Originalan naučni rad
UDK 343.3/.8:004.738.5
Primljeno: 22.05.2015
Odobreno: 18.06.2015.

Mina Zirojević,
Institute of Comparative Law, Belgrade[1]

COMPUTER RELATED CRIME – OFFENCES AGAINST THE CONFIDENTIALITY, INTEGRITY, AND AVAILABILITY OF COMPUTER DATA AND SYSTEMS [2]

Abstract

The significance of information and communication technologies has created the need to establish worldwide measures and mechanisms for the protection of society and the individual against abuses in this area, through adopting appropriate legislative solutions and improving international cooperation. The result of these efforts, among other things, the adoption of Council of Europe Convention on Cybercrime , which has established minimum standards that are necessary, in the opinion of the international community to meet the national legislation in order to effectively combat the abuse of high technology.

Key words: Internet, abuse, Conventions, computer data, technology.

GENERAL LEGAL DEVELOPMENT

The significance of information and communication technologies has created the need to establish worldwide measures and mechanisms for the protection of society and the individual against abuses in this area, through adopting appropriate legislative solutions and improving international cooperation. The result of these efforts, among other things, the adoption of Council of Europe Convention

1 E–mail: mina.zirojevic@gmail.com.

2 The work is part of scientific research and engagement of researchers on the project "Serbian and European law – comparison and harmonization". Project number 179033 funded by the Ministry of Science and Technological Development and implemented by the Institute for Comparative Law in the period 2011-2014.

on Cybercrime[3], which has established minimum standards that are necessary, in the opinion of the international community to meet the national legislation in order to effectively combat the abuse of high technology. Criminal-law solutions in this field in Serbia can be classified into two groups. The first group makes a substantive provision which stipulates that actions are socially unacceptable behaviour that violate or infringe certain protective structures. It's Criminal Code[4]. The provisions of this legal text were analysed primarily in the part relating to offenses against the security of computer data, as well as to crimes that are under the provisions of the Convention on Cybercrime grouped with computer offenses and which, by their nature they are, although they in the Criminal Code are grouped into chapters that protect business operations, sexual freedom, copyright, intellectual property and others. The second group consists of the Criminal Procedure Code[5] and the Law on Electronic Communications[6] (as well as certain by-laws) that establish a procedural framework, but the framework provided by the Convention and without procedural nature, which have provided mechanisms and powers of state agencies in the detection procedures, evidence collection, criminal prosecution and trial of offenders cybercrime.

Significant concerns in this segment was created on the issue of the organization of the judicial system of the state towards creating conditions for successful combat and combat new forms of criminal activity. Specifically, whether to opt for a comprehensive systemic change, or change a number of regulations in order to create an adequate legal framework, or be oriented towards a partial amendment of certain legal provisions in order to create conditions for the timely and adequate response to new forms of criminal behaviour, that is the question each state has solved or is dealing in accordance with their capacities. The first method is without a doubt very effective, but also very demanding, since it requires a high degree of political and social consciousness of the necessity of changes that should be followed, while the second method is more economical and less demanding method, as it does not impinge on the basis of the system, but who can leave behind a series of unresolved issues such as the question of jurisdiction for certain crimes, the collision of new and existing legislation, and so on. In accordance with the

3Convention on Cybercrime, Council of Europe, Budapest, 23. XI 2001.; European Treaty Series(ETS) - No. 185 <http://conventions.coe.int/Treaty/en/Treaties/Word/185.doc>(August 5, 2010)

4 "Official gazette of RS", nr. 85/2005, 88/2005 - change, 107/2005 - change, 72/2009, 111/2009 i 121/2012

5"Official gazette of RS ", nr. 72/2011, 101/2011, 121/2012, 32/2013 i 45/2013

6" Official gazette of RS ", nr. 44/2010, 60/2013 – Constitutional Court Decision and 62/2014

resources available, Serbia, with the aim of criminal law protection of new forms of computer crime, opted for a different way of organizing its judicial system, oriented for partial changes of certain legal provisions and the adoption of new laws, establishing new state authorities for procedure in criminal cases in this area.

In order to complete the analysis of criminal-law provisions in Serbia at the beginning will be presented to Council of Europe Convention on Cybercrime and its Additional Protocol, and then the substantive and procedural provisions of legal solutions in the field of ICT abuse.

Offences against the Confidentiality, Integrity, and Availability of Computer Data and Systems

This group of offenses is a direct result of the implementation of the Convention on Cybercrime – CETS 185. Prescribing criminal act under title: Unlawful acts with the data (displacement and disruption of data and system interference)[7] on the computer, the CETS 185 provides it in terms of intentional partial or total damage, deletion, destruction, changes content, or compression[8] of the original data(art. 4). This act may at first glance look like an illegal approach, but must be understood primarily as a complement to him: illegal access to (in order to modify the data) to the commission of the offense. The procedures described in Part illegal access, such as "Trojan horses" and "logic bombs," as the ultimate goal have unauthorized treatment of data on your computer, which includes sending them to the author of the malware or a third party - purchaser (for further abuse, the most common to create zombie computers even, networks of the same). It should be noted that this does not incriminate damage and deletion of data, such as, for example, virus damage, but to the traditional forms of manipulation are added acts that lead to similar consequences. An example is the provision of data - if the virus randomly changes the contents of the document the damage can be compared to deleting files.

The act of data changes is linked to intrusion into a computer network or system, which is defined as the intentional, serious and unauthorized manipulation of computer system input, transmission, damaging, deleting, destroying, changing or compressing computer data. The act incriminates blanket provision, citing a series of actions, covering every situation that implies disabling operation or modification of computer systems or networks. It is understood that in this act is included

7This criminal act is covered in Serbian law system by art. 298, 299, 301, 302, CC of RS.

8In Internet related identity theft, A discussion paper, Prepared by Marco Gercke, www.coe.int/cybercrime it is determined as act which negatively influences on accessibility of data to wider circle of people who have access to media on which it was stored.

the physical server shutdown, as well as DoS (Denial of Service attack, this refers to a corresponding computer network for illegal intrusion into its data) and virus. The intent is necessary and must be included unauthorized computer network or system to make this act existing. In the case of this act perpetrators in order to increase the amplification consequences are increasingly applying botnets, large groups of infected zombie computers that have had a strong attack on the computer.

CETS 185 prescribes Illegal access (hacking) (Art. 2) information contained in a computer or computer system, in order to seize the information, change it or destroy[9]. For this Act, therefore, is needed intention, so that the signatory states can have the option to criminalize only the specific actions that lead to illegal access to a computer or network. A typical example of such work is the insertion of "Trojans" into someone's computer.

Illegal access without authority, often, is the first act of a combination of actions (as elements of complex crimes), for example, phishing[10] or identity theft. The Convention does not incriminate the method in which this act will be realized, but remains neutral in terms of technology used, and the basic requirement is premeditation and unauthorised access.

Specific crimes, prescribed by the statutory criminal law, are primarily those relating to the security of computer data. The Criminal Code prescribed those in Chapter XXVII (Articles 298-304a).

I THE CRIMINAL CODE

1. Etymological aspect

According to the Criminal Code provisions relating to the field of computer crime are contained primarily in the general part of the Code, in Article 112, in the part relating to the meaning of the term in the sense of criminal law. In this manner is prescribed by law what is considered to be a computer, computer data, computer network, computer program, computer viruses and computer system. So, the computer represents every electronic device on the basis of automatic processing and data exchange (paragraph 33, Article 112 of the Criminal Code). Computer data is any representation of facts, information or concepts in a form suitable for processing in a computer system, including an appropriate program based on which

9More criminal acts cover this in CC RS: article 298, article 299. article 300.

10 Definition can be found at: http://www.coe.int/t/dghl/cooperation/lisbonnetwork/meetings/Bureau/TrainingManualJudges_ en.pdf.

computer system performs its function (paragraph 17, Article 112 of the Criminal Code). As a computer network is considered to be a collection of interconnected computers or computer systems that communicate by exchanging data (paragraph 18, Article 112 of the Criminal Code). Computer program shall be considered a furnished set of commands that are used to manage the operations of the computer, as well as to solve a specific task using a computer (paragraph 19, Article 112 of the Criminal Code). A computer virus is a computer program or other set of commands entered in a computer or computer network which is made of replicating itself and is working on other programs or data to a computer or computer network by the addition of a program or a set of commands to one or more computer programs and data (paragraph 20, Article 112 of the Criminal Code). The computer system is any device or a group of interconnected or dependent devices of which one or more of them, according to a program, performs automatic processing of data (§ 34, Article 112 of the Criminal Code). This represents part of the definition of certain terms used in the Criminal Code and their significance in terms of the provisions of the Code, which are related to the field of computer crime.

2. Damage to computer data and programs (Article 298 Criminal Code)

This criminal offense has the basic two serious forms. The basic form consists in the unauthorized deletion, modification, damage, concealment, or otherwise suppression of computer data or programs. The act therefore can only be done in relation to computer data or programs, and with more alternative activities planned, with the aim of fully or partially disabling the use of computer data or programs. For this offense is punishable by a fine or imprisonment up to one year. The first serious form of this act if there is an action taken which has caused damage in excess of four hundred and fifty thousand dinars. Amount of damage caused represent the qualifying circumstances for which is prescribed a punishment of imprisonment of three months to three years. The most severe form of the offense for which is prescribed a punishment of imprisonment of three months to five years, if there is an action taken which has caused damage in excess of one million five hundred thousand dinars. Tools used in commiting this offense shall be confiscated if they are in the property of the offender. The intention of the legislator was that by the prescribing of this crime protect the integrity of these components in computer technology against unauthorized operation.

As can be seen, the offense can be done alternatively in several ways: 1) by deleting, or 2) changing, so that a computer program or data is completely destroyed or changed to become useless to continue the execution of intended function, or 3 .)

damaging, by which program or data are partially destroyed and reduced its use value, or 4) concealing, when it comes to concealing of a computer program or data, and the act can be done in any other way that makes the program unusable for its purpose[11]. It is important to understand that under other modes of making it unusable of means and making unavailable, so in this way incriminate cases the functioning of various backdoor or trojan programs which are specific programs on the computer disguise, as preparatory work for, say, computer extortion.

The implication of this act is to make useless programs or data. The act is done by taking any of these actions to the achievement of prescribed outcomes. If more action is taken towards an object, or a computer program or data, it will be realized only one offense. The perpetrator of this section may be any person, in respect of culpability required intent. For proper qualification of the criminal offense, it is necessary to determine whether the perpetrator acted without authorization, the exact time and place of the offense, the manner in which the offense was committed - whether in terms of physical access to the computer program or data, or the offense is committed within the computer network internally or via the Internet, and, if made by another computer, with the help of the programs, as well as the consequences that have occurred, or if the object of criminal act has been made unusable. It is necessary to identify and attribute the offender, or whether it is official or responsible person within a legal person, or a person who was on the basis of a law regulated relations in power to any set way manipulate a computer program or data, to update or change it.

For proper qualification work it is necessary to establish several important facts. First of all, it is necessary to determine the real offender, or whether the perpetrator acted without authorization or been authorized to take certain action, then the exact time and place of commission of the offense, the manner in which the offense was committed (internal or external attack) and within that to whether the offender used certain equipment (and which) during the commission of the offense, the nature and severity of consequence, and so on.

The most common form of execution of this act is the demolition of websites, which is an everyday activity of hacker groups. According to the unwritten rules of hacking, the object of attack is only part of the site, usually the title page, which is being changed so that it leaves the hacker group signature, message or greeting, but in addition to blocking accesses other site content. From this kind of attacks from are not protected sites of educational institutions, Ministries, Parliament,

11Lazarević, Lj.: „Komentar Krivičnog zakonika Republike Srbije“, Savremena administracija, Beograd, 2006, p. 745

Serbian Orthodox Church, etc.. Attacks on websites are taking place continuously, but to the public eye come only those attacks that were successful.

3. Computer sabotage (Article 299 Criminal Code)

The offense does a person who enters, destroys, deletes, modifies, damages, conceals or otherwise renders unusable computer data or program or destroys or damages a computer or other device for electronic processing and transmission of data with the intent to prevent or significantly hinders the process of electronic and data that are important for public authorities, public services, institutions, companies or other entities. From the legal definition can be seen that there are two objects of attack. First, it's a computer program or data, while the second object of the attack is a computer or other device for electronic processing and transmission of data. By performing this crime are damaged state agencies, public authorities, institutions, companies and other entities, and law prescribes a prison sentence of six months to five years.

With regard to the prescribing of this offense protects computer technology intended for electronic processing and transmission of data that are important for public authorities, public services, institutions, companies or other entities that crime will not exist if it was made towards the computers that are not relevant to these subjects. It is important to distinguish this act from the previously explained criminal offense Damage to computer data and programs. Although the actions of these two acts are very similar, there are a number of specific features that must be observed when qualifying offense in particular, with of course a far greater consequences in the case of the crime of computer sabotage.

The perpetrator of this section may be any person, in respect of culpability required intent. The main feature of the act is the intention of the offender by taking actions that prevent or hinder the electronic processing and transmission of data relating to the aforementioned. It is important to determine whether it caused the damage - the destruction of or damage to computer data or programs, by taking some of the alleged actions and the consequences if not performed, it is necessary to identify all the foregoing for the purpose of later prosecution, given that it is possible that the consequences manifest and later in the work of these devices.

As with previous criminal offenses, for the proper qualification of this act is necessary to establish several important facts: the attributes of the offender, then the exact time and place of commission of the offense, the manner in which the offense was committed (internal or external attack) and in part on whether the offender

used certain equipment (and which one) during the execution of the work, the type and severity of the consequences, and so on.

4. Creating and inserting computer viruses (Article 300 CC)

The offense has a basic and a more severe form. The basic form does a person who makes a computer virus with intention of inserting it into someone else's computer or computer network. The act is done therefore torque making this virus with the intent to be inserted in someone else's computer or computer system, regardless of whether such intention was realized in this case. In this sense, the question is whether it is necessary to provide a source code or it can be taken as a basis on which to create new forms of viruses with modifications that may be made by any person. We think that it is already by creating a base, which in itself is not malicious it has provided opportunity for further work towards the creation of the virus, given that on the Internet there are a lot of DIY videos. This provides both a means and an opportunity for the exercise of this act. For this form there is prescribed a fine or imprisonment up to six months. A severe form of the work does a person who enters a computer virus into someone else's computer or computer network, thereby causing damage. For this type of legislator foresaw a fine or imprisonment up to two years. A device and a means to make the forms of this offense shall be seized.

Criminal Code in Article 112, paragraph 20 defines the meaning of the term computer virus. There were several reports against unknown perpetrators due to insertion of the virus, and police and prosecutors are working to discover their identity. In comparative practice so far has been more action against persons who have created and spread computer viruses. Thus, in 2005 in the German city of Verdun eighteen year old hacker was sentenced to a suspended term of imprisonment of 21 months, because he wrote and left the network Sasser worm, which in 2004 for only a week of existence has infected nearly 20 million computers around the world.

The fact that the case law in relation to this offense does not exist in any case does not mean that this type of activity does not exist on the territory of Serbia. On the contrary, it becomes clear that in this area there is a dark figure committed criminal acts, which directly indicates insufficiently developed awareness of the general public as well as scientists and experts in this field.

5. Computer Related Forgery (Article 301 CC)

Computer forgery provided by CETS 185 applies only to intentional, unauthorized insertion, modification, deletion or hiding of computer data, which as a result has change of the data content, regardless of whether they are on the way to get a different purpose and meaning, or become unusable, and with the intention that such data could be later used as the authentic in legal traffic. States are given the option to provide for a special type of intent to commit fraud in order to have this crime.

The subject of computer counterfeiting, as the object of attack, are only data and the Convention requires that, in terms of intentional part (*Mens rea*) of offenses where data elements are concerned, include two categories of documents: public and private documents. Forgery is defined as the intentional, unauthorized insertion, deletion, alteration, or concealment of computer data, as well as any other interference with the operation of a computer system, in order to obtain an unlawful material benefit for himself or a third person.

In the criminal law of the Republic of Serbia Article 301 is titled computer fraud. The act has a basic, two serious and one particular form. The basic form of the act does a person enters incorrect data, omissions entering correct data or otherwise conceals or falsely presents information and thus affect the result of electronic processing and transmission of data in order to obtain for him(her)self or another person unlawful material gain for the second time and causes property damage. The offense is done at the time the enforcement action was taken with the intent to obtain for him(her)self or another unlawful material gain or to cause another kind of property damage. For the basic form of act law has prescribed fine or imprisonment up to three years. There are two serious forms of act, depending on the amount of the illegal gain. The first serious form exists when there is an acquisition of a property in the amount of four hundred fifty thousand dinars, and it is punishable by imprisonment of one to eight years. Another serious form exists when there is a material gain exceeding one million five hundred thousand, and it is punishable by imprisonment of two to ten years. A special privileged form of this criminal act exists there when the action execution take only the intention to damage the other person. For this form law says that it is punishable by a fine or imprisonment up to six months.

The offense of computer fraud should be distinguished from criminal charges of fraud (Article 208 of the Criminal Code) and insurance fraud (Article 208a CC both belong to the group of offenses against property Title XXI of the Criminal Code). These two types of fraud can be performed using computer technology,

provided that in such circumstances, both offenses are fundamentally different from computer fraud. So, Fraud does a person with intent to obtain for himself or another unlawful material benefit brought by false representation or concealment of facts in a misleading or maintain other person in error and thereby instigate to to do or not do something that could damage his or her or someone else's property, while insurance fraud does the person who with intent to obtain for himself or another unlawful material benefit brought by false representation or concealment of facts, opinions and giving false statements, submitting a false judgment, submitting false documents or otherwise mislead or maintain in error somebody in connection with insurance and thus it instigate this person to do or not do something to detriment of his (or her) own or someone else's property.

The intention of the legislator was that prescribing a criminal offense Computer fraud protects the credibility and integrity of the data being electronically processed or transmitted electronically. It is necessary to determine in each particular case and the intent of the perpetrator, which consists in the fact that, for him (her) or for other illicit material benefit, and thereby cause other property damage.

Since the action of the offense is defined alternatively as entering incorrect data or omission in entering correct data or any other concealment or misrepresentation of data, offense is done when taken some of mentioned actions, with the existence of the described intentions and when there has been caused property damage, where it is not necessary due to the actions taken to have illegally obtained gains. This offense may be committed premeditated by any person who undertakes legally prescribed action.

For proper qualification of the crime and its successful proving it is necessary to determine the time and place of the offense, the exact action that was taken, and the manner in which incorrect data is entered. About the entered data it is necessary to determine their untruthfulness, what is the falsity in real and how did it influence to the result of electronic processing and transmission of data, then if it is a failure of accurate input data[12], how it is omitted, or in any other way is concealed or falsely displayed data, and to influence the result of the processing and transmission. It is necessary to determine and whether the data entered via physical access to the device eligible for transfer or electronic data processing or is it done through a network, what is the amount of material gain to be included in the intent of the perpetrator and then, what is the amount of damage. To prove

12In that case criminal act is done through omissive action and that omission has to be in course of omission of impute for such important data, or data which can cause some negative result for electronic procession of data.

the offenses referred to in paragraph 4, it is necessary to determine the type of damage that was included in the intention, whether such damages has occurred, it is necessary to determine the means by which the crime was committed and, if possible, make their seizure.

In recent years, electronic commerce becomes the dominant way of doing business in Serbia. The business segment transactions are carried out electronically and that opens up many possibilities for abuses by which may be affected all economic actors if there isn't effective protection of the integrity and authenticity of electronic data during their processing.

In previous domestic case law, there were several cases of prosecution of perpetrators of this crime, and the examples given show that computer fraud is becoming increasingly common crime. Thus, the Office of Cyber Crime launched an investigation against the suspect T. A for reasonable suspicion that during 2007 and 2008 on two occasions he was through using computer systems entered into bank systems in Australia and Switzerland, and issued false orders for the transfer of funds, which were in the amount of 51,990 CHF, and tried from a Swiss bank without authorization to transfer funds in the amount of 19,000 USD.

Since Serbia has a large number of sports betting, which have a wide network of branches and whose business is inconceivable without computer networks often it is the abuse of such systems. Perpetrators are in different ways trying to influence the outcome of the electronic data processing and using given software solutions, forge played ticket.

6. Unauthorized access to a protected computer, computer network and electronic data processing (Article 302 of the Criminal Code)

Through the act of unlawful interception of communications, the Convention FTC is trying to leverage the treatment of electronic communication with telephone communications and, in this way, introduces criminalization of electronic communications interception. Issue at stake is the unauthorized interception of personal data (Convention speaks of non-public) transmitted between two computer systems, data communications, in content, but also on traffic[13], including electromagnetic emissions from a computer that carries this information (article 3). Public data transmission and other ways of obtaining such data are absent from these charges. The non-public communication according to the explanatory report

13http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-toolkit-cybercrime-legislation.pdf p.16. last accessed on 01.06.2010.

on the Convention[14] includes those situations where the nature of the process of transmission is confidential. Private individual communication (such as sending and receiving e-mail or download from Internet sites) can generally be considered non-public. The Convention gives countries the option thus to define criminal act with obligatory requirements of an intention. As in the previous case, this fact is important primarily because of the possibility that someone without their knowledge, or at least without any intention, came into the possession of someone else's data on a computer network. The objective is to protect the integrity of non-public communication.

It is important to note that the application of this work is very limited because the criminalization is focused on intercepting the transfer process, and thus can not be extended to the moment when the person who intercepts transfer the same data stores on some kind of medium. Incriminated is only the process of interception of data transmission and not preservation. Example for interception give us "key loggers" and " screen loggers". A special problem exists in cases where the interception of data is not performed by technical means - because this work can be defined as any form of obtaining data in the process of transfer, but article 3. does not cover acts of social engineering, and, therefore, this act can not be when accomplished counted as criminal act covered by art. 3.

The criminal act has a basic and two serious forms. The basic form does person who in violation of the protection measures, unauthorized breaks into computer or computer network, or establishes unauthorized access to electronic data processing. The plot of this act is commited without authorization, in violation of planned security measures. For this form is punishable by a fine or imprisonment up to six months. The first severe form, which is punishable by a fine or imprisonment up to two years, does the person who records or uses data obtained in the through commitment of basic form. The most severe form of act exists if due to actions taken while committing basic form is caused an impasse or serious disruption of electronic processing functioning and transmission of data, or network or other serious consequences have occurred. For this form of offense perpetrators are punishable by imprisonment of up to three years.

Through prescribing of this offense shall be protected computers, computer networks and data to be processed electronically.

The criminal act (*actusreus*) of this crime consists in the unauthorized accessing into computer/computer network or unauthorized access to electronic data

14Explanatory report nr.60.

processing or use of data obtained in these ways. This offense may be committed by any person who possesses specific expertise, given that it is a protective barrier to overcome before the accessing to a computer or computer network. The perpetrator of the criminal act undertakes act of commiting with the intent, which covers unauthorized accessing a computer or computer network, using data obtained in the above manner and the possible occurrence of consequences set out in paragraph 3 of Article 302 of the Criminal Code.

The perpetrator of the offense referred to in paragraph 2, may be the person who committed the offense specified in paragraph 1, but it could be any other person who has come into possession of data. If an individual has taken the actions specified in paragraphs. 1 and 2, then there is criminal liability of such person only to paragraph 2, considering that the action referred to in paragraph 1 are only preparatory work. Perpetrator of the act referred to in paragraph 1 may only be a person who is not authorized to engage in computer or electronic data processing approaches.

In order to properly qualify a criminal offense, it is necessary to determine the time and place of the offense; authority of the perpetrator, if it comes to offense from paragraph 1 .; the way they overcome barriers, as well as the way in which access to a computer or computer network; then, for what purposes the data were collected, and in particular, what constitutes the most serious consequences, if it is performed (if it has stopped or serious disruption of functioning electronic processing and transmission of data, or network or other serious consequences).

Object of protection of this crime are protected computer or computer network or data that are processed electronically. The consequence of the offense is the unauthorized intrusion or access to, or use of the data thus obtained. It is necessary that the perpetrator with no awareness that unauthorized uses – involves a breach in computer security measures, or unauthorized access to EOP. If the owner specifically protect this connection, each device and program used to make this kind of connection by the person who controls it is assumed that it participates in the commission of the offense. If we do not secure access to it (computer or a network) a consequence of the offense exists, then it is a criminal act prescribed in art. 304 of the Criminal Code of RS. (or is it subject only to private suits).

In each case it is necessary to accurately determine what measures of protection are violated and how, which is the important feature of this offense. A separate issue is the question of obtaining information (user names and codes) for the execution of this crime, as well as their re-sell and offer for sale. These acts are not

criminalized as a separate criminal offense, and may represent a specific form of identity theft. It can be subject of article 225 of CC. Special attention must turn to the determination of the existence and consequences of its weight because of it depends on the qualification of the work.

Criminal offense of unauthorized access to a protected computer, computer network and electronic data processing may be similar criminal offense Espionage (Article 315 CC, Chapter XXVIII - Criminal acts against the constitutional order and security of the Republic of Serbia), if the perpetrator breaking into computer systems came to secret military , economic or official information or documents. Secret are those military, economic or official information or documents which by law, regulation or other decision of the competent authority based on the law declared to be secret, and whose disclosure would cause or might cause adverse effects to the security, defence or for political, military or economic interests of the country (paragraph 6, Article 315 of the Criminal Code). Therefore, it is important in each case to determine the intention of the offender, the importance of the attacked computers/computer networks, especially the type of data in relation to the collection of which there is no intent of the perpetrator.

7. Preventing and limiting public access to the computer network (Article 303 of the Criminal Code)

The act has a base and a more severe form. The basic form of the work for which is punishable by a fine or imprisonment up to one year, does a person who makes an unauthorized preventing or hinders access to a public computer network. If the same act is committed by an official in the discharge of his duty, it is a more severe offense for which a punishment of imprisonment could be of up to three years. In the second case, it is actually a special form of the offense of abuse of powers by public officials which prevents or interferes with another individual or legal entity unimpeded access and use the public computer network.

Criminal Code in Article 112, paragraph 18 defines the meaning of the term computer network. The legislature prescribing this part of protecting public computer network accessible to all persons, and that citizen's use every day as part of various business and private activities.

This offense may be committed by any person who undertakes enforcement action which was premeditated. The condition is that the perpetrator must act without authorization, because crime does not exist unless there is a legal basis for preventing a person to access a public computer network.

The plot of the offense is determined alternatively, respectively, the offense will be taken if any activity that prevents (completely disable) or hinders (confuses) access to a public computer network, or if the above activities are carried out by public officials.

In order to properly qualify a criminal offense, it is necessary to establish a network feature (if it comes to a public computer network, available for everyone to access or not); whether the offender acted without authorization, or is the prevention/obstruction of access to a public computer network carried out on some kind of legal basis; time and place of the offense, and so on.

To prove the criminal offense referred to in paragraph 2, it is necessary to establish status of a certain public official of the perpetrator and the committed action. In practice, it is necessary to pay attention to whether the alleged offense was committed in the function of some other offense or is accompanied by even an act which by its elements of a being of another criminal offense, in which case we can have question of their mutual relations and connections.

One of the most common ways to prevent or restrict access to a public computer network is the DoS attack and its specific manifestations called DDoS (Distributed DoS). To this type of attack are exposed all the information systems in the world, with respect to the above program performs detection of unprotected or inadequately protected computer, so there is no space of our country which has been spared the adverse effects of this form of cybercrime. A particularly dangerous type represents PDOS attacks (Permanent denial of service) that can permanently damage the hardware on servers with remote access. The attack is based on the use of "firmware system update" that server sends over a network or the Internet, and who is able to trick the hardware and flash any part of the system, which could lead to permanent and complete hardware fails.

During 2008, in Serbia were moreDDoS attacks. We will single out examples of attacks on the websites of the Serbian Orthodox Church, which is considered one of the fiercest attacks ever rendered, as well as knockdown of Internet presentations radio show "Hourglass".

DoS and DDoS attacks are very dangerous and usually lead to serious financial losses for companies, institutions or agencies whose system were attacked. It is true that the identity of the perpetrators is almost impossible to establish, since the attacks carried out with infected computers that are connected to the botnet networks, whose owners in most cases and are unaware of what is going on with their computer, especially since attackers still changing and faking IP addresses

from which attacks suggest. We are aware that in the territory of Serbia there is a vast number of undetected cases in relation to those registered and that the cyber space in the domain of every state, including Serbia is exposed to this type of attack. All of this should be an additional incentive for further investment of resources and efforts to mitigate the effects of the consequences that may occur.

8. Unauthorized use of a computer or computer network (Article 304 of the Criminal Code)

CETS 185 provides for the criminalization of the misuse of the device. The severity of the occurrence of various high-tech devices that allow the realization of abuses by diverse users of this kind of technology devices becomes subject to these charges. Performing various offenses which carry very vicious and insidious ways of inflicting the consequences to victims or to damage persons as a mandatory part of offenses is facilitated through such devices. Here lies the *ratio* for incriminating of this criminal offense. States - Parties are undertaking obligation (article 6 of Convention) to punish any intentional illegal manufacture, sale, possession, lending, obtaining, distribution and any other way of making available to unauthorized persons any "device", this includes computer programs (designed or adapted primarily for the purpose of committing any offenses referred to in Art. 2 of the Convention), computer passwords, access codes, and any other similar form of data with by which is possible to do the offenses set forth in Articles of the Convention (2-5).

Thus defined problems in the Convention are very cleverly packaged as a combination of constraints on the devices, which as the main purpose have execution of criminal act, with the combination of the mental element of "the existence of intent to use the same for the commission of acts referred to in article 2-5 of the Convention."

The criminal act does an unauthorized person who uses a computer or computer network with intent to obtain for him (her) self or another unlawful material gain. This criminal offense is specific in that it is the prosecution of the offender is initiated by private citizens, and the law prescribes it punishable by a fine or imprisonment of up to three months.

The perpetrator of this crime can be any person who acts with direct intent. The plot of the offense consists in the unauthorized use of a computer or computer network, where the intent of the perpetrator is aimed at obtaining (for him/her or another) illegal profit.

However, in the case of this criminal act authorized officers are required to take actions within its jurisdiction and to gather the necessary evidence, if there are grounds to suspect that, in connection with the acts that fall into this crime was committed with (or as a part of) any other criminal offense for which prosecution is done *ex officio*, in which case are applied the powers and provisions relating to the filing of criminal charges.

To the commission of offenses in this area benefits the fact that awareness of the dangers that can come from the Internet still isn't sufficiently developed. Citizens often leave detailed personal information or data related to the business segment on various Internet sites, unaware of the possibilities that these data may become subject to abuse at any time. Number of crimes like this is growing daily[15]. As for the detection and prosecution of these crimes and their perpetrators, there is a big dark figure, which tells us that a very small percentage of the criminal acts are discovered and understood.

9. Producing, obtaining or providing to the other means to commit offenses against the security of computer data (Article 304 CC)

The criminal act is done by a person who possesses, purchases, sells or gives to another the computers, computer systems, computer data and programs for execution of all previously analysed offenses from the Chapter XVII of the Criminal Code. Items that are used for this act are subtracted, and the offenses are punishable by imprisonment of six months to three years. It also stipulates that the prosecution of this act is undertaken by a private complaint.

Offender can be any person acting wilfully with intent to supply, sell or give to other for use computers, computer systems, computer data and programs in order to commit offenses against the security of computer data. If it comes to creating of these elements of information systems, we can see that it is necessary that a particular person as perpetrator possesses professional knowledge and thereby act with the intent to commit the crimes alleged.

The plot of the offense is determined alternatively, that person may: 1) possess or 2) manufacture or 3) obtain or 4) sell or 5) to give to the other for use computers,

15 Compare with the results published in Žarković, M. Drakulić, M. Miladinović, S. Urošević, V. Batrićević, A, Lukić V. Ivanović, Z. Drakulić, R. Jovanović, S. Janković, Đurašković, M. Stojičić, S. Milanović, L. Veze *Cyber* kriminala sa iregularnom migracijom i trgovinomljudima, (there is a English version of this book and two cd of bilingual character) Ministarstvo unutrašnjih poslova, Urednik Vladimir Urošević, 2014.

computer systems, computer data and programs to commit criminal acts from Chapter XVII of the CC. From of the this crime qualifications we can infer that it shows that only the possession, production, supplying, selling or giving to another, is in itself a criminal offense, regardless of whether there was a crime against the security of computer data. In this segment, it is important that there is an intention to commit the alleged crimes. In line with this, it is particularly important to determine the intent of the perpetrator of the crime, as well as his status and the circumstances under which he acted, then the type and content of computer data, programs and systems, the reasons for their possession (especially if they are harmful), the time and circumstances of making , acquisition, sale or delivery of the second and other essential information needed to determine the motives of actions and whether in this case there was any commitment the crime, and the criminal liability of the offender. Items that are used for this act must be seized.

CONCLUSION

Significant concerns in this segment was created on the issue of the organization of the judicial system of the state towards creating conditions for successful combat and combat new forms of criminal activity. Specifically, whether to opt for a comprehensive systemic change, or change a number of regulations in order to create an adequate legal framework, or be oriented towards a partial amendment of certain legal provisions in order to create conditions for the timely and adequate response to new forms of criminal behaviour, that is the question each state has solved or is dealing in accordance with their capacities. The first method is without a doubt very effective, but also very demanding, since it requires a high degree of political and social consciousness of the necessity of changes that should be followed, while the second method is more economical and less demanding method, as it does not impinge on the basis of the system, but who can leave behind a series of unresolved issues such as the question of jurisdiction for certain crimes, the collision of new and existing legislation, and so on.

References:

- “Off. Gazette of RS”, no. 85/2005, 88/2005 - corr., 107/2005 - corr., 72/2009, 111/2009 and 121/2012

- Act on Mutual Legal Assistance in Criminal Matters, “RS Official Gazette”, no. 20/2009

- Brkić, S.: „Krivičnoprocesnopravo II“, Pravnifakultet u NovomSadu, Novi Sad, 2010

- Criminal Code, “Off. Gazette of RS”, no. 85/2005, 88/2005 - corr., 107/2005 - corr., 72/2009, 111/2009 and 121/2012

- Grupa autora: „Priručnik za istragukrivičnihdela u oblastivisokotehnološkogkriminala“, SavetEvrope, 2008

- Komlen-Nikolić, L.; Gvozdenović, R.; Radulović, S.; Milosavljević, A.; Jeković, R.; Živković, V.; Živanović, S.; Reljanović, M.; Aleksić, I.: „Suzbijanjevisokotehnološkogkriminala“, Udruženjejavnihtužilaca i zamenikajavnihtužilacaSrbije, Beograd, 2010

- Korać, S.: „Suzbijanjedečijepornografijenainternetu: EU standardi“, Centar za bezbednosnestudije, Godina II, Br. 11/2008, Beograd

- Law on Amendments to the Criminal Law of the Republic of Serbia, “ Off. Gazette of RS “, no. 39/2003

- Law on Organization and Jurisdiction of Government Authorities in the fight against cyber crime, “RS Official Gazette”, no. 61/05 and 104/09

- Law on Ratification of the Convention on Cybercrime, “Official Gazette”, no. 19/2009

- Lazarević, Lj.: „KomentarKrivičnogzakonikaRepublikeSrbije“, Savremenaadministracija, Beograd, 2006

- Prlja, D. i Reljanović, M.: „Pravnainformatika“, PravnifakultetUniverziteta Union, JavnopreduzećeSlužbeniglasnik, Beograd, 2010

- Prlja, D.; Reljanović, M.: „Visokotehnološkikriminal – uporednaiskustva“, Stranipravniživot, br. 3/2009, Institut za uporednopravo, Beograd

- Radulović, S.: „Specifičnostpribavljanjaelektronskihdokaza o izvršenjukrivičnihdelavisokotehnološkogkriminala“, Revija za bezbednost, br. 12/08, godina II, Centar za bezbednosnestudije, Beograd

- The Code of Criminal Procedure, “Off. Gazette of RS”, no. 72/2011, 101/2011, 121/2012, 32/2013 and 45/2013

- Urošević, V.: „Nigerijskaprevara u RepubliciSrbiji“, Bezbednost, Br. 3/2009, God. LI, Beograd

Internet:

Aćimović, B.: „ŽestokDoSnapadna pet gigantskihsajtova“, Linux.rs, <http://www.linux.rs/content/view/112/20/> (May 7, 2009);

Convention on Cybercrime, Council of Europe, Budapest, 23. XI 2001.;European Treaty Series (ETS) - No. 185 <http://conventions.coe.int/Treaty/en/Treaties/Word/185.doc> (August 5, 2010)

Council of Europe, Convention on Cybercrime, ETS No. 185 – Explanatory Report <http://www.conventions.coe.int/Treaty/en/Reports/Html/185.htm> (December 20, 2013)

„PodignutaoptužnicaprotivautoraSassera“, Mikro-PC World; <http://www.mikro.co.yu/main/index.php?q=vestiarhiva&godina=&mesec=&ID=6192> (May, 7, 2009)

„Softverskapiraterijaoštetilabudžet za 72 milionadolara“, Danas, 09.05.2008.; <http://www.danas.rs/vesti/ekonomija/softverska_piraterija_ostetila_budzet_za_72_miliona_dolara.4.html?news_id=92482> (May 10, 2009)

<http://arstechnica.com/tech-policy/news/2007/04/child-porn-case-shows-that-an-open-wifi-network-is-no-defense.ars> (May 01, 2009)

KOMPJUTERSKI KRIMINAL - DELA PROTIV POVERLJIVOSTI, INTEGRITETA I DOSTUPNOSTI KOMPJUTERSKIH PODATAKA I SISTEMA

Apstrakt

Značaj informacionih i komunikacionih tehnologija je stvorio potrebu za uspostavljanjem mera i mehanizama za zaštitu društva i pojedinca protiv zloupotreba u ovoj oblasti, kroz usvajanje odgovarajućih zakonskih rešenja i unapređenje međunarodne saradnje. Rezultat ovih napora, između ostalog jeste i usvajanje Konvencije Saveta Evrope o sajber kriminalu, koja je stvorila minimalne standarde koji su po mišljenju međunarodne zajednice neophodni i sve to u cilju usaglašavanja sa nacionalnom zakonodavstvom, kako bi se omogućila efikasna borba protiv zloupotrebe visokih tehnologija.

Ključne reči: Internet, zloupotreba, konvencije, računarski podaci, tehnologija.