UDK:343:004]:340.13(497.5)

INTERNATIONAL LEGAL FRAMEWORK FOR COMBATING CYBER CRIME WITH REFERENCE TO THE LEGISLATION OF THE REPUBLIC OF CROATIA*

Vanda Božić, Dr.Sc
Department of Criminal law, Faculty of Law University of Zagreb, Croatia
vanda.bozic@pravo.hr

ABSTRACT

Modern society is characterized by a meteoric technical and technological development and an era of computers that are now an integral part of the life and work of a huge number of users: private individuals, businesses, government bodies, non-governmental organizations, civil associations and others. The development of information technology has led, through large abuse in this area, to the emergence and development of cyber crime and intensification of other forms of crime. Security of the information systems, the social networks (Internet) and their users is now imperative for modern society. At the international level, several significant legislative solutions have been adopted at the level of the UN, Council of Europe and the EU, which we highlight in the central part of the paper. The Republic of Croatia has aligned its national legislation with the relevant international sources in this matter, particularly with the law of the EU, to which it is a full member. In the conclusion, we present a few suggestions for improvement of the legal framework for combating cyber crime, especially in Croatia and the Region.

Keywords: cyber crime, abuse of information technologies and systems, international legislation, Croatia, EU.

1. INTRODUCTION

At the beginning of the 3rd millennium there was a climax in the development of science and technology which had both positive and negative consequences in society. The positive effects are related to the general progress of humanity, the emergence of new technologies and thus new products appearing on the market, which are, to a large extent, facilitating the daily lives of ordinary people. This primarily refers to computers that are now an integral part of both work and private life of every individual. Nowadays, it is unthinkable to live and work without computers, their rapid development in the last 15 years has made their use and application almost necessary in all business sectors, as well as in private life. There is no profession in which computers have not found their application. Computers have special significance in the economic activities without which the elementary business functions are impossible (e.g. necessary daily connection with the tax administration in order to issue bills and submit forms, banking transactions, etc.), in addition to their primary role in creating profits.

*This research has been fully supported by the Croatian Science Foundation, under project number 1949. "Multidisciplinary Research Cluster on Crime in Transition - Trafficking in Human Beings, Corruption and Economic Crime."

However, the emergence and use of computers has its negative sides, among which the most important are the alienation of people, the dependence of young people on the Internet and thus computer equipment, various types of abuse and, finally, the emergence and development of computer crime as a new manifestation. It is the expansion and accessibility of computers that has created and continues to create a basis for a variety of abuses. Computer attacks, receiving viruses that infect the electronic mail[1] are almost a daily occurrence. Cyber crime, computer fraud, computer or information crime, misuse of computers are only a portion of the terms that ultimately involve cybercrime.

The most developed countries were the first to respond to the misuse of computers and computer crime by initiating the adoption of special regulations on the national level, as well as the passing and adoption of important international documents (conventions, resolutions) by which the State Parties have the obligation to harmonize their national legislations and develop mutual cooperation in combating cybercrime.

2. THE CONCEPT AND CHARACTERISTICS OF CYBERCRIME

a) The first case of cybercrime was registered in the United States in 1958, while the first prosecuted case occurred a few years later, in 1966, in the criminal case of falsification of bank data in Minneapolis. In Europe, on the other hand, the first case was recorded in 1968 in Finland, whereas in the Republic of Croatia, which was at the time part of Yugoslavia, the first case of cybercrime was registered in Pula in 1983 in the Istrian Bank.[2]

b) The term cybercrime is not uniquely determined in doctrine and practice, bearing in mind the different legal systems (common law, civil law and others) and the various solutions in the national legislations of individual countries. From the aspect of criminal law, cybercrime involves misuse of computer systems, programs and data explicitly incriminated in the criminal code. The crimes that are the result of misuse of IT resources can be divided into: 1. acts in which the computer is the object of the acts of commission (*computer crime*), 2. offenses in which the computer is a means of execution (*computer related crime*) and 3. acts of illegal use of the Internet (*net crime*).[3]

The OECD in 1992 in its Guidelines for the Security of Information Systems determined that the term *information systems* means computers, communication facilities, computer and communication networks and data and information that may be stored, processed, retrieved or transmitted by them, including programs, specifications and procedures for their operation, use and maintenance.[4]

According to Directive 2013/40/EU, *information system* means a device or group of inter-connected or related devices, one or more of which, pursuant to a program, automatically processes computer data, as well as computer data that stored, processed, retrieved or transmitted by that device or group of devices for the purposes of its or their

[1] See more in: Šimundić S, Franjić S, Vdovjak K, *Hoax*, Proceedings of the Faculty of Law in Split, year 49, 3/2012, p. 459- 480.

[2] Ranđelović D, *High-tech Crime*, KPA, Beograd, 2013, p.257-265.

[3] See more: Stojanović Z, *Modern technical means and criminal law with special emphasis on Cybercrime*, Round Table Modern technology and criminal justice, XXV Counseling Association of Criminal Law and Criminology Yugoslavia, Novi Sad, 1987.

[4] Annex to the Recommendation of the Council of 26 November 1992, Guidelines for the security of information systems 26 November 1992 I. AIMS, available at:http://www.oecd.org/sti/ieconomy/oecdguidelinesforthesecurityofinformationsystems1992.htm,(10/01/2017)

operation, use, protection and maintenance.[5]*Computer system* is any device or group of interconnected or related devices, of which one or more of them on the basis of a program automatically processes data, as well as computer data that are stored in it, processed, loaded or transferred for purposes of its operation, use, protection and maintenance.[6]

On the Tenth UN Congress on the Prevention of Crime and the Treatment of Offenders,*cybercrime* is defined in a narrow and a broad sense. *Cybercrime in a narrow sense* (computer crime):Any illegal behavior directed by means of electronic operations that targets the security of computer systems and the data processed by them.*Cybercrime in a broader sense* (computer-related crime):Any illegal behavior committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession (and) offering or distributing information by means of a computer system or network.[7]

Computer data is any representation of facts, information or concepts in a form suitable for processing in a computer system,[8] while a set of computer data suitable to cause a computer system to perform a function is called a *computer program*.[9]

c) The complex structure of acts of computer crime, the special environment of committing such acts, the specific ways and means of carrying out these criminal acts, the special facility of protection and great social danger are amongst the main elements that make up the basic characteristics and features of cybercrime, which knows no bounds. An indispensable element in the commission of these crimes is *dolus specialis,* the intention of the perpetrator to obtain material or non-material benefits for themselves or others or to cause damage to others.

There is a great dark figure of the commission of acts of computer crime as they are very difficult to detect and prove given the fact that this is a complex form of crime with the possibility of concealing the offense, with special properties of the perpetrator (*delicta propria*) considering the fact that these criminal acts can be committed only by persons who have very good knowledge of information technology and that it involves a special space in which these acts can be committed. Due to the high growth rates and the specific ways of committing these types of crimes and the special characteristics of the perpetrators, crimes against computer systems, programs and data represent a serious social problem.

In terms of the status and trends of computer crime, the FBI official estimate is that less than 1% of this type of crime has been discovered, whereas only 12% is reported.[10] In combating cybercrime, the FBI is working with a large number of specialized agencies and international organizations, especially highlighting the cooperation with CERT (*Computer Emergency Response Team*).

---

[5]Art.2.a.Directive 2013/40/EU of the EU Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA OJ L 218, 14/08/2013, p. 8–14

[6]Art.87.par.18. CC RC

[7] UN definition of cybercrime, available at: http://idn-wi.com/united-nations-definition-cybercrime/(10/01/2017)

[8]Art.87.par.19. *Ibid.*

[9] Art.87.par.20. *Ibid.*

[10]www.fbi.gov, *cyber crime*, (10/01/2017)

See more: Obradović S, Mijalković M, Perić D, Puača D, *Crime Investigation on computers*, Infoteh-Jahorina Vol. 6, Ref. E-III-14, p. 455-459, 03/2007

3. INTERNATIONAL LEGAL FRAMEWORK FOR FIGHTING CYBERCRIME

a) The international legal source par excellence in matters related to combating cybercrime is the Convention on Cybercrime of the Council of Europe adopted in Budapest in 2001, which Croatia signed on 23 November 2001 and one year later it was ratified by the Law on Ratification of the Convention on Cybercrime.[11] Furthermore, the Additional Protocol concerning the criminalization of acts of racist and xenophobic nature committed through computer systems was adopted in Strasbourg on 28 January 2003, which Croatia ratified by a special Act.[12] The Protocol criminalized punishable behaviors that were not criminalized by the Convention and that relate to the spread of hatred, intolerance and bigotry through computer systems, towards racial, religious and ethnic groups and communities.[13]

The Convention consists of four chapters: Chapter I – Use of Terms, Chapter II – Measures to Be Taken at the National Level, Chapter III – International Co-operation and Chapter IV – Final Provisions.The first section lays down the terminology guidelines for the most important concepts in matters of cybercrime, which is especially important for harmonization of national legislations and harmonization of legal practice.

The central part of the Convention is Chapter II which prescribes the measures that the States Parties are to undertake in the field of criminal substantive and criminal procedural law. As for the criminal substantive law, the States Parties are required to criminalize the following crimes in their national Legislation: a) Offenses against the confidentiality, integrity and availability of computer data and systems, b) Computer-related offenses, c) Content-related offenses and d) Offenses related to infringements of copyright and related rights.Furthermore, it prescribes the institutes of attempting, encouraging and assisting in the commission of any of these crimes and the responsibility of the legal persons, as well as the sanctions and measures. The substantive legal framework is designed with the intention to improve the resources for prevention and prosecution of major crimes of this specific type of crime committed with the use of computers.

In terms of the criminal procedure (procedural) law, it provides legal mechanisms such as: a) urgent preservation of stored computer data, b) obligations concerning the delivery of computer data (Art. 18 Production Order), c) search and seizure of stored computer data, and d) real time computer data collection.[14]

Chapter III of the Convention refers to the international cooperation and mutual legal assistance to States Parties. It lists, *inter alia*, the provisions relating to requests for mutual assistance in the absence of relevant international treaties and mutual assistance in respect to the provisional measures and investigative powers.

---

[11] OG, IA no 9/02

[12] *Ibid.* no4/08

[13] Law on Ratification of the Additional Protocol to the Convention on Cybercrime Concerning the Criminalization of Acts of a Racist and Xenophobic Nature Committed Through Computer Systems, available at:https://www.istra-istria.hr/fileadmin/dokumenti/upravna_tijela/UO_za_tal_nac_zaj/Instrumenti_zastite_ljudskih_prava/I.Multilateralni_odnosi/3.Vijece_Europe/I-3.17Dodatni%20protokol%20uz%20konvenciju%20o%20kibernetickom%20kriminalu%20o%20inkriminiranju%20djela%20rasisticke%20i%20ksenofobne%20naravi%20pocinjenih%20pomocu%20racunalnih%20sustava.pdf, (10/01/2017)

[14] Art.2-22. ETS 185 – Convention on Cybercrime, 23/11/2001 available at:http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf, (10/01/2017)

The offenses explicitly listed in the Convention represent today an international legal standard, as well as an obligation for the Parties to include the above provisions in their domestic national legislations.

b) The second most important international document in this matter is Directive 2013/40/EU[15] on attacks against information systems, adopted on 12 August 2013 by the EU Parliament and the EU Council, on the basis of Art. 83. Par. 1. of the Treaty on the Functioning of the EU. The Directive replaces the previously adopted Council Framework Decision 2005/222/PUP[16] and is in line with the Convention on Cybercrime.

The Directive has the purpose to establish the minimum conditions for the criminalization of offenses in the field of information systems of the States Parties. Significant innovations introduced in the Directive in the field of substantive law are: expansion of criminal conduct, introduction of aggravating circumstances and determination of sentences.[17]

c) As an important international legal source in combating cybercrime are the following EU Directives on combating computer crime: Directive 2009/24/ EC of the EU Parliament and of the Council of 23 April 2009 on the legal protection of computer programs [18] according to which the Member States protect computer programs by copyright, then Directive 2006/24/EC of the EU Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC[19], which was adopted with the intention of efficiently detecting and prosecuting criminal acts whose execution leaves electronic traces.

d) Among other relevant international legal sources relevant to combating computer crime, we can mention the United Nations Convention against Transnational Organized Crime (*Palermo Convention*),[20] the Convention on International Police Cooperation in SEE and the SELEC Convention.[21]

4. NATIONAL CRIMINAL LEGAL FRAMEWORK OF THE REPUBLIC OF CROATIA FOR COMBATING CYBERCRIME

The CC of Croatia, which entered into force on January 1, 2013, in Chapter XXV, under the title Crimes against computer systems, programs and data stipulates eight offenses (Art. 266 -273) in this domain: unauthorized access, obstruction of a computer

[15] Regulation on the takeover of Directive 2013/40/EU on attacks against information systems and Directive 2014/62/EU on the criminal justice protection of the Euro and other currencies against counterfeiting, OG, IA No 102/15

[16] Art.15. Directive 2013/40/EU

[17] Kokot I, *Criminal law protection of computer systems, programs and data*, Zagreb Law Review, Vol. 3 No. 3, 2014, p.301-327.

[18] OG EU L 111/16, available at:http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32009L0024, (10/01/2017)

[19] OG EU L 105/54, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32006L0024, (10/01/2017)

[20] See more: Božić V, Nikač Ž, *Criminal incriminations based on the United nations Convention Against Transnational Organized crime in the criminal legislation of the Republic of Croatia and the Republic of Serbia,* Proceedings of the International Conference, Faculty of Security in Skopje, 2016

[21] See more: Nikač Ž, Božić V, *International Cooperation of Southeast Europe in the fight against crime*, Львівський державний університет внутрішніх справ, Ukraina, Lviv, International scientific conference "Theory and Practice of Law Enforcement Activities," Conference Proceedings, Lviv, 2016, p.431-443.

system, damage to computer data, unauthorized interception of computer data, computer forgery, computer fraud,[22] abuse of devices and grave offenses against computer systems, programs and data.[23] The previous offenses against computer systems, programs and data were taken from the Chapter on Crimes against property and are in line with the Convention on Cybercrime.[24]

Unauthorized access to a computer system or computer data (Art. 266) is punishable by imprisonment of up to two years. The unauthorized access is in the domain of criminal responsibility and criminal liability due to the fact that such action is usually the first step (preparatory action) towards the commission of a more serious criminal offense. It is important to note that the unauthorized access includes physical access to a computer and access to the same computer from another computer. The qualified form is intended in the case when the crime was committed in relation to a computer system or computer data of a governmental body, the Constitutional Court and international organizations to which the Republic of Croatia is a member, units of the local or regional government, public institutions or a company of special public interest. The prescribed penalty is imprisonment of up to three years. The attempt is punishable both for the basic and the qualified form of commission of this offense.[25]

Disabling or impeding the work or use of a computer system, computer data or programs or computer communication (Art. 267), as well as the attempt for such offense, is punishable by imprisonment of up to three years.[26]The action of committing this offense consists of damaging, altering and deleting computer data, as well as of any other act which aims to make electronic data unusable. This act is a crime of computer sabotage.

Damage to computer data (Art. 268), also a crime of computer sabotage including unauthorized damage, modification, deletion, destruction, performance or display of unusable or inaccessible computer data or programs, in whole or in part, shall be punished by imprisonment of up to three years, as will be the attempt of such an offense.[27] The performance of the act refers to the invasion into a complete computer program or computer data, including development and introduction of a virus into the system in order to attack the programs. The incriminated offense is in line with the *Council Framework Decision 2005/222/JHA of 24 February 2005* on attacks against information systems.[28]

Unauthorized interception of computer data (Art.269), the so-called *computer espionage,* orunauthorized interception of communication between remote computers, punishable by imprisonment of up to three years, involves the unauthorized interception or recording of a non-public transmission of computer data, including electromagnetic emissions of the computer system and the availability of the data obtained. The attempt of a criminal offense is punishable by the same sentence and the data produced by the offense will be destroyed.[29] The incriminated offense is in line with Art.3 of the Convention on Cybercrime.[30]

---

[22] See more: Vuletić I, Nedić T, *Computer fraud in Croatian Criminal Law,* Proceedings of the Faculty of Law of the University of Rijeka v.35, no.2, p. 679-692 (2014)
[23]Criminal code RC, OG No 125/11,144/12,56/15,61/15
[24]Op.cit.14.
[25] Art.266.par.3. CC RC
[26] Art.267. *Ibid.*
[27] Art.268. *Ibid.*
[28] Art. 4. Council framework decision 2005/222/JHA of 24 February 2005 on attacks against information systems, OG EU L 069/67
[29] Art.269. CC RC
[30]Op.cit.14.

The crime of *Computer Counterfeiting* (Art.270) is committed by anyone who, without authorization, produces, enters, alters, deletes or renders unusable or inaccessible computer data that is of value for the legal relations, in order for them to be used as authentic, or who uses or purchases such information for use, and shall be punished by imprisonment of up to three years. The attempt is also punishable, while the data produced by the perpetration of the criminal offense will be destroyed.[31]

Computer fraud (Art. 271), punishable by imprisonment of six months up to five years, has criminalized the entering, modifying, deleting, damaging, making useless or unavailable computer data or interfering with the functioning of a computer system which can cause damage to another, all with the aim to acquire property gain for oneself or others.[32]The qualified form is intended for the case when the offense is used for substantial financial gain or when considerable damage is caused, [33] and is punishable by imprisonment of one to eight years. The data resulting from the commitment of the criminal offense shall be destroyed. The difference between fraud as a property offense and computer fraud is reflected in the fact that in computer fraud the victim is neither misled nor held in error.

The *misuse of devices* (Art.272) criminalizes the actions relating to the preparation, supply, import, selling, possessing or making available to others devices or computer programs or computer data created or adapted for committing crimes against computer systems, programs and data with the aim to be used to commit any of these offenses. This offense includes punishable preparatory action relating to the commission of offenses against computer systems, programs and data. It is punishable by imprisonment of up to three years. The privileged form, punishable by imprisonment of up to two years, will be used to punish all who design, procure, import, sell, possess or make available to others computer passwords, access codes or other data which can be used to access a computer system with the aim to be used for the commission of the above criminal offenses. The special devices and applications shall be seized and the data shall be destroyed.[34]

The *serious offenses against computer systems, programs and data (Art.273)* also include the criminal offenses of obstruction of a computer system, damage to computer data, unauthorized interception of computer data and computer forgery, if they are committed in relation to a computer system or computer data of a governmental body, the Constitutional Court of Republic of Croatia and international organizations to which the Republic of Croatia is a member, units of the local or regional government, public institutions or companies of special public interest for which a punishment of imprisonment of six months up to five years is prescribed.[35]The same penalty shall be imposed for the commision of the criminal acts of unauthorized access, obstruction of a computer system, damage to computer data, unauthorized interception of computer data, concealing the real identity and causing misconception about the authorized holder of identity.[36] The qualified forms of serious criminal offenses against computer systems, programs and data have been prescribed for committing the criminal acts of obstruction of a computer system, damage to computer data or unauthorized interception of computer data by means intended for the execution of an attack on a larger number of computer

[31] Art.270. CC RC
[32] Art.271. *Ibid.*
[33] Value of the damage is significant and if it exceeds HRK 60,000.00. Art.87.par.29.Ibid.
[34] Art.272. *Ibid.*
[35] Art.273. par.1. *Ibid.*
[36] par.2. *Ibid.*

systems or which cause substantial damage and are punishable by imprisonment of one to eight years.[37]

5. FORMS OF CYBERCRIME IN PRACTICE - REVIEW

The methodology of combating cybercrime as the most sophisticated form of crime implies complete education about all forms and modes of committing this criminal offense, in order to make the reactions of the states and the international community efficient to the greatest possible extent.

In practice, we meet many forms of cybercrime. Identity theft and misuse of personal data on the Internet are taking on new forms on a daily basis, personal data are being appropriated without their consent and knowledge in various ways, by fraud and theft. Thus obtained data are further used to commit certain criminal acts mainly with the aim of acquiring material gain, provided that the data may not be immediately used, but only after a certain lapse of time and can also be sold to other persons.

There is a fairly large number of criminal acts related to intellectual property, such as the illegal sale of unauthorized copyright works recorded on multimedia carriers and their resale to end users and there have been cases of unauthorized distribution of books in electronic form via the Internet.[38]

One of the most common crimes is the abuse of electronic data on payment cards on the Internet and other forms of financial fraud. Thus obtained electronic data continues to be mainly used for the purchase of various goods on the Internet.[39]In addition to financial fraud, other forms of cyber crime are currently used in practice, such as: theft of goods, various acts of sabotage, theft of information, attacks on computer systems (network interference), various forms of financial crime (online fraud, fishing), abuse of children and young people for child pornography and sexual exploitation.[40]

The social reaction to these forms of cybercrime is based on the above international and national legislation. The States parties to international documents have harmonized their national legislations and established specialized bodies for combating cybercrime.

The Republic of Croatia has acted in the same way, both at the legal and institutional level. Within the General Police Directorate of the Ministry of Interior of the Republic of Croatia – the Criminal Police has established a special Department for High-tech Crime to systematically analyze, monitor and study the phenomenological and etiological aspects of cyber (computer) crime, proposing solutions to its suppression, conducting complex criminal investigations in criminal matters committed against and by means of computer systems and networks and performing forensic analysis and control of the Internet.The Department for High-tech Crime is also the operational national contact point for international cooperation and exchange of information relating to offenses against computer systems, programs and data.[41]

---

[37] par.3. *Ibid.*

[38] Nikač Ž, Urošević V,*Place and role of Ministry of the interior of the Republic of Serbia in prevention of high tech crime*, Conference Proceedings Forum BISEC 2010, Belgrade, p.53-58.

[39] See more in: Božić V,*The intention as essential element of criminal act of fraud in Croatian Criminal Law*, master's thesis, Zagreb, Faculty of Law, 03/11/2010, p.10-15.

[40]See more: Nikač Ž, *International police cooperation*, KPA, Belgrade, 2015, p.110-112.

[41]https://www.mup.hr/UserDocsImages/minstarstvo/USTROJ_MUP_RH/Odjel_za_visokotehnoloski_kriminalitet.pdf, (10/01/2017)

6. OVERVIEW AND ANALYSIS OF CRIMES COMMITTED AGAINST COMPUTER SYSTEMS, PROGRAMS AND DATA IN CROATIA

Table 1 below shows the number of reported and resolved computer related criminal offenses in 2014 and 2015.

Table 1 - Comparative overview of reported and solved criminal acts of computer crime in 2014 and 2015[42]

CRIMINAL OFFENSES	REPORTED Number of offenses		SOLVED Number of offenses	
	2014	2015	2014	2015
Unauthorized access	16	29	13	21
Obstruction of a computer system	1	2	1	2
Damage to computer data	4	7	4	3
Unauthorized interception of computer data	3	5	3	4
Computer forgery	169	80	169	82
Computer fraud	960	1361	864	1215
Misuse of devices	19	69	18	69
TOTAL	1172	1553	1072	1396

Most reported criminal offenses, among the acts of computer crime, are under *Computer fraud* (960 reported in 2014 and 1,361 in 2015). The criminal offense of *Computer forgery* was second (169 reported) in 2014 and 80 were reported in 2015.

The least number of reported offenses is related to the criminal offense of *Obstruction of a computer system* (1 report).

Table 2 shows the number of perpetrators of criminal acts of computer crime in 2014 and 2015 and the ratio of increase or decrease in crime in the following year and the average number of offenses per offender. In 2014, most offenders committed *Computer fraud* (70), while in 2015 there was an increase in the perpetrators of 11.4% (78). Second was the crime of *Computer forgery* with 10 offenders in 2014 and only 1 offender in 2015. It is interesting to note that for this crime, the average number of offenses per offender was 16.9 in 2014, while a rapid increase was recorded in 2015 (80 offenses per offender).

Among the criminal acts of computer crime, the least number of criminal offenses was recorded for crimes of *Obstruction of a computer system* and *Damage to computer data*.

[42]According to the Service for strategic planning, analytics and development of the Ministry of Interior of Republic of Croatia: Statistical overview of the basic security indicators and performance in 2015, Zagreb, 01/2016

Table 2 - Perpetrators of criminal acts of computer crime in 2014 and 2015[43]

Criminal offense	Perpetrators of criminal offenses 2014	Perpetrators of criminal offenses 2015	+ - %	Average number of offenses per offender - 2014	Average number of offenses per offender - 2015	+ -
Unauthorized access	7	8	+14.3	2.3	3.6	+1.3
Obstruction of a computer system	-	1	-	-	2.0	-
Damage to computer data	1	1	0.00	4.0	7.0	+3.0
Unauthorized interception of computer data	1	4	+300.0	3.0	1.3	-1.8
Computer forgery	10	1	-90.0	16.9	80.00	+63.1
Computer fraud	70	78	+11.4	13.7	17.4	+3.7
Misuse of devices	4	-	-	4.8	-	-
Total	93	93	235.7	44.7	18.55	69.3

Table 3 shows the most common offenses of computer crime according to the submitted charges and the resolved and subsequently discovered offenses in 2015. These are the data on unknown perpetrators, as well identified perpetrators.

Table 3 - The most frequent criminal acts of computer crime – charges, resolved and subsequently discovered cases in 2015[44]

Criminal offense	Total charges	Caught	Unknown	Number of offenses	%	Number of subsequently detected offenses	%	% of charges
Computer fraud	1361	1	1249	1215	89.3	1103	88.3	21.5
Computer forgery	80	-	79	82	102.5	81	102.5	1.3
Total	1441	1	1328	1297	95.9	1184	95.4	11.4

Computer fraud ranks first according to the number of filed criminal charges compared to all other criminal acts of computer crime. In relation to the charges submitted in 2015 (1361), a large number of criminal offenses was resolved (1215); it should, however, be

[43] *Ibid.*
[44] *Ibid.*

mentioned that there is an enormous number of unknown perpetrators of this crime (1249), but also of subsequently discovered offenses (1103).

Computer forgery, although with a significantly smaller number of charges (80), is second according to the number of charges filed for computer-related criminal offenses in 2015. Computer forgery, despite the large number of resolved cases (82), records a large number of unknown perpetrators of crimes (79), as well as a high number of subsequently detected offenses (81).

7. CONCLUSIONS

Cybercrime is one of the most sophisticated forms of crime that manifests itself every day through new perpetration methods. Due to the specific area in which it takes place, the special characteristics of the offender, the manner of execution, the difficulty in proving and prosecuting it, as well as other elements, cybercrime is an extraordinary threat to society. There is a large number of crimes committed against computer systems, programs and data that we will never know about, and with respect to the reported offenses, very few have had their final court epilogue.

At the international level, the biggest step was adoption of the Convention on Cybercrime, which is the most important international legal source in this matter. The Convention provisions established the most important solutions in the field of criminal substantive and criminal procedural law and have imposed obligations to the State Parties to harmonize their national legislations and establish international cooperation.

The Republic of Croatia has complied with the provisions of the Convention and now, as a member of the EU, it went a step further, incorporating the above solutions in its national legislation and ratifying EU Directive 2013/40/EU on attacks against information systems. However, it should be noted that certain criminal offenses in the Criminal Code of the Republic of Croatia are defined beyond the minimum framework of the stated international sources. Additionally, the attention is drawn to the diversity of translations of certain terms between international and national sources, which can lead to different interpretations in practice. Although the legal framework is very well resolved, it is necessary to effectively implement the provisions of the law in practice.

Computer crime is increasing progressively and each day brings new potential forms and modes of execution. This necessitates constant monitoring of the movement of this type of crime and accordingly, possible legislative amendments. The employees of the Department of High-tech Crime in the Criminal Police Department of the Ministry of the Interior of Republic of Croatia should have the obligation of further training, upgrading and specialization of cyber crime detection skills and knowledge. This is especially true of the international cooperation in the field of information exchange, technical cooperation and training of personnel according to international standards (certificates, procedures, on-line application, nomenclature, digital forensics). The greatest damage caused by the attacks on computer systems, programs and data is suffered by public institutions, legal persons and other organizations engaged in economic activities. In economic relations, the electronic payment systems that require constant control, monitoring and protection are particularly vulnerable. Therefore, it is necessary to take preventive measures to protect the security of the computer systems, achieve higher level of information of the staff and improve the keeping of official secrets and business data. A very important element in combating cybercrime is related to identity theft over the Internet, which affects both natural and legal persons and special attention in monitoring the Internet communications and protecting personal data is therefore necessary.

And finally, there is an obvious need to develop a multi-agency access to specialized services and interested parties at the national level, as well as international co-operation of authorized agencies in combating criminal acts of computer crime with an international element.

8. REFERENCE

1. Annex to the Recommendation of the Council of 26 November 1992, Guidelines for the security of information systems 26 November 1992 I. AIMS
2. Božić V, *The intention as essential element of criminal act of fraud in Croatian Criminal Law*, master's thesis, Zagreb, Faculty of Law, 03/11/2010, p.10-15.
3. Božić V, Nikač Ž, *Criminal incriminations based on the United nations Convention Against Transnational Organized crime in the criminal legislation of the Republic of Croatia and the Republic of Serbia,* Proceedings of the International Conference, Faculty of Security in Skopje, 2016
4. Convention on Cybercrime - ETS 185
5. Council framework decision 2005/222/JHA of 24 February 2005 on attacks against information systems, OG EU L 069/67
6. Criminal code RC, OG No 125/11,144/12,56/15,61/15
7. Directive 2013/40/EU of the EU Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA OJ L 218, 14/08/2013, p. 8–14
8. Directive 2006/24/EC of the EU Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OG EU L 105/54
9. Directive 2009/24/ EC of the EU Parliament and of the Council of 23 April 2009 on the legal protection of computer programs, OG EU L 111/16
10. Kokot I, *Criminal law protection of computer systems, programs and data*, Zagreb Law Review, Vol. 3 No. 3, 2014, p.301-327.
11. Law on Ratification of the Additional Protocol to the Convention on Cybercrime Concerning the Criminalization of Acts of a Racist and Xenophobic Nature Committed Through Computer Systems
12. Nikač Ž, Božić V, *International Cooperation of Southeast Europe in the fight against crime*, Львівський державний університет внутрішніх справ, Ukraina, Lviv, International scientific conference "Theory and Practice of Law Enforcement Activities," Conference Proceedings, Lviv, 2016, p.431-443.
13. Nikač Ž, Urošević V, *Place and role of Ministry of the interior of the Republic of Serbia in prevention of high tech crime*, Conference Proceedings Forum BISEC 2010, Belgrade, p.53-58.
14. Nikač Ž, *International police cooperation*, KPA, Belgrade, 2015, p.110-112.
15. Obradović S, Mijalković M, Perić D, Puača D, *Crime Investigation on computers*, Infoteh-Jahorina Vol. 6, Ref. E-III-14, p. 455-459, 03/2007
16. Ranđelović D, *High-tech Crime*, KPA, Beograd, 2013, p.257-265.
17. Regulation on the takeover of Directive 2013/40/EU on attacks against information systems and Directive 2014/62/EU on the criminal justice protection of the Euro and other currencies against counterfeiting, OG, IA No 102/15

18. Statistical overview of the basic security indicators and performance in 2015, Ministry of Interior of Republic of Croatia, Zagreb, 01/2016
19. Stojanović Z, *Modern technical means and criminal law with special emphasis on Cybercrime*, Round Table Modern technology and criminal justice, XXV Counseling Association of Criminal Law and Criminology Yugoslavia, Novi Sad, 1987.
20. Šimundić S, Franjić S, Vdovjak K, *Hoax*, Proceedings of the Faculty of Law in Split, year 49, 3/2012., p. 459.- 480.
21. Vuletić I, Nedić T, *Computer fraud in Croatian Criminal Law,* Proceedings of the Faculty of Law of the University of Rijeka v.35, no.2, p. 679-692 (2014)

Web

- https://www.mup.hr/UserDocsImages/minstarstvo/USTROJ_MUP_RH/Odjel_za_visokotehnoloski_kriminalitet.pdf
- http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32009L0024
- http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32006L0024
- https://www.istra-istria.hr/fileadmin/dokumenti/upravna_tijela/UO_za_tal_nac_zaj/Instrumenti_zastite_ljudskih_prava/I.Multilateralni_odnosi/3.Vijece_Europe/I-3.17Dodatni%20protokol%20uz%20konvenciju%20o%20kibernetickom%20kriminalu%20o%20inkriminiranju%20djela%20rasisticke%20i%20ksenofobne%20naravi%20pocinjenih%20pomocu%20racunalnih%20sustava.pdf
- http://www.oecd.org/sti/ieconomy/oecdguidelinesforthesecurityofinformationsystems1992
- http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf
- http://www.oecd.org/sti/ieconomy/oecdguidelinesforthesecurityofinformationsystems1992.htm
- http://idn-wi.com/united-nations-definition-cybercrime/
- www.fbi.gov

40 years
Faculty of security
Skopje

МЕЃУНАРОДНА НАУЧНА КОНФЕРЕНЦИЈА

БЕЗБЕДНОСНИ КОНЦЕПТИ И ПОЛИТИКИ - НОВА ГЕНЕРАЦИЈА НА РИЗИЦИ И ЗАКАНИ

INTERNATIONAL SCIENTIFIC CONFERENCE

SECURITY CONCEPTS AND POLICIES - NEW GENERATION OF RISKS AND THREATS

МЕЃУНАРОДНА НАУЧНА КОНФЕРЕНЦИЈА

БЕЗБЕДНОСНИ КОНЦЕПТИ И ПОЛИТИКИ - НОВА ГЕНЕРАЦИЈА НА РИЗИЦИ И ЗАКАНИ

04 - 05 Јуни 2017, Охрид

Том III

Скопје 2017

INTERNATIONAL SCIENTIFIC CONFERENCE

SECURITY CONCEPTS AND POLICIES - NEW GENERATION OF RISKS AND THREATS

04 -05 June 2017, Ohrid

Volume III

Skopje 2017

Издавачи:

Универзитет „Св. Климент Охридски“
Битола
Факултет за безбедност – Скопје

За издавачите:

проф. д-р Сашо Коруновски, ректор на
Универзитетот „Св. Климент
Охридски“ – Битола
проф. д-р Оливер Бачановиќ, декан на
Факултетот за безбедност – Скопје

Уредник на изданието:
Доц. д-р Марјан Ѓуровски

Лектор на англиски јазик:
Рози Гроздановска Велеска

Компјутерска обработка:
Оливера Трајанова Ѓорѓијовски
Кемал Рушид

Печати:
АД „Ван Гог“ - Скопје

Адреса на издавачите:

Факултет за безбедност 1000 Скопје
П. Фах 103
тел: 022546211

Универзитет „Св. КлиментОхридски“
1ви Мај б.б. 7000 Битола,
тел: 047223788

Publishers:

University “St. Kliment Ohridski”
Bitola
Faculty of Security- Skopje

For the Publishers:

Sašo Korunovski, PhD Rector of
the University “St. Kliment
Ohridski”- Bitola
Oliver Bačanović, PhD Dean of
the Faculty of Security- Skopje

Editor in Chief:
Marjan Gjurovski, PhD

Lecturer in English:
Rozi Grozdanovska Veleska

Computer Processing:
Olivera Trajanova Gjorgjijovski
Kemal Rushid

Print:
“Van Gog” - LTD Skopje

Address of the Publishers:

Faculty of Security1000 Skopje
P.O. Box 103
tel: ++389(0)22546211

University “St. KlimentOhridski”
1 Maj b.b.7000 Bitola
tel: +++389(0) 47223788

PROGRAMME COMMITTEE:

Dr.Sc. Oliver Bacanovic, Dean of the Faculty of Security, Skopje, Republic of Macedonia, Chairman
Bogdan Mirchev, Hanns Seidel Stiftung Foundation
Dr.Sc. Cane Mojanoski, Faculty of Security, Skopje, Republic of Macedonia
Dr.Sc. Tome Batkovski, Faculty of Security, Skopje, Republic of Macedonia
Dr.Sc. Miodrag Labovic, Faculty of Security, Skopje, Republic of Macedonia
Dr.Sc. Zlate Dimovski, Faculty of Security, Skopje, Republic of Macedonia
Dr.Sc. Bogdanco Gogov, Faculty of Security, Skopje, Republic of Macedonia
Dr.Sc. Ferenc Banfi, Director of CEPOL (European Union for Law Enforcement Training)
Norbert Leitner, President of the Association of European Police Colleges
Prof. (em.) Dr.Georg Lohmann, Guericke University of Magdeburg, Berlin
Dr.Sc.Taro Tsukimura, Doshisha University, Kyoto, Japan
Dr.Sc. Marco Lombardi, University Cattolica, Milano, Italy
Dr.Sc.Vinay Kaura, Sardar Patel University of Police, Security and Criminal Justice, Rajasthan, India
Dr.Sc. Galit Ben-Israel, Ben Gurion University of the Negev, Bar-Ilan University, The Hebrew University of Jerusalem, Izrael
Dr.Sc. Goran Boskovic, Acting Dean of the Academy of Criminalistics and Police Studies, Serbia
Dr.Sc. Torje Daniel - Costel, Rector of the Police Academy "Alexandru Ioan Cuza", Romania
Dr.Sc. Nedelco Lazarov Stoichev, Rector of the Academy of the Ministry of Interior, Bulgaria
Dr.Sc. Andrej Sotlar, Dean of the Faculty of Criminal Justice and Security, Slovenia
Dr.Sc. Ivica Radovic, Dean of the Faculty of Security Studies, University of Belgrade, Serbia
Dr.Sc. Nedzad Korajlic, Dean of the Faculty of Criminalistics, Criminology and Security Studies, University of Sarajevo, Bosnia and Herzegovina
Dr.Sc. Ivan Toth, Dean of the University of Applied Sciences, VVG, Croatia
Dr.Sc. Marta Zorko, Vice-dean of Faculty of Political Science of Zagreb, Croatia
Dr.Sc. Denis Caleta, President of the Council, Institute for Corporate Security Studies ICS Ljubljana, Slovenia
Dr.Sc. Josko Vukosav, Dean of the High Police School, Zagreb, Croatia
Dr.Sc. Mile Shikman, Head of the Administration for Police Education of Republika Srpska, Bosnia and Herzegovina
Dr.Sc. Goran Ajdinski, Dean of Faculty of Philosophy, University St. Cyril and Methodius, Skopje, Republic of Macedonia
Dr.Sc. Mirjana Franceshko, Dean of Faculty of Law and Business Studies Lazar Vrkatic, University UNION, Novi Sad, Serbia
Rajko Pekovic, Director of the Police Academy, Montenegro
Verica Stefanovska Milevska, Chamber of Republic of Republic of Macedonia for private security
Dr.Sc.Urim Vejseli, Crisis management center, Government of Republic of Macedonia
Dr.Sc. Vesna Trajkovska, Secretary of Programme Committee

ORGANIZING COMMITTEE:

Dr.Sc Marjan Gjurovski, Chairman
Dr.Sc Boris Murgoski
Dr.Sc Zhidas Daskalovski
Dr.Sc Marjan Nikolovski
Dr.Sc Sashe Gerasimoski
Dr.Sc Snezana Mojsoska
Dr.Sc Nikola Dujovski
Dr.Sc Rade Rajkovcevski
Dr.Sc Tatjana Gerginova
Dr.Sc Natasha Jovanova
Dr.Sc Ice Ilijevski, Secretary of Organizing Committee

CONTENTS:

LAW, DEMOCRACY, RULE OF LAW AND HUMAN RIGHT

CRIMINOLOGY AND CRIMINAL LAW IN THE FUNCTION OF SECURITY