CYBER KRIMINAL

CYBER CRIME

Renata Gligorević, dipl. ek.

Stručni članak DOI 10.7251/OIK1301011G, UDK 343.53:[004.738.5 005.742 **Professional paper**

REZIME

Cyber kriminal je prisutan od samog početka upotrebe računara i računarske opreme. Cyber kriminal je oblik kriminalnog ponašanja, kod koga se računarske mreže pojavljuju kao sredstvo izvršenja kriminalnog djela. Na početku, takvo kriminalno ponašanje je bilo beznačajno.

Riječ je o kriminalnom djelu koje, uglavnom, obavljaju pojedinci, ali, u nekim slučajevima, i same organizacije. Takvo kriminalno ponašanje ima za posljedicu neovlašćen pristup povjerljivim informacijama kao i njihovo nedozvoljeno objavljivanje.

Ključne riječi: cyber kriminal, kriminalno ponašanje, računarske mreže i računarska oprema.

SUMMARY

Cyber crime is present from the beginning of the use of computers and computer equipment. Cyber crime is a form of criminal behaviour, in which computer networks appear as a medium of a criminal act. At the beginnings, such criminal behaviour was insignificant.

It is a criminal act which is mainly done by individuals, but the organisations also. Such criminal behaviour has as a result unauthorised access to confidential information and unauthorized publishing.

Key words: cyber crime, criminal behaviour, computer networks and computer equipment.

UVOD

Ljudska potreba za brojnim pogodnostima koje pruža upotreba savremene tehnologije, za kratko vrijeme je dovela do opasne zavisnosti od umreženih sistema. Nacionalna infrastruktura se našla pod kontrolom složenih kompjuterskih sistema. Vremenom se ova informaciona tehnologija „uvukla“ u svaki segment ljudskog života.

Kompjuteri upravljaju velikim dijelom našeg života. Brz razvoj i upotreba savremene tehnologije upravljaju našim komunikacijama, vozilima, poslovima, transakcijama, ama baš svim. Sve to ima i prednosti i mane. Jedan od glavnih problema sa kojim se susrećemo pri upotrebi računara jeste upravo kompjuterski kriminal.

Cyber kriminal se odnosi na zloupotrebu računarske tehnologije, a neki od primjera zloupotrebe su utaja, pronevjera, krađa. Podaci

INTRODUCTION

The human need for the numerous benefits provided by the use of modern technology, in a short time led to a dangerous dependence on networked systems. National infrastructure came under the control of complex computer systems. Over time, the information technology was dragged into every aspect of human life.

Computers direct large part of our lives. The rapid development and use of modern technology directs our communications, cars, jobs, transactions, absolutely everything. For all that there are both advantages and disadvantages. One of the major flaws and problems with which, we are meeting when we use a computer is just a computer crime.

Cyber crime is in fact related to the abuse of computer technology, a few examples of the misuse are fraud, embezzlement, theft. The

koji se dobiju na neovlašćen način, tj. zloupotrebom računara mogu da posluže za pribavljanje brojnih koristi.

KOMPJUTERSKI KRIMINAL

U današnjem svijetu sve više se koristi pojam „cyber“, a da u stvari i ne znamo šta on znači. Pojam „cyber“ prvo se pojavio u vojnoj terminologiji, u smislu predviđanja budućih oblika ratovanja. „Cyberwar“ predstavlja ratovanje znanjem, odnosno informacijama. Radi se o ratu visoke tehnologije, koji se odnosi na prikupljanje povjerljivih informacija.

Pojam cyber kriminal se može definisati kao oblik kriminalnog ponašanja za čije izvršenje se koristi računarska oprema. Lica koja obavljaju takve kriminalne radnje su cyber kriminalci. Uglavnom su to muškarci između 19 i 30 godina starosti. Postoji veoma mali broj žena koje se bave ovim nedozvoljenim radnjama, ali se one uglavnom pojavljuju kao saučesnici (Mesarović, 2006).

Cyber kriminalom su se mladi hakeri dokazivali u društvu, ali, kako se tehnologija razvijala, i cyber kriminalci su postajali ozbiljniji i zreliji ljudi, koji su imali motive za takvo ponašanje.

Cyber kriminalci su vrlo inteligentni i obrazovani ljudi koji dosljedno prate razvoj savremene tehnologije. Samouvjereni i sigurni u svoje znanje, teže da još dublje prodru u virtualni svijet kako bi ostvarili svoje ciljeve.

Sa većim razvojem savremene tehnologije, povećava se i broj kriminalnih radnji kao i broj njihovih izvršilaca. Svakim danom broj cyber napada je sve veći i sve više negativno utiče na cijelo društvo. Riječ je o ozbiljnom problemu, koga većina ljudi nije ni svjesna.

Mnogi cyber kriminalci su dovoljno inteligentni da iskoriste i najmanju grešku računarske mreže. Njihove najvažnije mete su kreditne kartice, najčešće kreditne kartice evropskih zemalja i Kanade. (Gleni, 2011, str. 10). Cyber napade izvode profesionalni kriminalci, koji kradu milione i koji žele pri-

data obtained in an unauthorised manner, i.e. misuse of computers can be used to obtain a number of benefits.

COMPUTER CRIME

Today, many people use the term „cyber“, but they do not know what its meaning. The term “cyber” first appeared in military vocabulary, in terms of predicting future forms of warfare. “Cyber war” is a war of knowledge or information. It is a war of high technology, which refers to the collection of confidential information.

The concept of cyber crime can be defined as a form of criminal behaviour that is performed by the use of computer equipment. Persons who perform such criminal activities are cyber criminals. They are mostly men between 19 and 30 years of age. There are few women involved in these illegal activities, but they mostly appear as accomplices (Mesarovic, 2006).

Cyber crime used to be a way of young hackers proving themselves in the society but as development of technology is growing, more serious and mature people are becoming cyber criminals with motives for such behavior.

Cyber criminals are very intelligent and educated people who consistently follow the development of modern technology. Confident and sure of their knowledge, they tend to penetrate deeper into the virtual world in order to achieve their goals.

By the increasing development of modern technology, number of crimes and number of their executors increases. Each day the number of cyber attacks is growing as more and more negative effects are on the whole society. This is a serious problem, which most people are not aware of .

Many cyber criminals are intelligent enough to take advantage of the smallest erron on a computer network. Their main targets are mostly credit cards, usually credit cards of European countries and Canada. (Gleni, 2011, p.10). Cyber attacks are performed by professional criminals who steal millions and

stup računarima, brojevima kreditnih kartica i slično.

Cyber kriminalci „vrebaju“ iza svojih monitora i teško je dokazati ko je, u stvari, osoba koja pokreće sav taj haos u virtualnom svijetu. Na mrežama je teško odrediti ko Vam ne misli dobro. Zakoni koji se odnose na internet, se razlikuju od države do države. Za kriminalističke službe najveći problem jeste anonimnost, jer se ne može sa sigurnošću dokazati ko upravlja računarom ili računarskom opremom. Glavni cilj cyber kriminalca je da ostane anoniman i da izbriše svaki trag, koji bi otkrio njegov identitet i lokaciju. Upravo zbog toga, oni, uglavnom, vrebaju iz lokalnih internet kafea.

Cyber operacije se mogu podijeliti na: (1) računarski Mrežni napad - CNA, (2) računarska mrežna odbrana - CND i (3) Računarska mrežna eksploatacija - CNE (Popić, 2012).

Cyber kriminal je takav oblik kriminalnog ponašanja kod koga je cyber prostor okruženje u kome se računarska mreža koristi kao osnovno sredstvo izvršenja krivičnog djela. Cyber prostor podrazumijeva visoku tehničku opremeljenost.

Računarske mreže stvorile su mogućnost za novi oblik kriminala. Organizovanje takvog kriminala zahtijeva dobro poznavanje kompjuterske tehnologije. Kompjutersku tehnologiju najčešće koriste dvije grupe ljudi koje se bave ovakvim kriminalom: pravi hakeri i pravi kriminalci. Radi se o zaista ozbiljnom organizovanom kriminalu.

Pravi hakeri i pravi kriminalci čine grupe od kojih jako mali procenat ljudi predstavlja ozbiljnu prijetnju za virtualni svijet. Ostali su sitni lopovi koji rade samostalno i tu je riječ o manjim sumama novca. Njih se ne isplati loviti s obzirom na oskudne resurse sa kojim raspolažu kriminalističke službe.

Svijet se danas susreće sa sve mlađim osobama, tzv. hakerima, koji dobro poznaju savremenu tehnologiju i koji detaljno prate njen razvoj. Dok se na jednoj strani nalaze pojedinci sa velikim znanjem o informaciono – komunikacionoj tehnologiji, na drugoj strani se

who want access to computers, numbers of credit cards and other similar things.

Cyber criminals are lurking behind their monitors and it is very difficult to prove who the person who has initiated all this chaos in the virtual world actually is. It is much more difficult online to determine whose intentions are bad. Laws relating to the Internet are different from country to country. For law enforcement agencies the biggest problem is the anonymity because you can not prove with certainty who operates the computer or computer equipment. The main goal of cyber criminals is to remain anonymous and to beat every trace that might discover their identity and location. Because of this, they usually lurk from local internet cafés.

Cyber operations can be divided into: (1) Computer Network Attack - CNA. (2) Computer Network Defence -CND. (3) Computer Network Exploitation - CNE (Popic, 2012).

Cyber crime is such a form of criminal behaviour where the cyber space is environment in which the computer network is used as the primary means of committing the crime. Cyber space involves high technical equipment.

Computer networks have created the opportunity for new forms of crime. Organising such a criminal activity requires possession of a good knowledge of computers. Such techniques are commonly used by two groups of people who are involved in this crime: the real hackers and real criminals. This is a really serious organised crime.

The real hackers and the real criminals form the group from which a very small percentage of people represent a serious threat to the virtual world. Others are little thieves who work alone and they are after small sums of money. These players are not worth the hunt, given the scarce resources available to the law eforcement services.

Today, the world is faced with younger people called hackers who have very good understanding of modern technology and who closely follow its development. While there are individuals with extensive knowledge of information - communication technology, on the

nalazi veći broj ljudi, koji o toj tehnologiji ne zna ništa.

Cyber kriminal svakim danom sve više raste i stvara ogroman problem i pojedincima i državi. Zemlje u razvoju su posebna meta hakera ili cyber kriminalaca, koji vrebaju iz malih nerazvijenih i mnogo siromašnijih zemalja.

Kao što je već rečeno, to su, uglavnom, mladi ljudi, koji na samom početku bavljenja takvim nelegalnim djelatnostima nisu ni svjesni da čine ozbiljno kriminalno djelo. Njihov motiv jeste da se dokažu u društvu ili da otkriju nešto novo što do sada niko nije uspio. Vidjevši da iz svega toga mogu da izvuku i određenu korist, motivisani su da nastave dalje, nadajući se da ih niko neće otkriti.

Cyber kriminal je takav oblik kriminalnog ponašanja kod koga je teško ući u trag izvršiocima, ali sa velikim naporima i zalaganjima i to je moguće. Ključ uspjeha i opstanka kriminalističkih službi jeste da budu u kontaktu sa svojim kolegama u drugim zemljama. Upravo zbog toga što se zakon o cyber kriminalu razlikuje od države do države.

Cyber kriminal danas pravi veću štetu nego trgovina drogama. Jedan od najvećih problema jeste što nema adekvatnog zakona za ovu vrstu kriminala, jer internet nema granica.

Lica koja se bave ovim nelegalnim radnjama su, uglavnom, studenti, informatički stručnjaci, bivši inspektori kriminalističkih službi i brojni drugi koji dobro poznaju savremenu tehnologiju.

VRSTE I TIPOVI CYBER KRIMINALA

Na svom Desetom kongresu za suzbijanje kriminala i postupanju prema prestupnicima, 2000. godine, UN su podijelile cyber kriminal na dvije podkategorije:

1. cyber kriminal u užem smislu, koji podrazumijeva svako nezakonito ponašanje usmjereno na elektronske operacije sigurnosti kompjuterskih sistema i podataka, koji se u njima obrađuju;

other hand there is a larger number of people who do not know anything on this technology.

Cyber crime grows more and more every day and creates enormous problems to the authorities and society in general. Developing countries are especially a targeted zone for hackers and cyber criminals who are preying from undeveloped and poor countries.

It was aforementioned that these are mostly young people who at the beginning of dealing with such illegal activities are not even aware that it is actually a serious cyber crime. Their motive is to prove themselves in the society or to discover something new that no one has succeeded in before. Being aware of the possibility to derive a certain benefit, has certainly given them an even greater incentive and motivation to continue , hoping that no one will discover them.

Cyber crime is a form of criminal behaviour in which it is very difficult to trace a criminal but with a great effort and dedication it is possible. The key to success and efficiency of law enforcement is to keep in touch with colleague in other countries. It is because the law on cyber crime varies from state to state.

Cyber crime now makes more damage than drug trafficking. One of the biggest problems is that there are not laws against this type of criminal activity, because the Internet has no boundaries.

Persons who are dealing with these illegal activities are mainly students, IT professionals, former law enforcement inspectors and many others who have extensive knowledge of modern technology.

KINDS AND TYPES OF CYBER CRIME

In 2000 at UN Tenth Congress for Crime Prevention and the Treatment of Offenders, cyber crime was divided into two sub-categories:

1. Cyber Crime in the narrow meaning is any illegal activity directed to electronic operations security of computer systems and data which are processed within.

2. cyber kriminal u širem smislu, odnosno svako nezakonito ponašanje vezano za ili u odnosu na kompjuterski sistem i mrežu, uključujući i takav kriminal kakvo je nezakonito posjedovanje, nuđenje i distribuisanje informacija preko kompjuterskih sistema i mreža (Ugren, 2012, str. 9).

Istim dokumentom su definisani i konkretni oblici ovog kriminaliteta, u skladu sa Preporukom Savjeta Evrope i listom OECD-a, te u djela cyber kriminala u užem smislu spadaju: (1) neautorizovani pristup kompjuterskom sistemu ili mreži, kršenjem mjera sigurnosti; (2) oštećenje kompjuterskih podataka ili programa; (3) kompjuterske sabotaže; (4) neovlašćeno presretanje komunikacija od i u kompjuterskim sistemima i mrežama; (5) kompjuterska špijunaža (Ibidem).

Kao oblici cyber kriminala u širem smislu najčešće se pojavljuju: (1) kompjuterski falsifikati; (2) kompjuterske krađe; (3) tehničke manipulacije uređajima ili elektronskim komponentama uređaja; (4) zloupotreba sistema plaćanja, kao što su manipulacije i krađe elektronskih kreditnih kartica ili korišćenje lažnih šifri u nezakonitim finansijskim aktivnostima (Ibidem).

Evropska konvencija o cyber kriminalu previđa četiri grupe djela:

1. djela protiv povjerljivosti, integriteta i dostupnosti kompjuterskih podataka i sistema – njih čine nezakoniti pristup, presretanje, uplitanje u podatke ili sisteme, korišćenje uređaja (proizvodnja, prodaja, uvoz, distribucija), programa, lozinki;
2. djela vezana za kompjutere kod kojih su falsifikovanje i krađe najtipičniji oblici napada;
3. djela vezana za sadržaje – dječija pornografija je najčešći sadržaj koji se pojavljuje u ovoj grupi cyber kriminala;
4. djela vezana za kršenje autorskih i srodnih prava, obuhvataju reprodukovanje i distribuciju neautorizovanih primjeraka djela kompjuterskim sistemima (Ibidem, str. 10).

U Enciklopediji cyber kriminala navodi se da FBI i Nacionalni centar za kriminal bijelih kragni SAD (National White Collar Cri-

2. Cyber Crime in a broader meaning is any unlawful conduct related to or in relation to a computer system and network including such crimes as the unlawful possession, offering and distribution of information through computer systems and networks (Ugren, 2012, p. 9).

The same document also defines specific forms of crime in accordance with Council of Europe recommendations and a list of the OECD, so that the acts of cyber crime in the narrow meaning include: (1) Unauthorized access to a computer system or network, or breach of security measures; (2) Damage to computer data or programs; (3) Computer sabotage; (4) Unauthorized interception of communications and computer systems and networks; (5) Computer espionage (Ibidem).

As the forms of cyber crime in a broader sense, the most frequently occurring are: (1) Computer forgeries; (2) Computer theft; (3) Technical manipulation devices and electronic components of the device; (4) Misuse of payment systems, such as electronic manipulation and theft of credit cards or use of fake code in illegal financial activities (Ibidem).

European Convention of Cybercrime foresees four groups of works:

1. Offenses against the confidentiality, integrity and availability of computer data and systems – made up of illegal access, interception, interference with data or systems, the use of the device (production, selling, importing, distribution) of programmes, a password;
2. Offenses related to computers in which forgery and theft are the most typical forms of attack;
3. Offenses related content - child pornography is the most common content that appears in this group of cyber crime;
4. Offenses related to infringement of copyright and related rights, including reproduction and distribution of unauthorized copies of a work by computer systems. (Ibidem, p. 10).

The Encyclopaedia of cyber crime, according to FBI and the National Center for white-collar crime the U.S. (National White Collar Crime

me Center) otkrivaju i prate sljedeće oblike: (1) upade u kompjuterske mreže; (2) industrijsku špijunažu; (3) softversku pirateriju; (4) dječiju pornografiju; (5) bombardovanje elektronskom poštom; (6) „njuškanje“ password-a; (7) „prerušavanje“ jednog računara da elektronski „liči“ na drugi, kako bi se moglo pristupiti sistemu, koji je pod restrikcijom; (8) krađu kreditnih kartica (Ibidem).

U zavisnosti od tipa počinjenog djela, cyber kriminal može biti:

1. politički, koji čine cyber špijunaža, hakovanje, cyber sabotaža, cyber ratovanje i cyber terorizam;
2. ekonomski cyber kriminal čine cyber prevare, hakovanje, krađa internet usluga i vremena, piratstvo softvera, piratstvo mikročipova i baza podataka, cyber industrijska špijunaža, prevare internet aukcije;
3. proizvodnja i distribucija nedozvoljenih i štetnih sadržaja čine dječija pornografija, pedofilija, vjerske sekte, širenje rasističkih i nacističkih kao i sličnih ideja i stavova, zloupotreba žena i djece, manipulacija zabranjenim proizvodima, supstancama i robom (droga, ljudski organi, oružje);
4. povrede cyber privatnosti čine nadgledanje e-pošte, spam, phiching, prisluškivanje, praćenje e-konferencija, itd (Ibidem, str. 10-11).

CYBER BEZBJEDNOST

Bezbjednost se odnosi na zaštitu vrijedne imovine od gubitka, odnosno oštećenja. Postoje mnoge pojave koje mogu da ugroze bezbjednost informacionih sistema određenih organizacija. Neke od tih pojava su sankcionisane zakonom (Krsmanović & Polić, 2012, str. 72).

Tehničke mjere zaštite su: identifikatori korisnika, lozinke, firewall i slično. Softverska rješenja koja se koriste za bezbjednost informacionih sistema su: mrežni firewall, upravljanje ranjivošću, upravljanje mrežnom bezbjednošću, obezbjeđenje bežične mreže (wireless) itd. (Ibidem, str. 80).

Center) detects and monitors the following forms: (1) Hacking the computer network; (2) Industrial espionage; (3) Software piracy; (4) Child pornography; (5) The bombing of the electronic mail; (6) “Sniffing” passwords; (7) “Disguise” of a computer to electronically “look like” the other, in order to be able to access the system which is under restriction; (8) The theft of credit cards (Ibidem).

Depending on the type of offense committed, cyber crime can be:

1. Political cyber crime made up of cyber espionage, hacking, cyber sabotage, cyber warfare and cyber terrorism.
2. Financial cyber crime made up of cyber fraud, hacking, theft of Internet services and time, piracy software, microchips and databases, cyber industrial espionage, Internet auction fraud.
3. Production and distribution of illegal and harmful content include child pornography, pedophilia, religious sects, spreading of racist, Nazi and similar ideas and attitudes, abuse of women and children, manipulation of prohibited goods, substances and goods (drugs, human organs, arms).
4. Affliction of cyber policy content include: monitoring of e-mail, spam, phiching, tapping, following of electronic conferences (Ibidem, p. 10-11)

CYBER SECURITY

Security refers to the protection of valuable assets from loss or damage. There are many factors that may endanger security of information systems of a company. Some of these phenomena are sanctioned by law (Krsmanovic & Polic, 2012, p. 72).

Technical protection measures are user IDs, passwords, firewalls and other. Software solutions that are used to ensure the safety of information systems are network firewall management, vulnerability management, network security, securing a wireless network (wireless) (Ibidem, p. 80).

Razvoj savremene tehnologije ima svoje prednosti i mane. Glavni problem ili poteškoća sa kojom se susreću osobe, koje koriste savremenu informaciono – komunikacionu tehnologiju jeste cyber bezbjednost. Informacioni sistemi treba da pruže sigurnost upotrebe ove tehnologije kako bi se steklo povjerenje u njeno korišćenje.

Postoji veliki procenat ljudi koji nisu sigurni u računarske mreže i ne usuđuju se da ih koriste. Strahuju da će se njihovi lični podaci i informacije naći na meti cyber kriminalaca. Gledajući trenutno stanje, može se reći da imaju razlog za strah. Ko može da garantuje da će njihovi podaci biti zaštićeni od zloupotrebe?

Da bi se steklo povjerenje u cyber okruženje, potrebno je uspostaviti politiku bezbjednosti. Politika bezbjednosti treba da pokaže da je internet sigurno sredstvo i da nema razloga za brigu. Najmanja greška ili propust za cyber kriminalca predstavlja pun pogodak da na lak način zloupotrijebi ili ukrade povjerljive informacije. Riječ je o nemilosrdnom obliku kriminala za koji odgovara jako mali broj cyber kriminalaca.

Krsmanović i Polić navode neke od tehnika za sticanje povjerenja u digitalno okruženje: sertifikovani digitalni potpis i kriptografska zaštita podataka. Kriptografija predstavlja proces konvertovanja digitalnih informacija u šifrovani tekst sa jednim algoritmom za šifrovanje (enkripciju) i dešifrovanje (dekripciju). Kriptografija treba da obezbijedi povjerenje, autentičnost, integritet i neporicanje (Ibidem, str. 21).

Šifrovanje (enkripcija) predstavlja element kriptografije. To je postupak transformacije čitljivog teksta u nečitljiv tekst za onoga kome taj tekst nije namijenjen (Ibidem).

Dešifrovanje (dekripcija) je takođe element kriptografije i predstavlja postupak transformacije nečitljivog teksta u čitljiv tekst, za onoga kome je taj tekst namijenjen (Ibidem).

Internet se susreće sa dva osnovna problema: sigurnost prenošenja podataka i ostvarivanje sigurne komunikacije. To su problemi koji se uvijek pojavljuju i koje je potrebno riješiti kako bi se steklo povjerenje u digitalno okruženje.

The development of modern technology has both advantages and disadvantages. The main problem or difficulty people who use modern information - communication technology are faced with is cyber security. Information systems need to provide safe use of such technology in order to keep confidence in its use.

There is a large percentage of people who do not trust computer networks and do not dare to use them. They are afraid that their personal data and information may become target of cyber criminals. Analysing the current situation, we can say that they have justified cause to fear. Who can guarantee that their data will be protected from abuse?

In order to gain confidence in the cyber environment, it is necessary to provide security policy. Security policies need to show that the Internet is a safe place and that there is no reason to worry. The smallest error or omission can represent a bingo opportunity for cyber criminals misuse or steal confidential information. It is a ruthless form of crime which corresponds to a very small number of cyber criminals.

Krsmanovic and Polic suggest some of the techniques for gaining confidence in the digital environment: certified digital signatures and cryptographic data protection. Cryptography is the process of converting digital information into an encrypted text with an algorithm for encryption and decryption. Cryptography should provide confidence, authenticity, integrity, and non-repudiation (Ibidem, p. 21).

Encryption is an element of cryptography. It is a process of transformation of readable text into unreadable text to the person whom the text is not intended for. (Ibidem).

Decryption is also an element of cryptography and represents a process of transformation of unreadable text into a readable one for the person whom the text is intended (Ibidem).

The Internet is facing with two main problems: security of data transfer and exercising of secure communications. These are problems that always occur and they need to be solved in order to gain confidence in digital environment.

NAJVEĆI CENTRI CYBER KRIMINALA

Norton u svom izvještaju za 2013. godinu navodi da cyber kriminal nema granica i da se najveći broj žrtava nalazi u Rusiji (85%), Kini (77%), Južnoj Africi (73%). Godišnji broj žrtava cyber kriminala, procjenjuje se na 378 miliona (Security affairs, 2013).

Finansijski troškovi zbog cyber kriminala iznose: SAD (38 milijardi doalra), Evropa (13 milijardi dolara), Kina (37 milijardi dolara), Brazil (8 milijardi dolara), Indija (4 milijarde dolara), Meksiko (3 milijarde dolara), Australija, Japan i Rusija (1 milijarda dolara) (Ibidem).

Najčešći oblici cyber kriminala koji se koriste u pomenutim zemljama su: prevare 38%, krađa podataka 21%, izmjena podataka 24% i ostali oblici 17% (Ibidem).

Norton (2013) navodi da sve većom upotrebom mobilnih telefona („pametnih telefona“) dolazi do povećanja broja cyber napada. Jedna polovina korisnika tih uređaja ne koristi osnovne mjere predostrožnosti, zbog čega postaju žrtve cyber napada (Ibidem).

Interesantan je primjer Austrije gdje je cyber kriminal u značajnom porastu, što pokazuje izvještaj Savezne kriminalističke službe (BK). Sa nešto više od 10.000 prijavljenih slučajeva u 2012. godini broj prekršaja ovog tipa se, u poređenju sa 2011. godinom, gotovo više nego udvostručio. BK procjenjuje da je tačan broj cyber krivičnih djela daleko veći i ukazuje da su „pametni telefoni“ sve češća meta cyber napada (Vijesti online, 2013).

U 2012. godini je prijavljeno ukupno 10.231 krivično djelo iz oblasti cyber kriminala, što je više od dvostrukog povećanja u poređenju sa 2011. godinom, kada je podnesena 4.831 prijava. Stopa riješenih slučajeva iznosila je oko 25%, što je smanjenje za oko 20% u poređenju sa 2011. godinom, proizilazi iz izvještaja (Ibidem).

BK ističe da su uzroci za smanjenje stope sve veća profesionalizacija kriminalnih bandi koje su organizovane i međunarodno umrežene, kao i zbog sve učestalije upotrebe programa koji nanose štetu raču-

THE BIGGEST CENTRES OF CYBER CRIME

Norton (2013) says in his report that cyber crime has no borders and majority of victims are located in Russia (85%), China (77%), South Africa (73%). The annual number of victims of cyber crime is estimated at 378 million (Security affairs, 2013).

The financial costs arising from cyber crime are: USA ($ 38 billion), Europe ($ 13 billion), China ($ 37 billion), Brazil ($ 8 billion), India ($ 4 billion), Mexico (3 billion), Australia, Japan and Russia (1 billion) (Ibidem).

The most common forms of cyber crime which are used in these countries are 38% fraud, data theft 21%, exchange of data 24% and other forms 17% (Ibidem).

Norton (2013) states that by the increasing use of mobile phones (“smart phones”) there is an increasing number of cyber attacks. One half of all users of these devices do not use basic precautions what makes them become victims of cyber attacks (Ibidem).

Austria is an interesting example where cyber crime is significantly increasing as the Federal Law Enforcement agency (BK) report says. With over 10,000 reported cases of violation compared to the year 2011 cyber crime has almost more than doubled. BK estimates that the real number of cyber offenses is higher and suggests that “smart phones” are more frequently targeted by cyber attacks (Vijesti online, 2013).

In 2012 it reported a total of 10,231 criminal offenses of cyber crime, almost doubled compared to 2011 when they filed 4,831 applications. The rate of solved cases has risen to about 25%, a decrease of about 20% compared with 2011, resulting from the report (Ibidem).

BK points out that the causes of the reduction of the increasing professionalisation of criminal gangs that are organised and networked internationally, as well as for more frequent use of programmes that harm the

narima. Istovremeno je rad policije otežan zbog novih tehnologija i anonimnosti korisnika (Ibidem).

CYBER KRIMINAL U BOSNI I HERCEGOVINI

U cilju efikasnije borbe protiv cyber - kriminala, Bosna i Hecegovina je definisala Akcioni plan za borbu protiv cyber - kriminala, koji se provodi, te potpisala i niz međunarodnih konvencija i sporazuma među kojima su i oni o policijskoj saradnji sa gotovo svim zemljama u regiji, ali i šire (Start, 2012).

Borba protiv cyber - kriminala je sastavni dio Strategije BiH za prevenciju i borbu protiv terorizma od 2010. do 2013. u kojoj stoji da za sada ne postoje pouzdani pokazatelji na koji način, u kojoj mjeri i obimu je ovaj problem prisutan u BiH i da, prema raspoloživim podacima, u BiH za sada nije došlo do zloupotrebe interneta u klasične terorističke svrhe ili u funkciji cyber - terorizma, ali da postoji nekoliko web sajtova, koji prezentovanim sadržajima podstiču ili pozivaju na netrpeljivost, pa i mržnju i uglavnom se radi o sajtovima koji nisu registrovani u BiH, nego u pojedinim evropskim zemljama kao što su Austrija, Njemačka, Norveška i slično (Ibidem).

Tokom prethodne dvije godine nadležnim tužilaštvima u Bosni i Hercegovini podneseno je više od 50 izvještaja o počinjenim krivičnim djelima iz oblasti kompjuterskog kriminala. Na globalnom nivou, procjenjuje se da je trenutno na internetu više od milion slika djece koja su izložena seksualnom zlostavljanju i eksploataciji, a njihov broj se godišnje uvećava za 50.000 (Tuzlanski.ba, 2012).

U Bosni i Hercegovini su u 2012. godini registrovane 64 prijave cyber kriminala. U Derventi, marta 2011. godine. Federalna uprava policije RS je u računaru jednog korisnika pronašla 2 miliona fotografija i 7 000 video snimaka dječije pornografije (Ibidem).

Najveći problem, kada je riječ o cyber kriminalu u Bosni i Hercegovini je nepostojanje adekvatnih mehanizama koji će ga spriječiti.

computers. At the same time the police work is more difficult due to new technologies and anonymity of users (Ibidem).

CYBER CRIME IN BOSNIA AND HERZEGOVINA

In order to effectively combat cyber-crime, BiH has defined an action plan to combat cyber-crime which is being carried out and signed a number of international conventions and agreements, including those on police cooperation with almost all countries in the region and beyond (Start, 2012).

The fight against cyber crime is an integral part of the Strategy for the Prevention and Combating of Terrorism between 2010 and 2013 in which countries that currently have no reliable data on how much and to what extent and scope this problem is present in BiH and that, according to the available data, so far there has been no abuse of the Internet for terrorist purposes or classical operational cyber-terrorism in BiH, but there are several websites that present contents that encourage or call for intolerance and hatred and most of them are sites that are not registered in BiH but in other European countries such as Austria, Germany, Norway (Ibidem).

Over the past two years relevant prosecutors in Bosnia and Herzegovina filed more than 50 reports of crimes committed in the area of cyber crime. Globally, it is estimated that on the Internet currently exist more than a million images of children who are vulnerable to sexual abuse and exploitation and that their number is increasing by 50,000 per year (Tuzlanski.ba, 2012).

There are 64 files of cyber crime registered in Bosnia and Herzegovina in 2012. In Derventa in 2011 the Federal Police RS found 2 million photographs and 7,000 videos of child pornography in one computer (Ibidem).

The biggest problem when it comes to cyber crime in Bosnia and Herzegovina is the lack of adequate mechanisms to prevent it. Centre for

Pri Državnoj agenciji za istrage i zaštitu (SIPA) trebao je formirati Centar za borbu protiv cyber kriminala. Ministarstvo unutrašnjih poslova Republike Srpske (MUP RS) je učinilo prve korake te je u tu svrhu formiralo posebnu jedinicu za borbu protiv cyber kriminala, što je prvo odjeljenje te vrste u cijeloj Bosni i Hercegovini. Od hakera i cyber kriminala strahuje cijeli svijet, ali problem u Bosni i Hercegovini predstavlja nedostatak novca koji će se uložiti u sigurnosne sisteme (Ibidem).

fighting cyber crime should have been formed in the State Investigation and Protection Agency (SIPA). Ministry of Internal Affairs of Republic of Srpska (MUP RS) has made the first step and for this purpose formed a special unit to fight cyber crime which is the first department of this kind in the whole of Bosnia and Herzegovina. The whole world fears hackers and cyber criminals but the problem in Bosnia and Herzegovina is the lack of money that should be invested in security systems (Ibidem).

ZAKLJUČAK

Nalazimo se u digitalnom dobu koje polako ulazi u svaki segment ljudskog života. Upravlja našim komunikacijama, vozilima, poslovima, kupovinom i prodajom. Svako od nas je bar jednom obavio važnu poslovnu ili finansijsku transakciju koristeći računar i računarsku opremu, a da nismo razmišljali da li možemo vjerovati ovoj savremenoj, digitalnoj mreži. Pogodnosti koje ona mreža pruža su svakako primamljive, ali treba znati i njene loše karakteristike.

Informacioni sistemi treba da obezbijede politiku bezbjednosti kako bi se steklo povjerenje pojedinaca u poslovanje putem interneta. Međutim, kako postoje kriminalne radnje u realnom tako se one javljaju i u virtualnom svijetu. Razlika je u tome što u virtualnom svijetu pravi kriminalac vreba iza svoga računara, i teško ga je otkriti. Upravo zbog toga, samo mali procenat cyber kriminalaca odgovara za štetu, koju su počinili. I posle izvršenja svoje kazne, za takvog pojedinca niko ne može garantovati da neće ponoviti istu grešku.

Cyber kriminal – kriminal modernog, digitalnog doba.

CONCLUSION

We are living in the digital age which is slowly entering into every segment of human life. It manages our communications, cars, businesses, buying and selling. Each of us has at least once completed a major business or financial transaction using computers and computer equipment without thinking whether we can trust this modern, digital network or not. The benefits that the network provides are certainly tempting but one should know and bad characteristics too.

Information systems should provide security policy in order to gain the trust of individuals in the business dealings via the Internet. However, as there is fraud present in the real world, so there can also be fraud in the virtual world. The difference is that in the virtual world real criminal is lurking behind your computer and it is very difficult to detect them. This is why only a very small percentage of cyber criminals are found guilty of the damage that they have caused. And after serving their sentence there is no guarantee for such an individual that they will not make the same offense again.

Cyber Crime - Crime of modern, digital age.

LITERATURA

Cross Domain Solutions. (n.d.). *Cyber crime*. Preuzeto 18. januara 2014. sa sajta http://www.crossdomainsolutions.com/cyber-crime/

LITERATURE

Cross Domain Solutions. (n.d.). *Cyber crime*. Rectrived January 18, 2014, from http://www.crossdomainsolutions.com/cyber-crime/

Gleni, M. (2011). *Dark Market, Kako su hakeri postali nova mafija*. Beograd: Samizdat B92.

Krsmanović, B. & Polić, S. (2012). *Digitalna ekonomija*. Materijal sa predavanja, Univerzitet Istočno Sarajevo, Fakultet poslovne ekonomije Bijeljina.

Mesarović, S. (2006). Motiv i profil izvršilaca. U zborniku *Ziteh '06*. Beograd. IT veštak.

Popić, A. (2012). *Cyber kriminal načela i djelovanje*. Preuzeto 16. januara 2014, sa sajta http://digitalnasigurnost.com/cyber-kriminal-nacela-djelovanje/

Security affairs (2013). *2013 Norton Report, the impact of cybercrime according Symantec*. Preuzeto 17. januara 2014. sa sajta http://securityaffairs.co/wordpress/18475/cyber-crime/2013-norton-report.html

Start. (2012). *Cyber-kriminalci nisu zaigrani hakeri*. Preuzeto 17. januara 2014. sa sajta http://www.startbih.info/Novost.aspx?novostid=7325.

Tuzlanski.ba (2012). *Kompjuterski kriminal u BiH: Registrirane 64 prijave, zaplijenjeni milioni fotografija (VIDEO)*. Preuzeto 18. januara 2014. sa sajta : http://tuzlanski.ba/izdvojeno/89-izdvojeno/3500-kompjuterski-kriminal-u-bih-registrirane-64-prijave-zaplijenjeni-milioni-fotografija-video.html.

Vijesti online (2013). *Sajber kriminal u Austriji u zabrinjavajućem poratu*. Preuzeto 16. januara 2014. sa sajta http://www.vijesti.me/svijet/sajber-kriminal-austriji-zabrinjavajucem-porastu-clanak-149230

Ugren, V. (2012). *Cyber kriminal*. Master rad, Univerzitet Singidunum Beograd, Departman za poslediplomske studije. Preuzeto 17.01.2014. sa sajta http://www.singipedia.com/content/3523-Cyber-kriminal

Gleni, M. (2011). *Dark Market, as hackers have become the new mafia*. Beograd: Samizdat B92.

Krsmanović, B. & Polić, S. (2012). *Digital economy*. Material from lectures, University of East Sarajevo, Faculty of Business and Economics Bijeljina.

Mesarović, S. (2006). *The motive and the offender profile*. In *Ziteh '06*. Beograd. IT veštak.

Popić, A. (2012). *Cyber crime policies and actions*. Rectrived January 16, 2014, from http://digitalnasigurnost.com/cyber-kriminal-nacela-djelovanje/

Security affairs (2013). *2013 Norton Report, the impact of cybercrime according Symantec*. Rectrived January 17, 2014, from http://securityaffairs.co/wordpress/18475/cyber-crime/2013-norton-report.html

Start. (2012). *Cyber-criminals are not playful hackers*. Rectrived January 17, 2014, from http://www.startbih.info/Novost.aspx?novostid=7325.

Tuzlanski.ba (2012). *Computer crime in BiH: registered 64 applications, seized millions of images (VIDEO)*. Rectrived January 18, 2014, from http://tuzlanski.ba/izdvojeno/89-izdvojeno/3500-kompjuterski-kriminal-u-bih-registrirane-64-prijave-zaplijenjeni-milioni-fotografija-video.html.

Vijesti online (2013). *Cyber crime in Austria worrying harbor*. Rectrived January 18, 2014, from http://www.vijesti.me/svijet/sajber-kriminal-austriji-zabrinjavajucem-porastu-clanak-149230

Ugren, V. (2012). *Cyber kriminal*. Master's thesis, Singidunum University, Department of Postgraduate Studies. Rectrived January 17, 2014, from http://www.singipedia.com/content/3523-Cyber-kriminal