secured e-mail, which stipulates fine or imprisonment for up to 6 months.

The role of computer systems as an auxiliary tool in the production or distribution of child pornography Criminal Code of the Republic of Macedonia sanctioned as aggravated circumstance around the main provision under Article 193-A, Production and distribution of child pornography. Namely, if the production, distribution or otherwise making available child pornography, or if its supply or possession is done through a computer system or other means of mass communication, the Code stipulates for the perpetrator imprisonment of at least eight years.

Possession and use of computer systems, components and programs is an aggravating circumstance in the case of Article 271, Making, acquisition or sale of counterfeit money. In this Article, in paragraph 2 criminal liability is stipulated for unauthorized persons who manufactures, purchases, hold, sell or use instruments, tools, computer programs and other safety components which serve to protect against counterfeiting, as well as means of unauthorized acquisition of bank data for making counterfeit money or masking the real money or other payment instruments, securities or false payment cards.

Article 379-a incriminates situations of creating the so-called computer forgery or criminal responsibility of the person with the intention of using them as genuine without authorization develops,

introduces, amends, deletes or makes unusable computer data or programs that are specific or adequate to serve as evidence of facts which have value for the legal relations. The same paragraph provides responsibility for the person who uses such data or programs as genuine and shall be punished by a fine or imprisonment up to three years.

If such work or computer forgery is committed against the computer data or programs used in the operation of state entities, public institutions, companies or other legal entities and individuals who are working in the public interest or in the legal traffic abroad or if their use has caused significant damage, shall be punished with imprisonment of one to five years.

In connection with the logistical basis and tools for the creation of computer forgery, the law provides for liability for the person that manufactures, sells, keeps or is making them available to other: special devices, tools, computer programs or computer data intended or suitable to perform the computer forgery.

In addition to these legally regulated offences that are belonging in the narrow sense of to the group of computer crime, Macedonian CC has provisions for several criminal acts that only conditionally are placed in this group. Mainly, in this group we place offeneces that are related to the creation and use of false credit cards. The first offence is unauthorized manufacture, acquisition, holding, selling or giving for usage instruments, articles, computer programs and other components for security or protection which serve to protect against counterfeiting as well astools for unauthorized gathering bank data for making forgedpayment cards in addition to their encasingon banking devices in order for making forgedpayment cards or their usage in any other way in order to obtain data from a real bank payment cards and data for holders of such cards. This legal provision primarily regulates the misuse ofdevices for collection and the misuse of electronic data from credit cards. Such devices are also known as skimmers and they contain dedicated prepared part of which is built-in camera to capture PIN codes and additional part "data reader" from the magnetic tape, which also mounts on the ATM.

Also sanctioned is manufacture itself, acquisition and use of false credit card and other ways of obtaining data from a real bank payment cards and data for holders of these cards in order to use them for fabrication and use of forged payment card or such collected data is given to someone else with such intention.

Finally, as the latest amendment to the Code provides criminal liability for misuse of computer systems as a medium for the dissemination of racist and xenophobic material. Namely, it incriminates the usage of computer system to spread racist and xenophobic written material, picture or other representation of an idea or theory that helps, promotes or incites hatred, discrimination or violence against any person or group on the basis of race, colour, national or ethnic origin, or religious beliefs in public. For this offence the legislator provides imprisonment of one to five years, and if the offense is committed with abuse of power or authority or this offence provokes riots and violence against people or property damage to a large extent, the provisioned prison sentence is one to ten years.

Accordingly to this legal structure and substantial definitions of computer crime in the Criminal Code and its role in standardization of conditions and content of the right of the state to impose criminal sanctions on the perpetrators of criminal acts on the one hand, and on the other hand given the role of criminal procedural law to define the conditions and actions for the implementation of substantive criminal law, or the necessity of complementary and functional unity of the two legal disciplines in achieving the goals of the criminal policy, imposes the need for separate procedural solutions that arise in the role of the necessary preconditions to the correct, fair and full implementation of the norms of substantive law.

Without going into this point in to the details of the particularity of detection, prosecution and proving the computer crimesbut we will address several specific solutions that are included in the new Macedonian Law on Criminal Procedure[16], and have a direct impact in the offences from the scope of computer crime.

Thus with Article 184 of the new LCP, in the part referring to the procedural rules regarding measures for finding and securing persons and objects, to be more precise concerning the provisions on the search of the homes, the LCP regulates the procedure for performing a search of a computer system and computer data. Regarding it, the legislator firstly in Article 181 paragraph 2, stipulates that the search of the computer system is to be done only with the prior existence of a written and reasoned court order (warrant), obtained at the request of the public prosecutor, and in cases where it is likely to delay the proceedings, at the request of the judicial police.Hence, Article 184 stipulates the obligation of the person using the computer or have access to it or to

[16]The new Macedonian LPC establishes a new type of procedure, which is based on principles set out in the Strategy for the reform of criminal law, such as the expansion of the application of the principle of opportunity in crime persecution, extrajudicial settlements, plea bargaining and simplified procedures. Also, the new LCP is based on making distance from the judicial paternalism and placing the burden of proof on the interested parties; providing an active and leading role of public prosecution in the pre-trial proceedings with effective control of police; abolition of the judicial investigation, providing major role in the investigation for the public prosecutor; introduction of the preclusion of certain procedural actions and measures against the abuse of procedural powers by the parties; strict deadlines; rationalization of the system of legal remedies; implementation of the recommendations of the European Union and the Council of Europe on the criminal proceedings; creating more efficient public prosecution through the establishment of a new operative management bodies as well as leadership and cooperation with the police and other agencies involved in law enforcement

another device or data carrier to allow access to them and to provide the necessary information to the enforcement agent of the aforementioned court order to guarantee the smooth achieve the goal of the search.

Also, in paragraph 2 of this article is provided for the duty of the person - the user of the computer system, or the person who has access to it or to another device or data carrier, to immediately take measures to prevent the destruction or alteration of data. From this solution is evident intention of the legislator, at least legally, to regulate the preservation of key information with potentially unstable character like the data stored in the so called RAM (Random Access Memory).

The sanction for failing to respond to the mentioned legal provisions for the person using the computer or have access to it or to another device or data carrier is provided as a fine of 200 to 1,200 euros, with the possibility that amount to increase tenfold if despite the imposed fine, the person still does not act on the court order.

The Criminal Procedure Code contains provisions that address the specifics of temporary seizure of computer data. It is the data stored in the computer and similar devices for automated or electronic data processing, devices which are used for collection and transmission of data, data carriers and subscriber information available to the service provider and data that according to the Criminal Code must be seized or which may serve as evidence in criminal proceedings. Seized data is given for storage to the public prosecutor or authority designated by a special law or otherwise provides their storage. The judge of the previous procedure on the proposal of the public prosecutor with special decision can determine protection and storage of computer data until it is needed, at a maximum of six months. After this period, the data will be returned, unless if that data is involved in committing the following crimes: Damage and unauthorized access into a computer system under Article 251, Computer Fraud under Article 251-B and Computer forgery under Article 379. Also, seized data won't be returned if the datais included in the commission of another (different) criminal act committedwith the help of a computer or if it serves as evidence of a crime.

As for the practical application of this legal framework for incrimination of computer crime, as illustrative, both in terms of numbers and dynamics, and in terms of efficiency in tackling, we present the results of Skopje Basic Public Prosecution Office regarding Unauthorized access into a computer system under Article 251 of the Criminal Code of the Republic of Macedonia which is probably the most typical offence for computer crimes.

Table 1. Volume of cases that were brought before the Basic Public Prosecution Office – Skopje, concerning Art. 251 of the Criminal Code of Republic of Macedonia

Year	2010	2011	2012	2013
Total criminal charges	10	7	12	10
Request for additional information to Ministry of interior	1			
Indictment	3	2	4	3
Rejected criminal charges	2	1	4	4
Waiver of prosecution			2	
Investigation	2	1		3
Termination of investigation	1			
Verdict	1 (probation)	3 (probation)	2 (probation) 1 fine 1 imprisonment	4 (probation) 2 imprisonment

From the presented table is visible the relative stability of the number of criminal charges for which acted Skopje public Prosecution Office, and the relatively small size of the incidence of such crime in the overall operation of this prosecution. Also, from the relatively large number of dropped charges, the obvious conclusion is relatively low quality and reliability of the charges, which is an indication of the need for intensive training of competent authorities for better handling in dealing with this type of crimes. However, one of the arguments justifying this low number of criminal charges for computer crimes lies in the fact that a great number of the cases are basically criminal acts with a foreign element and were solved using the institutes of international legal assistance and cooperation.

Another obvious fact of this relatively modest research on the dynamics and the prevalence of cybercrime are relatively mild judicial penalties that the convicted perpetrators of this crime received, which is partly explained by the relative youth of the perpetrators and the fact that in almost all cases they were first time offenders and previously had absolutely no conflicts with criminal or tort law, but on the contrary, were considered promising and valued members of the community.

CONCLUSION

Cybercrime is one of the newest and one of the most dangerous forms with greatest potential to threaten the quality of human life and safety. After all its features it carries and practically demonstrate potentially devastating effect primarily due to our vulnerability arising from our reliance on the use of digital devices in everyday life and communication.

Hence as a priority stands out a question of finding appropriate and effective ways to deal with this threat. The first step in this direction is the establishment of adequate legislative basis that will put in legal limit the possible responses to the threat of computer crime. In the process of establishing such a legislative solution must be taken in to account that on one side the legal basis must be wide enough to cover all potential forms of computer crime (which in itself is a challenge mainly because of extremely rich phenomenological picture of this type of crime), and on the other side to be flexible enough to cover new forms of computer crimes thatappear every day. Finally this legislative framework must be balanced in such a way so it does not limit the legitimate use of computer and network technology in everyday stations.

On the other hand, it is important to work on the internationalization of efforts to deal with this kind of offences primarily because of its international nature. Partial approach is doomed to failure from start. European Convention together with the Additional Protocol is the first, but insufficient step, however it traces the possible solutions for the establishment of unified universal approach in dealing with computer crime. In it, in emphasis is put to a comprehensive approach, which incorporates substantial definitions of computer offences and procedural prerequisites for the prosecution of these cases accompanied with the principles and conditions that determine the international assistance and cooperation in dealing with the computer criminal acts.

The case of the Republic of Macedonia is representative of relatively firmly set legal basis for prosecution of computer related offences. Substantive legislation is packed with a wide range of incrimination that include most forms of computer crime, and it is in accordance with the requirements of the European Convention. On the other hand, frequent changes of criminal legislation enabling timely innovation and customization of incrimination contained in the Criminal Code allow relatively comprehensive system that adequately responds to the new challenges. What is missing is a greater staffing and greater competenceof the involved actors to deal with these crimes which would enable timely detection, clarification, proving and crime prevention.

REFERENCE

1. Buzarovska L. G., Mickovski N., International cooperation in criminal matters in the Republic of Macedonia, Proceedings of International Conference Rule of Law and Democracy, Law faculty, State University of Tetovo
2. David R. Johnson &David G. Post, *Law and Borders-The Rise of Law in Cyberspace,* 48 STAN. L. REv.1367 (1996)
3. Desante Anthony F., *Evidentary Consideration for Collecting and Examining Hard- Drive Media,* The George Washinton University, 28.11. 2001, Forensic Sciences 262
4. I. Marcella, Albert J. II. Greenfield, Robert, Cyber Forensics, CRC Press
5. Icove, D., Segar, K., and VonStorch, W., *Computer Crime, A Crimefighter's Handbook,* O'Reilly & Associates, 1999
6. Harley, B., A Global Convention on Cybercrime?, The Columbia Science and law Review, 2010
7. James Boyle, *Foucault in Cyberspace: Surveillance, Sovereignty, and Hardwired Censors,* 66 U. CIN. L. REv.177, 179 (1997).
8. Kaspersen, Henrik W.K, Cyber Racism and the Council of Europe's reply, Computer/Law Institute, VrijeUniversiteit Amsterdam the Netherlands
9. Krsul I, *Authorship Analysis: Identifying the Author of a Program,* Department of Computer Sciences, Purdue University, M.S. Thesis, CSDTR-94-030, 1994.
10. Pettinari Dave, *Handling Digital Evidence from Seizure to Court Presentation*, IOCE conference, june 2000

11. Pollit Mark M., *Report on Digital Evidence,* (FBI CART report, DC Washington, USA), Interpol Forensic Science Symposium, Lyon, France, 16-19.10.2001
12. Rosenblatt, K. S., High Technology Crime — Investigating Cases Involving Computers, KSK Publications, San Jose, CA, 1995.
13. Schnider L. D., Scene of the cybercrime, Syngress Publishing, 2002,
14. Vatis, M.A., The Council of Europe Convention on Cybercrime, Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy http://www.nap.edu/catalog/12997.html
15. Weber, Amalie M., The Council of Europe's Convention on Cybercrime, Berkeley Technology Law Journal, Volume 18 | Issue 1, January, 2003
16. Whitcomb C. M., *A Historical perspective of Digital Evidence*: *A Forensic Scientists View,* International Journal of Digital Evidence, proleće1. 2002, vol.1, issuue 1.