capital region due to less stringent laws and legislation. The law enforcement agencies should be more empowered and the laws; more strict, to curb such scenario.

It is interesting to note, however that as compared to standard ballistic protocols, the terminal injury pattern varied quite a lot keeping in mind the use of home-made firearms (desi kattas). These weapons are designed to cause propulsion of projectiles using combustive exhaust and thus in a manner of speaking remain classified under firearm. Keeping in mind this argument these weapons do not undergo the design scrutiny and rigorous ballistic testing that standard firearm manufacturing protocols dictate. Thus these weapons have an inherent safety flaw and an unreliable ballistic profile and quite an unpredictable gyroscopic and flight path trajectory which would elude standard ballistic thinking. This fact is further highlights the requirement of a broader and more open approach to the scrutiny and analysis in the terminal ballistic wound analysis on the crime scene being investigated. It is quite important to keep in mind that these weapons can have aberrant functionality anywhere from basic design flaw to incomplete propulsive release to fracturing, fragmentation and deviation of the projectile ejected. It is of medico-legal importance that ballistic labs could struggle with identification and classification of such "bullets" and thus a more broad based thinking would be required to analyze and classify these projectiles, bearing in mind that the firearm in question cannot always be traced and the bullet recovered would be the only scientific evidence for prediction and reconstruction of the events at the time the crime occurred.

On further analysis it would be interesting to note whether the increase in firearm crime was attributable to increase in a specific increase in standardized firearm import and production or whether there is a flourishing country made firearm industry which needs to be urgently regulated and be brought under framework and policy control.

Although the demographic parameters from the study shows consistency with the various other studies, the virtue of gun crime is sporadic and non-normally distributed in society, thus leading to difficulty in statistical interpolation, however the rising incidence incites the need for introspection for the phenomenon and formulating rational and enforceable policies for their control.

References:

[1] Saukko P, Knight B. Knight's Forensic Pathology, 3Ed. CRC Press; 2004.p. 245-248.
[2] Kohli A, Aggarwal NK. Firearm fatalities in Delhi, India. Legal Medicine. 2006 Oct;8(5):264–8.
[3] Karlsson T, Isaksson B, Ormstad K. Gunshot fatalities in Stockholm, Sweden with special reference to the use of illegal weapons. J Forensic Sci 1993;38(6):1409–21.
[4] Ornehult L, Eriksson A. Fatal firearm accidents in Sweden. Forensic Sci Int 1987;34(4):257–66.
[5] Hardt-Madsen M, Simonsen J. Firearm fatalities in Denmark 1970– 1979. Forensic Sci Int 1983;23(2–3):93–8.
[6] J. Rainio, A. Sajantila, Fatal gunshot wounds between 1995 and 2001 in a highly populated region in Finland, Am. J. Forensic Med. Pathol. 26 (2005) 70–77.
[7] Karger B, Billeb E, Koops E. Accidental firearm fatalities. Forensic and preventive implications. Int J Legal Med 2002;116(6):350–3.
[8] Meel BL. Firearm fatalities in the Transkei region of South Africa, 1993–2004. S Afr Med J 2005;95(12):963–7.
[9] Onuminya JE, Ohwowhiagbese E. Pattern of civilian gunshot injuries in Irrua, Nigeria. S Afr J Surg 2005;43(4):170–2.
[10] Amiri A, Sanaei-Zadeh H, Towfighi Zavarei H, Rezvani Ardestani F, Savoji N. Firearm fatalities. A preliminary study report from Iran. J Clin Forensic Med 2003;10(3):159–63.
[11] Elfawal MA, Awad OA. Firearm fatalities in Eastern Saudi Arabia: impact of culture and legislation. Am J Forensic Med Pathol 1997;18(4):391–6.
[12] Ikeda RM, Gorwitz R, James SP, Powell KE, Mercy JA. Trends in fatal firearm-related injuries, United States, 1962–1993. Am J Prev Med 1997;13(5):396–400.
[13] Rouse D, Dunn L. Firearm fatalities. Forensic Sci Int 1992;56(1):59–64.

International Scientific Conference
"ROMANIAN EDUCATIONAL SYSTEM OF FORENSIC SCIENCE"
5th Edition, Bucharest, Romania, April 27-28 2017
ISSN 2501-3742 DOI 10.18283/C01-2017-035

Criminal law and Criminalistic forensic approach to fighting Cyber Crime/ Dreptul penal și abordarea criminalistică a criminalității în lupta împotriva criminalității informatice

Vanda BOŽIĆ PhD[1], Željko NIKAČ PhD[2]
[1] Faculty of Law - Trg M.Tita 14 Zagreb– Rep.of Croatia,
[2]Serbian Police Academy - Cara Dusana 196, Zemun, Belgrade – Rep.of Serbia
[1] vanda.bozic@pravo.hr, [2] zeljko.nikac@kpa.edu.rs

Abstract (en): Computers, computer systems, Internet and social networks represent today one of the most important achievements of technical and technological development of human civilization. In addition to the enormous benefits to humanity of these inventions are unfortunately abused and become a means for the execution of specific criminal acts named cyber crime. At the center of this type of crime is information technology as software for execution these criminal actions. International documents and with them harmonized national legislation are the legal framework in the fight against cyber crime. Work on discovering and proving criminal offenses of cyber crime is very difficult due to the specific ways of committing, the characteristics of the offender, place of committing as well as the time and place of occurrence of consequences. The primary role in proving this type of crime has a criminalistic forensics to obtain relevant evidence with a view to prosecuting the perpetrators. The paper presents the analysis of certain crimes committed in the area of cyber crime in the Republic of Croatia and the Republic of Serbia and given significant results in detecting and proving these criminal offenses. In concluding remarks are given suggestions de lege ferenda in order to improve the legal and institutional framework for combating cyber crime.

Keywords: cybercrime, international legal framework, criminal law, forensics.

Abstract (ro): Computerele, sistemele informatice, internetul și rețelele sociale reprezintă astăzi una dintre cele mai importante realizări ale dezvoltării tehnice și tehnologice a civilizației umane. În plus, față de beneficiile enorme pentru omenire, aceste invenții sunt din păcate abuzate și devin un mijloc de executare a unor acte criminale specifice numite infracțiuni cibernetice. În centrul acestui tip de infracțiuni este tehnologia informației ca software pentru executarea acestor acțiuni criminale. Documentele internaționale și, împreună cu acestea, legislația națională armonizată reprezintă cadrul legal în lupta împotriva criminalității cibernetice. Lucrul în descoperirea și dovedirea infracțiunilor de criminalitate cibernetică este foarte dificilă, datorită modurilor specifice de comitere, caracteristicilor infractorului, locului de comitere, precum și timpului și locului de apariție a consecințelor. Rolul principal în dovedirea acestui tip de infracțiune îl are o analiză criminalistică pentru a obține dovezi relevante în vederea urmăririi penale a infractorilor. Lucrarea prezintă analiza anumitor infracțiuni comise în domeniul criminalității cibernetice în Republica Croația și Republica Serbia și a dat rezultate semnificative în detectarea și dovedirea acestor infracțiuni. În comentariile finale sunt prezentate sugestii de lege ferenda pentru a îmbunătăți cadrul juridic și instituțional pentru combaterea criminalității cibernetice.

Cuvinte-cheie: criminalitatea cibernetică, cadrul juridic internațional, dreptul penal, criminalistică.

I. INTRODUCTION

At the beginning of the third millennium, science, engineering and technology experienced a peak in its development which has resulted in both positive and negative effects to society. The positive side is evident in relation to the general progress of humanity, development of new technologies and the emergence of modern products on the market, which greatly facilitate the lives of ordinary people. Computers are one of the most important technical and technological innovations that have made the Copernican turn in the modern world and become an integral part of the private and business life of people. Today, life in a modern society is simply unthinkable without computers,

which are in all the spheres of community, and this is supported by their enormous development and implementation in all business activities and private lives of people.

In practice, there are almost no professions or activities where computers have not found their application. Computers have exceptional importance in economic activities because without them business operation is not possible even at the basic level, while their role in generating profits goes without saying. Great is the importance of computers in accomplishing everyday communication with state authorities and local governments, as is the case with the tax authorities in relation to issuing invoices and submitting forms, banks in terms of transactions, etc. [1]

The downside of the development of computer technology is reflected primarily in the alienation of personality, addiction of young people to the Internet and computers, and in this regard with various forms of abuse. As the catastrophic phenomenon is the occurrence of cyber crime as a manifestation of a specific crime. There is a wide range of forms of cyber crime, among which are attacks on computers, sending and receiving computer viruses, infected emails [2] and other forms that have become an integral part of crime in the modern society. In the doctrine and practice current are different forms such as: cybercrime, computer fraud, computer or information crime, misuse of computers, and other terms that together form cybercrime as a genus term.

Social response to cyber crime takes place at the national and international level, and includes measures at the regulatory and operational level. More broadly countries and international organizations have adopted and signed certain important international acts (conventions, resolutions, declarations), which treat the area of cybercrime as an international problem, and accordingly call for international response and cooperation of states. States are as a rule committed to the harmonization of norms of domestic law with international standards and the development of international cooperation in the fight against cybercrime. Operational response includes activities, measures and actions at national and international level in the fight against cybercrime. This primarily refers to the exchange of information, joint operations and other actions, joint investigation teams and all forms of cooperation in combating cybercrime. [3]

Status and trends of cybercrime in the contemporary moment suggests that this form of crime is in the large increase and that is follows the general crime trends. Accordingly, it is necessary to constantly monitor all its forms, adopt legal and other novels, harmonize the court practice and improve police work in discovering and processing of all forms of cybercrime. An important element is the training and professionalization of personnel who is authorized by law to combat cybercrime.

II. CYBER CRIME - CONCEPT AND CHARACTERISTICS

The first case of cyber crime in the world was recorded in 1958 in the USA, and in 1966 the first case of falsification of bank data was formally prosecuted in Minneapolis. On the old continent, the first case was recorded in 1968 in Finland. In the former Yugoslavia the first case of cybercrime dates back to 1983 related to the case of Istria Bank in Pula. [4]

a) The term cybercrime is not uniquely determined in doctrine and practice, firstly because of different legal systems (common law, continental law) and accordingly there are different solutions in national legislations of individual countries. There are also difficulties in defining cybercrime due to the fact that it is a relatively new form of criminal conduct as well as due to very pronounced phenomenological diversity, which makes it difficult to cover cybercrime with one definition.

Semantic term cybercrime can be first seen from the standpoint of its meaning in the English language: Cybercrime includes illegal activities performed on the computer or in which the computer is a means of execution. It covers criminal intrusion in the second computer system, theft of computer data, or use the on-line system to execute or assist in the commission of frauds. [5] One of the first authors who tried to define cybercrime was Don Parker who said it was a general form through which to express different activities, form which will in the future become dominant. [6] Parker concludes that the "misuse of computers" is every event concerning the use of computer technology in which the victim suffers or is likely to suffer loss, but the offender acts with the intention to obtain or could obtain a benefit. [7]

The term cybercrime from the point of criminal legislation covers the misuse of computer systems, programs and data taxatively incriminated in the criminal code. In general, the crimes that are the result of misuse of IT resources can be divided into: a) acts in which the computer is the object of the acts of commission (computer crime), b) offenses for which the computer is a means of execution (computer related crime) and c) acts of illegal use of the Internet (net crime). [8]

In the Guidelines for the Security of Information Systems OECD in 1992 defined information systems. It 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.[9] At the 10th UN Congress on Crime Prevention and Treatment of Delinquents a view was taken that cyber crime is a general term that includes crimes that are carried out by means of a computer system or network, to them or against them. Cybercrime includes any crime that takes place in an electronic environment. [10] 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. [11]

At EU level cyber crime is determined in accordance with the Directive 2013/40/EU on attacks against information systems. Information system means a device or group of inter-connected or related devices, one or more of which, pursuant to a programme, automatically processes computer data, as well as computer data stored, processed, retrieved or transmitted by that device or group of devices for the purposes of its or their operation, use, protection and maintenance.[12]

According to CC RC, a 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. [13] Computer data is any representation of facts, information or concepts in a form suitable for processing in a computer system [14], while a set of computer data that can enable a computer system to perform a function is called a computer program. [15]

The problem of defining cyber crime and the determination of its characteristics is open primarily because of the different approaches of individual authors, so we think it necessary to have an extensive approach. A comprehensive definition of the concept must incorporate a minimum of the following three important elements in its structure: method of carrying out the crime, means of performing the crime and results of the criminal activity. The method of performing the crime implies the use of a computer, which may be the primary means for the execution of the crime, whereby it is necessary to have consequences that are punishable by law. [16] In our view, computer crime can be defined as a form of criminal conduct in which the use of computer technology and information systems manifests itself as a method of carrying out the crime or the computer is used as a tool or a target of execution, which, in a criminal sense, realizes relevant consequences.

b) Characteristics of cyber crime are related to the special ambience of committing criminal acts of this kind, their complex structure, specific ways and means of committing the crime, and special object of protection and enormous social danger. The crimes of this kind do not recognize state borders nor physical barriers and are manifested in a special environment.

The intent of the perpetrator (dolus specialis) to acquire unlawful material or non-material benefit for himself or others, or to inflict damage to others, is an essential element in the commission of this type of crime.

Another important feature of cybercrime are the extremely high numbers in this kind of crime which is particularly reflected in the difficulties in detecting, proving and prosecuting these criminal offenses and offenders. As reasons we give the complex structure of acts of cybercrime, specific characteristics of the perpetrator (delicta propria), superior expertise of perpetrators given that this type of crime as a rule consists of experts in the field of ITS (information technology and systems) and the place in the form of extensive interpretation of the place where the crime is committed.

The crimes of cybercrime today represent a very serious social problem due to the specific ways and place of committing the crime, because of the large number of users of social networks, the special characteristics of the perpetrator and particularly due to high growth rates. In view of the situation and trends of cybercrime the official estimate of the FBI is that less than 1% of this type of crime was discovered, while only 12% is reported. [17] In its work on combating cyber crime FBI cooperates with specialized agencies and international organizations in this area, such as the cooperation with CERT (Computer Emergency Response Team). [18].

III. LEGAL FRAMEWORK FOR COMBATING CYBERCRIME

International legal sources

The main international legal source to combat cyber crime, the *Convention on Cyber crime of the Council of Europe* (CETS No.185) was adopted in Budapest in 2001 [19]. The Republic of Croatia signed and ratified the Convention with the *Law on Ratification of the Convention on Cybercrime*, [20] and the Republic of Serbia did the same by the *Law on Ratification of the Convention on High-Tech Crime.* [21] The States Parties to the Convention commit themselves in their national legislation to criminalize the following offenses: a) Offences against the confidentiality, integrity and availability of computer data and systems, b) Computer-related offences, c) Content-related offences and d) Offences related to infringements of copyright and related rights.[22] Significant are the provisions of the Convention relating to international co-operation of States Parties and their mutual legal assistance.

Two years after the adoption of the Convention the *Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems* was adopted in Strasbourg. [23] The Protocol commits the State parties to adopt all necessary legislative and other measures in their national legislation and to establish as criminal offenses the following conducts committed intentionally and without right: dissemination of racist and xenophobic material through computer systems, threats over a computer network motivated by racism and xenophobia, publicly insulting persons using a computer system because they belong to a group distinguished by race, color, descent, or national or ethnic origin and religion, distributing or making available through a computer system to the public material which denies, essentially minimizes, approves or justifies acts of genocide or crimes against humanity, and aiding and encouraging the commission of any of these offenses. [24]

European Parliament and the Council adopted on the 12 August 2013 the *Directive 2013/40/EU* on attacks against information systems, which replaces the Council Framework Decision 2005/222/PUP.[25] This Directive requires States Parties to in their national legislation criminalize offenses such as illegal access to information systems, illegal system interference, illegal data interference, illegal interception, incitement, aiding and abetting and attempt, with prescribed liability of legal persons. Directive broadens the criminal conduct and introduces the aggravating circumstances. [26]

Among the significant international legal documents in the fight against cybercrime we must also mention the *Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs*, [27] according to which the original computer program is protected in a way that represents the author's own intellectual creation and no other criteria can be applied in determining its suitability as well as Directive *2006/24/EC* of the European 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 [28] adopted with a view to more effectively combat cybercrime based on electronic traces and other relevant evidence.

Significant law sources at the international level are the *United Nations Convention against Transnational Organized Crime* [29], *Police Cooperation Convention for Southeast Europe* [30] and *Convention of the Southeast European Law Enforcement Center* [31], which foresee important

criminal justice and police operating mechanisms in combating transnational crime such as special techniques, methods, and special bodies. [32].

National legal sources of Croatia and Serbia, a review

The Criminal Code of Croatia in Chapter XXV incriminates offenses against computer systems, programs and data: [33] unauthorized access to a computer system or computer data, disabling or impeding the work or use of a computer system, computer data or programs or computer communication, damage to computer data, unauthorized interception of computer data, computer counterfeiting, computer fraud, misuse of devices and serious offenses against computer systems, programs and data. Prescribed eight criminal offenses are in line with the Convention on Cybercrime. Table 1 lists the offenses and applicable sanctions.

No	Criminal Code - Croatia	Penalty
1	*Unauthorized access to a computer system or computer data (Art. 266)*	- *Imprisonment up to 2 years* - *Imprisonment up to three years* for aggravated forms (when the offense is committed in relation to a computer system or computer data of a governmental body, the Constitutional Court of Republic of Croatia and international organizations whose member Croatia is, bodies of local or regional government, a public institution or a company of special public interest.)
2	*Disabling or impeding the work or use of a computer system, computer data or programs or computer communication (Art.267)*	- *Imprisonment up to 3 years*
3	*Damage to computer data (Art. 268)*	- *Imprisonment up to 3 years*
4	*Unauthorized interception of computer data (Art.269)*	- *Imprisonment up to 3 years*
5	*Computer Counterfeiting (Art.270)*	- *Imprisonment up to 3 years*
6	*Computer fraud (Art. 271)*	- *Imprisonment from 6 months to 5 years* -*Prison sentence of 1-8 years* for an aggravated form (when the offense has produced substantial financial gain or caused considerable damage)
7	*Misuse of devices (Art.272)*	- *Imprisonment up to 3 years* - *Imprisonment up to 2 years* for a simple form
8	*Serious offenses against computer systems, programs and data (Art.273)*	- *Imprisonment from 6 months to 5 years* -*Imprisonment of 1-8 years* for aggravated forms

Table 1. Criminal offenses against computer systems, programs and data according to the CC RC

Criminal Code of the Republic of Serbia in the Chapter XXVII criminalizes eight criminal acts against the security of computer data: *damage to computer data and programs, computer sabotage, making and introducing computer viruses, computer fraud, unauthorized access to a protected computer, computer network and electronic data processing and prevention and the limitation of access to a public computer network.* [34]

Table 2 lists the offenses and applicable sanctions.

No	Criminal Code - Serbia	Penalty
1	*Damage to computer data and programs (Art.298)*	- *Imprisonment up to 3 years* (in case of unauthorized deletion, altering, damaging, concealing or otherwise rendering useless computer data or programs) - *Imprisonment of 3 months to 3 years* (if the offense has caused damage in excess of four hundred and fifty thousand dinars)

		- *Imprisonment of 3 months to 5 years* (if the offense caused damage in excess of one million and five hundred thousand dinars)
2	*Computer sabotage (Art.299)*	- *Imprisonment from 6 months to 5 years*
3	*Making and introduction of computer viruses (Art.300)*	- *Fine or imprisonment of up to 6 months* - *Fine or imprisonment of up to 2 years* (if a computer virus is introduced into someone else's computer or computer network, thereby causing damage)
4	*Computer fraud (Art.301)*	- *Fine or imprisonment of up to 3 years* - *Imprisonment of 1-8 years* (if the material gain exceeds the amount of four hundred and fifty thousand dinars) - *Imprisonment of 2-10 years (if the material gain exceeds the amount of one million and five hundred thousand dinars)* - *Fine or imprisonment up to 6 months* (if the offense is done only with the intention to cause damage to another)
5	*Unauthorized access to a protected computer, computer network and electronic data processing (Art. 302)*	- *Fine or imprisonment of up to 6 months* - *Fine or imprisonment up to 2 years (if one records or uses data obtained in an unauthorized manner)* - *Imprisonment of up to 2 years (if there was stoppage or serious disturbance in functioning of electronic processing and data transmission or network or other serious consequences)*
6	*Prevention and the limitation of access to a public computer network (Art.303)*	- *Fine or imprisonment of up to 1 year* - *Imprisonment up to 3 years for a qualified form* (if the offense was committed by an official in discharge of duty)
7	*Unauthorized use of a computer or a computer network (Art.304)*	- *Fine or imprisonment of up to 3 months*
8	*Making, procuring or providing other means to commit offenses against the security of computer data (Art.304a)*	- *Imprisonment from 6 months to 3 years* - *Fine or imprisonment of up to 1 years (if one has funds with the intention of committing cyber crime)*

Table 2. Criminal offenses against the security of computer data according to the CC RS

IV. CRIMINAL-OPERATIONAL AND FORENSIC ASPECT OF COMBATING CYBER CRIME

The fight against cyber crime has legislative and operational aspects, taking place at both the international and national level. The legal framework, which is established by norms of international and domestic law, is the basis for criminal-operational and forensic response in combating cyber crime.

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, followed by a reaction of the state and the international community.

Manifestations of cyber crime in the contemporary moment are very different and are steadily developing because they monitor technical-technological progress, so their detection and prosecution is much more difficult. The most important forms of cyber crime today are the following: financial fraud, theft of goods, abuse of data, identity theft, computer sabotage, unauthorized use of computer systems, stealing information and deception. [35] Especially current are cyber crimes committed on the Internet and other social networks that take on new forms, and change and modify existing forms. Identity theft and misuse of data obtained through the Internet and in other illegal means are steadily increasing, and the data is used for various crimes and obtaining illegal gain. The data is often used after a certain time period, and can be assigned to other perpetrators of criminal acts. [36]

The expansion of the attacks on computer-hardware and software (network interference), various forms of financial crime (on-line fraud, fishing), attempts of sexual exploitation and abuse of young people. Still present are ome specific forms of cyber crime such as: hacking, computer viruses, software piracy, denial of service, electronic harassment, theft of computer services, etc. We especially emphasize the abuse of electronic data on payment cards on the Internet and other forms

of financial fraud, when illegally obtained electronic data is further used to buy things over the Internet. [37] A large number of crimes of theft of intellectual work, unauthorized copying on multimedia carriers and resale (i.e. e-books via the Internet). [38]

Offenders of cyber crime are not only experts in this area, but there is now a large number of people who have computers readily available and who are able to use the Internet and other social networks. Particular danger comes from the engagement of organized criminal groups that abuse computers to carry out serious criminal offenses, and the formation of cyber crime networks is often the case that takes place in a specific (computer) environment. [39] Modern hackers perform unauthorized break-ins into systems of state bodies by exploiting weaknesses of a computer system comprising from host computers (consoles, printers, readers memory, magnetic tapes, soft discs), personal computers (PC personal computer) and typewriters with memory. [40]

Criminal-operational and forensic aspects of combating cyber crime are based on preventive measures, such as special protection passwords and codes. In the case of compromised passwords and codes following are reactive measures against intruders that include: locating, eliminating, identifying and repressive activities of the police, prosecution and courts. These measures are based on international and national normative-legal solutions which were first adopted by developed countries such as: Sweden - Swedish Data Act 1982, USA- Computer Fraud and Abuse Act 1986, UK - Law on Abuse of Computers in 1990, Russia - Amendments to the Act on information in 1992 and the Law on amendments of the Penal Code in 1996. [41] The next important step was the creation of specialized organizational units of the police, prosecution and courts for the detection and prosecution of criminal offenses of cyber crime.

Republic of Croatia has harmonized its national legislation with the norms of international law, and then there was the establishment of specialized bodies - police, prosecution and court for combating cybercrime. Within the General Police Directorate of the Ministry of Interior of Republic of Croatia - Criminal Police has formed 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. Department for High-tech Crime is the operational national contact point for international cooperation and exchange of information relating to offenses against computer systems, programs and data. [42]

In Republic of Serbia there was also first the harmonization of norms of the internal legislation with international legislation, and then the Law on Organization and Jurisdiction of State Authorities to Combat High-Tech Crime [43] established a specialized body to combat cyber crime offenses. Within the Police Directorate of the Ministry of Interior of Republic of Serbia - Criminal Police Directorate of the Department for Combating High-Tech Crime, which is a part of the Department for Combating Organized Crime (SBPOK). [44]

International criminal law and police cooperation are important elements in combating cybercrime in a time of technological development and progress of IT systems. In addition to the cooperation of states, important role is placed on the cooperation that takes place through Interpol, Europol and other specialized organizations in the fight against crime. Due to the actuality of cyber crime in the contemporary moment within Interpol and Europol there are separate sections (crime areas) for their monitoring, control, information exchange and international cooperation. [45]

Effective investigation and proving of criminal offenses of cyber crime presupposes organized and team work of operational workers of Criminal Police and computer experts, using circumstantial and other criminal methods as techniques for the operation and functioning of the computer system. We can agree with the position W. Sessions who states the following:This crime will be addressed by applying traditional legal and investigative techniques whenever possible, but it is necessary to develop a new strategy to adapt to the needs in accordance with the trends of cyber crime in the future. [46] This includes taking the following actions: investigation and securing the crime scene, taking control of the computer, access ban for unauthorized persons, gathering information from related

parties, checking the profile of suspects and other actions aimed at collecting relevant evidence in criminal proceedings. [47]

V. CONCLUSION

Cybercrime is one of the most sophisticated forms of crime today that manifests itself through various methods of committing the crime. Specificity of cyber crime is primarily in the special area in which it takes place, then the exceptional degree of social danger, the way of committing the crime, knowledge, skills and characteristics of perpetrators, difficulties in providing valid evidence and prosecuting the perpetrators. The problem is worse because of the large number of criminal acts of cyber crime that are not even reported (dark figure) and a small number of criminal offenses that will ultimately get a court epilogue and perpetrators will get the deserved penalty.

The international community and the developed countries have been the first to react by adopting the Convention on Cybercrime, which is a legal source par excellence in this matter. The Convention has established important legal solutions of the criminal substantive and criminal procedural law in the area of cyber crime on the basis of which the Contracting States undertook to harmonize national legislation, to adopt concrete adequate measures and establish international cooperation in combating cybercrime.

Croatia and Serbia acted in a same way by ratifying the Convention and harmonizing national regulations. Croatia is better off as a country that is already an EU member, while Serbia has submitted an application for membership and opened individual chapters in this process. However, despite the harmonization of standards with international standards, there are a number of legal and practical problems that make it difficult to combat cybercrime. At first glance noticeable are linguistic, lexical and semantic differences in the definition of certain terms of cyber crime and harmonization with the provisions of the Convention and the EU Directive 2013/40/EU on attacks against information systems. It is further noted that certain criminal offenses in the Criminal Code of Croatia and Serbia are defined much broader than the minimum provided under international standards. These and other differences can lead to different legal interpretations of certain terms and institutes which may be at the expense of effective enforcement in practice.

Current status and trends of cybercrime indicate that this form of criminality is on the constant rise and that it very often has attributes of organized crime. All the more necessary is the adequate criminal-legal and criminal-operative reaction of the most important subjects in the fight against crime, as Croatia and Serbia have done in a certain way by forming specialized agencies within the Criminal Police (Department for Combating the High-Tech Crime). The fight against cybercrime still means adequately equipped and trained personnel within the police, prosecution, court and other law enforcement officers. Given that the burden of proof (evidence collection) is on the side of the State Attorney and his subordinate police, special significance is on the crime-operative and forensic approach to cybercrime. Multi-agency approach at the national level is today the standard which has been established long ago by developed European and other countries.

Finally, the importance of the activities to combat cybercrime involves international cooperation of States and international organizations, in particular because the area of cybercrime is broad and as a rule international.

References

[1] Božić V, International legal framework for combating cyber crime with reference to the legislation of the Republic of Croatia, Proceedings of the Faculty of Security Skopje, Ohrid 2017
[2] Šimundić S, Franjić S, Vdovjak K, Hoax, Proceedings of the Faculty of Law Split, year. 49, 3/2012, p.459.- 480.
[3] Nikač Ž, Međunarodna policijska suradnja, KPA, Belgrade 2015, p.109-112.
[4] Ranđelović D, Visokotehnološki kriminal, KPA, Belgrade, 2013, p.257-265.
[5] Encarta, World English Dictionary, North AmericanEdition, 2001 Microsoft Corporation (14.03.2017).
[6] See more: Parker D, Fighting computer crime, New York, 1983
[7] See more: Parker D, Computer Abuse, Springfield, 1973
[8] See more: Stojanović Z, Savremena tehnička sredstva i krivično pravo sa posebnim osvrtom na kompjuterski kriminalitet, SFRJ, Novi Sad, 1987.

[9] 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, (13.03.2017)
[10] X UN Congress on the Prevention of Crime and the Treatment of Offenders,2000, Background paper for the workshop on crimes related to the computer network: Crime-fighting on the Net.
[11] http://idn-wi.com/united-nations-definition-cybercrime/ (14.03.2017)
[12] 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, 14.8.2013, p. 8–14
[13] Art.87.par.18. CC RC Official Gazette no 125/11,144/12,56/15,61/15
[14] Ibid. art.87.par.19.
[15] Ibid. art.87.par.20.
[16] See more: Aleksić Ž, Škulić M: Criminalistics, Faculty of Law Beograd, 2007.
[17] Obradović S, Mijalković M, Perić D, Puača D, Istraživanje kriminala na računarima, Infoteh-Jahorina Vol. 6, Ref. E-III-14, p. 455-459, 03/2007
[18] https://www.fbi.gov/investigate, Cyber crime (15.03.2017)
[19] Convention on Cybercrime, ETS 185, 23.11.2001 available at: http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf, (10.03.2017.)
[20] Official Gazette RC, IA no 9/02
[21] Official Gazette RS no. 19/09
[22] Ibid. Op.cit.1.
[23] European Treaty Series - No. 189, Strasbourg, 28.I.2003, available at: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/090000168008160f, (10.03.2017.)
[24] Art.3.-7. Ibid.
[25] Directive 2013/40/EU of the European parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:218:0008:0014:en:PDF, (10.03.2017.)
[26] See more: Kokot I, Criminal-law protection of computer systems, programs and dana, Zagreb Law Review, Vol. 3 No. 3, 2014, p.301-327
[27] Directive 2009/24/EC, Official Journal of the European Union, L 111/16, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32009L0024, (10.03.2017.)
[28] Directive 2006/24/EC, Official Journal of the European Union, L 105/54, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32006L0024, (10.03.2017.)
[29] United Nations Convention against Transnational Organized Crime, available at: https://www.unodc.org/unodc/treaties/CTOC/, (10.03.2017.)
[30] Police Cooperation Convention for Southeast Europe, available at: http://www.pccseesecretariat.si/index.php?item=9&page=static, PCC SEE 2006 2011.pdf, (10.03.2017.)
[31] SELEC Convention, available at: http://www.selec.org/docs/PDF/SELEC20Convention%20%5Bsigned%20on%2009.12.2009%5D.pdf(10.03.2017.)
[32] See more: Nikač Ž, Božić V: International Cooperation of Southeast Europe in the fight against crime, International scientific conference "Theory and Practice of Law Enforcement Activities," Conference Proceedings, Ukraina, Lviv, 2016, p.431-443.
[33] Art.266.-273. Criminal code RC, Official Gazette no 125/11,144/12,56/15,61/15
[34] Art.298.-304a. Criminal code RS, Official Gazette no. 85/05, 88/05, 107/05 , 72/09, 111/09, 121/12, 104/13, 108/14, 94/16
[35] Ibid. Op.cit.3. p.110-112.
[36] Ibid. Op.cit. 1.
[37] See more: 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.
[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] Ibid. Op.cit. 8.
[40] Tappolet J, Zlouporabe u informatici, Revue Internationale de criminologie et de police technique, No. 3, Geneve 1988, p.351–357.
[41] Cetinić M, Rešenje kompjuterskih krivičnih dela u novom KZ Rusije, Anali Pravnog fakulteta, br. 4–6, Belgrade, 1996, p.190–199.
[42] https://www.mup.hr/UserDocsImages/minstarstvo/USTROJ_MUP_RH/Odjel_za_visokotehnoloski_kriminalitet.pdf, (20.03.2017.)
[43] Official Gazette RS no. 61/05, 104/09
[44] www.mup.gov.rs (20.03.2017)
[45] www.interpol.int (21.03.2017); www.europol.europa.eu (21.03.2017)
[46] Sessions S, W, Kompjuterski kriminal-trend koji eskalira, Priučnik, Zagreb, 3/91
[47] See more: Bošković M, Kriminalistička metodika 2, Police Academy, Belgrade, 2000

The paper is the result of work on the project: „Multidisciplinary Research Cluster on Crime in Transition - Trafficking in Human Beings, Corruption and Economic Crime," Croatian Science Foundation no. 1949. and "Innovation of forensic methods and their application," Ministry of Education, Science and Technological Development of RS with no. tr 34019.

CONFERENCE PROCEEDINGS

of

International Scientific Conference

„Romanian Educational System of Forensic Science"

5th Edition

ISSN 2501-3742

DOI 10.18283/C01-2017

Published by
Research & Science Publishing House
Bucharest, Romania, 2017

International Scientific Conference

"ROMANIAN EDUCATIONAL SYSTEM OF FORENSIC SCIENCE"

5th Edition, Bucharest, Romania, April 27-28, 2017

SCIENTIFIC COMMITTEE:

President: Prof. Daniel TORJE PhD

Members of Scientific Committee:

Prof. Sergiu VASILE PhD, Prof.Claudiu ŢUPULAN PhD, Prof. Laurenţiu GIUREA PhD, Prof. Adrian IACOB PhD, Prof.Bogdan ŢONEA PhD, Assoc.prof. Ciprian CONSTANTIN PhD, Assoc.prof.Cristian ŞTEFAN PhD, Assoc.prof. Georgică PANFIL PhD, Assoc.prof. Marin RUIU PhD, Assoc.Prof. Cristina PIELMUŞ PhD, Assoc.Prof. Andreea CĂLUGĂRIŢA PhD, Assoc.prof. Viorel VASILE PhD, Lect.Daniel ATASIE PhD, Florin STANCIU PhD, Georgeta STOIAN PhD, Grigore STOLOJESCU PhD, Petruţ ENACHE PhD, Romică POTORAC, Adrian MITROFAN, Alexandru DENA, Irina SLABU, George DOBRIN

ORGANISING COMMITTEE

Lect.Horia RAŢĂ PhD, Cătălin TOADER PhD, Cezar CIOACĂ, Dănuţ NECHITA, Sorin ŞOIMU, Marius ANDRIŢA, Andrei NELEAPCĂ, Diana DUMITRESCU, Teodora SABABEI

CONFERENCE CHAIRS

Assoc.Prof.Georgică PANFIL PhD, Assoc.Prof. Marin RUIU PhD

KEYNOTE SPEAKERS

Caroline WILKINSON
Dennis MCAULEY
Axel MANTHEI
Florin STANCIU
Rahul PATHAK

PROCEEDINGS EDITOR

Assoc. Prof. Georgică PANFIL PhD

ORGANISERS AND PARTNERS:

Alexandru Ioan Cuza Police Academy – Bucharest, Romania
European Association of Scientific Research – Bucharest, Romania
National Institute of Forensic Science – Bucharest, Romania
The Institute of Studies for Public Order – Bucharest, Romania
Center for Criminal Justice and Research Studies – Romania

SPONSORS AND SUPPORTERS

VI TECHNOLOGIES SRL
AMPED SOFTWARE
EVENT JUST SRL
PI ADVISOR PRINTING & IMAGE

The Conference Proceedings have been indexed within following databases: Elsevier - Social Sciences and Research Network (SSRN); CrossRef (DOI); Google Scholar; Academia.edu; - ResearchGate Scientific Network

TABLE OF CONTENTS

International Scientific Conference
"ROMANIAN EDUCATIONAL SYSTEM OF FORENSIC SCIENCE"
5th Edition, Bucharest, Romania, April 27-28, 2017

International Scientific Conference
"ROMANIAN EDUCATIONAL SYSTEM OF FORENSIC SCIENCE"
5th Edition, Bucharest, Romania, April 27-28, 2017

CUPRINS

ISSN 2501-3742 DOI 10.18283/C01-2017-001

Manslaughter - a crime against traffic safety on public roads / Uciderea din culpă - infracțiune contra siguranței circulației pe drumurile publice

Andreea Florina STĂNILĂ (SIMION) [1], Dănuț LEFTER[2]
[1,2]Brăila County Police Inspectorate – 12 Mihail Sebastian Str., Brăila - Romania
[1]andreeastanila99@yahoo.com, [2]lefterdanut@yahoo.com

Abstract (en): Road accidents may be defined as those effects resulting from the breach of public road legislation within which the human being has a dual role, as its producer as well as the one who suffers from it. According to statistical summaries, there is an impressive increase in the number of road accidents occurring in Romania resulting in loss of life, personal injury or only in material damage, and, in this respect, an important contribution is represented by the increasing pace of modern life, which leads to the need for a more intense and rapid traffic. The right to life that the law guarantees for every person involves the protection of life and against offenses committed by negligence because, although less serious than those committed with intent, they have essentially the same result, namely a person's death. The criminalization of the offense of manslaughter was driven by the need to preserve human life against any action or inaction through which the driver of a vehicle does not show necessary caution and care in order to avoid the death of one or more persons as road users. Such a concentration of attention and prudence shown to others is becoming increasingly necessary in the current conditions of technological progress and the increased factors endangering a person's life. Manslaughter of a person leads to consequences for both the society and the victim's family, which is why the criminal law must intervene, sanction and to fight against this attitude of ease or negligence in traffic, resulting in the death of a person.
Keywords: road accident, criminal prosecution, body, suspect/ defendant, victim, criminal record.

Abstract (ro): Accidentele rutiere pot fi definite ca fiind acele efecte ale încălcării legislației privind circulația pe drumurile publice în cadrul cărora, ființa umană are rol dublu, întrucât este atât cea care le produce, cît şi cea care are de suferit de pe urma lor. Conform situațiilor statistice, se observă o creştere impresionantă a numărului accidentelor rutiere produse în România soldate atât cu pierderi de vieți omenești, vătămări corporale sau doar pagube materiale , iar un aport important în acest aspect îl reprezintă ritmul alert al vieții moderne care conduce la necesitatea unei circulații tot mai intense şi rapide. Dreptul la viață pe care legea îl garantează fiecarei persoane implică ocrotirea penală a vieții şi împotriva faptelor săvârşite din culpă, întrucât, deşi sunt mai puțin grave comparativ cu cele săvârşite cu intenție, în esență produc același rezultat, respectiv moartea unei persoane.Incriminarea infracțiunii de ucidere din culpă a fost determinată de necesitatea ocrotirii vieții persoanei împotriva unor acțiuni sau inacțiuni prin care conducătorul unui autovehicul nu manifestă prudența şi atenția necesare în vederea evitării morții uneia sau mai multor persoane, în calitate de participanți ai traficului rutier.O asemenea concentrare a atenției şi a prudenței manifestată față de cei din jur este din ce în ce mai necesară în condițiile moderne ale progresului tehnic şi a sporirii factorilor care pun în primejdie viața persoanei.Uciderea din culpă a unei persoane conduce la producerea de consecințe atât pentru societate, cât şi pentru familia victimei, motiv pentru care legea penală trebuie să intervină, să sancționeze şi să combată această atitudine de uşurință sau neglijență manifestată în traficul rutier, care are ca urmare decesul unei persoane.
Cuvinte-cheie: accident rutier, organ de urmarire penala, suspect/inculpate, victim, dosar penal

I. INTRODUCERE

Dreptul la viață reprezintă dreptul fundamental al omului, în absența căruia celelalte drepturi nu şi-ar mai avea sensul. Datorită importanței sale, reuşeşte să depăşească sfera interesului personal, având astfel relevanță pentru întreaga societate. Protejarea dreptului la viață prin legi interne şi internaționale reprezintă atât o obligație, cât şi o necesitate, statul fiind cel care deține instrumentele prin care poate asigura protecția efectivă a dreptului la viață.Obligațiile statului implică nu numai adoptarea unei legislații în materie, dar şi luarea măsurilor necesare pentru ocrotirea vieții.