Eur J Crim Policy Res
DOI 10.1007/s10610-015-9277-7

Cybercrime Tendencies and Legislation in the Republic of Macedonia

Dragi Rashkovski[1] · **Vasko Naumovski**[1] · **Goce Naumovski**[1]

Abstract The advancement of information and communication technologies opens new venues and ways for cybercriminals to commit crime. There are several different types of cybercrime offences that need to be treated in a separate and different manner. The major international source that provides guidelines for treatment of cybercrime is the Convention on Cybercrime adopted by the Council of Europe and the European Commission Action Plan. The purpose of the paper is to present, discuss and analyze the Macedonian legislation treating cybercrime, with respect to the specific cases typically encountered in practice and the international guidelines concerning cybercrime. The major source of cybercrime legislation in Macedonia is the Criminal Code with provisions thereof in ten of its articles; it addresses cybercrimes such as personal data abuse, copyright and piracy issues, production and distribution of child pornography, computer viruses, intrusions into computer systems, computer fraud and computer forgery. We also present and analyze reports on cybercrime complaints and victims from Macedonia, issued by the Internet Crime Complaint Center and the Macedonian Ministry of Internal Affairs. The reports reveal the unusually high number of complaints for perpetrators and victims originating from Macedonia. Furthermore, we highlight several recent cybercrime cases reported in Macedonia. All things considered, the Macedonian penal legislation is modern and it follows the current European and world standards. It provides guidelines for successful resolution of cybercrime committed in the Republic of Macedonia. However, it could be improved by a more active inclusion of Macedonian authorities in the global response to cybercrime and by stronger enforcement of cybercrime prevention measures and strategies.

Keywords Criminal law · Cybercrime · Macedonian legislature

✉ Dragi Rashkovski
Dragi.Rashkovski@gmail.com

[1] Iustinianus Primus Law Faculty, Ss. Cyril and Methodius University, Blvd. Goce Delcev 9B, 1000 Skopje, Macedonia

Published online: 10 May 2015

Introduction

The development of computers and information and communication technology plays three different roles in the punishable crimes. To begin with, they could be the target of a punishable crime. Typical examples of this role are the cases including viruses, hacking, etc. Next, computers could appear as media for data storing when committing crimes, i.e., computers are enabling or enhancing crimes. Finally, they could be means for committing a crime (Fen Lim 2007, p. 248–251). All of this lead to the appearance of the term *cybercrime*.

The term *cybercrime* encompasses not only the crimes linked to the Internet network, but also to other computer networks and devices of information and communication technology, even telephone lines and mobile networks. Apart from the use of the terms "Internet crime" and "cybercrime" in field of penal law, we should also mention the computer or information penal law (Kambovski 1997), while in the field of criminology the term "cyber criminology" is more and more used (Jaishankar 2007).

In addition to this, the evolution of the Internet introduces new types of punishable crimes and a higher level of diversity (UNODC 2013). As part of the cybercrime, in the broader sense of the term, the Internet crime encompasses all the illegal acts committed on the Internet or with the help of the Internet. Considering the diversity of the available services provided by the information and communication technology and their ever-growing user-base, cybercrime presents a special challenge for the contemporary penal law and criminological sciences. It is highly relevant and as such it has caused an avalanche of research as well as broad legislative activity both internationally and nationally. Sources of information about cybercrime committed world-wide are the Internet Crime Complaint Center (IC3) annual reports.[1] Namely, Macedonia is mentioned in the last two available IC3 reports for the years 2012 and 2013. In the 2012 report, Macedonia is ranked 6th by the total number of complaints and 29th by the reported loss (with the total amount of 765,840.14 US dollars), while in the 2013 report, Macedonia is ranked 14th by the total number of complaints received with subject information included in the complaint and 6th by the total number of victim originated complaints.

Other reliable and valuable sources of information about the cybercrime in Macedonia are the annual reports of the Ministry of Internal Affairs and its special unit for investigation of information and communication technologies related crimes. The data reveal that both the number of registered offences and the number of reported offenders increases until 2009. Then, the number of reported offenders drastically decreases, while the number of registered offences is slightly increased.

The study reveals that Macedonia is not an exception when it comes to cybercrime. There are several cases that have been treated with success in the past. The Macedonian authorities are relatively well equipped both in terms of technical equipment and personnel to deal with such cases. Moreover, the Criminal Code of Macedonia follows the guidelines outlined by major international conventions and treaties, including the Convention of the Council of Europe on cybercrime.

The remainder of the paper is organized as follows. In Sect. "Cybercrime in practice", we overview the forms of cybercrime typically encountered in practice. Next, we outline the classification of cybercrime in the literature in Sect. "Classification of cybercrime types in the literature". We then focus in Sect. "Legal classification of cybercrime" on the treatment of

[1] The annual IC3 reports are available for download at http://www.ic3.gov/media/annualreports.aspx

cybercrime both at international level and the Macedonian legislation. Finally, in Sect. "Conclusion", we provide conclusions and final remarks.

Cybercrime in Practice

Cybercrime in the United States

According to the US FBI's Internet Crime report for 2007,[2] 35.7 % of all the reported cases of crime in the US were Internet crimes, while the damages from the Internet frauds were estimated to be around 239 million US dollars. In the newest report for 2013,[3] the estimated loss is just above 574 million US dollars. The most frequent types of Internet frauds reported to the IC3 for 2013 include the following:

- Car fraud: Criminals attempt to sell vehicles they do not own by offering a very tempting offer on various online platforms and services.
- Impersonation e-mail scams: The criminals send threatening e-mails impersonating various government agencies and respective high-ranking officials, or a hit man hired to kill the victim. The e-mail instructs the recipient to pay a fee to remain safe and avoid being hurt.
- Intimidation/extortion scams: The perpetrators extort funds from victims by intimidation with false claims in which the perpetrators pretend to be government officials monitoring the victims' Internet usage. These scams include cryptolocker ransomware (a pop-up appears that states that some files on the victims' computer are encrypted), child pornography scareware (a message appears that the victims' computer is locked due to allegedly visiting sites with child pornography thus breaking US federal laws), citadel ransomware (a message appears on the victims' computer that their computer was used for illegal activities, such as downloading copyrighted material or child pornography). In all of these scams, the only way for unlocking the computer is to pay a certain fee.
- Real estate fraud: The perpetrators send e-mails or even make phone calls to the victims representing themselves as real-estate agents listing homes for rent with prices much below the usual market price. Similar to this is the timeshare vacation houses scam.
- Grandparent telephone scams: A perpetrator contacts an elderly individual posing as a relative in a desperate need of an assistance, such as an accident or an arrest, thus creating sense of urgency. Once victims appear to believe the perpetrator, they are provided with instructions to wire money to an individual, e.g., a "bail bondsman", for saving their close relative from the unpleasant situation.
- Work-at-home (employment) scams: Organized cyber criminals usually recruit victims through ads, online employment services, e-mails and social networking websites. Victims then become their "mules" whose financial accounts are used to steal and launder money.
- Software company telephone scams: Perpetrators call victims impersonating representatives from legitimate and famous software companies notifying the victims that malware

[2] 2007 Internet Crime Report, FBI's Internet Crime Complaint Center (IC3), http://www.ic3.gov/media/annualreports.aspx

[3] 2013 Internet Crime Report, FBI's Internet Crime Complaint Center (IC3), http://www.ic3.gov/media/annualreports.aspx

was detected on their computer. The perpetrators offer to remove the malware after paying a fee.
- Payday loan and loan modification scams: The perpetrator relentlessly attempts to contact victims via their home, cell and work phone numbers. Victims are told they are overdue on a payday loan and must repay the loan to avoid legal consequences or offers a loan modification plan. These schemes are so successful because the perpetrators use accurate information about the victims (typically obtained through an identity theft), including personal identification numbers, dates of birth, addresses, employer information, bank account numbers, names and sometimes even telephone numbers of relatives and friends.
- Romance and sextortion scams: Perpetrators usually initiate contact via social media websites and/or online dating websites, and entice and manipulate the victims under the promise of love and romance. They engage the victim in video chats and manipulate them to expose themselves in sexually compromising situations. The perpetrator then threatens to make the videos available to all of the victims' social networking friends and other online contacts unless payment is made.
- Gun sale scams: Criminals attempt to sell firearms (often rifles or long guns) by offering a very tempting offer on various online platforms and services.
- Photo/mug shot scam: Perpetrators upload photos or mug (police) shots of individuals to some web services with the aim of extorting money. Victims are required a copy of their driver's license, court record and other personal identifying information in order to remove the material from the services. This provides the perpetrator with information they can exploit for a variety of other crimes.
- College and university scams: These include two types of scams. In the first scam, the perpetrators register domains similar to domains owned by well-known colleges and universities and open an e-mail address that appears to be from a legitimate institution. The perpetrators then create fake purchase orders or requests for quotations and place orders with various merchants for items such as routers, toner, or hard drives. The second scam involves spear-phishing e-mails that are sent to university employees to dupe them into giving up their log-in credentials to the schools' websites.

All things considered, the cases of internet fraud are very much diverse and the perpetrators are very resourceful in coming up with new schemes and scams.

Cybercrime in the European Union

The European Union established a European Cybercrime Centre (EC3) at Europol as a main tool in the EU's fight against cybercrime. Its main goal is to "support Member States and the European Union's institutions in building operational and analytical capacity for investigations and cooperation with international partners".[4] Note that Macedonia is not yet a member state of the European Union, hence EC3 does not monitor the state of the cybercrime in Macedonia. EC3 officially started working on 1 January 2013 with a main focus on the following areas of cybercrime:

- Committed by organized groups to generate large criminal profits such as online fraud
- Causing serious harm to the victim such as online child sexual exploitation

[4] https://www.europol.europa.eu/ec3

– Affecting critical infrastructure and information systems in the European Union

EC3 published the 2014 Internet Organized Crime Threat Assessment (iOCTA) — the first report of its kind treating the cybercrime issues in EU. In the report, EC3 highlights the following cybercrime types encountered in the EU:

– Crime-as-a-Service: Usage of underground forums for offering criminal services, including infrastructure for launching criminal cyber-attacks, selling large volumes of compromised personal and financial data, hacking services aimed toward social networking sites, stealing of private data or even economic espionage, and money-laundering services.
– Malware: Deployment of malicious software using various attack vectors (ways of intrusion in the system). The typically deployed malware is criminal botnets, ransomware and banking trojans.
– Child sexual exploitation online: The perpetrators create, store and share sexually explicit materials depicting children. They usually do not form typical organized crime groups, nonetheless they still organize themselves in an analogous hierarchy on platforms where they exchange child abuse material, either in video, pictures or even text format. The content is gathered by using sextortion scams. The perpetrators typically meet in various Internet news groups or darknet[5] sites.
– Payment fraud: These include the use of stolen credit card for purchasing goods or cash withdrawal.
– Criminal finances online: These include the exploitation of money mules and/or virtual currencies for money laundering.
– Crimes relating to social engineering: These include sending spam e-mails, and phishing for luring victims to websites attempting to elicit login credentials and other sensitive data from them, or hosting exploits specifically tailored for compromising the visitor's computer.
– Data breaches and network intrusions: Various attacks aimed at compromising data either personal data (e.g., credit card information) or company (sensitive) information. A vast majority of these attacks (over 90 %) are performed using nine basic attack methods, such as web application attacks, cyber espionage, point of sale, Intrusions, crimeware (banking trojans), insider misuse (including as victims of social engineering attacks), physical loss/theft, card skimmers, DOS attacks, and miscellaneous errors (e.g., human error such as misdelivery).
– Vulnerabilities of critical infrastructure: Critical infrastructure are physical and virtual assets or systems such as power/energy supply, water treatment and supply, and public transport. A potential attack would have a significant impact on safety, security, public health, the economy or social well-being of a large population.

The assessment of EC3 calls for a joint action of the EU member states to address the increasing number of cybercrime cases. Moreover, it recommends to put more focus on the prevention by properly educating the citizens about cybercrime and the danger it may pose. Finally, it invites the legislators in the EU to prepare "a balanced and coherent package of legislative measures that protect citizens and businesses online and enable law enforcement

[5] A darknet is a private network connecting only trusted peers, called "friends" (F2F), by using non-standard protocols and ports. The sharing of files in the darknets is anonymous (i.e., IP addresses are not publicly shared).

and prosecution services to intervene where necessary". Such a package needs to contain the right balance between protecting the privacy of the citizens, while enabling law enforcement to effectively investigate indications of criminal activity.

Cybercrime in Macedonia

We now analyze and discuss cybercrime tendencies in Macedonia. We begin by presenting the data from the Internet Crime Complaint Center (IC3) for the year 2013. Next, we overview the annual reports of the Macedonian Ministry of Internal Affairs and its special unit for investigation of information and communication technologies related crimes. Finally, we highlight some typical cybercrime offences reported in Macedonia.

IC3 Reports About Macedonia

Valuable sources of information about cybercrime being committed world-wide are the Internet Crime Complaint Center (IC3) annual reports.[6] Macedonia is mentioned in the last two available IC3 reports for the years 2012 and 2013. The 2012 report of IC3 about Internet crime also provides some statistic about Macedonia. Macedonia is ranked 6th by the total number of complaints (victims from cybercrime) and 29th by the reported loss. More specifically, the total reported loss by Internet fraud in 2012 in Macedonia amount to 765,840.14 US dollars.

The 2013 report of IC3 lists Macedonia with 508 complaints as 14th by the total number of complaints received with subject information included in the complaint. Furthermore, Macedonia with 1670 complaints is listed as 6th by the total number of victim originated complaints received by IC3 in 2013 and their countries of residence. However, Macedonia is not listed with the top 50 countries by reported loss. The number of complaints for both reports from 2012 to 2013 includes both the complaints that list dollar loss amounts and complaints that do not list dollar loss amounts. The reduction of the loss amounts from 2012 to 2013 may be due to the change from credit card frauds to offences related to the social networking media such as identity theft, sextortion/extortion etc.[7]

We analyze the 2013 IC3 report from several aspects and the outcomes of the analysis are depicted in Figs. 1 and 2. The complete data used to produce the figures are given in the Appendix. Considering the size of the countries on the list both in terms of population[8] and in terms of economy,[9] Macedonia is the smallest country. Macedonia also has the smallest number of estimated internet users 1,314,696,[10] with Internet penetration score of 63.1 %.[11]

We first focus on Fig. 1 and the number of complaints received. The total number of complaints worldwide for the year 2013 was 262,813. The country with the most complaints is

[6] The annual IC3 reports are available for download at http://www.ic3.gov/media/annualreports.aspx
[7] http://www.mvr.gov.mk
[8] The population data was collected from Wikipedia and the national statistical services (data accessed on 20.01.2015).
[9] The data about the size of the economies as given by the gross domestic product (derived using the purchasing power parity) and the gross domestic product per capita was collected from the International Monetary Fund (IMF)
[10] The data about the number of Internet users was obtained from the Population data, Int. Programs, U.S. Census Bureau.
[11] The data about the Internet penetration was obtained from the International Telecommunications Union (Geneva).

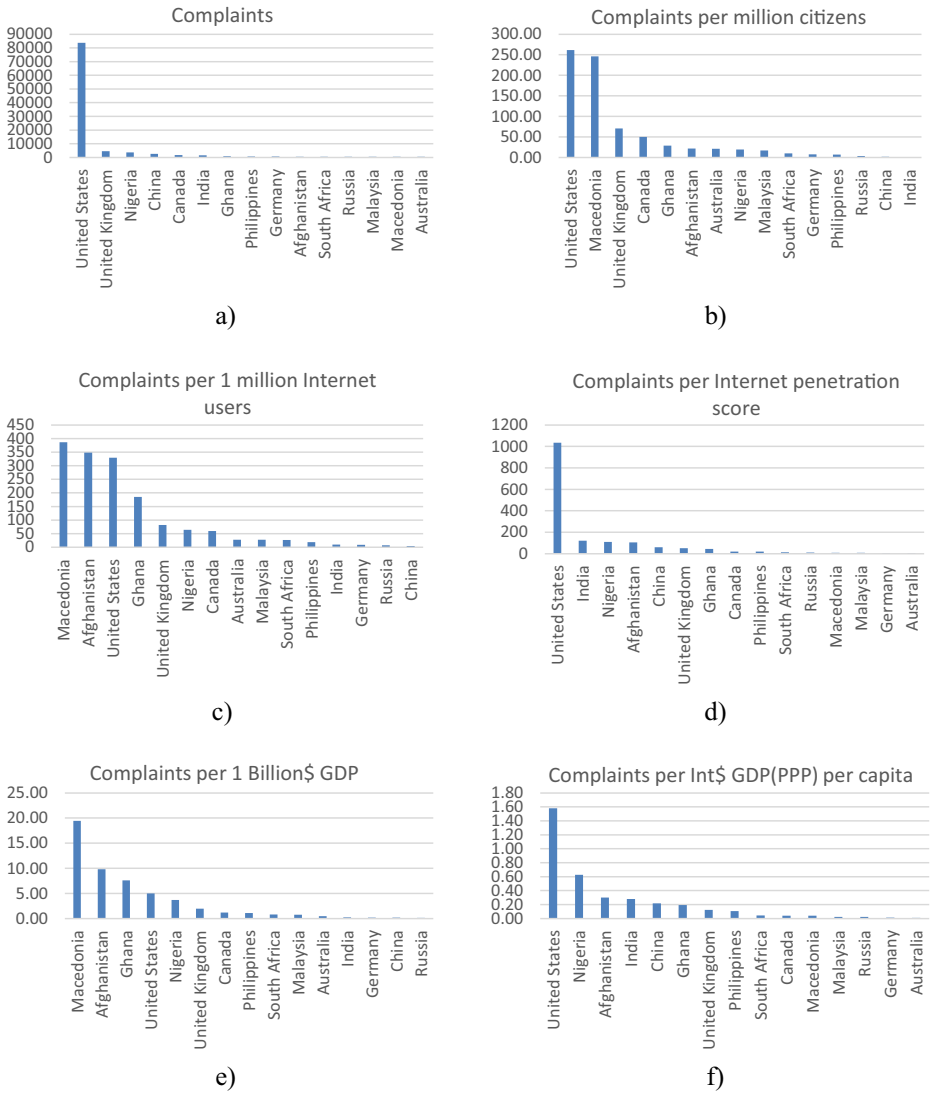

Fig. 1 Analysis of the data about the top 15 countries ranked by the total number of complaints submitted to the IC3 for 2013 ranked by the total number of complaints. **a**) per country; **b**) per 1 million of citizens; **c**) per 1 million Internet users; **d**) per Internet penetration score; **e**) per 1 billion USD$ of gross domestic product (derived from purchasing power parity); and **f**) per Int$ of GDP per capita

the United States accounting for 31.89 % from the total number of complaints received. Macedonia is ranked 14th with 508 complaints (Fig. 1a). The number of complaints per 1 million citizens puts Macedonia in 2nd place, right behind the United States of America (Fig. 1b). We next order the countries by the estimated number of Internet users, i.e., the citizens that have a potential to commit cybercrime (Fig. 1c). Macedonia is top ranked in this case. Furthermore, we look at the number of complaints per the Internet penetration score of the countries (Fig. 1d). Macedonia on this list is ranked 11th. Next, we discuss the impact of

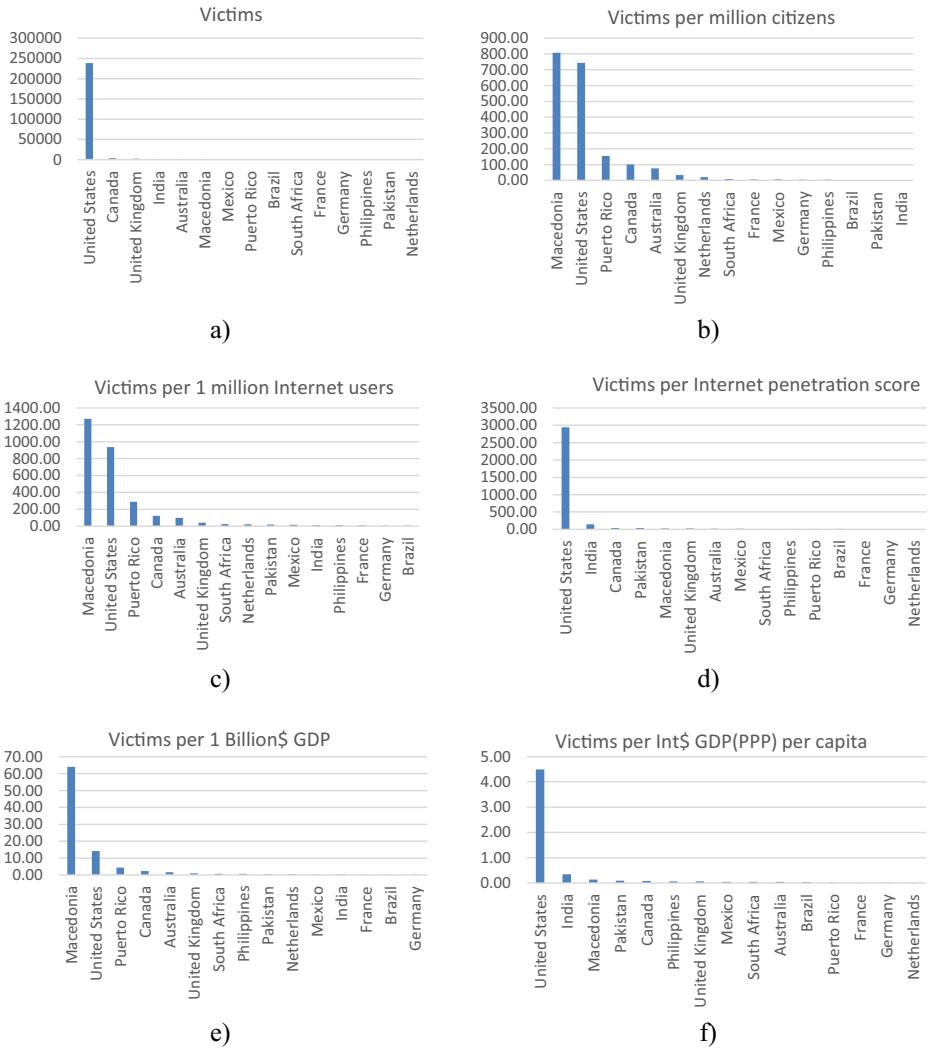

Fig. 2 Analysis of the data about the top 15 countries ranked by the total number of victim originated complaints submitted to the IC3 for 2013 ranked by the total number of complaints. **a**) per country; **b**) per 1 million of citizens; **c**) per 1 million Internet users; **d**) per Internet penetration score; **e**) per 1 billion USD$ of gross domestic product (derived from purchasing power parity); and **f**) per Int$ of GDP per capita

the size of the economy on the number of complaints. We see that Macedonia is the top ranked country by the number of complaints per 1 billion USD of gross domestic product (Fig. 1e), while is ranked 12th by the Int$[12] GDP per capita.

In Fig. 2, we provide analysis of the data on total number of victim originated complaints submitted to the IC3 for 2013. Top ranked country by number of victims is the United States

[12] Int$ is a hypothetical unit of currency that has the same purchasing power parity that the U.S. dollar had in the United States at a given point in time. This currency is used to derive the purchasing power parities of the different countries.

with 90.63 %, while Macedonia is ranked 6th with 0.64 % of the victims reported to IC3 (Fig. 2a). We then look at the number of victims per 1 million of citizens. Macedonia is top ranked on this list, slightly ahead of the United States (Fig. 2b). The situation is similar if we focus on the number of victims per 1 million of Internet users (Fig. 2c). Next, Macedonia is ranked 5th by the number of victims per Internet penetration score (Fig. 2d). Furthermore, from the point of view of the size of the economy, Macedonia is the top ranked country by the number of victims per 1 billion of USD of gross domestic product (Fig. 2e) and 3rd by the number of victims per Int$ GDP per capita. All in all, this analysis shows that Macedonia is a high risk country for cybercrime considering its population and economy size.

Ministry of Internal Affairs Reports About Cybercrime in Macedonia

Another source of information concerning the cybercrime in Macedonia are the annual reports of the Ministry of Internal Affairs and its special unit for investigation of information and communication technologies related crimes. We summarize the reports by the number of registered offences and reported offenders in Fig. 3. It can be seen that both the number of registered offences and the number of reported offenders increases until 2009. Then, the number of reported offenders drastically decreases (from 73 in 2009 to 15 in 2013), while the number of registered offences is slightly increased (from 63 in 2009 to 74 in 2013). This means that there are fewer people that commit larger number of offences. The observed phenomenon might be due to three reasons: the increased awareness of the general population about the dangers of cybercrime, the small number of offenders perform series of crimes and the majority of the complaints are not submitted to the Ministry of Internal Affairs, but to IC3.

Highlighted Cases of Cybercrime Offences in Macedonia

In the crime reports of the Macedonian Ministry of Internal Affairs,[13] we can notice that the following cybercrime types are encountered most frequently: credit card frauds, child pornography, personal data abuse, sextortion scam, and hacking and illegal penetrating in computer systems. We highlight several of these cases.

The most frequent cybercrime type encountered in Macedonia is the *credit card frauds*. There are several cases where criminals were caught with large number of credit cards with stolen user data. For example, in June 2014, two perpetrators were arrested because they acquired 14,825 credit card information over the period of 2008–2012. The perpetrators used stolen, physical credit cards to alter the data stored on them with some of the credit card data they acquired with the purpose of using the forged cards to gain personal wealth. Moreover, they were selling some of the stolen credit card information to person(s) from Bulgaria, Russia, Ukraine, United States, Greece, Romania, and Slovenia. Next, in July 2009, a perpetrator was caught with forged credit cards that managed to acquire over 4 million Macedonian denars (just over 75,000 USD). Furthermore, in July 2014, ten perpetrators managed to acquire nearly 100,000 USD and 100,000 EUR using banking data obtained from phishing sites. The perpetrators used the stolen data to send money to themselves or close relatives through money sending services, such as Western Union and Moneygram. Finally, in June 2012, the Macedonian Ministry of Internal Affairs was a part of a large international effort called CARD

[13] The highlighted cases are available at the web pages of the Macedonian Ministry of Internal Affairs http://mvr.gov.mk/

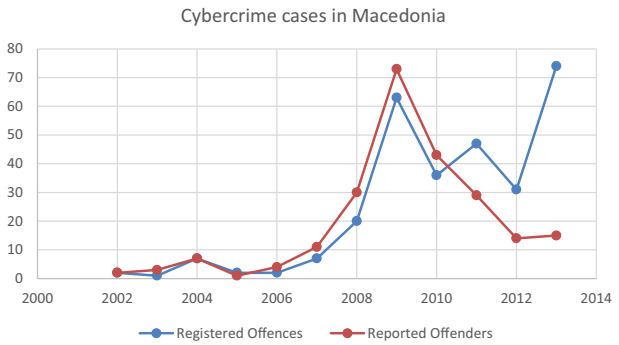

Fig. 3 Cybercrime cases reported to the Macedonian Ministry of Internal Affairs for the period 2002–2013

SHOP with the aim of capturing perpetrators that use fraudulent credit cards. This international effort was led by the US Federal Bureau of Investigation and considered 13 countries. The operation CARDSHOP was conducted for 2 years 2010–2012. The Macedonian authorities charged two perpetrators for credit card fraud.

The *child pornography* is also often encountered in the reports of the Macedonian Ministry of Internal Affairs. We enumerate a couple of these cases. In March 2014, a perpetrators was charged for distribution of child pornography. Namely, the perpetrators used fake Facebook profiles to send sexually explicit photos of minors to another minor. Next, in June 2010, a perpetrator was arrested that was storing over 300 videos and over 30,000 photos containing child pornography. In July 2014, a perpetrator was charged for storing and distributing child pornography to other people. Namely, the perpetrator was sending recordings of his own sexually explicit acts with a minor to other people. Moreover, the perpetrator also performed *sextortion scam* by black-mailing the victim of the recordings with wider distribution of the recordings. Finally, in June 2010, a perpetrator was reported for sextortion of a victim for money. More specifically, the perpetrator threatened the victim with uploading the recordings on social networking sites, such as Facebook, unless the victim pays the amount of 2000 EUR.

Classification of Cybercrime Types in the Literature

In the scientific theory, there are numerous qualifications of the forms of cybercrime. According to Burden and Palmer (2003), cybercrime refers to two groups of punishable crimes. The first group encompasses the so-called "punishable cybercrimes" which include cases of: hacking, cyber vandalism, dissemination of viruses, denial-of-service attacks, and cybersquatting. The second group incorporates cases of "electronically enabled punishable crimes" such as credit cards abuse, information abuse or theft, slander, blackmail, child pornography, hate web sites, money laundering, violation of copyright and related rights, cyber terrorism and encryption. In the case of "punishable cybercrimes", the computers and information and communication technology are the target of the crime, while in the case of "electronically enabled punishable crimes" they are the tools for committing other crimes.

Apart from the common classification, Fen Lim (2007, p.281) also gives an interesting, more specific classification to particular cases of punishable crimes in the field of cybercrime. These cases are typically from the group of crimes "enabled" by computer and information and communication technology. They encompass activities such as Internet pedophilia, fraud,

cyber stalking, gambling, selling alcohol, securities fraud and page jacking (stealing/copying the contents of a known Web site).

McQuade's classification of cybercrime forms takes as the basic criterion the way in which the crime is committed, i.e., the specific form of information technology abuse (McQuade 2006). Those forms include writing and spreading malicious codes, thefts and frauds, interfering with computer services, computer spying and illegal trespassing, unlawful exchange of files, abuse of computers and electronic devices in the academic environment, on-line harassment and computer linked punishable crimes against sexuality.

Having in mind all of this, the cybercrime forms can be globally classified in several groups: thefts and frauds; computer spying; hacking and illegal penetrating in computer systems; viruses distribution and other forms of malicious software (malware); cyber stalking; production and distribution of illegal pornography; cyber terrorism; and violation of intellectual property rights. This categorization of cybercrime is much more specific than the one provided in the Convention on Cybercrime adopted by the Council of Europe and the European Commission Action Plan and the one available in the Macedonian penal law. This is due to the fact that the Convention and the Action Plan provide general definitions and guidelines for the national and international authorities for handling the cases of cybercrime. Consequently, they do not provide very specific descriptions of the types of the cybercrime. Similarly, the Macedonian legislation is based on both the Convention of the Council of Europe and the EC Action plan, thus the categories used there are similar to the ones from the Convention and the Action plan. Nonetheless, we map the categories presented in this section into the general categories from the Convention, the Action plan and the Macedonian legislature. In the remainder of this section, we briefly describe each one of these.

Thefts and Frauds

The most common forms of thefts and frauds that include abuse of information and communication technology are frauds with credit cards and securities, identity thefts and intercepting and usurping computer services.

Frauds with Credit Cards and Securities

With the credit cards fraud, the perpetrator uses data from victims' credit card in order to illegally make a certain purchase of goods or services or to make other changes on the account. The credit card fraud is such a widely spread form of cybercrime that there is even special illegal software for searching data from existing, issued or forged credit cards.

The possibility for fraud also exists in case of securities trade performed via the Internet, known as stock or investment fraud (Fen Lim 2007). It is a scheme that misleads investors to make sales or purchase decisions on the basis of false information. Securities fraud can also include other schemes such as embezzlement by stockbrokers, stock/market manipulation, tampering of the financial reports of a public company, insider trading, and giving false statements to auditors.

Identity Theft

Identity theft is a case of illegal acquisition and use of personal data in order to get goods and services on somebody else's behalf. The identity theft is often accompanied with the credit card fraud, but it could have other goals, such as committing frauds in the course of electronic

agreements (for example selling or buying real estate), electronic payment of bills, etc. The US Federal Trade Commission Identity Theft Survey Report shows that in the 1998–2003 period over one million users of computer services were victims of identity theft (Synovate 2003).

Intercepting, Usurping, and Interfering with Computer and Telecommunication Services

Intercepting and usurping computer services encompasses all forms of interfering or preventing computer or telecommunication services that could have damaging consequences for a broad range of users of these services. Among the most frequent forms of intercepting, usurping, and interfering with computer services are the following (McQuade 2006):

- *The theft of a signal broadcasted by cable TV providers*: all acts of modifying the existing devices or using new devices in order to enable illegal physical access to the signal.
- *Denial of service attack*: an attack on computers or networks by disassembling them into their components, attacking the software in order to prevent its functioning, and overburdening the system in order to disable it.
- *Sending unwanted and disturbing e-mails (spamming)*: sending enormous number of e-mails of commercial or marketing nature with (often) disturbing or insulting contents.
- *Adware*: installing a computer program that enables pop up of certain contents of advertising nature (banner) on the desktop or integrating these contents in the communication software.

Computer Spying

Computer spying encompasses acts of using special computer software ("spyware") that 'nests' in the computer in order to take over the control of the system for the purpose of collecting and receiving information, installing other types of software, redirecting the internet browser to other pages, etc. The term spyware originates from 1995 and is related to a comment regarding the business practices of Microsoft and it referred to using hardware devices for spying (such as small dimensions cameras). However, this term was used for the first time for software in 2000.[14] Spyware, as a term, especially by the computer security experts is frequently replaced with "malware" in order to underline the maliciousness of the software (*malus* = bad), while the creators of this software call it "adware".

The actions of the "spying" software are on the rise due to at least two reasons: rise of the so called "peer-to-peer" applications (e.g., torrent downloads) and the marketing elements on the web pages. For these reasons, people have been speaking about a "spyware inferno". The legislation tries to respond to this challenge. One of those attempts in the US legislation is the Spyware Control Act adopted by the State of Utah that has been showing certain results (Wienbar 2009).

Hacking (Illegal Penetrating of a Computer System)

The standard broad definition of hacking encompasses all forms of using technology for purposes for which that technology is not intended (Taylor 1999; McQuade 2006). Computer

[14] In this context the term was used by Gregor Freund, the founder of Zone Labs, at a press conference for the promotion of a new product (www.zonealarm.com).

hacking as such represents accessing a computer system without expressed or indirect permission by the owner of the computer system (Bainbride 2004). The more restricted meaning of the term hacking, i.e., unauthorized penetration in the computer system as a form of cybercrime is illegally gaining access to one or more computer systems by abusing the security shortcomings and overcoming the security obstacles such as passwords and firewalls in order to use or steal data or to insert new (external) program functions (McQuade 2006).

Viruses Distribution and Other Forms of Malicious Software (Malware)

The term computer virus was used for the first time in the 1970s within the ARPANET in order to mark computer self-applying programs that were harmful to the computer system (Chen and Robert 2004). Apart from the term "computer virus" another term is also used: "computer infection program", i.e., malicious software (malware). The difference between computer viruses and computer spying is that the former can cause physical damage to the targeted system (e.g., erasing of the disks, gauging the network communication etc.), while the latter has the purpose of recording the victims' information and sharing it with the perpetrators. According to Filiol (2005 p.82), the computer infection programs refer to four categories of malware: logical bombs, Trojan horses (Trojans), viruses, and worms. The nesting phases and the existence of a virus are (Filiol 2005): infection (spreading the virus in the overall environment, i.e., the attacked computer system), incubation (virus's survival in the environment), and realization (infecting of the system). Distribution of computer viruses is one of the most common forms of cybercrime according to the data provided by the US Attorney General Office in 2001. Moreover, 29.1 % of the cybercrime cases concerned the distribution of viruses/malware (Smith et al. 2004, p.22).

Cyberstalking

Cyberstalking means using a computer or another form of information technology for following other people's activities and movements without them knowing about it for the purpose of frightening them, sexual pleasure and domination or other illegal motives (McQuade 2006). Cyberstalking, as a form of cybercrime, consists of two elements: a) collecting information about the victim (on the Internet or from other sources) and b) stalking, disturbing/harassment, frightening the victim. The latter element is often performed without a physical contact, but it includes appearance of the stalker in front of the home of the victim, telephone calls, leaving written messages, property damaging, etc. Cyberstalking, has certain similarities and differences when compared to conventional stalking ("Offline" stalking) that are listed in Table 1 (Fen Lim 2007).

The criminology experts differentiate a number of categories of cyberstalking. According to Ogilvie (2000), there are three categories of cyberstalking that correspond to the three categories of functions that are typical for the Internet as a medium.

- Convincing: sending e-mails to the victim with threats, attempts for initiating or renewing a love affair, frightening, etc.;
- Control: the perpetrator controls the computer or other devices that belong to the victim, and
- Broad range: endangering the victim and spillover of consequences from the virtual into the real world. An example of this type of cyberstalking is placing discrediting pornographic photos or personal information about the victim on certain web sites.

Table 1 Similarities and differences between cyberstalking and "offline stalking" (Fen Lim 2007)

	Cyberstalking	"Offline" stalking
Victim	Most frequently a woman	Most frequently a woman
Perpetrator	Most frequently a man	Most frequently a man
Motive	Desire to control the victim	Desire to control the victim
Distance of the perpetrator from the victim	Big or small	Small
Potential new perpetrators	The perpetrator could encourage third parties to harass the same victim	Small probability
Prosecution of the perpetrator	More difficult due to anonymity	Easier

In regard to legislative initiatives on cyberstalking, a positive experience is the UK adoption of the Protection from Harassment Act in 1997 that encompasses comprehensive regulations about this type of cybercrime.

Production and Distribution of Illegal Pornography

Information technology and especially the Internet enable easy production and distribution of child and other types of illegal pornography, primarily due to the fact that it ensures anonymity. In comparative law, the actions of production, downloading, dissemination as well as simple possessing of materials with illegal pornographic contents are punishable. Distribution often is performed usually through communication and internet chat software or news groups (Fen Lim 2007). According to the data provided by the US Justice Department starting from 1995 the number of cases linked to child pornography on the Internet shows an increase of ten percent annually (PWG 2000). Apart from child pornography in most legislations, production and distribution of illegal pornography refers also to contents of zoophilia, necrophilia, and forms of sadomasochism (McQuade 2006).

Cyberterrorism

The term cyberterrorism refers to all acts that combine forms of terrorism and cyberspace. It was first introduced by Colin (1997). According to Denning (2000), the acts of cyberterrorism have two important features:

1. These are illegal attacks and threats of attacks of computers, networks, and information aimed at threatening governments and people in order to achieve certain political or social goals and
2. The attack results in violence against persons or property or at least threatening persons or property to a certain degree in order to cause fear.

Criminology experts point at a number of common features on cyberterrorism and organized crime (Shelly 2002): firstly the victims are either individuals or groups; secondly the perpetrators are hierarchically structured in networks or organization; and thirdly both groups of perpetrators use computer or telecommunication technologies for achieving their goals.

According to the Centre for the Study of Terrorism and Irregular Warfare, Naval Postgraduate School in Monterey, CA USA (1999) there are three types of cyberterrorism:

- Simple (non-structured): Basic attacks against individual systems using tools created by others.
- Advanced (structured): Sophisticated systems and networks are used, and the attackers develop their own basic tools; and
- Complex (coordinated): Integrated complex tools are used with a high level of coordination and organization of the attack.

The actions of cyberterrorism can cause huge material damages. For instance, the costs for dealing with the consequences from the infecting of 300,000 computers as a result of the Code Red attack (whose target was the White House), amounted three billion dollars even though this has never been officially confirmed (McQuade 2006). However, cyberterrorism still has not reached the proportions of conventional terrorism.

Having in mind the level of interaction of information technology and terrorist activities, it is absolutely possible to expect cyberterrorism to gain even broader dimensions. It is a challenge to which the national legislation needs to respond. To this end, the United Nations Office on Drugs and Crime (UNODC 2012) published a study on the use of the Internet for terrorist purposes where it outlines the means by which the Internet can be utilized for terrorist purposes, the international context and the potential international response to such acts. The study calls for a coordinated and cooperative national and international action in terms of legislature, policy, and enforcement.

Violation of Intellectual Property Rights

The need for criminalizing the violation of the intellectual property rights in the context of cybercrime results from the following. Firstly, the perpetrators of the violation tactically and strategically are capable of avoiding the measures of civil-legal protection. Secondly, usually these are perpetrators that repeat the violations, frequently organized in criminal groups and their activities threaten the security or the health of the people. Thirdly, a criminal organization in the field of intellectual property is characterized with illegal distribution through a network that intends to avoid police and customs controls (Harms 2007).

The violation of intellectual property rights as a form of cybercrime is always performed by using information and computer technology as means of committing the crime. The criminalization of these violations, nomo-technically, could be covered either by the criminal codes or by the laws that regulate the right to intellectual property. Among the more significant examples from the comparative law are the Digital Millennium Copyright Act from 1998 (DMCA) and Lanham Act from 1946 in the US law as well as Copyright, Designs and Patents Act (complemented by the 2002 Copyright and Trademark-Offences and Enforcement Act) in the UK law. Within the European Union, the EU Directive on criminal measures aimed at ensuring the enforcement of intellectual property rights — IPRED2 was prepared. Still this Directive has not been adopted because there are reactions among the scientific and expert public, both in regard to whether the EU is at all competent about this matter and with regard to the procedure of adopting it.[15]

Especially important is the criminalization of digital piracy as a form of violation of copyright and related rights, since it is a phenomenon that causes enormous material losses. According to Graborsky and Smith (1998, p.89), digital piracy often is defined as illegal

[15] More about the reactions on the Directive's text see: Letter of the Dutch Parliament to EU Commissioner Frattni, concerning the IPERD2 Directive, July 2006, available at europapoort.nl (10.01.2009).

reproduction of works that belong to somebody else in order to be used free of charge or presented as their own intellectual works.

According to the European Union data losses from digital piracy amount to hundreds of billions of Euros and about 200,000 jobs are threatened.[16] With regard to software piracy, according to the data of the Business Software Alliance the piracy rate globally in 2013[17] was 43 % with losses of over 62 billion US dollars, in the EU member-countries — 31 % and losses of over 13 billion US dollars. In the Republic of Macedonia, the software piracy rate for 2013 was estimated significantly higher (at 65 %) and loss worth over 19 million of US dollars. In Table 2, we give the values for the piracy rates and the losses due to piracy for Macedonia, United States of America and the European Union for the period 2007–2013. We can note that the data about Macedonia follow the global trend of a slight decrease in the piracy rates recorded for both USA and EU. However, the financial loss has increased from 2007 until 2011, then for 2013 there is a slight decrease of the estimated loss due to piracy.

Legal Classification of Cybercrime

Convention on Cybercrime of the Council of Europe

The most relevant international source concerning the treatment of the cybercrime is the Convention on Cybercrime adopted by the Council of Europe (2001).[18] It is the first international treaty addressing Internet and computer crime by harmonizing national laws, improving investigative techniques, and increasing cooperation among nations.

The Convention consists of four sections. The first section contains definitions of the basic notions. The second section regulates the measures that should be undertaken on national level by the member-countries: measures that refer to the substantive and procedural penal law and competence. Within this section the following offences that are punishable in the area of internet crime are defined:

- Offences against confidentiality, integrity, and availability of computer data and systems that incorporate: a) illegal access; b) illegal interception of computer data; c) illegal damaging of databases; d) system interference; and e) misuse of devices. These offences cover the following categories of cybercrimes: computer spying, hacking and illegal penetrating in computer systems, viruses and malware, cyberstalking and cyber terrorism.
- Computer-related offences a) Computer-related forgery; and b) Computer-related fraud. These offences cover cyber thefts and frauds.
- Content-related offences (child pornography). These offences cover the cybercrime of production and distribution of illegal pornography.
- Offences related to infringements of copyright and related rights. These offences cover the violation of intellectual property rights.
- Ancillary liability and sanctions: a) Aiding or abetting the commission of offences that are punishable; and b) Corporative liability.

[16] Combating Counterfeiting and Piracy in the Single Market COM (98) 569, Final act.
[17] Study reports available at http:// http://globalstudy.bsa.org/
[18] The Convention and its Explanatory Report were adopted by the Committee of Ministers of the Council of Europe (109th Session on 8 November 2001) and consequently opened for signature in Budapest, on 23 November 2001. It entered into force on 1 July 2004.

Table 2 Piracy rates for Macedonia, United States of America (USA), and the European Union (EU) for the period 2007–2013 according to the estimates of BSA Software Alliance

	Piracy rates [%]			Loss due to piracy [millions $USD]		
	Macedonia	USA	EU	Macedonia	USA	EU
2007	68	20	35	11	8040	12,383
2009	67	20	35	15	8390	12,469
2011	66	19	33	22	9773	14,433
2013	65	18	31	19	9737	13,486

The third section of the Convention regulates the international cooperation and legal aid. Finally, the fourth and last section contains the final provisions.

By November 2013, 41 countries signed and ratified the Convention, while the additional 11 countries have signed it but have not ratified it yet. Republic of Macedonia signed the Convention on 23 November 2001 (on the opening for signatures) and ratified it on 15 September 2004. The Convention entered into force in Macedonia on 1 January 2005.

European Commission Action Plan

Considering the international level, the G-8 ministers of justice and internal affairs with their activities from December 1997 as well as the 1996 European Commission Action Plan contributed to the more precise definition of the Internet punishable crimes. Both these platforms on the Internet abuse, setting off from the transnational character of the Internet crimes consider as Internet crimes all the cases in which one or more of the following goods are violated (Adamski 1998):

- National security (instructions for making bombs, illegal production of drugs, terrorist activities). These violations are covered by cyber terrorism.
- Protection of minors (marketing abuse, violation, and pornography). These violations are covered by the cybercrime of production and distribution of illegal pornography.
- Protection of human dignity (racial hatred and racial discrimination). These violations are usually part of cyber stalking.
- Economic security (frauds, directions for credit cards piracy). These violations are covered with the frauds with credit cards and securities.
- Information security (hacking). These violations are covered with the following cybercrimes: hacking and illegal penetrating in computer systems, viruses, and malware distribution and intercepting, usurping and interfering with computer and telecommunication services.
- Privacy protection (illegal communication of personal data, electronic harassment). These violations are covered with the following cybercrimes: identity theft, computer spying, and cyber stalking.
- Reputation protection (slander and offensive articles, illegal comparison advertising). This is tightly connected with cyber stalking.
- Intellectual property (illegal distribution of creators' works, for example software or music). These offences cover the violation of intellectual property rights.

Legislation of the Republic of Macedonia

The Criminal Code of the Republic of Macedonia follows the guidelines from the European Council's Convention given in the previous section and the guidelines from the 1996 European Commission Action Plan. It envisages several offences that are punishable and which are linked directly or indirectly to information technology. These offences are identified as follows:

- Personal data abuse (art. 149)
- Theft of a satellite signal (art. 157-a)
- Infringement of copyright (art. 157)
- Piracy of audiovisual work (art. 157-b)
- Phonogram piracy (art. 157-c)
- Unauthorized use of software or invention (art. 286)
- Production and distribution of child pornography through a computer system (art. 193-a)
- Creation and insertion of computer viruses (art. 251-a)
- Unauthorized intrusion into a computer system (art. 251)
- Computer fraud (art. 251-b)
- Computer forgery (art. 379-a)

In the remainder of this section, we discuss these offences in more detail.

Personal Data Abuse

The violations that come from personal data abuse are sanctioned in Article 149 of the Criminal Code. This article relates to the cybercrime of identity theft and cyber stalking. In compliance with it, collecting, processing or use of personal data without consent of the citizen represents a case of personal data abuse. Protection of personal data is one of the constitutional categories (safety and confidentiality of personal data). For cybercrime, relevant is the form of abuse of personal data that consists of penetration in the personal data computer information system with an intention by the perpetrator to acquire benefit for himself or somebody else or to inflict damages (Article 149, Paragraph 2). The sanction for performing this offence is a fine or an imprisonment for up to 1 year.

The most serious form of abuse of personal data is if the crime is committed by an official in the course of performing his/her official duties for which a sentence imprisonment of 3 months up to 3 years is envisioned (Kambovski 1997 p.129). Moreover, the attempt for personal data abuse is also a punishable crime.

Theft of a Satellite Signal

The Criminal Code in its article 157-a stipulates a sentence of imprisonment of 6 months up to 3 years for the person(s) that will interrupt, manipulate, re-distribute, rent or otherwise transmit publicly a specially protected satellite signal, if that signal is protected and this is done without the permission of the signal operators. If the goal of the offense is to gain personal wealth or substantial damage is caused, then the punishment is imprisonment of 1 year up to 5 years. If this crime is performed by a legal entity, then the punishment is monetary.

Punishable Crimes Which Subject of Protection is Intellectual Property

The Criminal Code of the Republic of Macedonia envisages several punishable crimes in which computers are used as means for committing the crime or a medium for storing data when committing the crime where the subject of protection is intellectual property (Naumovski et al. 2007), i.e., violation of intellectual property rights.

The violation of copyright or related rights represents unauthorized publication, presentation, reproduction, distribution, performing, broadcasting or in any other way illegal encroaching on somebody else's copyright or related right, i.e., a work, performance or subject of related right (Article 157 Paragraph 1). The sanction is monetary or sentence imprisonment of 6 months up to 3 years. When a computer system is used to commit the above offences, then only the imprisonment sentence can be carried out. If the crime from Paragraph 1 was used for acquisition of a personal property, the sanction is sentence imprisonment of 6 months up to 5 years. Moreover, if the crime from Paragraph 1 was used for acquisition of significant property, the sanction is sentence imprisonment of 1 up to 5 years.

The subject of protection of the punishable crime of an unauthorized use of somebody else's invention or software (Article 286) is the right of the inventor, legally regulated and protected as an industrial property right. The crime is committed by the one who with no authorization uses, publishes, gives or transfers somebody else's registered or protected invention, as well as the one who uses somebody else's software in an unauthorized manner. The sanction is monetary or sentence imprisonment of up to 3 years. If this violation is performed with the aim of gaining a considerable amount of wealth then the sentence is monetary and imprisonment from 1 up to 5 years. Moreover, if the crime is committed by an organized group or the well-being of some person is at risk the sentence is monetary or at least 3 years imprisonment.

The punishable crime of audiovisual work piracy (Article 157-b) concerns the audio-visual work, i.e., videogram or its, in unauthorized way multiplied, copies regardless whether those are 35 mm (cinema right), video and DVD rights or Video–CD rights. These works are protected from illegal production, import, reproduction, distribution, storage, renting, selling or in another way making it available to the public. The frequent violations of copyright and related rights of music works impose the need of introducing the crime of Phonogram Piracy (Article 157-c) thus incriminating phonogram piracy regardless whether it is a musical work reproduced on a cassette, CD, DVD or Video-CD rights. The sanction for committing any of the violations in Articles 157-b and 157-c is imprisonment of 6 months up to 3 years. If this violation is performed with the aim of gaining considerable amount of wealth or a considerable amount of damage is being caused then the sentence is imprisonment from 1 up to 5 years.

Production and Distribution of Child Pornography Using a Computer System

Production of child pornography for the purpose of its distribution as well as transfer or offering or in some other way making child pornography available via a computer system represents a punishable crime according to Article 193-a. The sanction for this is a sentence imprisonment of at least 5 years. Acquisition of child pornography using a computer system for oneself or somebody else, as well as possession of child pornography in the computer system or medium that serves for storing computer data with the intention of showing them to third parties or for distribution is punishable with a sentence imprisonment of 5 up to 8 years. If these violations are committed using a computer system or other device for mass communication then the punishment is at least 8 years of imprisonment.

Creation and Insertion Computer Viruses

Article 251-a from the Criminal Code regulates the making or taking over of computer viruses from somebody else, with the intention of inserting it in third party's computer or computer network. The sanction for this crime is monetary or sentence imprisonment of up to 1 year.

A more serious form of this offence is the use of a computer virus and causing damages in somebody else's computer, system, data or program. In this case the sanction is a sentence imprisonment of 6 months up to 3 years (Paragraph 2). If with this offence, a more significant damage was caused or the offence was committed as part of a group for committing such an offence, the perpetrator will be punished with sentence imprisonment of 1 to 5 years.

Damaging and Illegal Penetrating in a Computer System

The offence of "damaging and illegal penetration in a computer system" from Article 251 of the Criminal Code encompasses: entering, altering, hiding, deleting or destroying, or making the computer data and programs unusable or making the use of the computer system or the computer communications more difficult (Paragraph 1).

The offence is also committed by someone who penetrates the computer system for the purpose of acquiring illegal property or other benefit for himself/herself or for somebody else or causing property damage or other damages; and for the purpose of transferring computer data that he/she is not supposed to have (Paragraph 2).

In both cases, the sanction is either monetary or sentence imprisonment of up to 3 years. Moreover, the attempts of committing these violations are also punishable. More serious forms of the offence are if the perpetrator:

- Commits the offences from Paragraphs 1 and 2 against a computer system, data or programs that are protected with special protection measures or are used in the work of the state bodies, public enterprises or public institutions or in the international communications or as a member of a group created for committing such crimes. In this case the sanction is a sentence imprisonment of up to 5 years (Paragraph 3).
- Commits the offences from the Paragraphs 1 and 2 and acquires significant property benefit or causes a significant damage. In this case, the perpetrator would be punished with sentence imprisonment of 6 months up to 5 years.
- Commits the offence from Paragraphs 3 and acquires significant property benefit or causes significant damages. In this case, the perpetrator would be punished with sentence imprisonment of 1 up to 10 years.

The crime of damaging and illegal penetration in the computer system refers also to illegal production, acquisition, selling, storing or making available to others special devices, means, computer programs or computer data intended or suitable for committing the offences from Paragraphs 1 and 2. The sanction is monetary or sentence imprisonment of up to 1 year.

Computer Fraud

The Criminal Code with Article 251-b envisages a monetary sanction or a sentence imprisonment of up to 3 years in the cases of illegal acquisition of property for oneself or somebody

else by entering in a computer or information system false data; by failing to enter true data; by forging an electronic signature; or by causing false results to appear for somebody else during electronic processing and transfer of data. If the perpetrator acquires more significant property he/she should be sanctioned with sentence imprisonment of up to 5 years, and if the perpetrator acquires significant property he/she should be sanctioned with sentence imprisonment of 1 to 10 years. If the violation is performed with the aim to harm another person then the sentence is monetary or imprisonment of up to 1 year.

Illegal production, acquisition, selling, storing or making available to others special devices, means, computer programs or computer data intended for committing the crime from Paragraphs 1, will be sanctioned with monetary sanction or sentence imprisonment of up to 1 year. All attempts to commit a fraud as provided in Article 251-b are also punishable.

Computer Forgery

According to Article 379-a of the Criminal Code as computer forgery is considered unauthorized production, entering, altering, deleting of computer programs that are decided or suitable to serve as a proof of facts that have value in legal relations or making them unusable, as well as use of the modified data or programs as true. The sanction is a monetary fine or sentence imprisonment of up to 3 year.

A qualified form of computer forgery exists when the crime is committed in relation to computer data or programs that are used in the work of public bodies, public institutions, enterprises or other legal and physical persons that perform activities of public interest, or in the legal traffic with abroad, or if their use causes significant damages. In these cases the sanction is a sentence imprisonment of 1 up to 5 years (Paragraph 2).

Illegal production, acquisition, selling, storing or making available to others special devices, means, computer programs or computer data intended for making computer forgeries is punishable with a monetary fine or sentence imprisonment of up to 3 years (Paragraph 3).

Comparative Analysis

We first compare the Macedonian cybercrime legislature with the international conventions and guidelines for addressing cybercrime. We can note that the Macedonian Criminal Code follows the guidelines outlined in the Convention of the Council of Europe: it regulates all of the punishable cybercrimes outlined in the Second section of the Convention. Next, compared to the European Commission Action Plan it has a very good overlap. The Macedonian Criminal Code does not specifically regulate the threats for the national security from cybercrime (i.e., cyberterrorism) and the (cyber) racial hatred and discrimination, instead, these offences are regulated through the more general offences of terrorism and discrimination.

We next discuss the Macedonian Criminal Code with respect to the proposed classification of cybercrime from the literature and the cases of cybercrime encountered in practice. First, we can note that the Macedonian Criminal Code covers the majority of the types of cybercrime as provided by the literature-based classification of cybercrime. There are no specific provisions only for cyberstalking and cyberterrorism. These two crimes are addressed through the more general types of crime: stalking and terrorism. Furthermore, based on the reports from the Macedonian Ministry of Internal Affairs, we can note that cybercrime offenders can be successfully persecuted and that the Ministry is equipped with a team to handle such cases. However, forming a special unit for monitoring the national and international attempts at

cyberterrorism will additionally strengthen the capacity of the authorities to handle these cases provided they occur. Moreover, such a special unit could represent a strong link for collaboration with the international authorities on these matters.

Conclusion

In this paper, we have presented, analyzed, and discussed the status of the criminal/penal law concerning cybercriminal in the Republic of Macedonia. The evolution of the information and communication technologies opens new possibilities for cyber criminals. To this end, the legislation must also adapt and adjust to the new challenges.

In a global context, the cybercrime offences can be categorized into several groups: thefts and frauds; computer spying; hacking and illegal penetrating in computer systems; viruses distribution and other forms of malicious software (malware); cyber stalking; production and distribution of illegal pornography; cyber terrorism; and violation of intellectual property rights. The most relevant international source concerning the treatment of the cybercrime is the Convention on Cybercrime adopted by the Council of Europe (2001). Majority of European countries have adopted this Convention and harmonized the national legislatives according to it. Notwithstanding from this is the Republic of Macedonia.

The issue of Cybercrime in Macedonia is addressed within the Criminal code of the Republic of Macedonia and especially Articles 149, 157, 157-b, 157-c, 286, 193-a, 251, 251-a, 251-b, and 379-a. These articles concern the following criminal acts: personal data abuse, infringement of copyright, piracy of audiovisual work, phonogram piracy, un-authorized use of software or invention, production and distribution of child pornography through a computer system, creation and insertion of computer viruses, un-authorized intrusion into a computer system, computer fraud and forgery.

We discuss in detail the reports on cybercrime complaints from the Internet Crime Complaint Center (IC3) annual reports and the annual activity reports of the Macedonian Ministry of Internal Affairs. These reports revealed that the frequency of cybercrime offences in Macedonia are at an alarming level. Considering the size of the economy and the population in Macedonia, the number of complaints and victims for year 2013, ranks Macedonia on the top by the number of complaints victims per capita, per internet user, and per gross domestic product value.

Given the current trends and recommendation in the regulation of the cybercrime, we can state that the Macedonian penal legislation is modern and follows the current European and world standards. However, it could be further improved by more active inclusion of the Macedonian authorities in the global response to the cybercrime, since, by all means the cybercrime is a global phenomenon that requires a global, international and cooperative action. Next, the cybercrime evolves together with the evolution of the technology and it diverges down different paths with each new year, or even month, passing. The cybercriminals change and adapt the way they organize themselves and the way they target new users. Consequently, the legislation should continuously adapt and change in order to intercept such changes. Finally, the authorities should work more strongly on enforcing cybercrime prevention measures and strategies, which will in turn reduce the risk of such crimes occurring and thus diminish the potential harmful effects on individuals and society.

Appendix

Table 3 Data about the top 15 countries by the total number of complaints reported to the IC3 for 2013

Country	Complaints	Percentage	Population	Complaints per capita	GDP(PPP)	Complaints per 1 billion$ GDP	GDP(PPP) per capita	Complaints per GDP(PPP) per capita	Internet users	Complaints per 1 million Internet users	Internet penetration score	Complaints per Internet penetration score
United States	83,799	31.89 %	320,226,000	261.69	16,768.1	5.00	53,001	1.58	254,295,536	329.53	81.0	1034.56
United Kingdom	4511	1.72 %	64,105,654	70.37	2320.4	1.94	36,208	0.12	54,861,245	82.23	87.0	51.85
Nigeria	3598	1.37 %	183,523,000	19.61	972.6	3.70	5746	0.63	55,930,391	64.33	32.9	109.36
China	2601	0.99 %	1,367,740,000	1.90	16,149.1	0.16	11,868	0.22	568,192,066	4.58	42.3	61.49
Canada	1782	0.68 %	35,675,834	49.95	1518.4	1.17	43,253	0.04	29,760,764	59.88	86.8	20.53
India	1529	0.58 %	1,265,660,000	1.21	6776.0	0.23	5450	0.28	151,598,994	10.09	12.6	121.35
Ghana	782	0.30 %	27,043,093	28.92	103.0	7.59	4029	0.19	4,217,454	185.42	17.1	45.73
Philippines	714	0.27 %	100,875,600	7.08	643.1	1.11	6597	0.11	37,602,976	18.99	36.2	19.72
Germany	603	0.23 %	80,767,463	7.47	3512.8	0.17	43,475	0.01	68,296,919	8.83	84.0	7.18
Afghanistan	578	0.22 %	26,556,800	21.76	58.8	9.83	1924	0.30	1,659,269	348.35	5.5	105.09
South Africa	534	0.20 %	54,002,000	9.89	662.6	0.81	12,507	0.04	20,012,275	26.68	41.0	13.02
Russia	533	0.20 %	146,300,000	3.64	3491.6	0.15	24,298	0.02	75,926,004	7.02	53.3	10.00
Malaysia	524	0.20 %	30,466,700	17.20	693.6	0.76	23,160	0.02	19,200,408	27.29	65.8	7.96
Macedonia	508	0.19 %	2,065,769	245.91	26.1	19.46	12,587	0.04	1,314,969	386.32	63.1	8.05
Australia	500	0.19 %	23,716,600	21.08	1052.6	0.48	45,138	0.01	18,129,727	27.58	82.3	6.08

Table 4 Data about the top 15 countries by the total number of victim originated complaints reported to the IC3 for 2013

Country	Victims	Percentage	Population	Victims per capita	GDP(PPP)	Victims per 1 billion$ GDP	GDP(PPP) per capita	Victims per GDP(PPP) per capita	Internet users	Victims per 1 million users	Internet penetration score	Victims per Internet penetration score
United States	238,189	90.63 %	320,226,000	743.82	16,768.1	14.20	53,001	4.49	254,295,536	936.66	81.0	2940.60
Canada	3621	1.38 %	35,675,834	101.50	1518.4	2.38	43,253	0.08	29,760,764	121.6786.8	41.72	
United Kingdom	2225	0.85 %	64,105,654	34.71	2320.4	0.96	36,208	0.06	54,861,245	40.56	87.0	25.57
India	1867	0.71 %	1,265,660,000	1.48	6776.0	0.28	5450	0.34	151,598,994	12.32	12.6	148.17
Australia	1810	0.69 %	23,716,600	76.32	1052.6	1.72	45,138	0.04	18,129,727	99.84	82.3	21.99
Macedonia	1670	0.64 %	2,065,769	808.42	26.1	63.98	12,587	0.13	1,314,969	1269.99	63.1	26.47
Mexico	711	0.27 %	121,005,815	5.88	2058.9	0.35	17,390	0.04	44,173,551	16.10	38.4	18.52
Puerto Rico	550	0.21 %	3,548,397	155.00	127.0	4.33	34,752	0.02	1,897,555	289.85	51.4	10.70
Brazil	505	0.19 %	203,759,000	2.48	3012.8	0.17	14,987	0.03	99,357,737	5.08	49.8	10.14
South Africa	502	0.19 %	54,002,000	9.30	662.6	0.76	12,507	0.04	20,012,275	25.08	41.0	12.24
France	463	0.18 %	66,100,000	7.00	2534.5	0.18	39,813	0.01	54,473,474	8.50	83.0	5.58
Germany	438	0.17 %	80,767,463	5.42	3512.8	0.12	43,475	0.01	68,296,919	6.41	84.0	5.21
Philippines	434	0.17 %	100,875,600	4.30	643.1	0.67	6597	0.07	37,602,976	11.54	36.2	11.99
Pakistan	391	0.15 %	188,739,000	2.07	835.1	0.47	4574	0.09	18,960,037	20.62	10.0	39.10
Netherlands	348	0.13 %	16,886,100	20.61	780.3	0.45	46,440	0.01	15,559,488	22.37	93.0	3.74

References

Bainbride, D.I. (2004). Introduction to Computer Law, Pearson.

Burden, K., & Palmer, C. (2003). Internet crime: cyber crime-A new breed of criminal? *Computer Law and Security Report, 19*(3), 222–227.

Chen, T., & Robert, J. (2004). *Statistical methods in computer security.*

Colin, B. (1997). The Future of Cyberterrorism*, Crime and Justice International*, 13(2).

Combating Counterfeiting and Piracy in the Single Market COM (98) 569, Final act.

Denning, D. E. (2000). Cyberterrorism, Testimony Before the Special Oversight Panel on Terrorism Committee on Armed Services, U.S. House of Representatives, Georgetown University.

Fen Lim, Y. (2007). *Cyberspace Law: Commentaries and Materials*, 2nd edn, OUP Sydney.

Filol, E. (2005). Computer Viruses: From Theory to Application, Birkhauser.

Graborsky, P.N., Smith, R.G., (1998). *Crime in the digital age: Controlling telecommunications and cyberspace illegalities*. New Brunswick: Transaction.

Harms, L. (2007). *The enforcement of intellectual property rights by means of criminal sanctions, an assessment*. Geneva: WIPO Advisory Committee on Enforcement. November 2007.

Cyberterror: Prospects and Implications (1999). Centre for the Study of Terrorism and Irregular Warfare, Naval Postgraduate School in Monterey.

Kambovski, V. (1997). Kazneno pravo, poseben del, Prosvetno delo, Skopje, Macedonia.

Letter of the Dutch Parliament to EU Commissioner Frattni, concerning the IPERD2 Directive, July 2006, available at europapoort.nl (10.01.2009).

McQuade, S.C III. (2006). Understanding and Managing Cybercrime, Pearson.

Naumovski, G., Gruevska, A., Stefanoski, Lj., (2007). Kazneno-pravnite aspekti na intelektualnata sopstvenost vo Republika Makedonija, Zbornik vo cest na Panta Marina, Faculty of Law "Iustinianus primus" Skopje.

Ogilvie, E. (2000). *The internet and cyberstalking, paper presented at the Stalking Criminal Justice Response Conference*. Sydney: Australian Institute of Technology.

PWG. (2000). The President's Working Group on Unlawful Conduct on the Internet, Appendix to the Electronic Frontier: The Challenge of Unlawful Conduct Involving the Use of the Internet, 03/2000.

Shelly, L. (2002). The Nexus of International Criminals and Terrorism. *International Annals of Criminology, 20*(1/2), 85–92.

Smith, R., Grabosky, P., Urbas, G. (2004). *Cyber Criminals on Trial*, Cambridge.

Synovate. (2003). FTC Identity Theft Survey Report, Washington D.C.

Taylor, P. A. (1999). *Hackers: Crime in the digital sublime*. London: Rutledge.

United Nations Office on Drugs and Crime (2012). The use of the Internet for terrorist purposes.

United Nations Office on Drugs and Crime (2013). Comprehensive study on cybercrime, Draft, 02.

Wienbar, S. (2009). Perspective: The Spyware Inferno (http://news.cnet.com/2010-1032-5307831.html; 01.03. 2009).

Adamski A. (1998). Crimes Related to the Computer Network. Threats and Opportunities: A Criminological Perspective. Helsinki, Finland: European Institute for Crime Prevention and Control, affiliated with the United Nations (HEUNI). Retrieved on December 15, 2006, from http://www.ulapland.fi/home/oiffi/enlist/resources/HeuniWeb.htm.

Jaishankar K. (2007). Cyber Criminology: Evolving a novel discipline with a new journal. *International Journal of Cyber Criminology*, Vol. 1 Issue 1 January 2007. Retrieved on March 15, 2007, from http://www40.brinkster.com/ccjournal/editorial.htm.