Computer crime forms and mechanism for security and protection

Snezana Savoska[1], Vesna Tozievska[1]
[1]Faculty of Information and Communication Technologies
University „St.Kliment Ohridski“ – Bitola, 7000, R. Of Macedonia,
snezana.savoska@fikt.edu.mk, vesnaprculovska@hotmail.com

Abstract. The constant technology development in the past seven decades has made the computers necessary in all areas of modern life, for which also influence the decreasing of the technology's today's price, especially of computers as a big part that now can be found in almost every home and in every human being hands. As a tool that speeds up every work and facilitates access to information, it's hard to imagine modern life without the use of a computer. Unfortunately, the emergence of computers and the further development of technology have led to the emergence of new forms of criminal offenses and new ways of their execution. The way the computer is used is suitable for knowledge of the workings with a computer of the average person, so that potential perpetrator of crimes can be anyone, and the global use of the Internet allows such works to be made everywhere in the world. Criminals exploit the enormous speed, simplicity and, above all, the "anonymity" offered by modern technology aiming to carry out various crimes. In this paper, the most common forms of cybercrime is mentioned as attacks on computer systems and networks, identity theft and data from other persons, distribution of pornographic content from children, fraud, piracy in the field of computer software and other computer products, etc. The forms of software tools for fighting cybercrime are mentioned.

Keywords: Cybercrime, Cyberterrorism, Cybercrime authorities in the R. of Macedonia

CEUR-WS.org/Vol-2464/paper7.pdf

1. Introduction

Today, all the world is at technological change and innovation, which leads to changes in all parts of modern life and establishment of the so-called. information society. Moving toward this paradigm of advanced information society, R. Macedonia has to analyze number of issues as cybercrime and cyberterrorism. Information society development in the state has to deal with a great number of challenges in the fighting against cybercrime and computer terrorism as a new patterns of threats in the

Copyright © 2019 for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

21st century. The more information technology becomes sophisticated, the more complex methods and tools are used to fight with criminal activities, especially with computer terrorism [23].

The Republic of Macedonia is not an exception from the developed countries that constantly and to a large extent face this sophisticated type of organized crime. The goal is to be part of a global security network in the fight against money laundering, organized crime, the financing of terrorism, and the entry of "dirty money" into the economy. The country is making efforts to protect itself from various criminal activities such as theft of personal data, high security secrets, military plans and fraudulent activities such as "stealing money" from credit / debit cards, and more. Computer or cyber terrorism and criminal activities have a visible adverse impact on the country, ie its economy, citizens' safety, public life and human rights and freedoms. For all of the above reasons, this new form of organized crime should be prevented from further spreading not only on our territory, but also around the world.

This paper take into consideration the forms and shapes of cybercrime and their characteristics. Also, as part of the survey, the types of cybercrimes that appear in the R.of Macedonia over the past years are reviewed and an analysis has been made of the forms that appear. For all these actions, a forensic tool is used as a collection of evidence for cybercrime and tools for intrusion detection that are not the subject of this paper.

The first part of the paper take into consideration related works about definitions, concepts and laws that connect the whole concept of cybercrime, the international activities that are undertaken for cybercrime sanctioning and securing according to its characteristics, information and data that are subject to the law on protection of private information. The second chapter describes the authorities in the Republic of Macedonia who are committed to dealing with cybercrime. The third chapter provides an overview of crimes related to cybercrime in the R.of Macedonia. Next chapter describes the course of investigation and use of software tools by sectors that are fighting cybercrime. Concluding observations summarize the perceptions of paper and summarize how the R. of Macedonia handles cybercrime and cyberterrorism.

2. Related works with Cybercrime and Related International Activities

There is an understanding in criminological literature that cybercrime is a part of economic crime, but also it is a crime closest to the field of property protection. The most widespread definition in criminology defines cybercrime as a set of all kinds of delinquent behavior by which data processing devices are used as a means of committing offenses or as a direct target for punishable offenses [1].

The Commission of the European Union in a Communication given in 2001 defined cybercrime in the widest possible sense, so that cybercrime means any crime that in any way involves the use of information technology [2].

From the former Yugoslavia area, the definition that paid attention is of course the one given by prof. Dr. Ignjatovic [3], according to which cybercrime is a special form of incriminating behavior in which the computer system appears as a means of execution or as a subject of a crime, or if that work in a different way, or on other object, or it cannot be performed or it would have completely different characteristics.

One of the most widely and commonly used definitions is that cybercrime is a socially dangerous phenomenon, for which the perpetrator uses knowledge of computer technology, such as a computer system understood in the broadest sense of the word, used as a means or as a subject of a criminal attack or both and the other [4].

From all definitions it can be noticed that the scope of criminal activities is wide and that the term cybercrime covers every crime that has been done with the help of computers, computer networks and programs. In addition to activities that aimes at obtaining illegal property benefits, computer crime also has activities that were made from other motives, such as creating and distributing viruses and malware, publishing confidential personal and business data on the Internet, etc [5].

Prof. Vodinelic defines cybercrime in narrower and broader term, so in a narrow sense it covers computer fraud, sabotage and espionage, and in a wider sense refers to the abuse of computers and its components from theft , embezzlement and so on. [6] According to prof. Spasic, cybercrime, is a crime that takes place in the digital environment and represents a specific form of unlawful action in which the computer network appears as a tool, a target, or evidence for committing a crime [7].

So, taking into consideration all these definitions and facts that computer crime is emerging threat in every computer activity, the most significant and numerous international acts have been adopted within the European Union: [8]

-1998 a special study entitled "Legal Aspects of Computer-related Crime in the Information Society" (COMCRIME study) was developed by professor Uhrlich Ziber, University of Wiesbourg, that explores the basics of cybercrime as a special form [9]. The study combined with other documents derived from the Lisbon Council of Europe of 2000, presents the guidelines for activities related to cybercrime.

-Europe Action Plan from the same year, also is relates to activities to ensure the network security and establish cooperation of the members states and their common approach to cybercrime. The same year, a Council Proposal for a legal framework for decision-making related to attacks on information systems was adopted (the Proposal for a Council Framework Decision on attacks against the information system). After one year, the document is complemented by unauthorized access to information systems and unauthorized interference with systems and data.

-In 2000, the Directive on electronic commerce was adopted, in which special attention was paid to the problem of abuse [10]. Also, the same year, various documents related to the legal regulation of cybercrime are adopted: Decision of the Council for prevention of child pornography on the Internet, Convention on Mutual Assistance in Criminal Matters, Recommendation for the Strategy in the new Millennium for the Protection and Control of Computer Crime. The next document that should provide a secure information society through a secure information infrastructure and combating computer-related crime is improving the Security of Information Infrastructures and Combating Computer-related Crime [11]. This year is of historical importance, since a number of documents are being adopted that regulate the legal framework for combating cybercrime or also known as high-tech crime.

In 1983, within the Organization for Economic Cooperation and Development (OECD), a Study on the International Application and Harmonization of Criminal Law related to the problems of cybercrime and abuse was adopted, and three years later, in the frame of Computer related crime, the list: analysis and legal policy was published. The 1999 year is marked as a year when a set of information security systems manuals are established, set that establish rules and take appropriate measures to achieve security. At the end of 1998, the Council of Europe began preparations for the adoption of the Convention on Cybercrime starting public debate in 2000. The convention today is one of the most important documents that besides the European countries have been accepted by Japan, USA, Canada and South Africa. The Convention which came into force in July 2004 is accompanied by a number of documents adopted within the Council. They are listed below:

- Trust and Security in Cyberspace: The Legal and Policy Framework for Addressing Cybercrime (2002);
- Cyber-Rights & Cyber-Liberties, Advocacy Handbook for NGOs (2003);
- Racism Protocol to the Convention on Cybercrime (2003);
- The Protocol to the Cybercrime Treaty (2002);
- Additional Protocol to the Cybercrime Convention Regarding "Criminalization of Acts of a Racist or Xenophobic Nature Committed through Computer Networks ";
- Report Revised draft of the Protocol on Racist Speech (2002);
- Background Materials on the Racist Speech Protocol ;
- Draft Protocol on Racist and Zenophobic Speech: Prelimiary draft (2001);
- Second Protocol on Terrorism (2002)

In the G8 group framework in 1997, the action plan for dealing with cybercrime was proposed and then adopted in 1998. It was proposed by the expert group for cooperation in the area of justice and internal affairs. The ministers of justice and internal affairs have on several occasions discussed on the principles of that struggle, for the needs of international cooperation in investigations and apprehending

perpetrators, as well as accepting the standards defined by the Council of Europe Convention. This organization also adopted the following documents:

- Recommendations for Enhancing the Legal Framework to Prevent Terrorist Attacks ;
- Recommendations on Special Investigative Techniques and other Critical Measures for Combating Organized Crime and Terrorism ;

Recommendations for Sharing and Protecting National Security Intelligence Information in the Investigation and Prosecution of Terrorists and Those Who Commit Associated Offenses: Best Practices for Network Security, Incident Response and Reporting to Law Enforcement.

3. Cybercrime authorities in the R. of Macedonia

Cybercrime Control Authority in the Republic of Macedonia is the Sector for Cybercrime and Digital Forensics (SCDF). The beginnings of the Sector for Cybercrime and Digital Forensics was in February 2005 when, for the first time, a Unit for Cybercrime and Counterfeits was established within the Sector for Financial Crime of the Department of Organized Crime. In October 2008, the Unit became a Unit for Cybercrime within the Department for Organized and Serious Crime. In November 2014, the Unit set aside the Department of Organized Crime and grew into a Computer Crime and Digital Forensic Department within the Central Police Services. In doing so, the Sector has jurisdiction to act on the entire territory of the R. of Macedonia. Now, SCDF consist of two departments:

Sector for Cybercrime Investigation, which has two sections:

- Investigation Department of Abuse of Payment Cards and
- Department of Computer Incident Investigation

The sector primarily deals with criminal issues in the area of cybercrime, which are provided for in the criminal law of the Republic of Macedonia as:

- Acting on crimes in the area of Damage and unauthorized entry into the computer system (Articles 251 and 251a)
- Acting on crimes in the area of sexual abuse of minors or children (Art.193, Art.193-a, Art.193-b)
- Acting on crimes in the area of Internet fraud (Art.247)
- Acting on criminal acts in the field of personal data (Article 149)
- Act on crimes in the field of abuse of payment cards (Art.271, Art.274-b).

Sector for digital forensic, consists of two sections:

- Computer Hardware investigation and testing Unit and
- Mobile devices investigation

The Cybercrime sector and digital phorensic collaborate with Interpol and Evropol. There is not specialized institutions dealing and investigation cyber terrorism. This is because in Macedonia cyber terrorism is not legally defined, regulated and accepted.

4. Review of criminal offenses related to cybercrime in the R. of Macedonia

Table 1 gives an overview of crimes that enter into computer crime on the territory of the R. of Macedonia.

Table 1. Overview of crimes that consist computer crimes in the period of time 2009-2014

Year	crimes and perpetrators	Damage and unauthorized entry into the computer system Art.251	Computer fraud Art.251 б	Issue a check without cover and abuse of a payment card Art.274	Creating and using a fake payment card Art.274 б	Computer Forgery Art.379a	Total
	Crimes	63	5	5	/	1	74
2009	Perpetrators	73	2	6	/	11	92
	Crimes	36	5	10	/	1	52
2010	Perpetrators	43	6	17	/	1	67
	Crimes	47	1	/	13	/	61
2011	Perpetrators	29	2	/	23	/	54
	Crimes	31	7	2	10	1	51
2012	Perpetrators	14	5	/	28	1	48
	Crimes	74	4	2	13	1	94
2013	Perpetrators	15	1	1	24	/	41
	Crimes	76	4	4	18	1	103
2014	Perpetrators	22	5	/	20	/	47
	Crimes	40	8		9		71
2015	Perpetrators	33	3		6		55
	Crimes	70	12		13		116
2016	Perpetrators	40	3		25		82
2017	Crimes	43	13		12		81

In the period 2009-2014, on the territory of the R.of Macedonia, there are no criminal acts "making and entering computer viruses", Article 251 a of the Criminal Code, while in the period 2015 - 2017, other forms of cybercrime have been registered in the table 2.

Table 2. Overview of others crimes in the period 2015-2017

Years and forms of cybercrime	2015		2016		2017	
	Crimes	Perpetrators	Crimes	Perpetrators	Crimes	Perpetrators
Endangering safety Article 144/4	3	2	3	1	5	2
Abuse of personal data Article 149/2			1	1	1	1
Violation of the distributor's right to a technically separate, secure satellite transmission Article 155 a	1	1				
Showing pornographic material to a child Art. 193	3	3	8	5		
Production and distribution of child pornography Article 193 a	7	7	7	5	4	6
Obstruction of sexual intercourse or other sexual activity of a child who has not reached 14 years of age. 193 b					2	2
Making, acquiring or disposing of means of counterfeiting Article 271/3			2	2	1	1

The total number of the crimes in the period 2009-2017 is shown on Fig.1. Most of the crimes are made in 2016 and the lowest number is in 2012.

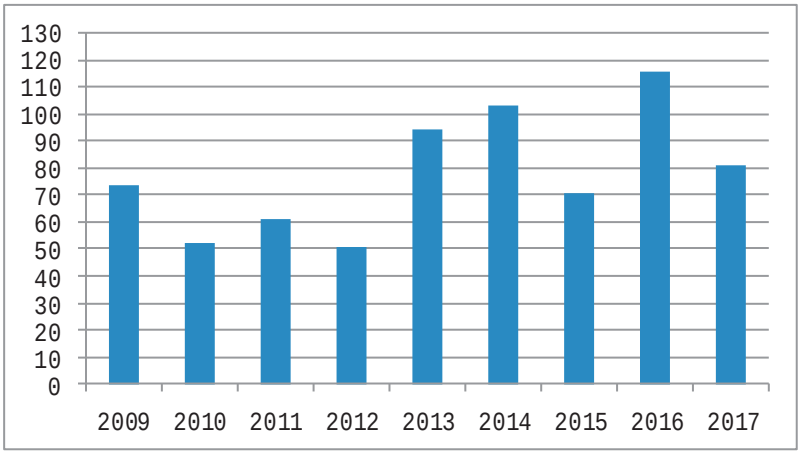

Fig. 1 Total number of crimes in the period 2009 – 2017

The total number of perpetrators in the period 2009-2017 is shown in the Fig.2. The highest value of perpetrators has 2009 and the lowest number is in 2013.

Fig.3 shows the distribution of crimes in the period 2009 - 2017. It can be noted that the biggest number is the crime of damaging and unauthorized entry into a

computer system, with the largest number of this form in 2013 and 2014. The second place in the number of occurrences is the criminal case Making and using a fake payment card. The smallest number of registration has a criminal offense Computer Forgery.

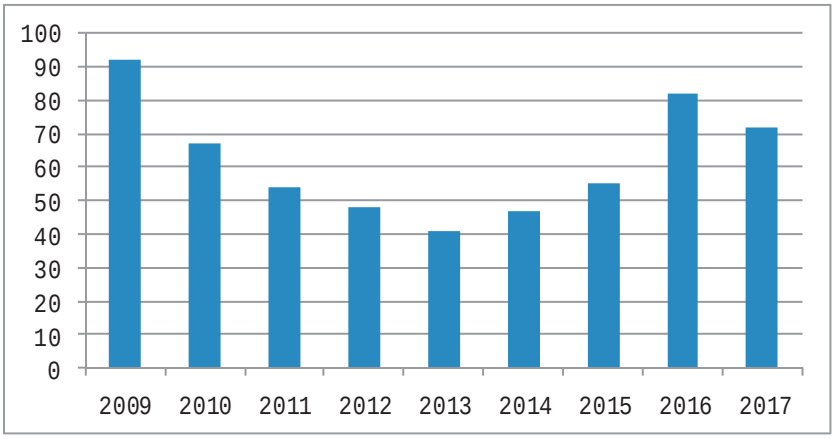

Fig. 2 Total number of perpetrators in the period of 2009- 2017

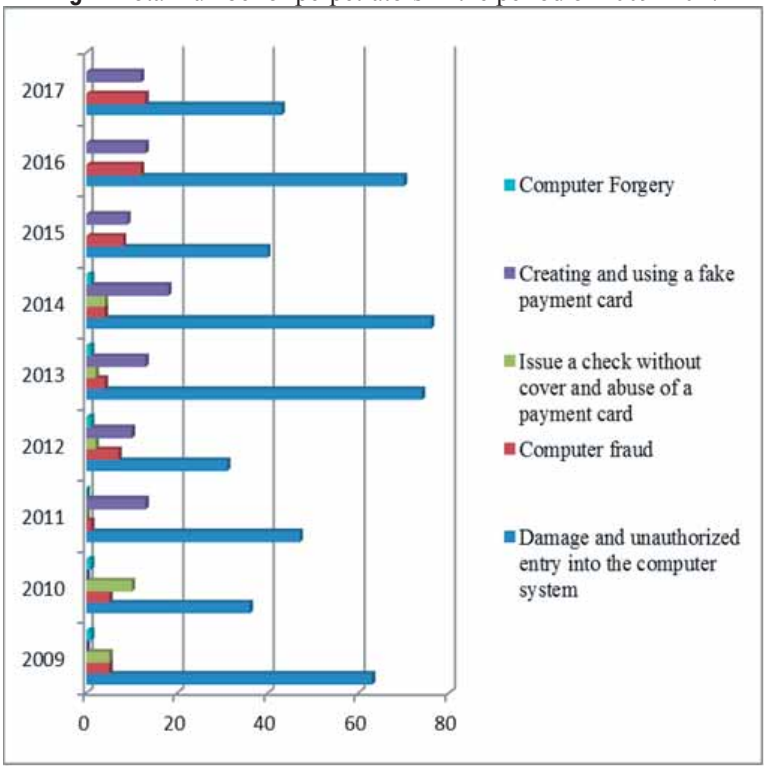

Fig. 3 Distribution of crimes in the period 2009- 2017

Fig.4 shows the distribution of other crimes registered in the R.of Macedonia for the period from 2015 to 2017, whose data were given in Table 2. From the picture it

can be noted that of these other criminal acts, the most occurrence is shown in the display of pornographic child material and production and distribution of child pornography in 2016.

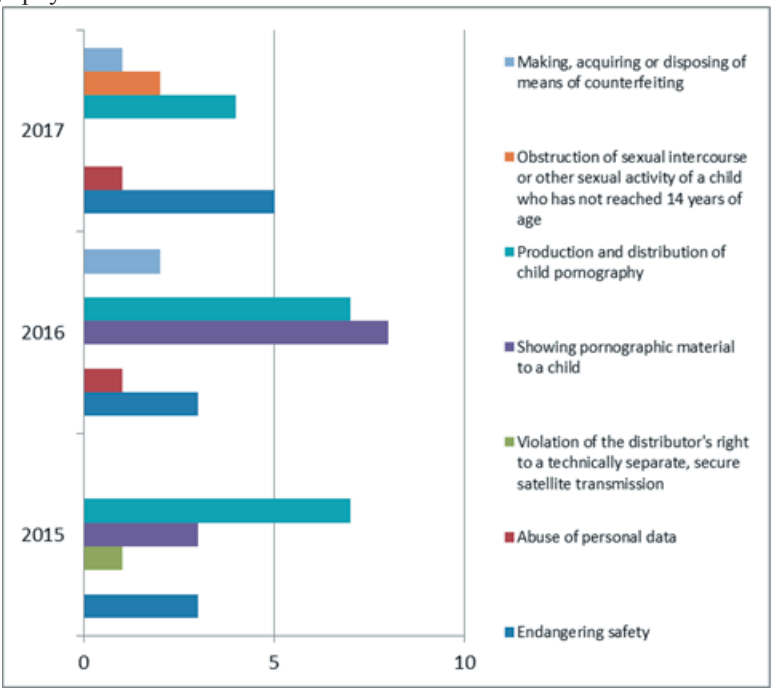

Fig. 3 Overview of others crimes in the period 2015-2017

5. Course of investigation and use of software tools by sectors that fight cybercrime

Qualification of the crime

The qualification of the crime, that is, the determination of the criminal offense is of great importance for starting and managing cases in the area of cybercrime.

Receiving an application from the damaged party

One of the most common ways of finding out about any crime, as well as criminal offenses in the field of cybercrime, is certainly the application from the damaged party. In this sense, the term impaired can be physical and legal entities, state bodies and institutions. For example, when professionals who maintain and administer information systems will notice that unauthorized entry into the system they maintain from outside and that some damage has occurred in terms of loss of data or the overall operation of the system, this unauthorized penetration they should report it to an appropriate state body that is competent to act further in order to find and sanction the perpetrator. The competent authorized persons of this body will assess the type and extent of the damage incurred and will take further actions.

When submitting an application for a committed criminal act, the damaged party besides the explanation, it is necessary to provide evidence that a crime has been committed, because certain evidence, if they are not provided immediately for a certain period of time, may be unavailable (deleted). In doing so, the injured party needs to provide the following information: to provide clarification about the committed crime, with a detailed description of what happened, to provide information on the circumstances whether it sustained pecuniary damage and the amount of the damage and Submit other evidence confirming the offense committed.

Operational checks for determining the perpetrator

In order to determine the place from which the criminal offense was committed, and hence further to the perpetrator thereof, after obtaining the knowledge, information or application from the damaged party, additional operational checks are carried out in order to determine the place from which the crime was committed the crime (IP address), the time and date when the crime was committed, and so on. This is done by analyzing the supplied evidence such as logs from a server, email headers and the like. After this, checks are carried out on who owns the IP address (provider). Information about which Internet service provider is the owner of a particular IP address are public and available on the Internet on the web site www.ripe.net, after this with a prior order issued by the Court or a request by the Public Prosecutor, checks are made by the provider who used the specified IP address in the given day, hour and hour zone.

Operational checks for the perpetrator's profile and identification of possible places from which the crime was committed

After determining the IP address of the user, operational checks are performed in order to determine the profile of the possible perpetrator of the offense. This is done through checks in the permanent database of the Ministry, using open sources of information (Internet) or through on-the-spot checks.

Search perpetrator’s home and other premises

After determining the possible perpetrator, as well as the exact address from which the crime was committed, a search of the home and other premises of the possible perpetrator of the crime is performed with a preliminary court order. The search of the home and other premises is regulated according to Art.181 to Art.204, where according to Art.181 "Searching home of the defendant and other persons can be undertaken when it is probable that the defendant wanted for arresting or traces of the criminal act or objects important for the criminal procedure will be found. "The purpose of the search is to provide digital evidence that will be evidence in the criminal procedure. Certain digital evidence will be seized on the spot, depending on whether the provision of digital e Kazi suffers a delay or not, and according to Article 184 of the LCP, while the remaining digital evidence will be provided in such a way that all suitable digital evidence carriers (USB, Hard Drives, CDs and DVDs and other memeor devices), then digital evidence will be provided in laboratory conditions.

Analysis of confiscated computer equipment

The expertise of computer equipment is carried out in accordance with Article 236 of the low of criminal low procedure (CLP), according to which the expert report shall be determined with a written order, that in the preliminary procedure is adopted

by the Public Prosecutor. The order shall state in relation to which facts an expert's report is performed and to whom it is entrusted.

Depending on the type of criminal offense, and in order to find all electronic evidence, different requests for expert examination of confiscated computer equipment can be made. The identification of the criteria for the search have to be be closely related to the information that the authorized officials obtained from the investigation, from the interviews with the injured parties, the suspects and witnesses. All information that the inspectors deem appreciated to be useful in the analysis of computer equipment need to be included in the expertise requirements in order to help them find the electronic.

There are general data that need to be stated in all requests for expertise regardless of the type of crime, which are: the name and surname of the suspect, name and surname of damaged, name and surname of the person from whom the computer equipment was seized, location from where computer equipment is taken away and the condition in which it was found. If the computer equipment was found to be included, indicate the date and time when it was turned off, the date when the seizure of computer equipment was carried out and detailed description of the confiscated computer equipment (brand, model and serial number).

Researchers of this type of crime sometimes use the original application program, and sometimes special software analysis and research tools. Researchers have found ways to collect traces from a remote computer to which they do not have immediate physical access, by accessing a telephone line or network connection. It is even possible to monitor the activities of a computer network over the Internet. These procedures form part of what is called computer forensics. Computer forensics is proof that the computer that needs to be sustained, convincing and sufficient for the court to accept it. In forensic-information procedures, no matter how careful people aiming to steal electronic information, they leave traces of their activities. Just when the perpetrators try to destroy the evidence that is on the computer they leave traces behind them. In both cases it can be shown that these traces can be traced and presented to the court. Computer forensic specialists do more than switching on the computer and listening to folders and searching for files. They should be able to perform complex "evidence recovery procedures" with skill and expertise that will keep the credibility of electronic evidence in court. Basically these procedures include: copying data, seeking evidence from e-mail and other Internet communication, data recovery, searching for documents and other data.

Initiating and filing criminal charges

After the checks and evidence provided for the perpetrator of the criminal act, as well as for the crime itself, criminal charges are filed by SCDF, then the crime convection is pursuant according Article 280 of the Criminal Procedure Law.

Software tool for Cybercrime detection

While conducting cybercrime investigations and providing evidence, several software tools are used, which in most cases are free software tools and can be found online (FTK Imager, Process Explorer, process monitor, etc.). Sometime, are used tools contained within the operating system itself (Windows CMD or Terminal with Linix), and many online tools (for example online tools for analyzing email headers and the like). Also, open sources of information, such as databases on the Internet are used. In addition, licensed softwares as Encase portable for live data forensic are

used. Licensed softwares such as Encase, FTK (forensic tool kit), Paraben, Paladin, Internet Evidece Finder and others are used in the analysis of computer equipment in the digital forensic laboratory. In the case of analyzing mobile devices in the digital forensic laboratory, licensed software such as X-Ray and Cellebrite are used. In the recent years, new applications and technologies in the cryptocoins (as BitCoin) have been used. Also, various web pages on the Internet network are used to collect a growing number of information and evidence as blockchain.info, blockexplorer.com and blockseer.com. Techniques to provide evidence for court trial such as Transaction, Hash and Bitcoin Address are also used, as well as software such as Bitcoin Core - wallet v0.15.0.1 and Armory application, as very important within the investigation.

6. Conclusion

The Republic of Macedonia is not excepted from the countries that are increasingly facing cybercrime. The purpose is to be part of the global security network in the fight against money laundering, organized crime, the financing of terrorism and the entry of "dirty money" into the economy. Our country take steps to protect itself from various criminal activities such as theft of personal data, high security secrets, military plans and fraudulent activities as "stealing money" from credit / debit cards. Cybercrime and cyberterrorism as well as criminal activities have a visible adverse impact on the country, ie its economy, citizens' safety, public life and human rights and freedoms. Because of all of the above reasons, this new form of organized crime should be prevented from further spreading not only on our territory but also around the world.

Computer forensics is used as a proof of a computer that needs to be sustained, convincing and sufficient for the court to accept it. In forensic-information procedures, no matter how careful people aiming to steal electronic information, they leave traces of their activities. Just when the perpetrators try to destroy the evidence that is on the computer they leave traces behind them. In both cases it can be shown that these traces can be traced and presented to the court. Computer forensic specialists do more than switching on the computer and listening to folders and searching for files. They should be able to perform complex "evidence recovery procedures" with the skill and expertise that will hold the credibility of electronic evidence for court.

The use of scientifically derived and proven methods for the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence obtained from digital sources in order to facilitate or continue the reconstruction of criminal events, or helping to predict unauthorized actions that turned out to be unacceptable for the planned operations representing digital forensic operations.

The working process in digital forensics involves creating a disk image (copies of the original original disk), hashing or confirming the integrity of the image on the disk, writing block disk image (read-only setting to verify the integrity of the disk disk image), and analysis of the drive and its contents.

7. References

[1] Konstantinović-Vilić, S., Nikolić-Ristanović, V., Kriminologija, Niš, 2003, str.178-179
[2] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2001:0051:FIN preuzeto 20.07.2015. godine
[3] Ignjatović, Đ., Pojmovno određenje kompjuterskog kriminala, Beograd, 1991, str. 142–143
[4] Simonović, B., Kriminalistika, Pravni fakultet u Kragujevcu, Kragujevac, 2004, str. 665
[5] Aleksić, Z., Škulić, M., Kriminalistika, Beograd, 2007, str. 46-63
[6] Šarkić, N., Prlja, D., Damnjanović, K., Marić, V., Ţivković, V., Vodinelić, V., Mrvić-Petrović, N.: Pravo informacionih tehnologija, Beograd, 2011, str.3
[7] Spasić, V., Aktuelna pitanja u oblasti sajber kriminala (članak), Bilten sudske prakse Vrhovnog suda Republike Srbije broj. 1/2006, Beograd, str.107.
[8] Зврлевски М., Прирачник за компјутерски криминал, http://www.osce.org/mk/skopje/121224?download=true
[9] Legal Aspects of Computer-related Crime in the Information Society – COMCRIME study, http://www.edc.uoc.gr/~panas/PATRA/sieber.pdf
[10] Directive on electronic commerce http://eur-lex.europa.eu/LexUriServ /LexUriServ.do?ur i=OJ:L:2000: 178: 0001: 0016:EN:PDF
[11] Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime, http://www.justice.gov/criminal/cybercrime /intl/EUCommunication.0 101.pdf
[22] Big Data and Visualization: Methods, Challenges and Technology Progress, http://pubs.sciepub.com/dt/1/1/7/, Accessed 20.5.2017
[23] http://eprints.ugd.edu.mk/10870/1/Skripta%20za%20Sigurnost%20na%20kompjuterski%20sistemi%2C kompjuterski%20kriminal%20i%20terorizam_revJA_2.pdf, Accessed 12.5.2018