ТМ	**Г. XXXVIII**	**Бр. 1**	**Стр. 417-431**	**Ниш**	**јануар - март**	**2014.**

UDK 004.738.5:343
Прегледни рад
Примљено: 15.3.2012.
Ревидирана верзија: 15. 10. 2013.
Одобрено за штампу: 18. 2. 2014.

Siniša G. Minić
University of Priština, temporarily
seated in Kosovska Mitrovica
Teacher Training Faculty
Leposavić
Žaklina Spalević
Singidunum University
Belgrade

ABUSE OF COMPUTER NETWORKS IN CYBER SPACE: THE ROLE OF FAMILY IN THE MODERN INFORMATION AGE[*]

Abstract

The Internet introduced a global change in the methods and speed of communication, exerting significant influence on the quality of life of a "common individual". This influence can be observed in all spheres of social life in our environment. Nevertheless, positive and constructive achievements of modern information technology also caused a series of problems related to the emergence and expansion of diverse forms of computer crime. This is a relatively new form of criminal behavior that exhibits major phenomenological diversity and that cannot be defined by a single definition. Even though certain definitions have been adopted, the phenomenon of cyber crime has appeared as a much broader concept. There are numerous documents that classify various forms of cyber crime. The fact is that uncontrolled and aimless use of the Internet implies numerous dangers. Internet abuse is often associated with pornography, which implies that various websites with illegal content also influence the long-term "poisoning" of children. Despite the primary and essential role of the parents, the support of all social segments is necessary in order to raise collective awareness through media and educational campaigns dedicated to youth and children, all for the purpose of providing information about potential Internet abuses and methods of safe usage.

Key words: Computer Networks, Cyber Space, Cyber Crime, Internet Abuse, Internet Pedophilia

sinisa.minic@pr.ac.rs

[*] This paper was supported by the Ministry of Education, Science and Technological Development of the Republic of Serbia under the project TR32023

ЗЛОУПОТРЕБА РАЧУНАРСКИХ МРЕЖА У САЈБЕР ПРОСТОРУ: УТИЦАЈ ПОРОДИЦЕ У МОДЕРНОМ ИНФОРМАТИЧКОМ ВРЕМЕНУ

Апстракт

Интернет је донео глобалне измене у начину и брзини комуникација и врши значајан утицај на „заједнички индивидуални“ квалитет живота. Овај утицај се може посматрати у свим сферама друштвеног живота у нашем окружењу. Позитивна и конструктивна достигнућа савремених информационих технологија такође је изазвала низ проблема који се односе на ширење различитих облика компјутерског криминала. Исти представља релативно нови облик криминалног понашања који показује велику феноменолошку разноврсност и не може се одредити једном дефиницијом. Иако су неке дефиниције усвојене, феномен „сајбер криминала“ се појавио као свеобухватнији појам. Постоје бројни студије које класификују различите облике сајбер криминала. Чињеница је да неконтролисана и бесциљна употреба интернета проузрокује бројне опасности. Злоупотреба интернета је често у директној вези са порнографијом, што подразумева да разни сајтови са нелегалним садржајем такође утичу на дугорочно "тровање" деце. Упркос примарној и суштинској улози родитеља, подршка свих друштвених сегмената је неопходна како би се подигла колективна свест путем медија и образовних кампања намењених младима и деци у циљу пружања информација о потенцијалним интернет-злоупотребама и методама безбедног коришћења истог.

Кључне речи: Рачунарске мреже, сајбер простор, сајбер криминал,
злоупотреба интернета, интернет педофилија

INTRODUCTION

The Internet caused a global change in methods and speed of communication in the end of the 20th century. During its two decades of existence, for a very brief period, it exerted a major influence on the life of a *common individual*.

The answer to a widespread preoccupation of youth with online social networks (*Facebook*, *Twitter*, *or chatting in general*) has been sought by sociologists, psychologists, pedagogues, and many other experts, but their views vary. On the one hand, it is evident that new technologies introduce various benefits and challenges that should be answered by creative intelligence, but on the other hand, the Internet carries multiple risks to which young people are particularly exposed, i.e. a large percentage of youth thrilled by the Internet establish communications that do not contribute to the advancement of the humankind but rather increase the sense of disorientation and isolation leading to the disregard of reality. In this context, due to the advantages of new technologies, there is reasonable uncertainty and fear of conflicts that vulnerable individuals could find themselves in, whereby it might become impossible to distinguish the truth from fallacy, thus causing a fusion of reality and virtual reality.

In addition to these common characteristics and various contradictory views, the negative aspects of Internet use carry serious connotations. The development of science and technology concurrently enabled integrative powers on our planet and, in order to achieve a better quality of people's lives, also created favorable conditions for those who wish to take advantage of certain innovations for the purpose of criminal activities (Bjelajac, 2011, p. 34). Positive and constructive innovations of new information technology also introduced a series of problems related to the emergence and expansion of diverse forms of computer crime. The particular attribute of these torts is the method of execution, which is based on computer use (Draft Convention on Cyber crime, 2000). Thereby, computer use can be expressed in a complete or segmented manner in the incriminated acts. The computer can be, and often is, the main tool for executing such criminal acts, in case there is a punishable consequence in terms of criminal justice. The opportunities for abuse are plentiful and diverse. Computer technology creates room for specific acts of manipulation, ranging from certain traditional types of crime, such as embezzlement, fraud, or theft, to more sophisticated ones, used to obtain data without authorization for the purpose of achieving illegal benefit.

Internet pedophilia represents a specific type of computer crime, as pedophiles increasingly wander through electronic networks in search of potential victims. Unfortunately, these victims are children, the most sensitive and vulnerable members of human population. Therefore, the spread of Internet pedophilia has recently become a topic of discussion, particularly in terms of whether these acts represent organized crime, as they are rarely related to a single case. In fact, the Internet has become a new *playground* available to pedophiles, where children are constantly exposed to inappropriate sexual content or upsetting and hostile messages, which strongly influence their physical and mental development and may turn out to be decisive for their future bio-psychological status.

GENERAL FEATURES OF CYBER CRIME

Defining computer crime is rather difficult. There are several reasons to support this claim:

- It is a relatively new form of criminal behavior, which has not been fully distinguished from other types of crime;
- Computer crime demonstrates great phenomenological diversity that can hardly be covered by a single definition;

- Numerous laws designate computer torts as specific criminal acts; however, science cannot rely on positive criminal law when defining the concept of computer crime (Dimitrijevic, 2011).

In the broadest sense, high-technology or computer crime is any criminal activity performed by the use of a computer, computing systems, and networks. There is a wide and diversified range of such criminal activities, including a series of illegal actions, from unauthorized distribution of pirated copyrighted material to multi-million-dollar thefts and frauds resulting from unauthorized access to individuals' bank accounts. In addition to actions aimed at making unlawful gain, computer crime also includes actions otherwise motivated, such as development and distribution of viruses and malicious software, publication of confidential personal or business data, etc. (Drakulic & Drakulic, 2010). Nevertheless, several years have passed from the initial emergence of computer crime in anticipation of the efforts to clearly determine or define it. Regardless of the different definitions, just as certain basic definitions were being developed and stabilized, the new phenomenon of cyber crime appeared. Examining and interpreting the global range of this type of crime, in the document "Crime related to computer networks", the expert group at the 10th United Nations Congress on the Prevention of Crime and Treatment of Offenders (Vienna, Austria, 10-17 April, 2000), defined cyber crime as *any crime that can be committed by means of a computer system and network, in a computer system or networks, or against a computer system or network* (Vienna Declaration on Crime and Justice: Meeting the Challenges of the Twenty-first Century, 2000).

Information technology or computer networks may undertake several roles (Robinson, 2000), such as:

- The object of attack – the services, functions, and content of the network are being attacked.
- Means – criminals have always been using stones, knives, poison, guns, and similar weapons and tools, whereas modern criminals use computer networks to realize their intentions and commit the act.
- Environment – setting of the attack. This environment often serves to conceal criminal activity, as in the case of Internet pedophilia, as well as other criminal actions where it has been proven rather effective.
- Evidence – just as knives, weapons, or other tools are used in traditional crimes to commit criminal acts, a network may be used as evidence in the presentation of evidence of cyber crime.

Computer network also serves as a network that connects numerous subjects. In addition to its supportive role, it also represents a symbol. However, a network in cyber crime exclusively serves the function of deception, interference, and intimidation.

TYPES OF CYBER CRIME

Various documents offer different classifications of the types of cyber crime. For instance, the material for the workshop on network crime at the 10th UN Congress divides this type of crime into two subcategories:

- Cyber crime in a narrow sense – any illegal behavior directed by means of electronic operations that targets the security of computer systems and the data processed by them;
- Cyber crime in a broader sense – any illegal behavior committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession, offering or distributing information by means of a computer system or network (Vienna Declaration on Crime and Justice: Meeting the Challenges of the Twenty-first Century, 2000).

This document, in accordance with the 1989 Council of Europe Recommendation and the 1985 OECD list, presents the actual manifestations of this type of crime, including unauthorized access to a computer system or network by breaching security measures (hacking), damage to computer data or software, computer sabotage, unauthorized interception of communications to, from, or within computer systems and networks, and computer espionage. Cyber criminal offences supported by computers are being added to these manifestations. These acts mainly refer to distribution or possession of certain materials. Among them, particularly important are child pornography and various illegal materials distributed via the Internet.

The aforementioned European Convention on cyber crime defines four groups of offences:

- Offences against confidentiality, integrity, and availability of computer data and systems – these include illegal access, interception, and interference with data or systems, as well as utilization of hacking devices and password trafficking;
- Computer-related offences – theft and forgery represent the main forms of attack;
- Content-related offences – child pornography represents the dominant content in this group; offences include possession, distribution, transmission, maintenance, or provision of these materials;
- Offences related to infringement of copyright and related rights – these include unauthorized reproduction and distribution of copies of computer systems.

Both computer crime and cyber crime require appropriate legislation. From the original forms of cyber crime in the beginning of the 1990s and until the present day, numerous international bodies have focused on this type of crime. There is international, as well as common national regulation of cyber crime and some of its forms. In addition, self-governing bodies have also attempted to deal with this phenomenon. This means that regulation takes place at several levels. Interestingly, it seems that more activities take place at the international level than at the national or the self-governing one.

This is somewhat expected due to the characteristics of these offences and criminals who commit them (Drakulic & Drakulic, 2012). The majority of the most important international acts have been enacted in the EU framework. One of the most significant documents, adopted by states outside the EU as well, is the international convention that regulates cyber crime, the Council of Europe Convention on Cyber Crime, adopted in 2001 in Budapest, which came into force in July 2004. The Convention has set absolute standards regarding international regulation of this phenomenon and represents a guideline for the states that wish to develop their legislation in order to suppress this type of crime.

The subject of the Convention on Cyber Crime includes: crimes against confidentiality, integrity, and availability of computer data and networks (unauthorized access, damage of data, networks, etc.); computer crimes (unauthorized data entry or deletion); computer fraud; crimes related to child pornography; crimes against infringement of copyright and related rights; ancillary liability and sanctions (attempt, aiding, and abetting); liability of legal entities; sanctions; procedural law; protection of human rights; confiscation of the proceeds of the crime; collection of real-time computer data, etc. (Prlja, 2013, p. 781).

Cyber space in Serbia follows the global cyber crime expansion trend. In Serbia, there is a plethora of cyber crime activities, ranging from dissemination of viruses, piracy, and unauthorized access to computer networks, to pornography, credit card frauds, and bank robberies. As regards the suppression of hi-tech crime in Serbia, the greatest step has been made by the establishment of specialized bodies and the enlistment of specially trained experts.

Within the Serbian Ministry of Interior, a special unit against hi-tech crime has been formed. Additionally, a special prosecutor for hi-tech crime has been appointed and court jurisdiction has been determined for the entire territory of the Republic of Serbia.

Computer crimes have also been included in the Serbian Criminal Code (SCC) in 2005. They are envisaged in article 27 as crimes against the security of computer data. These crimes include the following: damage of computer data and software, computer sabotage, development and introduction of computer viruses, computer fraud, unauthorized access to protected computers, networks, or electronic databases, prevention and restriction of access to a public computer network, and unauthorized exploitation of computers and computer networks (Art. 298-304 SCC).

The most prominent forms of computer crime in Serbia, according to the data provided by the special prosecutor against high technology crime, are the following: copyright infringement, credit card fraud, and Internet pedophilia (Streater, 2010, p. 28).

COMMON FEATURES OF INTERNET PEDOPHILIA

Pedophiles used to have a *narrow* acting space. They used to go to children playgrounds and school yards, and performed common pedophile activities, such as observation, monitoring, and questioning children, and giving them chocolate, chewing gum, or candy. Such methods and approaches implied the risk of exposure. Nowadays, the Internet provides pedophiles with easy and safe monitoring of children, their activities, games, and entertainment. It also provides the exit strategy, or the ability to hide in anonymity in case of the danger of being exposed.

By analyzing this phenomenon, it is difficult to agree with the opinion that computers and the Internet represent the dark side of the world. However, the notion that aimless and uncontrolled use of the Internet carries a variety of risks appears more appropriate. "The Internet is used today by about 15% of the world population (consciously), and even 20% unconsciously (through different devices, phones, TV). A half of these users are aged 5 to adolescent age. A simple Google search of the word *encyclopedia* will provide about 1,700,000 results, while the word *sex* provides 26,500,000 results" (http://sr.wikipedia.org/sr-el/razgovor_sa_korisnikom: Internetservis; date of consideration: 29.12.2012).

This data is alarming for the society and, in particular, for the parents, who unfortunately have no clear understanding of the implications of this phenomenon and no awareness of the problem or of the ways to adequately recognize it. The development of IT, its interactivity, and its great communication possibilities have created increased risk for all the users, predominantly children, who are exposed to hidden traps and to individuals who misuse computers in order to satisfy their own perverted needs.

Therefore, an absurd question arises whether children are safer with the Internet or in the street. Accordingly, the following represent the advantages and risks of the Internet and modern forms of communication, as well as the particularities of electronic violence (Buljan Flender, 2011):

1. Certain advantages include:
   - Quicker information availability, learning;
   - Quick and easy news review;
   - Instant availability;
   - Source of entertainment, i.e. playing online games;
   - Communication regardless of the location;

- Exchange of experiences, opinions, and information with peers or adults with similar interests and problems;
- Improvement of writing skills – writing represents a dominant method of Internet and mobile phone communication;
- Reinforcement of creativity;
- Development of problem solving skills and information selection.

2. Certain risks related to modern forms of communication are:
   - Exposure to inadequate sexual content;
   - Internet as a new playground for pedophiles;
   - Exposure to distressing hostile messages;
   - Potential over-exposure of children and youth to a frequent or long-term use of the Internet.
3. There are certain features of electronic violence that discriminate it from violence in direct physical contact, such as:
   - 24/7 presence;
   - Exposure at home and other places previously deemed safe for children;
   - Multiple audiences and witnesses that increase rapidly;
   - Anonymity increases a victim's insecurity;
   - E-abuse may be present among peers, but adults can also become targets, i.e. teachers;
   - The lack of physical contact between the victim and the audience prevents children and youth to comprehend the potential damage of their words, as sometimes even the sent messages may unintentionally cause harm.

Internet abuse can be interpreted through the WHO definition that defines violence as "the intentional use of physical force or power, threatened or actual, against oneself, another person, or against a group or community, that either results in or has a high likelihood of resulting in injury, death, psychological harm, maldevelopment, or deprivation" (http://www.who.int/topics/violence/en/; date of consideration: 12.10.2012.).

THE ROLE OF FAMILY IN THE MODERN INFORMATION AGE

Among numerous other challenges, modern family faces technological challenges as well. Even though it emerged relatively recently (ca. 20 years ago), advanced IT heavily influenced modern family and the general development of a *technological consciousness*, eventually affecting the essence of family, contributing to stratification within it, as well as having other negative implications.

A common distinction between the real and the virtual, often used in discussions about the Internet and cyber space, can blur a number of issues and create an insufficiently clear and functional gap. Cyber space represents a technological space that involves various contexts and mutually overlapping environments. It appears and develops in a given historical moment, marked by numerous social, cultural, political, financial, technological, and other levels. The users enter with different desires, ambitions, and visions, and negotiate their position based on their given abilities. These abilities, however, by no means limit them or turn them into passive receivers of the available content, but rather offer them the possibility to become creative social actors (Panovic, 2004).

The majority of the population has an absolutely non-critical view towards new technologies and challenges of the modern society. Nevertheless, defining this highly prevalent matter of a symbolic *cyber space life* and the consequences associated with it becomes increasingly important. The development of the Internet and the digitalization of everyday life created new forms of social activity and fields of activity, involving the frequently noted cyber culture.

Cyber culture has several synonyms such as digital culture, Internet culture, virtual culture, network culture, etc. This phenomenon explains the role of the Internet in creating an individual in today's time and space. In fact, network culture is a form of Esperanto culture, *outside of time* and *outside of space* culture, which in its own terms exists only in real time, without direction in (territorial) space and links in (historical) time (Roberts & Webster, 2002, p. 242).

Cyber space became an integral part of our living space, the space of each family as the basic social cell. Apart from its numerous advantages, this space is at the same time associated with various forms of abuse. When it comes to children, some of this abuse includes manipulative actions for the purpose of selling various products, recruitment by sects (brainwashing), and often sexual abuse.

In all cases, the *bad guys* sweet-talk children and show a lot of understanding. When it comes to sexual abuse, they falsely present themselves as peers and establish a trusting relationship with a child, using it to cross the boundary and further discuss sex, which is followed by the exchange of photos or, in worse cases, even a face-to-face meeting. This is a typical pedophile strategy. Children, unaware of whom they are speaking to, often end up taking their clothes off in front of a web camera and sending images to *the peer*. These images often end up on pornographic websites (Bjelajac, 2011, p. 56).

Owing to the fact that society cannot rely on individuals' self-control, effective educational programs are increasingly being discussed in order to decrease the risk and protect users from electronic violence by establishing certain procedures and recommendations. Such recommendations must be focused on youth under eighteen, as well as on adult Internet users, parents, teachers, public institutions, and security services dealing with crime suppression.

Cyber violence contains all the elements of “regular” violence and causes real consequences even though it is committed in the so-called virtual space. The specificity of this form of violence is that it is committed through an electronic device, which essentially masks the actual danger, as it is believed that there is an easy way out, i.e. intended victims can simply turn off the device and exit the cyber space.

Lack of education hinders the possibility to view the problem realistically; otherwise, it would be generally accepted that cyber space has become a part of our everyday environment, and that temporarily exiting cyber space is the same as switching between actual physical environments, whereby all the related circumstances and consequences remain, including the key issue that this type of violence usually does not stop if one simply leaves an environment.

The conclusions of the participants of the expert meeting "Virtual childhood – focusing on problems, prevention, and recommendations" include the following (Expert Meeting, 2011):

- Virtual reality increasingly enters the lives of many people. Children have become mass users of IT and experienced a complete sense of virtual childhood;
- The millennial generation grew up with the Internet and is always online. Digital technologies represent merely a non-organic extension of their bodies, while social media are not only a virtual but a real environment;
- IT has become a part of everyday life of a contemporary family. Even preschool children use computers. Starting from the age of four or five, they are perfectly comfortable with playing computer games, while the parents are proud of their children’s intelligence, memory, and attention, as they achieve great results by using a computer – they are peaceful and attentive, they learn letters of the alphabet or the English language, etc. On the other hand, there is a significant increase in the number of children who experience problems with social interaction, difficulties in speech and communication, as well as attention deficit.
- IT has become an integral part of children’s life. However, in addition to the advantages and positive effects, its use exposes children to numerous dangers. There is a possibility to develop addictive behavior. In the virtual world, they may encounter numerous frauds and unpleasant situations;
- Parents of young children and teenagers are often astounded by how much time their children spend in front of a computer. Children’s thoughts are transferred into the virtual information world, entertainment, and virtual friendship, so they lose track of

time and forget their actual obligations. Prohibitions are mostly useless, since children can surf the Internet at school, at their friends', or wherever they are not being controlled;

- Research indicates that contemporary lifestyle decreases or eliminates certain biological abilities. Consequently, the program *NTC learning system* was developed based on the knowledge of neurophysiology, aimed at assisting and sustaining the development of children's biological potentials;
- The nihilism of modern technology destroys sensibility, solidarity, and critical thinking. Revitalization of religious and magic rituals in the context of techno-culture takes human soul as the victim, technologically shaking the very foundation of humanity;
- In children's minds, the virtual world has initiated a battle with the real world;
- The specificity of family law refers to the particularity of the social relations it regulates, which, considering the subjects, involves the need for privacy and non-interference by third parties on the one hand, as well as justified social interest and control on the other hand;
- Nowadays, the function of family is affected by forced individuality and rivalry. Dignity should be restored to family roles, so that the mother could really be the mother without playing the father's role and the father could reclaim the necessary authority.

PROTECTION OF CHILDREN FROM INTERNET ABUSE

Children education, guidance, and preparation for their independent life are unavoidable and endless topics. Together with numerous other influences, the Internet and computer technology also affect people's lives, both directly and indirectly. They are so intensive that they require increased preventive effort by the parents. Likewise, education is necessary and particularly useful because it enables people to recognize and face the problem of how computer games and virtual reality influence children and their development. Moreover, this involves the knowledge of how to safely introduce a child into the digital world and help them avoid any unpleasant experiences.

Accordingly, experts usually give parents the following suggestions:

- Creating a safe profile is the first step in personal data protection, with an emphasis that the information to be included should be carefully selected;
- Teach your children to use a neutral email address and username;

- Computer passwords should always be kept as a secret;
- Children need to learn to receive messages only from the people they know outside of the Internet;
- Try to protect your children from unpleasant experiences – show them how to protect their own privacy and respect other persons' privacy;
- Teach your children not to reply to offensive messages;
- Help your children to understand which messages may cause unpleasant feelings;
- Become familiar with the people from your children's environment – meet their friends, their friends' parents, their teachers, etc.;
- Explain to your children that if someone harasses them, it is not their fault;
- Be careful that your children visit only websites with legal content. Also, explain that reality is often not faithfully represented on the Internet;
- Explain to your children the risks of recording Internet material;
- Make sure that your computer is adequately protected. Always update your antivirus, *firewall*, and anti-spyware software;
- Teach children to use the antivirus software when transferring data on a hard disk;
- Before installing anything on the computer, read the text on the protection of data privacy and the user license agreement;
- Create a user account for your child in the computer's operative system (*parental control* function);
- Keep the addresses of the websites that children frequently use in a separate folder;
- Protection rules apply to your children and yourself. Teach them to always inform you in case they see something suspicious on the Internet (http://www.internetservis.co.rs/virtuelnodetinjstvo/VRD-PKS/BiltenVR.pdf; date of consideration: 12.10.2012.).

Evidently, modern age creates new and complex parental roles. However, there remains an open question of how insufficiently educated and trained parents can respond to these challenges that modern family faces in the information age.

CONCLUSIONS

Being aware of the expansion of cyber crime, the European Commission suggested the introduction of more stringent laws pertaining to cyber crime in the EU and warned that computer network abuse had already caused big problems in the EU member states. Pedophiles previously used traditional methods to approach their victims and they were exposed to a variety of risks. Nowadays, the Internet represents an ideal tool as it provides pedophiles with the possibility to undisturbedly observe children, participate in their activities, games, and entertainment, and disappear in anonymity if they risk being caught.

The role of the parents, teachers, professors, and the society in general is to use youth-oriented educational campaigns to highlight the positive aspects of the Internet and to point to various risks associated with illegal use and abuse of information technology for the purpose of conducting criminal acts.

Along with raising collective awareness, the development of a long-term strategy is also necessary at both the national and the supranational level with mandatory cooperation of the relevant bodies, institutions, and organizations that implement the rule of law, as well as the private sector, namely, Internet providers, advertising agencies, software companies, etc. Today, the functional role of the family is jeopardized by the promotion of rivalry and individuality. The millennial generation grew up alongside the Internet and is always online. Digital technology is merely a non-organic extension of their bodies, while social media represent both a virtual and a real environment. Apparently, the virtual world has initiated a battle with the real world. These worlds are mixed in children's minds, indicating the necessity for the family and society as a whole to protect children from Internet abuse. It is reasonable to expect that information technology will further develop rapidly, so it is also reasonable to expect that different forms of information technology abuse for the purpose of conducting criminal activities will increase.

REFERENCES

Bjelajac, Z. (2011). *Cyber crime and Internet pedophilia.* Novi Sad: University Business Academy.

Buljan Flander, G. (2008). The Internet and children – should we worry?. In: *2nd scientific and professional symposium "Abuse of children and among children"* (115-125). Osijek: University of Osijek, Faculty of Philosophy.

Criminal Code of The Republic Serbia. Official Gazette of The Republic of Serbia, No. 85(2005), 88(2005)-ch., 107(2005)-ch., 72/(2009), 111(2009), 121(2005) and 104(2013).

Dimitrijevic, P. (2011). *Computer crime – authorized lectures.* Niš: Faculty of law. Retrieved from http://www.prafak.ni.ac.rs/files/nast_mat/Kompjuterski_kriminal.pdf; date of consideration: 12.10.2012.

Drakulic, M. & Drakulic, D. (2012). *Cyber crime* – authorized lectures. Belgrade: Faculty of Organizational Sciences.

Drakulic, M. & Drakulic, R. (2010). *The regulation of Internet.* RATEL Serbia study.

Draft Convention on Cyber crime – Explanatory Report. (2000). Strasbourg: European Committee on Crime Problems and European Committee of Experts on Crime in Cyber-space, Draft N° 24 Rev. 2. Retrieved from: http://conventions.coe.int/Treaty/en/Reports/Html/185.htm, date of consideration: 12.10.2012.

http://sr.wikipedia.org/sr-el/razgovor_sa_korisnikom:Internetservis; date of consideration: 29.12.2012.

http://www.who.int/topics/violence/en/; date of consideration: 12.10.2012.

Panovic, I. (2004). *On Cyber Space and Identity*, *E-volution, CePIT, 3*, 7-11. Retrieved from: http://www.bos.rs/cepit/evolucija/html/3/TEMA1/ipanovic.htm, date of consideration: 12.10.2012.

Prlja, D. (2013). The virtual space, sovereignty, territory and power. In: *International Conference "Globalization and seizing sovereignty"* (777-791). Kosovska Mitrovica: University of Priština, Faculty of Philosophy.

Roberts, K. & Webster, F. (2002). Prospects of a Virtual Culture. *Science as Culture, Carfax Publishing (Taylor & Francis Group)*, 11(2), 235-257.

Robinson, J. (2000). *Internet as the Scene of Crime. In*: International Computer Crime Conference, Oslo. Retrieved from: http://www.justice.gov/criminal/ cybercrime/roboslo.htm, date of consideration: 12.10.2012.

Streater, K. (2010). Cyber Security Challenge. *ITNOW journal, Oxford University Press*, *52(6)*, 28-37.

Vienna Declaration on Crime and Justice: Meeting the Challenges of the Twenty-first Century. (2000). Vienna: Tenth United Nations Congress on the Prevention of Crime and the treatment of Offenders, United Nations Office on Drugs and Crime. Retrieved from: http://www.uncjin.org/Documents/congr10/4r3e.pdf, date of consideration: 12.10.2012.

Virtual childhood – focusing on problems, prevention and recommendations. (2011). Beograd: Expert Conference on the Virtual Childhood. Retrieved from: http://www.internetservis.co.rs/virtuelnodetinjstvo/VRD-PKS/BiltenVR.pdf, date of consideration: 12.10.2012.

Синиша Г. Минић, Унивезитет у Приштини са привременим седиштем у Косовској Митровици, Учитељски факултет, Лепосавић
Жаклина Спалевић, Универзитет Сингидунум, Београд

ЗЛОУПОТРЕБА РАЧУНАРСКИХ МРЕЖА У САЈБЕР ПРОСТОРУ: УТИЦАЈ ПОРОДИЦЕ У МОДЕРНОМ ИНФОРМАТИЧКОМ ВРЕМЕНУ

Резиме

Брзи развој информационих технологија проузроковао је формирање сајбер простора као безвласничке виртуелне творевине која данас паралелно коегзистира са реалним светом свуда где постоји интернет инфраструктура. Интернет је као глобална рачунарска мрежа проуроковао велике измене у начуну живота и брзини комуникација. У данашњем свету информација свест људи и њихов став према одређеним појавама се у највећој мери обликује под утицајем информација које нам се континуално пласирају на друштвеним мрежама.

У виртуелном сајбер простору у коме нема државних граница и у коме национално и међународно кривично законодавство не могу да испрате техничко-технолошке промене, дошло је формирања организованих криминалних група, чије деловање проузрокује последице у стварном свету. Све ове криминалне активности обухваћене су појмом „сајбер криминала“, који представља

унију скупова рачунарског, дигиталног, е-криминала, web криминала, криминала који обухвата напад на рачунарске мреже, крађу података, напада на системе и повреда ауторских права путем интернета. На основу Европске конвенције о сајбер криминалу, Кривични закон Србије дефинисао је кривична дела рачунарске саботаже, рачунарске преваре, оштећења рачунарских података и програма, прављења и уношења рачунарских вируса, неовлашћени приступ заштићеном рачунару, рачунарској мрежи и електронској обради података, као и спречавање и ограничавање приступа јавној рачунарској мрежи.

Посебна опасност је неконтролисана и бесциљна употреба интернета од стане деце. Злоупотреба интернета је често у директној вези са порнографијом, што подразумева да разни сајтови са нелегалним садржајем такође утичу на дугорочно "тровање" деце. Претерано свакодневно учешће на друштвеним мрежама има негативан утицај на здравље све деце, како у млађем тако и у тинејџерском узрасту. Адолесценти постају анксиозни, депресивни или агресивни.

Поред својих корисних страна, друштвене мреже крију и велике опасности, јер се на њима налазе појединци који су у стању да слике и видео-материјале деце преузму са мреже, злоупотребе га, преобликују, диструбирају га путем порнографских сајтова или уцењују децу са њиме било у виртуелном, било у стварном свету. На основу информација која деца остављају на мрежама педофили могу сазнати све о њиховом кретању и начину живота и угрозити им безбедноаст. Да би се деца заштитила од злонамерних лица и организованих група која желе злопотребити њихову приватност потребно је:

- Формирати посебне налоге за рад на рачунару деци и пратити њихово кретање на интернету,
- Објаснити деци значај непрекидног коришћена антивирус програма и заштитних зидова током присуства на мрежи,
- Упозорити децу да не смеју давати своје лозинке за приступ личном рачунару, електронској пошти и налозима за приступ друштвеним мрежама,
- Предочити ризике приступања непознатим сајтовима и преузимања материјала са истих.
- Објаснити деци како могу постати жртве организованих криминалних група интернет-порнографије, које могу злоупотребити слике и видео-материјал која деца могу оставити незаштићен на друштвеним мрежама и рачунарима без заштите.

Упркос примарној и суштинској улози родитеља, подршка свих друштвених сегмената је неопходна како би се подигла колективна свест путем медија и образовних кампања намењених младима и деци у циљу пружања информација о потенцијалним интернет-злоупотребама и методама безбедног коришћења истог.