Cybercrimes In Macedonian Criminal Code

Nikola Mickovski, PhD,
Associate professor at Faculty of Law, International Relations and Diplomacy, MIT University, Skopje, R. of Macedonia; e-mail: nmickovski@gmail.com

Elizabeta Spiroska, PhD,
Assistant professor at Faculty of Law, International Relations and Diplomacy, MIT University, Skopje, R. of Macedonia; e-mail: e.spiroska979@gmail.com

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 criminals, 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 criminals 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, Republic of Macedonia

Introduction
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. In that way as soon as it was widely recognized that computers canstore 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 information that 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

However, cybercrime did not spring up as a full-blown problem overnight. In the early days of computing and networking, the average criminal did not possess either the necessary hardware or the technical expertise to seize the digital opportunity of the day. Computers were million-dollar

mainframe monstrosities, and only a few of them were in existence. An aspiring cybercriminal could hardly go out and buy (or steal) a computer, and even if he did, it is unlikely that he would have known what to do with it. There were no “user-friendly” applications; working with early systems required the ability to “speak” machine language—that is, to communicate in the 1s and 0s of binary calculation that computers understood.

The cybercrime problem emerged and grew as computing became easier and less expensive. Today almost everyone has access to computer technology; children learn to use PCs and tablets in day care, and people who cannot afford computers of their own can use PCs in public libraries, or they can rent computer time at business centres or Internet cafés. Applications are “point and click” or even touch and voice-activated; it no longer requires a computer science degree to perform once-complex tasks such as 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 one of us carries a second ready computer, 24/7 connected to the 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), but most 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 a job 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 occurred there, in western developed countries, unfortunately on a daily basis are filling police reports in daily newspapers and are becoming constant concern for 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.

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 computer related crimes, Republic of Macedonia in its Criminal Code (CC) starting from its original form, has a numerous provisions concerning sanctioning of computer crimes. The general assessment for the Criminal Code is that, at least for now, it provides a wide range of provisions intended to cover current forms of computer crime. On the other hand, there is visible tendency of the legislator through relatively frequent changes of existing and creation 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 crimes.

This situation can be easily illustrated with the fact that the original legal solution in terms of provisions for computer crimes was only limited to unauthorized access and damage to the computer system. 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 Code, with the primary goal of providing 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 the appropriate program, necessary to activate the computer system.

As basic forms of computer crime, Code envisages three offences in articles 251, 251a and 251b.

The Article 251 - Damage and unauthorized access into computer system, represents “classical” form of computer crime that can be found in criminal codes of almost all countries in the world. From the legal definition of the crime becomes clearly visible the intention of the legislator to sanction the unauthorised malicious intrusions in someone else’s computers, i.e. 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 from the normative scope of the crime unfortunately remains uncovered the so-called part of "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 an aggravated form of the crime envisages 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 authorities, public enterprises and public institutions or international communications. The second aggravated form the basic crime is a crime committed with participation in an organized group created to perform such acts. As a separate form of this crime, CC 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 information system containing personal data, in order perpetrator, using the accessed data for himself or for others, to achieve an unlawful gain or to inflict damage.

Similar motivational background rests behind the legal solution in Article 251 – a, creation and infiltration of computer viruses. But in this case, unlike in the case of unauthorized intrusion and damage, legislator’s normative scope moves ahead by sanctioning even the creation of computer virus with the intention of infiltrating into 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 misuses 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.
The third primary cybercrime that Macedonian Criminal Code criminalizes is the crime under Article 251-B Computer fraud. The legal definition of this crime incriminates perpetrator who, with intent to obtain unlawful gains for himself or for others, enters into a computersystem untrue data. The crime can also be committed with not registering the factual data, changing, deleting or concealing computer data, falsification of electronic signature or otherwise causing false results from the electronic processing and transfer of data.

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 sanctions with monetary 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 crime from Article 149-a, Preventing access to public information system. Defined as unauthorized action that prevents or limits others from access to public information system, the legal norm is set to sanction the 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.

Consequently, 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 committing the crime, the Code has provisions for violation of the confidentiality of the secured e-mail, which stipulates monetary fine or imprisonment for up to 6 months.

The usage of computer systems as an auxiliary tool in the production or distribution of child pornography Criminal Code of the Republic of Macedonia sanctions 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 committed 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 also 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 and predicts criminal responsibility for perpetrator who, 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 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 computer forgery is committed against computer data or programs used in the operation of state authorities, 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, perpetrators 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 liability for the person that manufactures, sells, keeps or is making them available to others: 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 crimes, Macedonian CC has provisions for several criminal acts that only conditionally are placed in this group. Mainly, in this group we place offences that are related to the
creation and use of false credit cards. The first crime 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 as tools for unauthorized gathering bank data for making forged payment cards. This legal provision primarily regulates the misuse of devices for collection 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 the manufacture itself, the acquisition and usage of false credit cards and other ways for obtaining data from a real bank payment cards and data for holders of these cards in order to use them for fabrication of forged payment card.

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 crime is committed with abuse of power or authority or this crime provokes riots and violence against people or a property damage to a large extent, the provisioned prison sentence is one to ten years.

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

<table>
<thead>
<tr>
<th>Year</th>
<th>2013</th>
<th>2014</th>
<th>2015</th>
<th>2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total criminal charges for Article 251</td>
<td>10</td>
<td>7</td>
<td>12</td>
<td>10</td>
</tr>
<tr>
<td>Request for additional information to Ministry of interior</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Indictment</td>
<td>3</td>
<td>2</td>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td>Rejected criminal charges</td>
<td>2</td>
<td>1</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>Waiver of prosecution</td>
<td></td>
<td></td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>Investigation</td>
<td>2</td>
<td>1</td>
<td></td>
<td>3</td>
</tr>
<tr>
<td>Termination of investigation</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Verdict</td>
<td>1 (probation)</td>
<td>3 (probation)</td>
<td>2 (probation)</td>
<td>4 (probation)</td>
</tr>
<tr>
<td></td>
<td>1 fine</td>
<td>1 imprisonment</td>
<td>1 fine</td>
<td>1 imprisonment</td>
</tr>
</tbody>
</table>

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 that appear 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.

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. 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 competence of the involved actors to deal with these crimes which would enable timely detection, clarification, proving and crime prevention.

Reference

4. I. Marcella, Albert J. II. Greenfield, Robert, Cyber Forensics, CRC Press
8. Kaspersen, Henrik W.K, Cyber Racism and the Council of Europe's reply, Computer/Law Institute, VrijeUniversiteit Amsterdam the Netherlands