Republika Srpska
Vlada
Ministarstvo unutrašnjih poslova
Uprava za policijsko obrazovanje
Visoka škola unutrašnjih poslova

u saradnji sa

Hans Zajdel fondacijom

ZBORNIK RADOVA

Međunarodna naučnostručna konferencija

SUZBIJANJE KRIMINALA I EVROPSKE INTEGRACIJE, S OSVRTOM NA VISOKOTEHNOLOŠKI KRIMINAL

Laktaši, 28–30. marta 2012. godine

Izdavač
Visoka škola unutrašnjih poslova
Bulevar Živojina Mišića 10A
Banja Luka

Za izdavača
Mr Goran Amidžić

Glavni i odgovorni urednik
Doc.dr Mile Šikman

Tehnički urednik
Božana Đurić

Lektor
Jovanka Borić

Prevodilac
Jelena Vignjević

Tiraž
200 primjeraka

Štampa
Grafomark d.o.o. Laktaši

ISBN 978-99938-43-36-8

SUZBIJANJE KRIMINALA I EVROPSKE INTEGRACIJE, S OSVRTOM NA VISOKOTEHNOLOŠKI KRIMINAL

PROGRAMSKI ODBOR:

Doc. dr Mile Šikman, načelnik Uprave za policijsko obrazovanje, MUP RS, predsjednik
Mr Stevo Ivetić, načelnik Službe ministra, MUP RS
Mr Gojko Vasić, direktor policije, MUP RS
Prof. dr Stanko Stanić, rektor Univerziteta u Banjoj Luci
Prof. dr Vitomir Popović, dekan Pravnog fakulteta u Banjoj Luci
Doc. dr Uroš Pena, Direkcija za koordinaciju policijskih agencija BiH
Prof. dr Duško Vejnović, Visoka škola unutrašnjih poslova Banja Luka

Članovi iz inostranstva

Dr Klaus Fiesinger, Hans Zajdel Fondacija, Predstavništvo za Srbiju i Crnu Goru, Njemačka
Prof. Arkadiusz Letkiewicz, komandant – rektor, Visoka policijska škola, Poljska
Valeri Vjačeslovovič, v.d. rektora, Državni univerzitet unutrašnjih poslova Lavov, Ukrajina
Prof. dr Goran Milošević, dekan Kriminalističko-policijske akademije, Srbija
Prof. PhDr. Jiri Straus, prodekan Policijske akademije, Češka
Prof. dr Janko Jakimov, dekan Fakulteta za bezbednost Skoplje, Makedonija
Domenico Paterna, zamjenik šefa misije EUPM u BiH, Italija

ORGANIZACIONI ODBOR:

Mr Goran Amidžić, direktor Visoke škole unutrašnjih poslova, predsjednik
Vidica Drakulić, Hans Zajdel fondacija, Predstavništvo za Srbiju i Crnu Goru, Srbija
Lutz Kober, Hans Zajdel fondacija, Predstavništvo za Srbiju i Crnu Goru, Njemačka
Zoran Mandić, načelnik Uprave kriminalističke policije MUP RS,
Jovo Marković, načelnik Jedinice za tehničku podršku, MUP RS
Tatjana Telić, načelnik Odjeljenja za međunarodne odnose, MUP RS
Gojko Šetka, viši stručni saradnik za naučnoistraživački rad, VŠUP

RECENZENTSKI ODBOR:

Prof. dr Duško Vejnović, prof. dr Đorđe Đorđević, prof. dr Saša Mijalković, prof. dr Dane Subošić, prof. dr Braco Kovačević, prof. dr Mile Matijević, prof. dr Ljiljana Mašković, doc. dr Mile Šikman, doc. dr Uroš Pena, doc. dr Goran Bošković, doc. dr Miodrag Romić, mr Goran Amidžić, mr Stevo Ivetić, mr Gojko Vasić, mr Radomir Domuzin, mr Želimir Škrbić, mr Borislav Šarić, mr Milimir Govedarica, mr Gojko Šetka

PREDGOVOR

Ministarstvo unutrašnjih poslova Republike Srpske, odnosno Visoka škola unutrašnjih poslova Banja Luka je u saradnji sa *Hans Zajdel fondacijom* organizovala savjetovanje – naučnostručni skup pod nazivom „Suzbijanje kriminala i evropske integracije, s osvrtom na visokotehnološki kriminal“. U ovom zborniku je, zahvaljujući prevashodno uspješnosti saradnje poznate njemačke fondacije i Visoke škole unutrašnjih poslova, publikovan najveći broj na skupu prezentovanih radova.

Savjetovanje je imalo za cilj da se u naučnim i stručnim radovima iz oblasti kriminalističkih, policijsko-bezbjednosnih, pravnih i drugih nauka izvrši analiza trenutnog stanja i predlože nove metode suprotstavljanja kriminalu, posebno visokotehnološkom, sa aspekta međunarodnih standarda i pravne regulative.

Dvodnevna konferencija je, pored prezentovanja radova, obuhvatila i veoma bogatu diskusiju, stručnu i naučnu raspravu, iznjedrila prijedloge i iznijela nove dileme u vezi sa cjelokupnom problematikom suprotstavljanja kriminalu, a posebno visokotehnološkom.

Autori ovog predgovora nadaju se da će izdavanje zbornika naučnostručnih radova o suprotstavljanju kriminalu i evropskim integracijama, s osvrtom na visokotehnološki kriminal, doprinijeti upotpunjavanju znanja stečenih u ovoj oblasti i povećanju efikasnosti borbe protiv kriminala, naročito onih koji su svakodnevno profesionalno angažovani na ovim poslovima.

Na kraju, u svojstvu rukovodilaca tima koji je radio na realizaciji ovog savjetovanja, kao i u ime svih aktivnih učesnika savjetovanja, izražavamo posebnu zahvalnost *Hans Zajdel fondaciji,* bez čije podrške savjetovanje ne bi ni moglo biti održano, niti bi ovaj zbornik radova ugledao svjetlo dana.

PROGRAMSKI I ORGANIZACIONI ODBOR

VORWORT

Im Jahr 2001 hat die Hanns- Seidel- Stiftung (HSS) ihre Projektarbeit zur Verwaltungsförderung und zur Institutionenbindung in der damaligen Staatengemeinschaft von Serbien und Montenegro begonnen. Das eigens dafür geschaffene Stiftungsbüro in Belgrad arbeitete von Anfang an mit den verschiedensten Projektpartnern aus dem staatlichen Bereich sowie dem NGO-Sektor bei der Planung und Durchführung von landesweiten Seminaren, Konferenzen und fachspezifischen Beratungseinsätzen in den beiden Ländern zusammen. Die Förderung des demokratischen Umbaus von Verwaltung, Polizei und Justiz als Grundsäulen des Rechtsstaates stellt eine elementare Kernaufgabe in der Tätigkeit der HSS dar.

Bei der Verwirklichung dieser Zielsetzung hat sich die Ausrichtung der Polizei auf die kompromißlose Bekämpfung der Kriminalität als ein wichtiger Schwerpunkt der Stiftungsarbeit herauskristallisiert. Deshalb unterstützt das Belgrader Büro der HSS auch länderübergreifend die Polizeihochschule Banja Luka wie auch andere Bildungs- und Forschungseinrichtungen Bosnien – Herzegowinas bei der Planung und Durchführung von Konferenzen und Seminaren zur Erstellung von gemeinsamen länderübergreifenden Abwehrstrategien gegen die international organisierte Kriminalität sowie gegen terroristische Aktivitäten. Auf Grund der enormen nationalen und überstaatlichen Resonanz auf die Erkenntnisse dieser Tagungen haben sich die Organisatoren entschlossen, die wichtigsten Beiträge und Resultate der durchgeführten Veranstaltung in Form einer Artbeitensammlung zu veröffentlichen. Die Hanns- Seidel- Stiftung ist der Bitte der Projektpartner um Unterstützung bei der Herausgabe dieser Dokumentation sehr gern nachgekommen, weil sie sich davon eine schnelle und umfangreiche Verbreitung sowie eine rasche und zielstrebige Umsetzung der bedeutsamen Ergebnisse der Konferenzen in der polizeilichen Praxis der beteiligten Staaten verspricht. Darüber hinaus geht die HSS davon aus, daß durch die Weitergabe der vorliegenden Publikation auch in weiteren Nachbarländern erhebliche Synergieeffekte bei der Auseinandersetzung mit der international vernetzten Kriminalität und Korruption ausgelöst werden können.

Lutz Kober
Projektleiter der Hanns Seidel Stiftung
für Serbien und Montenegro

UVODNA REČ

Hanns Seidel Fondacija je 2001. godine u tadašnjoj Državnoj zajednici Srbije i Crne Gore započela svoj rad u okviru Projekta usmerenog na unapređenje administracije i izgradnju institucija. Upravo sa tim ciljem je otvorena Kancelarija u Beogradu koja je od samog početka svog rada sarađivala sa najrazličitijim partnerima iz vladinog i nevladinog sektora na planiranju i organizaciji seminara, konferencija i angažovanja eksperata širom čitave teritorije obeju zemalja.

Osnovni i suštinski zadatak Hanns Seidel Fondacije u njenom radu jeste pružanje podrške administraciji, policiji i pravosuđu, kao osnovnim stubovima pravne države, u okviru njihove demokratske transformacije.

Važno težište rada Fondacije prilikom ostvarenja postavljenih ciljeva postala je saradnja sa policijom koja čini velike napore u cilju beskompromisne borbe protiv kriminala. Upravo iz tog razloga Kancelarija Hanns Seidel Fondacije u Beogradu, pored svojih aktivnosti u Srbiji i u Crnoj Gori, podržava i Visoku školu unutrašnjih poslova u Banja Luci kao i druge obrazovne i istraživačke institucije u Bosni i Hercegovini prilikom planiranja i organizovanja konferencija i seminara čiji je cilj uspostavljanje zajedničkih prekograničnih strategija za borbu protiv međunarodnog organizovanog kriminala i terorističkih aktivnosti. S obzirom da saznanja sa ovih stručnih savetovanja nailaze na izuzeno interesovanje kako u zemlji tako i u inostranstvu, organizatori su doneli odluku da najznačajnije stručne radove i rezultate sa održane manifestacije objave u vidu Zbornika radova.

Hanns Seidel Fondacija je vrlo rado izašla u susret molbi svog partnera da mu pruži podršku prilikom izdavanja ove publikacije upravo zato što je mišljenja da će njeno objavljivanje osigurati brzo i sveobuhvatno prenošenje, a samim tim i neposrednu i ciljanu primenu najznačajnih saznanja sa konferencija u policijskoj praksi zemalja koje su učestvovale u njihovom radu.

Pored toga, Hanns Seidel Fondacija polazi od stanovišta da će davanjem na raspolaganje ove publikacije i drugim susednim zemljama, biti ostvareni izuzetni efekti sinergije u okviru suprotstavljanja međunarodnom kriminalu i borbe protiv korupcije.

Luc Kober
rukovodilac Projekta Hanns Seidel Fondacije
za Srbiju i za Crnu Goru

SADRŽAJ

SUZBIJANJE VISOKOTEHNOLOŠKOG KRIMINALA

NORMATIVNE PRETPOSTAVKE ZA SUPROTSTAVLJANJE VISOKOTEHNOLOŠKOM KRIMINALITETU U REPUBLICI SRBIJI I REPUBLICI SRPSKOJ **3**
Dr Mile Šikman
Dr Milan Milošević

VISOKOTEHNOLOŠKI KRIMINAL I KRIVIČNOPRAVNI INSTRUMENTI SUPROTSTAVLJANJA **17**
Akademik prof. dr Stanko Bejatović

BEZBEDNOST I INTERNET **31**
Prof. dr Radomir Milašinović
Prof. dr Saša Mijalković
Mr Goran Amidžić

INTERNET I TERORIZAM **43**
Prof. dr Želimir Kešetović
Mr Marija Blagojević

BORBA PROTIV SAJBER KRIMINALA U EVROPSKOJ UNIJI SA OSVRTOM NA REPUBLIKU SRPSKU **53**
Mr Stevo Ivetić,
Gojko Pavlović, MA

SECURITY-CRIMINALISTIC DIMENSIONS OF CYBER-TERRORIST ATTACKS
БЕЗБЕДНОСНО-КРИМИНАЛИСТИЧКЕ ДИМЕНЗИЈЕ САЈБЕР-ТЕРОРИСТИЧКИХ НАПАДА **65**
Dr. Zlate Dimovski, PhD
Ice Ilijevski, MSc
Kire Babanoski, MSc

STRATEŠKE KONCEPCIJE U SUPROTSTAVLJANJU VISOKOTEHNOLOŠKOM KRIMINALU **79**
prof. dr Goran Bošković
doc. dr Zvonimir Ivanović

ZNAČAJ DIGITALNIH DOKAZA U KRIVIČNOM POSTUPKU 93
Doc. dr Uroš Pena
Dragan Mitrović

IZRADA I UPOTREBA LAŽNIH PLATEŽNIH KARTICA KAO MASOVNI OBLIK KOMPJUTERSKOG KRIMINALA U REPUBLICI MAKEDONIJI 109
Doc. dr Svetlana Nikoloska

PRAVNI I INSTITUCIONALNI OKVIR SUPROTSTAVLJANJA VISOKOTEHNOLOŠKOM KRIMINALITETU U REPUBLICI SRPSKOJ 119
Doc. dr Nevenko Vranješ
Mr Srđan Rajčević, dipl. inž. rač.

EKONOMSKI SAJBER KRIMINAL U SRBIJI – ASPEKT ZAŠTITE INTERNET POTROŠAČA 129
Doc. dr Branislav Radnović
Mr Milena Ilić
Nemanja Radović

ANALIZA FENOMENA KRAĐE IDENTITETA 143
Doc. dr Zvonimir Ivanović,
Mr Sergej Uljanov
Dr Vladimir Urošević

IMPLEMENTACIJA STANDARDA SERIJE ISO/IEC 27000 KAO MJERA SUZBIJANJA VISOKOTEHNOLOŠKOG KRIMINALA 157
Dragan Popović
Dragan Vučanović,
Risto Lazarević

ZAŠTITA WEB APLIKACIJA I PROTOKA PODATAKA UPOTREBOM PKI SISTEMA I SMART KARTICE ZA AUTENTIFIKACIJU KORISNIKA 169
Dragan Popović,
Predrag Nagraisalović,
Aleksandar Krsmanović,
Milanko Topić,
Aleksandar Popović

KOMPJUTERSKI KRIMINALITET 181
Mr Gojko Vasić
Mr Borislav Šarić
Vlado Jovanić

MEĐUNARODNOPRAVNI DOKUMENTI KOJIMA SE UREĐUJE OBLAST VISOKOTEHNOLOŠKOG KRIMINALA..... 193
Dr Miodrag Romić
Nikolina Grbić-Pavlović, mr

VISOKOTEHNOLOŠKI KRIMINAL U REPUBLICI SRPSKOJ 207
spec. Gojko Šetka,
spec. Željko Ratković,

MERE I STRATEGIJE ZAŠTITE INFORMACIONIH SISTEMA OD VISOKOTEHNOLOŠKOG KRIMINALA..... 217
Mr Nenad Putnik
Nevena Gavrić

HOW A CYBERCRIMINAL DOES LOOK LIKE? BUILDING A PROFILE OF MODERN CRIMINALS..... 227
Stanojoska Angelina, MA
Petrevski Blagojce
Nikolova Kristina

DESIGNING CLASSROOM ACTIVITIES FOR TEACHING CYBER CRIME TO STUDENTS OF ENGLISH FOR LAW ENFORCEMENT 237
Vesna Trajkovska, MA
Radomir Trajkovic, BA

MJESTO I ULOGA PRIKRIVENOG ISTRAŽITELJA U SPREČAVANJU I SUZBIJANJU KRIVIČNIH DJELA IZ OBLASTI VISOKOTEHNOLOŠKOG KRIMINALITETA 249
Svjetlana Dragović
Dragana Milijević
Dražen Višnjić

KRIMINOGENI ASPEKT DRUŠTVENIH MREŽA 257
Aleksandar Miladinović
Vitomir Petričević

INTERNATIONAL ORGANIZATIONS LEGAL STANDARDS FOR COMBATING CRIMINAL ACTS OF HIGH TECH CRIME..... 271
Ivana Bodrozic, spec.

INTERNATIONAL COOPERATION IN RESPECT OF COMPUTER-RELATED CRIMES 281
Prof. Anton T. Girginov, PhD

DJEČIJA PORNOGRAFIJA KAO OBLIK NASILJA NAD DJECOM I VISOKOTEHNOLOŠKOG KRIMINALA 293
Mirela Jokić

PROBLEM SAVREMENE DOBI OBLICI KRAĐE I ZLOUPOTREBE IDENTITETA I MJERE PREVENCIJE 303
Slobodanka Milićević
Srđan Vujović

INTERNET U FUNKCIJI TEORIZMA..... 317
Dragan Ranđelović
Mladen Bajagić
Bojana Carević

PRAVNI OKVIR ZA EFIKASNU BORBU PROTIV KOMPJUTERSKOG KRIMINALITETA U REPUBLICI SRPSKOJ 331
Darko Jokić

SUZBIJANJE KRIMINALA I EVROPSKE INTEGRACIJE

SOCIOLOŠKO-DEFENDOLOŠKI ASPEKTI REGIONALIZACIJE I KLEPTOKRATIJA U HODU KA EVROPSKIM INTEGRACIJAMA..... 345
Prof. dr Duško Vejnović

O PREDSTOJEĆOJ REFORMI ZAKONA O KRIVIČNOM POSTUPKU BOSNE I HERCEGOVINE U KONTEKSTU DALJEG POŠTOVANJA EVROPSKIH STANDARDA.....357
Akademik prof. dr Miodrag N. Simović
Mr Marina M. Simović-Nišević

NE/EFIKASNOST AKTUELNOG KRIVIČNOG ZAKONODAVSTVA U SUZBIJANJU KRIMINALITETA, SA POSEBNIM OSVRTOM NA ISTRAGU 369
Prof. dr Mile Matijević
Dragan Mitrović

UNUTRAŠNJA BEZBEDNOST EU I POLICIJSKA SARADNJA U POSTLISABONSKOJ ERI 385
Prof. dr Snežana Nikodinovska-Stefanovska
Ass. mr Marjan Đurovski

SAVREMENI KONCEPT POLICIJSKOG RADA U ZAJEDNICI („COMMUNITY POLICING“) U FUNKCIJI SUZBIJANJA KRIMINALA..... 397
Mr Boban Simić,
Prof. dr Željko Nikač
Mr Marija Blagojević

THE SPECIAL INVESTIGATIVE MEASURES IN THE NEW MACEDONIAN LAW ON CRIMINAL PROCEDURE 409
Katerina Krstevska PhD
Ljupco Todorovski MA

SPECIFIČNOSTI OTKRIVANJA I DOKAZIVANJA KRIVIČNOG DELA TRGOVINE LJUDIMA 423
Mr Dragan Milidragović
Dejan Drobnjak
Mr Nenad Milić

MOVEMENT OF CRIME IN THE REPUBLIC OF MACEDONIA IN THE PERIOD 2001 - 2010, AND THE IMPORTANCE OF THE EUROPEAN INTEGRATION IN FIGHT AGAINST CRIME..... 437
M.A. Stevco Jolakoski

ADEKVATNI KADAR U PODSISTEMU PRIVATNE BEZBEDNOSTI – FAKTOR USPEŠNOG SUZBIJANJA KRIMINALA U R. MAKEDONIJI 449
Mr Borče Petrevski
Mr Aleksandra Dimitrovska

POLICE STRATEGY IN PREVENTIVE ERADICATION OF MODERN ORGANIZED CRIME..... 461
MA Tatjana Gerginova

STRATEGIC ASPECTS OF PREVENTING ILLICIT TRAFFICKING IN SMALL ARMS AND LIGHT WEAPONS..... 471
Ivan Ristov

CRIMINAL LAW AND EUROPEAN STANDARDS WITH THE OVERVIEW OF THE CRIMINAL LAW AND THE CONSTITUTION OF REPUBLIC OF MACEDONIA..... 481
PhD Marjan Arsovski

**PRISONERS'HEALTH CARE:
DEPRIVED OF THEIR LIBERTY
NOT THEIR DIGNITY..... 491**
Marija Milenkovska

PRILOG

CYBERCRIME IN POLAND 505
Jerzy Kosiński, PhD

SUZBIJANJE
VISOKOTEHNOLOŠKOG KRIMINALA

Pregledni rad - UDK 343.326: 004.738.5 (497.11+497.6RS)

NORMATIVNE PRETPOSTAVKE ZA SUPROTSTAVLJANJE VISOKOTEHNOLOŠKOM KRIMINALITETU U REPUBLICI SRBIJI I REPUBLICI SRPSKOJ

Dr Mile Šikman,
Uprava za policijsko obrazovanje, Banja Luka
Dr Milan Milošević,
Fakultet za obrazovanje diplomiranih pravnika i ekonomista za rukovodeće kadrove (FORKUP), Novi Sad

Apstrakt: Visokotehnološki kriminalitet predstavlja posebnu vrstu kriminaliteta koja se manifestuje u različitim formama zloupotreba informacionih tehnologija u kriminalne svrhe. Viskotehnološki kriminalitet može da proizvede daleko teže posledice po privatni i javni interes, jer geografska razdaljina i državne granice ne predstavljaju prepreku za izvršenje krivičnog dela. Dakle, transnacionalna priroda visokotehnološkog kriminaliteta učinila je neophodnim izradu i donošenje posebnih međunarodnih pravnih instrumenata kojima bi bila uređena oblast suprotstavljanja ovoj vrsti kriminalnog delovanja. Prepoznajući potrebu saradnje između država u borbi protiv visokotehnološkog kriminaliteta i potrebu zaštite legitimnih interesa u korišćenju i razvoju informacione tehnologije, u radu je analiziran katalog inkriminacija kojima se u Republici Srbiji i Republici Srpskoj suzbijaju takvi oblici kriminaliteta, kao i tekuće reforme specijalizovanih državnih organa u izmenjenom legislativnom i društvenom okruženju Republike Srbije i Republike Srpske. Takođe, ukazano je i na neke od postojećih i predstojećih problema u vezi sa otkrivanjem i procesuiranjem krivičnih dela visokotehnološkog kriminaliteta. U radu su navedene teme obrađene na način da je dat komparativni prikaz institucionalnog i krivičnopravog (materijalnog i procesnog) tretiranja problematike suzbijanja visokotehnološkog kriminaliteta u Republici Srbiji i Republici Srpskoj.

Ključne reči: Krivično pravo, Savet Evrope, visokotehnološki kriminal, policija, Republika Srbija, Republika Srpska.

MEDJUNARODNE OSNOVE SUPROTSTAVLJANJA VISOKOTEHNOLOŠKOM KRIMINALITETU

Razvojem informacijskih i komunikacijskih tehnologija nastaju mogućnosti za nove oblike kriminaliteta tako što se kriminalcima daju novi instrumenti za izvršenje starih vrsta kriminaliteta, kao i sredstva i tržišta za nove pojavne oblike kriminaliteta. Zbog toga je visokotehnološki kriminalitet sve zastupljeniji, dobija nove forme i predstavlja sve veću opasnost, naročito kroz oblike transnacionalnog kriminalnog delovanja, jer upravo informaciona tehnologija u potpunosti odgovara ostvarivanju kriminalnih ciljeva na transnacionalnom nivou (Šikman, 2011). Ta nova tehnologija može uticati i na strukturu kriminalnih organizacija i upravljanje preduzećima koja se bave kriminalom, pri čemu društva i preduzeća sa naprednom

ICT prate logiku mreže, a ne onu jasnih hijerarhija, a to važi i za organizovane kriminalne grupe koje pokazuju mrežni tip strukture (Castells, 2003: 21). U Republici Srbiji i Republici Srpskoj visokotehnološki kriminalitet je u nivou sa informatizacijom društva, odnosno sa stepenom rasprostranjenosti informacionih tehnologija, ali i međunarodnim refleksijama ove vrste kriminaliteta.

U benefite evropskih integracija svakako spadaju i inicijative za stvaranje pravnih pretpostavki za suzbijanje visokotehnološkog kriminaliteta udruženim naporima više zemalja. Reč je o nizu međunarodnih ugovora od esencijalnog značaja za borbu protiv ovog vida prekograničnog (transnacionalnog) kriminala. Između ostalih, ovde spadaju preporuke Saveta Evrope o kriminalitetu vezanom za kompjutere iz 1989. godine (Recommendationns No. R(89) i o sagledavanju problema u krivičnom procesnom pravu vezanom za informacionu tehnologiju iz 1995. godine (Recommendationns No. R(95), zatim Direktiva Evropske unije za zaštitu kompjuterskih programa iz 1991. godine, Akcioni plan Evropske unije o promovisanju bezbednije upotrebe interneta iz 1999. godine, itd.

Sa aspekta institucionalnog okvira za suprotstavljanje kriminalu koji se vrši putem visokih tehnologija, najvažniji međunarodni dokument predstavlja Konvencija Saveta Evrope o visokotehnološkom kriminalu[1], koja je potpisana u Budimpešti 23. novembra 2001. godine, odnosno Dodatni protokol uz ovu Konvenciju, koji se odnosi na inkriminaciju dela rasističke i ksenofobične prirode izvršenih preko kompjuterskih sistema, a sačinjen je u Strazburu 28. januara 2005. godine. Usvajanje ovih dokumenata rezultat je inicijative Saveta Evrope, koja je formalno pokrenuta 1996. godine osnivanjem Komiteta stručnjaka za kriminal u sajber prostoru. Zadatak ovog Komiteta bila je analiza krivičnih dela koja se mogu izvršiti putem telekomunikacionih mreža, prvenstveno Interneta, da bi se na osnovu nalaza sačinio nacrt međunarodne konvencije. Za krivična dela koja spadaju pod okrilje visokotehnološkog kriminaliteta, a koja za cilj imaju namerno i neovlašteno uzrokovanje štete na imovini drugoga, smatraju se dela činjena: a) bilo kakvim unošenjem, menjanjem, brisanjem ili činjenjem neupotrebljivima kompjuterskih podataka, b) bilo kakvim ometanjem funkcionisanja kompjuterskog sistema, v) s prevarnom ili nepoštenom namerom neovlaštenog pribavljanja ekonomske koristi za sebe ili drugoga. Tako, u drugom poglavlju, određena su sledeća krivična dela: krivična dela protiv poverljivosti, integriteta, i dostupnosti kompjuterskih podataka i sistema (nedozvoljen pristup, nedozvoljeno presretanje, ometanje podataka, ometanje sistema i zloupotreba uređaja), krivična dela u vezi sa kompjuterima (falsifikovanje koje je u vezi sa kompjuterima, prevare koje su u vezi sa kompjuterima), krivična dela u odnosu na sadržaj (krivična dela vezana za dečiju pornografiju i krivična dela koja se odnose na kršenje autorskih i njima sličnih prava). Glavni ciljevi Konvencije jesu da pruži smernice za: 1. usklađivanje nacionalnih krivičnih zakonodavstava u pogledu elemenata krivičnih dela u oblasti informatičkog kriminala; 2. usklađivanje nacionalnih propisa o krivičnom postupku radi definisanja ovlašćenja nadležnih državnih organa neophodnih za sprovođenje istrage i krivični progon počinilaca dela informatičkog kriminala; 3. ustanovljavanje brzog i efikasnog mehanizma međunarodne saradnje u ovoj

[1] Convention on Cybercrime, CETS No.: 185 (http://conventions.coe.int/Treaty /Commun/QueVoulezVous.asp?NT=185&CM=8&DF=11/13/2007&CL=ENG)

oblasti. Najbitniji deo Konvencije o visokotehnološkom kriminalu posvećen je obavezama evropskih država da stvore normativne pretpostavke za uvođenje dodatnih procedura i ovlašćenja, kako bi se omogućilo efikasno otkrivanje i procesuiranje slučajeva visokotehnološkog kriminala. Esencijalni značaj, u tom smislu, ima formiranje posebnih državnih organa specijalizovanih za takvu borbu. Specijalizacija državnih organa na ovom planu inače je neophodna ako se imaju u vidu specifičnosti visokotehničkog kriminala, kao i stalni razvoj tehnologije koji je potrebno pratiti radi njegovog otkrivanja i suzbijanja. Naime, otkrivanje, krivično gonjenje i suđenje za ova dela zahteva obrazovanje posebnih organizacionih jedinica postojećih državnih organa, čije bi delovanje na planu prevencije i, pogotovu, represije u budućnosti trebalo da doprinese boljoj zaštiti prava intelektualne svojine i da unapredi ambijent za investicije i poslovanje privrednih subjekata.

Prepoznajući potrebu saradnje između država i privatnih privrednih subjekata u borbi protiv visokotehnološkog kriminala i potrebu zaštite legitimnih interesa u korišćenju i razvoju informacione tehnologije, zakonodavni organi u Republici Srbiji i Republici Srpskoj usvojili su i novelirali više propisa kojima se u pravni sistem implementiraju pomenuta Konvencija sa Dodatnim protokolom i drugi dokumenti o visokotehnološkom kriminalu.

INSTITUCIONALNI OKVIR SUPROTSTAVLJANJA VISOKOTEHNOLOŠKOM KRIMINALU U REPUBLICI SRBIJI I REPUBLICI SRPSKOJ

Sa aspekta efikasnog suprotstavljanja visokotehnološkom kriminalitetu, u zakonskom tekstu mora se izgraditi što potpuniji krivičnoprocesni sistem reakcije na ovaj oblik kriminaliteta, koji odgovara i međunarodno prihvaćenim standardima. Naime, visokotehnološki kriminalitet kao transnacionalni društveni fenomen dovodi u pitanje osnovne vrednosti u najvećem broju savremenih država. Takođe, kriminalne aktivnosti koje su izražene kroz visokotehnološki kriminalitet teže se sprečavaju i otkrivaju, iako su istovremeno naglašeni zahtevi za efikasno preventivno i represivno delovanje organa krivičnog pravosuđa. Pored toga, krivičnopravnu reakciju na ova protivpravna ponašanja iz oblasti visokotehnološkog kriminaliteta prate i zahtevi za njeno postavljanje u okvire pravne države i vladavine prava. Isto tako, krivičnoprocesno suprotstavljanje visokotehnološkom kriminalitetu podrazumeva i međunarodnu saradnju na planu borbe protiv organizovanog kriminaliteta. U tom kontekstu ključna stvar je razmena informacija između subjekata suprotstavljanja kriminalitetu na međunarodnom nivou, prikupljanje i razmena dokaznih materijala, kao i sprovođenje zajedničkih istraga agencija za sprovođenje zakona različitih zemalja. Krivičnoprocesno suprotstavljanje visokotehnološkom kriminalitetu, zapravo, predstavlja predviđanje posebnih procesnih pravila, a time i posebnih institucija (pre svega specijalizovanih) i metoda otkrivanja i istrage krivičnih dela visokotehnološkog kriminaliteta, s ciljem da se na efikasan način dođe do dokaznih materijala za otkrivanje, rasvetljavanje i presuđivanje konkretne krivične stvari visokotehnološkog kriminaliteta (Šikman, 2007).

Institucionalni okvir suprotstavljanja visokotehnološkom kriminalu u Republici Srbiji – Prema konkretnim rešenjima iz Zakona o javnom tuži-

laštvu i Zakona o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala, za krivično gonjenje kod svih krivičnih dela izvršenih putem visokih tehnologija nadležno je isključivo *Više javno tužilaštvo u Beogradu*. Iz toga se zaključuje da, uprkos koncentrovanoj stvarnoj i mesnoj nadležnosti, krivično gonjenje u ovakvim predmetima vrši tužilaštvo opšte nadležnosti.[2] S druge strane, u okviru Višeg javnog tužilaštva u Beogradu formirano je Posebno odeljenje za borbu protiv visokotehnološkog kriminala („Posebno tužilaštvo"), koje čine: posebni tužilac za visokotehnološki kriminal, zamenici tužioca, portparol, sekretar i ostalo tužilačko osoblje. Po zakonu, ali i po samoj prirodi stvari, prednost prilikom postavljenja imaju oni zamenici tužioca koji poseduju posebna znanja iz oblasti informatičkih i radiodifuznih tehnologija[3]. Sva prvostepena suđenja po odgovarajućim predmetima ovog tipa u nadležnosti su *Odeljenja za borbu protiv visokotehološkog kriminala Višeg suda u Beogradu*. Za odlučivanje po pravnim lekovima (u drugom stepenu) za dela visokotehnološkog kriminala nadležan je *Apelacioni sud* u Beogradu. Predsednik Višeg suda u Beogradu raspoređuje sudije u Odeljenje za borbu protiv visokotehološkog kriminala iz reda sudija datog suda, uz njihovu saglasnost. Pri tome, prednost imaju sudije koje poseduju posebna znanja iz oblasti informatičkih tehnologija. Osim toga, predsednik Višeg suda u Beogradu može u Odeljenje rasporediti i sudije drugih sudova upućenih na rad u taj sud, uz njihovu saglasnost. U svakom slučaju, raspoređivanje traje najduže dve godine, a može biti i produženo odlukom predsednika Višeg suda u Beogradu, takođe uz pismenu saglasnost raspoređenog lica. Saglasno potrebnim kompetencijama i potrebama specijalizacije, prednost u raspoređivanju konkretnih sudija u Odeljenje imaju nosioci sudijskih funkcija koji imaju iskustva u borbi protiv visokotehnološkog kriminala.[4] Po prirodi stvari, takve bi trebalo da budu i one sudije koje su uključene u PACO program. Poznato je, naime, da je Projekat za borbu protiv ekonomskog kriminala u Republici Srbiji (PACO Serbia) započet tokom decembra 2005. godine, a bavi se edukacijom iz oblasti zloupotrebe informatičkih tehnologija u kriminalne svrhe. Sprovodi ga Savet Evrope, finansira Evropska unija, a realizuje Evropska agencija za rekonstrukciju.

Na planu obezbeđenja relevantnih dokaza za dela kompjuterskog kriminala i elektronskog piratstva deluje specijalizovana policijska *Služba za*

---

[2] Prema Zakonu o javnom tužilaštvu, u Republici Srbiji deluju javna tužilaštva opšte nadležnosti i javna tužilaštva posebne nadležnosti – u koje spadaju Tužilaštvo za organiozovani kriminal i Tužilaštvo za ratne zločine.

[3] Posebnog tužioca postavlja republički javni tužilac iz redova zamenika tužilaca, koji ispunjavaju uslov da budu zamenici višeg javnog tužioca, a uz pismenu saglasnost lica koje će biti postavljeno. Posebni tužilac se postavlja na period od četiri godine i može biti ponovo postavljen, ali ga republički javni tužilac može razrešiti i pre isteka vremena na koje je postavljen. Pre postavljenja posebnog tužioca, republički javni tužilac donosi rešenje o upućivanju datog lica u Posebno tužilaštvo, s tim što se po prestanku funkcije posebni tužilac vraća na funkciju koju je vršio pre postavljenja. Prema oficijelnim podacima, od osnivanja početkom 2006. godine, zaključno sa 1. oktobrom 2011 godine, Posebno tužilaštvo za visokotehnološki kriminal je postupalo ili postupa u preko 1.700 predmeta u okviru svoje nadležnosti.

[4] Najčešći oblik visokotehnološkog kriminala u Srbiji je neovlašćeno korišćenje intelektualne svojine, takozvana piraterija, kao i falsifikovanje i zloupotreba platnih kartica, neovlašćeni pristup zaštićenoj računarskoj mreži i elektronskoj obradi podataka, računarska sabotaža, razne vrste računarskih prevara, ali i širenje rasne, verske i nacionalne mržnje pomoću interneta i internet pornografija.

borbu protiv visokotehnološkog kriminala („Služba“). U stvari, ona je formirana kao Odeljenje za borbu protiv visokotehnološkog kriminala u okviru Službe za borbu protiv organizovanog kriminala (SBPOK). To znači da je „Služba“ sistematizovana u Upravi kriminalističke policije Direkcije policije, tj. u sedištu Ministarstva unutrašnjih poslova. U organizacionom smislu, Odeljenje za borbu protiv visokotehnološkog kriminala čini više organizacionih jedinica, među kojima je i Odsek za suzbijanje kriminaliteta u oblasti intelektualne svojine. Saglasno tome, starešinu „Službe“ postavlja i razrešava ministar unutrašnjih poslova po pribavljenom mišljenju posebnog tužioca. Isto tako, zakonom je predviđena obaveza ministara unutrašnjih poslova da bliže uredi rad Odeljenja za borbu protiv visokotehnološkog kriminala odgovarajućim podzakonskim aktom, a u skladu sa Zakonom o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala. Odeljenje za borbu protiv visokotehnološkog kriminala je po prirodi stvari upućeno na saradnju sa drugim organizacionim celinama Službe za suzbijanje organizovanog kriminala, posebno sa Odsekom za prikupljanje i obradu digitalnih dokaza u okviru Službe za specijalne istražne metode, ali i sa ostalim organizacionim jedinicama Uprave kriminalističke policije u Direkciji policije, na primer sa Odsekom za suzbijanje privrednog kriminala u oblasti privrednog poslovanja i intelektualnu svojinu. Isto važi i za odgovarajuću saradnju sa službama bezbednosti u Srbiji (BIA, VBA), ali i za odgovarajuću saradnju sa pojedinim službama stranih zemalja kojima je u nadležnost stavljeno otkrivanje, praćenje i dokumentovanje krivičnih dela protiv intelektualne svojine, imovine i pravnog saobraćaja. Takva je, na primer, britanska služba za suzbijanje organizovanog kriminala (SOCA), u okviru koje deluje Nacionalna jedinica za borbu protiv visokotehnološkog kriminala (NHTCU) sa sedištem u Londonu.[5] U međuvremenu je Odeljenje za borbu protiv visokotehnološkog kriminala razvijalo svestranu saradnju i sa Nacionalnim centralnim biroom Interpola Beograd, budući da visokotehnološki kriminal predstavlja jedan od najčešće korišćenih oblika prekograničnog (transnacionalnog) kriminala. Ovo utoliko pre što je mesto za kontakte koje je dostupno 24 sata svakog dana u nedelji („punkt 24/7“), trenutno locirano u okviru pomenutog Nacionalnog centralnog biroa.

Institucionalni okvir suprotstavljanja visokotehnološkom kriminalu u Republici Srpskoj – U Republici Srpskoj nije izvršena posebna specijalizacija za suzbijanje visokotehnološkog kriminaliteta na nivou tužilaštava i sudova, već samo unutar Ministarstva unutrašnjih poslova Republike Srpske. U tom kontekstu procesuiranje krivičnih djela visokotehnološkog kriminaliteta usmjereno je prema okružnim tužilaštvima i okružnim sudovima, uključujući i Specijalno tužilaštvo, kao i Posebno tužilaštvo za suzbijanje organizovanog i najtežih oblika privrednog kriminala pri Okružnom tužilaštvu Banja Luka. S tim u vezi, stvarno nadležni za postupanje u krivičnim predmetima visokotehnološkog kriminaliteta jesu Okružni

[5] Ovu oblast inače karakteriše intenzivna međunarodna operativna saradnja. Tako je na osnovu podataka srpske policije u Velikoj Britaniji uhapšeno više lica zbog distribucije maloletničke pornografije putem Interneta. Zatim, u sklopu akcije na suzbijanju pornografske zloupotrebe dece na Internetu dostavljeni su podaci britanskoj policiji za više od 50 lica. Takođe, po zahtevu Interpola Nemačke, 2010. godine su lišena slobode dva lica koja su na internetu postavljala scene seksualnog zlostavljanja dece.

sud u Banjoj Luci[6], Okružni sud u Doboju, Okružni sud u Bijeljini, Okružni sud u Istočnom Sarajevu i Okružni sud u Trebinju. Budući da se okružna tužilaštva osnivaju za područje okružnih sudova, nadležnost za sprovođenje istražnih radnji i gonjenje potencijalnih učinilaca krivičnih dela visokotehnološkog kriminaliteta data je Okružnom tužilaštvu Banja Luka, Okružnom tužilaštvu u Doboju, Orkužnom tužilaštvu u Bijeljini, Okružnom tužilaštvu u Istočnom Sarajevu i Orkužnom tužilaštvu u Trebinju. Kao što smo naveli, određene nadležnosti za postupanje u slučajevima visokotehnološkog kriminaliteta ima i Specijalno tužilaštvo, i to u onim slučajevima kada se radi o organizovanim oblicima visokotehnološkog kriminaliteta. Naime, Zakon o suzbijanju organizovanog i najtežih oblika privrednog kriminaliteta[7], kao *lex specialis,* donosi se u cilju efikasnog suzbijanja organizovanog i najtežih oblika privrednog kriminaliteta. Njime se uređuju osnivanje, organizacija, nadležnost i ovlašćenja posebnih organizacionih jedinca tužilaštva i suda, te drugih državnih organa u Republici Srpskoj, te se uređuju drugi uslovi radi efikasnog otkrivanja i krivičnog gonjenja učinilaca krivičnih dela određenih ovim zakonom. Tako, u Okružnom tužilaštvu Banja Luka, osniva se Posebno tužilaštvo za suzbijanje organizovanog i najtežih oblika privrednog kriminala, koje se naziva Specijalno tužilaštvo, i koje postupa u predmetima: a) krivičnih dela organizovanog kriminala iz člana 383a. Krivičnog zakona Republike Srpske, zatim, krivičnih dela sa elementima organizovanosti, kao i krivičnih dela povezanih sa takvim delima ili učiniocima takvih dela, a u slučajevima kada za postupanje nije nadležno Tužilaštvo i Sud Bosne i Hercegovine; b) najtežih oblika krivičnih dela protiv privrede i platnog prometa i protiv službene dužnosti, kada je zbog okolnosti izvršenja dela ili posledica dela krivično gonjenje od posebnog značaja za Republiku Srpsku, te krivičnih dela povezanih sa takvim delima ili učiniocima takvih dela; v) drugih krivičnih dela predviđenih krivičnim zakonodavstvom Republike Srpske, kod kojih je najmanja zaprećena kazna zatvora u trajanju od pet godina, a kada je zbog okolnosti izvršenja dela ili posledica dela krivično gonjenje od posebnog značaja za Republiku Srpsku, te krivičnih dela povezanih s takvim delima ili učiniocima takvih dela[8]. Specijalno tužilaštvo ima nadležnost na čitavoj teritoriji Republike Srpske, te

---

[6] Na primjer: Protiv C.G., A.D. G.L. (rumunski državljani) podignuta je optužnica u Okružnom tužilaštvu Banja Luka br. T13 0 KT 0001138 10. da su u vremenskom periodu od 27.02.2010. do 02.03.2010. godine u Prijedoru, Banja Luci, Doboju, Čelincu i Zvorniku, na bankomatima Balkan Investmen banke upotrijebili falsifikovane platne kartice izdavaoca VISA i MasterCard koje su prethodno napravili na taj način što su uz pomoć tehničkog pomagala tzv. "skimera" koji su stavljali na bankomate očitavali i neovlašteno prikupljali podatke sa originalnih platnih kartica, dok su podatke o PIN brojevima (lični identifikacioni broj koji korisnik ukucava na tastaturi bankomata prilikom podizanja novca) pribavljali uz pomoć kamere postavljene na bankomat tako da snima tastaturu bankomata u trenutku kada korisnik unosi PIN, nakon čega su uz pomoć računara sve prikupljene podatke prenosili na magnetnu pistu plastika koje se koriste u druge svrhe i nemaju elemente platnih kartica, a svi naprijed navedeni podaci o pomoćnim tehničkim sredstvima za neovlašteno očitavanje podataka sa platnih kartica i programi koji se koriste za upis podataka na kartice su bili pohranjeni na USB stiku, oštetivši Balkan Investment banku za iznos od 41.002,12 KM. Osuđeni kod Okružnog suda u Banjoj Luci nepravosnažnom presudom na kazne zatvora 10 mjeseci, 1 godina i 1 godina i tri mjeseca i oduzeta imovinska korist.

[7] Zakon o suzbijanju organizovanog i teških oblika privrednog kriminala – prečišćeni tekst, Službeni glasnik Repblike Srpske, broj 112/07.

[8] Specijalno tužilaštvo može preuzeti predmete drugih tužilaštava na osnovu odluke o preuzimanju predmeta koja se donosi u formi naredbe, što je detaljno regulisano trećim poglavljem, čl. 12–15 navedenog zakona.

je samostalno i nezavisno u svom radu. Specijalno tužilaštvo čine: glavni specijalni tužilac, zamenik glavnog specijalnog tužioca i onoliko specijalnih tužilaca koliko odredi Visoki sudski i tužilački savet Bosne i Hercegovine, na preporuku glavnog specijalnog tužioca i glavnog republičkog tužioca[9]. Pored Specijalnog tužilaštva u okviru Okružnog suda u Banjoj Luci, formira se Posebno odeljenje za organizovani i najteže oblike privrednog kriminala. Posebno odeljenje nadležno je na čitavoj teritoriji Republike Srpske za postupanje u gore navedenim slučajevima, bez obzira na propisanu kaznu za pojedino krivično delo, odnosno u svim slučajevima kada je od glavnog specijalnog tužioca doneta odluka o preuzimanju predmeta. Radom Posebnog odeljenja rukovodi predsednik Posebnog odeljenja za organizovani i najteže oblike privrednog kriminala[10].

Već smo navedi da je Ministarstvu unutrašnjnih poslova Republike Srpske izvršena specijalizacija za suzbijanje visokotehnološkog kriminaliteta, i to formiranjem Odjeljenja za sprečavanje visokotehnološkog kriminaliteta. Odjeljenje za sprečavanje visokotehnološkog kriminaliteta je oformljeno 1. 1. 2010. godine i nalazi se u sklopu Jedinice za operativnu i tehničku podršku unutar Uprave kriminalističke policije Ministarstva unutrašnjih poslova Republike Srpske. Naime, Ministarstvo unutrašnjih poslova Republike Srpske ima nadležnosti propisane Zakonom o unutrašnjim poslovima Republike Srpske.[11] Ministarstvo je organizovano kroz rad pet centara javne bezbednosti koji su direktno povezani sa sedištem Ministarstva. U funkcionalnom smislu, Ministarstvo sačinjava šest uprava, od kojih je jedna Uprava kriminalističke policije. Rad Uprave kriminalističke policije usmeren je, pored ostalog, na suzbijanje visokotehnološkog kriminaliteta, suzbijanje proizvodnje i prometa opojnih droga, privredni kriminalitet i korupciju, krađe motornih vozila, kao i dela iz domena opšteg kriminaliteta. Uprava kriminalističke policije vrši obradu najsloženijih krivičnih dela, vrši poslove kontrole, nadzora i instruktivnog usmeravanja rada svih organizacionih jedinica i jedinica za podršku kriminalističke policije na poslovima suzbijanja i otkrivanja krivičnih dela u oblasti ekonomskog kriminaliteta, organizovanog i teškog kriminaliteta, opšteg kriminaliteta, neovlaštene proizvodnje i prometa opojnih droga, uz podršku kriminalističko-obaveštajnih analiza, kriminalističkotehničkih metoda i sredstava, posebnih operativnih poslova i potraga, vrši nadzor nad zakonitosti rada organizacionih jedinica i jedinica za podršku na poslovima suzbijanja i otkrivanja krivičnih dela, pronalaženja i hvatanja izvršilaca krivičnih dela i obezbeđenja potrebnih dokaza za uspešno vođenje krivičnog postupka, i druge mere i radnje predviđene zakonom. Odjeljenje za sprečavanje visokotehnološkog kriminaliteta je

---

[9] Radom Specijalnog tužilaštva rukovodi i predstavlja ga glavni specijalni tužilac, kojeg na dužnost imenuje Visoki sudski i tužilački savjet Bosne i Hercegovine, u trajanju od 5 (pet) godina, uz mogućnost ponovnog raspoređivanja. Pored glavnog specijalnog tužioca, Visoki sudski i tužilački savet Bosne i Hercegovine na dužnost imenuje i zamenika glavnog specijalnog tužioca i specijalne tužioce. U Specijalno tužilaštvo imenuje se određen broj stručnih saradnika, tužilačkih istražilaca, te ostalog pratećeg osoblja.

[10] Predsednika i sudije Posebnog odeljenja raspoređuje predsednik Okružnog suda Banja Luka iz reda sudija tog suda. U slučaju potrebe, u Posebno odeljenje Visoki sudski i tužilački savet BiH može imenovati sudije iz drugih sudova u Bosni i Hercegovini. U hitnim slučajevima, Visoki sudski i tužilački savet BiH može privremeno uputiti i sudije iz drugih sudova u Posebno odeljenje, u skladu sa svojim nadležnostima. Sudije Posebnog odeljenja dužnost obavljaju bez ograničenja trajanja mandata, imaju potreban broj stručnih saradnika, te pratećeg osoblja.

[11] Zakon o unutrašnjim poslovima RS, Službeni glasnik Republike Srpske, broj: 4/12.

oformljeno sa ciljem efikasnijeg otkrivanja i krivičnog gonjenja počinilaca krivičnih dela visokotehnološkog kriminala na teritoriji Republike Srpske. U sprečavanju visokotehnološkog kriminaliteta koriste se specijalne metode za izvođenje istražnih radnji kada ne postoje drugi načini za prikupljanje dokaza, čime se stvaraju uslovi za njihovu primenu u skladu sa Zakonom o krivičnom postupku RS, a protiv lica za koja postoje osnovi sumnje da učestvuju u izvršenju krivičnih dela predviđenih Krivičnim zakonom RS. Odjeljenje za sprečavanje visokotehnološkog kriminaliteta do sada se istaklo čitavim nizom aktivnosti, uključujući ne samo poslove suzbijanja visokotehnološkog kriminaliteta, već i čitavim nizom preventivnih radnji. Jedna od njih je i pokretanje internet prezentacije (http://www.mup.vladars.net/vtk/index.html) putem koje predstavlja sve informacije iz oblasti visokotehnološkog kriminala u Republici Srpskoj, najnovije oblike izvršenja krivičnih dela iz oblasti tzv. "Cyber" kriminala, kao i korisne savete u cilju prevencije eventualne štete koja bi proistekla iz izvršavanja krivičnih dela.

INKRIMINACIJE KAO INDIKATORI VISOKOTEHNOLOŠKOG KRIMINALA U REPUBLICI SRBIJI I REPUBLICI SRPSKOJ

Visokotehnološki kriminal se u multilateralnim međunarodnom ugovorima shvata kao pojam i u užem i u širem smislu. Tako se, na primer, u oficijelnim dokumentima Ujedinjenih Nacija pod visokotehnološkim kriminalom u užem smislu (Cyber Crime) podrazumeva „svako nezakonito ponašanje usmereno na elektronske operacije sigurnosti kompjuterskih sistema i podataka koji se u njima obrađuju", dok se u širem smislu podrazumeva „svako nezakonito ponašanje vezano za ili u odnosu na kompjuterski sistem i mrežu, uključujući i takav kriminal kakvo je ilegalno posedovanje, nuđenje i distribuiranje informacija preko kompjuterskih sistema i mreža". (Stephson, 2000). Po međunarodnom pravu, dakle, pojmom visokotehnološkog kriminala obuhvata se širok spektar kriminalnih zloupotreba informacionih i radiodifuznih tehnologija, a posebno krivična dela protivpravnog korišćenja interneta (Netcrime) i dela kod kojih su računari sredstvo, odnosno objekt izvršenja. Dakle, visokotehnološki kriminalitet predstavlja oblik kriminalnog ponašanja kod koga se korištenje kompjuterske tehnologije i informacionog sistema ispoljava kao način izvršenja krivičnog dela ili se kompjuter upotrebljava kao sredstvo ili cilj izvršenja, čime se ostvaruje neka, u krivičnopravnom smislu, relevantna posledica. On predstavlja protupravnu povredu imovine kod koje se računarski podaci umišljajno menjaju (manipulacija računarom), razaraju (računska sabotaža) ili se koriste zajedno sa hardverom (krađa vremena).

Inkriminacije kao indikatori visokotehnološkog kriminala u Republici Srbiji – Polazeći od svega što je do sada izneto, a na osnovu sistemske analize aktuelnog zakonodavstva, sa sigurnošću se može zaključiti da u kategoriju visokotehnološkog kriminala u Republici Srbiji spada veći broj krivičnih dela koja se mogu grupisati na sledeći način:

(1) bezuslovno sva dela koja za grupni zaštitni objekat imaju bezbednost računarskih podataka, tj. delikti iz glave XXVII KZ,

(2) delikti protiv intelektualne svojine, imovine, privrede i pravnog saobraćaja kod kojih se kao objekat ili sredstvo izvršenja javljaju računari,

računarske mreže, računarski podaci, kao i njihovi proizvodi u materijalnom ili elektronskom obliku – ako broj autorskih primeraka prelazi 2.000 ili ako nastala materijalna šteta prelazi iznos od 1.000.000 dinara, i

(3) delikti protiv sloboda i prava čoveka i građanina, polne slobode, javnog reda i mira i ustavnog uređenja i bezbednosti Republike Srbije, za koje se zbog načina izvršenja ili upotrebljenih sredstava sa sigurnošću može zaključiti da su dela visokotehnološkog kriminala, u skladu sa članom 2. stav 1. Zakona o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala.[12]

Kao primer u navedenom smislu može se apostrofirati delatnost organizovane kriminalne grupe u javnosti označene kao „drumska mafija", koju su činili radnici naplate putarine i preduzeća koje se bavi kompjuterskim tehnologijama. Oni su izradili specijalan hardverski uređaj i softver kojim su prikrivali naplatu putarine duž auto-puta (dnevno, u proseku, 300–350 vozila stranih i domaćih registarskih oznaka), čime je, prema nekim podacima, Republika Srbija oštećena za preko 700 miliona dinara. Zbog toga je u postupku rasvetljavanja dela lišeno slobode više desetina lica, protiv kojih su podnete krivične prijave nadležnom tužilaštvu.[13] Prema tome, u karakteristične indikatore visokotehnološkog kriminala u Republici Srbiji se mogu svrstati sledeće inkriminacije iz glave XVIII KZ (krivična dela protiv polne slobode), iz glave XX KZ (krivična dela protiv intelektualne svojine), XXI (krivična dela protiv imovine), iz glave XXII KZ (krivična dela protiv privrede) i iz glave XXVII KZ (krivična dela protiv bezbednosti računarskih podataka): Prikazivanje, pribavljanje i posedovanje pornografskog materijala i iskorišćavanje dece za pornografiju – čl. 185 st. 3, glava XVIII KZ; povreda moralnih prava autora i interpretatora – čl. 198, glava XX KZ; neovlašćeno iskorišćavanje autorskog dela ili predmeta srodnog prava – čl. 199, glava XX KZ; neovlašćeno uklanjanje ili menjanje elektronske informacije o autorskim i srodnim pravima – čl. 200, glava XX KZ; povreda pronalazačkog prava – čl. 201, glava XX KZ; neovlašćeno korišćenje tuđeg dizajna – čl. 202, glava XX KZ; falsifikovanje i zloupotreba platnih kartica – čl. 225, glava XXI KZ; pravljenje, nabavljanje i davanje drugom sredstva za falsifikovanje – čl. 227 st. 2, glava XXI KZ; neovlašćena upotreba tuđeg poslovnog imena i druge posebne oznake robe ili usluga – čl. 233, glava XXII KZ; odavanje poslovne tajne – čl. 240, glava XXII KZ; oštećenje računarskih podataka i programa – čl. 298, glava XXVII KZ; računarska sabotaža – čl. 299, glava XXVII KZ; pravljenje i unošenje računarskih virusa – čl. 300, glava XXVII KZ; računarska prevara – čl. 301, glava XXVII KZ; neovlašćeni pristup zaštićenom računaru, računarskoj mreži i elektronskoj obradi podataka – čl. 302, glava XXVII KZ; sprečavanje i ograničavanje pristupa javnoj računarskoj mreži – čl. 303 KZ; neovlašćeno korišćenje računara ili računarske mreže – čl. 304, glava XXVII KZ; pravljenje, nabavljanje i davanje drugom sredstava za izvršenje krivičnih dela protiv bezbednosti računarskih podataka – čl. 304a, glava XXVII KZ. Iz ovako određenog kataloga inkriminacija – indikatora visokotehnološkog kriminala

[12] Član 2. stav 1. ovog Zakona glasi: „Visokotehnički kriminal ... predstavlja vršenje krivičnih dela kod kojih se kao objekat ili sredstvo izvršenja krivičnih dela javljaju računari, računarski sistemi, računarske mreže, računarski podaci, kao i njihovi proizvodi u materijalnom ili elektronskom obliku".

[13] Slično tome, a u sklopu razotkrivanja organizovanih oblika visokotehnološkog kriminala, tokom 2010. godine otkrivena je grupa od 18 članova koja je upotrebom kompjuterske tehnologije uticala na ishod televizijskih SMS licitacija i na taj način sticala imovinsku korist.

uočava se da su svojevremeno preduzeti neophodni koraci u pravcu usklađivanja krivičnog zakonodavstva Republike Srbije sa Konvencijom Saveta Evrope o visokotehnološkom kriminalu, na primer novelom iz 2009. godine propisano je novo krivično delo „Pravljenje, nabavljanje i davanje drugom sredstava za izvršenje krivičnih dela protiv bezbednosti računarskih podataka" (čl. 304a KZ).[14] U istoj noveli Krivičnog zakonika, očigledno je respektovan i stav Posebnog tužilaštva za borbu protiv visokotehnološkog kriminala da su „pozitivnopravnim propisima iz stvarne nadležnosti Posebnog tužilaštva neopravdano izostavljena krivična dela koja se odnose na zloupotrebu platnih kartica i internet pornografiju". Pokazalo se, naime, da u periodu od 2005. do 2009. godine, pomenutim katalogom nisu bila obuhvaćena neka od krivičnih dela iz ove kategorije koja su u praksi najbrojnija, odnosno dela čija je društvena opasnost znatno izražena. U prvom redu reč je o krivičnom delu falsifikovanja i zloupotrebe platnih kartica iz čl. 225. KZ. Isto važi i za distribuiranje tzv. dečje pornografije putem Interneta, tj. za krivično delo prikazivanja pornografskog materijala i iskorišćavanje dece za pornografiju iz čl. 185 st. 3 KZ.[15]

Sasvim na kraju može se zaključiti da je krajem 2009. godine došlo do manjih izmena i kod „bazičnih" inkriminacija visokotehnološkog kriminala, tj. kod dela iz glave XXVII Krivičnog zakonika Republike Srbije. Konkretno, izmenjen je teži oblik neovlašćenog pristupa zaštićenom računaru, računarskoj mreži ili elektronskoj obradi podataka (čl. 302 st. 2 KZ), tako da se izvršiocem smatra onaj ko snimi ili upotrebi podatak dobijen putem neovlašćenog pristupa zaštićenom računaru, računarskoj mreži ili elektronskoj obradi podataka. Zaprećena sankcija u tom slučaju je novčana kazna ili zatvor do dve godine.

Inkriminacije kao indikatori visokotehnološkog kriminala u Republici Srpskoj - Krivični zakon Republike Srpske[16] sadrži šest kompjuterskih krivičnih dela, i to: Neovlašćeno ulaženje u zaštićenu bazu kompjuterskih podataka (član 238. KZ RS), Upad u kompjuterski sistem (član 271. KZ RS), Neovlašćeno korišćenje ličnih podataka (član 176. KZ RS), Neovlašćeno fotografisanje (član 175), Iskorištavanje dece i maloletnih lica za pornografiju (član 199 KZ RS) i Proizvodnja i prikazivanje dečije pornografije (član 200 KZ RS). Kod tri prva navedena krivična dela radnja izvršenja se sastoji u neovlašćenom ulaženju, odnosno upadu u tuđu kompjutersku bazu podataka, pri čemu radnjama navedenim u opisu krivičnih dela učinilac izvršava neka od nabrojanih kompjuterskih krivičnih dela. Naročito je bitno istaći krivična dela iz područja dečije pornografije (član 199. i član 200. KZ RS), pod kojima se podrazumeva: a) proizvodnja dečije pornografije za svrhu njene distribucije putem kompjuterskih sistema; b) nuđenje ili činjenje dostupnim dečije pornografije putem

[14] Izvršilac delikta iz čl. 304a KZ je svako ko poseduje, pravi, nabavlja i daje drugom na upotrebu računare, računarske sisteme, računarske podatke i programe za izvršenje krivičnih dela protiv bezbednosti računarskih podataka. Za ovo delo je zaprećena kazna zatvorom od šest meseci do tri godine, a propisano je i da se takvi predmeti, tj. sredstva za izvršenje krivičnih dela protiv bezbednosti računarskih podataka, moraju oduzeti.

[15] O merama policije za suzbijanje „internet-pedofilije" i uopšte visokotehnoloških krivičnih dela, videti: Becker G. (1997). Einstatz von VE und technishen Mitteln im Deliktbereich «Kinderpornographie, Der Kriminalist, No. 3, pp. 141-147; Lorch S. (2001). Ermittungen im Internet : Eine Zwischenbilanz und Standortbestimung Telefonkarte, Kriminalistik, No. 5, pp. 328-333; i sl.

[16] *Krivični zakon Republike Srpske*, Službeni glasnik Republike Srpske, broj. 49/03, 108/04, 37/06, 70/06, 73/10.

kompjuterskog sistema; c) distribucija ili prenošenje dečije pornografije putem kompjuterskog sistema; d) pribavljanje dečije pornografije putem kompjuterskog sistema za sebe ili drugoga; e) posedovanje dečije pornografije u kompjuterskom sistemu ili na mediju za pohranu kompjuterskih podataka.

Izmenama i dopunama Krivičnog zakona Republike Srpske iz 2010. godine uvedena je nova glava (dvadeset četvrta), koja glasi: "Krivična djela protiv bezbjednosti računarskih podataka" i čl. 292a, 292b, 292v, 292g, 292d, 292đ. i 292e. kojima se značajno unapređuje krivičnopravna zaštita u oblasti računarskih podataka. Ovim inkriminacijama uvedena su sledeća krivična djela: Oštećenje računarskih podataka i programa (Član 292a. KZ RS); Računarska sabotaža (Član 292b. KZ RS); Izrada i unošenje računarskih virusa (Član 292v KZ RS); Računarske prevare (292g KZ RS); Neovlašćeni pristup zaštićenom računaru i računarskoj mreži, telekomunikacionoj mreži i i elektronskoj obradi podataka (Član 292d KZ RS); Sprečavanje i ograničavanje pristupa javnoj računarskoj mreži (Član 292đ KZ RS); Neovlašćeno korišćenje računara ili računarske mreže (Član 292e KZ RS) i Izazivanje nacionalne, rasne i verske mržnje i netrpeljivosti (Član 294a. KZ RS). Zaštićeni objekat ove grupe krivičnih dela je bezbednost računarskih podataka, pri čemu su objekat napada podaci, računarski programi, računar ili drugi uređaj za elektronsku obradu i prenos podataka, računarska i telekomunikaciona mreža. Radnja izvršenja ovih krivičnih dela sastoji se u neovlašćenom brisanju, menjanju, oštećenju ili na drugi način činjenjem neupotrebljivim računarskih podataka, kojom radnjom se napadaju računarske ili telekomunikcione mreže.

ZAKLJUČAK

Ubrzani razvoj informacionih tehnologija i telekomunikacija zahteva budnost zakonodavca i neprestano praćenje promena koje se dešavaju, ali i stalno podešavanje pozitivnog zakonodavstva kako bi se moglo odgovoriti novim pretnjama po bezbednost. U tom kontekstu neophodno je precizirati i proširivati nadležnost agencija za sprovođenje zakona koje se bave suzbijanjem visokotehnološkog kriminaliteta i na druge grupe krivičnih dela kod kojih se kao objekat ili sredstvo izvršenja javljaju računari, računarske mreže, računarski podaci, kao i njihovi proizvodi u materijalnom ili elektronskom obliku, odnosno na druga krivična dela za koja se zbog načina izvršenja ili upotrebljenih sredstava sa sigurnošću može zaključiti da su dela visokotehnološkog kriminala. Kao pozitivan primer može se navesti značaj koji ima novela člana 3 Zakona o organizaciji i nadleženosti državnih organa u borbi protiv visokotehnološkog kriminala, kojom je precizirana i proširena koncentrovana nadležnost posebnih državnih organa Republike Srbije i na krivična dela protiv privrede, kod kojih se kao objekat ili sredstvo izvršenja javljaju računari, računarske mreže, računarski podaci, kao i njihovi proizvodi u materijalnom ili elektronskom obliku, odnosno na druga krivična dela za koja se zbog načina izvršenja ili upotrebljenih sredstava sa sigurnošću može zaključiti da su dela visokotehnološkog kriminala. Nesporno je, naime, da je proširivanje nadležnosti posebnih državnih organa za borbu protiv visokotehnološkog kriminala i na takva krivična dela, omogućlo brže i efikasnije njihovo otkrivanje i procesuiranje.

Bez obzira na činjenicu da su ovako unapređena zakonska rešenja daleko kvalitetniji osnov za efikasno procesuiranje izvršilaca dela visokotehnološkog kriminala, s pravom im se upućuju i zamerke. Ovo utoliko pre, što je poznato da je tzv. tamna brojka kod ove vrste krivičnih dela i dalje visoka. Isto tako, poseban akcentat treba staviti na prevenciju visokotehnološkog kriminaliteta, kao najsigurnijeg oblika zaštite. Preventivne mere treba da budu usmerene na preduzimanje aktivnosti u cilju otklanjanja izvora, uslova, okolnosti ili propusta koji pogoduju neovlašćenom korišćenju ili zloupotrebi računara, računarskih podataka, sistema i mreža. Naime, najvažnije je obezbediti uslove da do napada ne dođe, ako dođe, da posledice budu izbegnute ili da budu što manje. Prevencija visoktehnološkog kriminaliteta nalaže preduzimanje čitavog niza mera koje se mogu ticati personala koji radi na sistemu, tehnologije i operacija. Potrebno je unapred pripremiti plan postupanja za slučaj utvrđivanja napada na sistem ili neovlašćenog prodora u sistem. Neophodno je ustanoviti mere fizičke sigurnosti, kontrolu i pristup pojedinim elementima kompjuterskog sistema, kao i proceniti stepen ugroženosti kompjuterskog sistema.

LITERATURA

1. Becker G. (1997). Einstatz von VE und technishen Mitteln im Deliktbereich Kinderpornographie, *Der Kriminalist*, No. 3, pp. 141-147.
2. Britz M.T. (2004). *Computer forensis and cyber crime: An introduction*, New Jersey: Pearson Education.
3. Castells, M. (2003). *Born of network society,* Oxford: Malden Victoria.
4. Convention on Cybercrime, CETS No.: 185 (http://conventions.coe.int/Treaty / Commun/QueVoulezVous.asp?NT=185&CM=8&DF=11/13/2007&CL=ENG)
5. Jerković, R. (2009). Visokotehnološki kriminal – akteri i žrtve“, *Revija za bezbednost*, br. 3, Beograd: Centar za sigurnosne studije, str. 27–34.
6. Komlen-Nikolić L. (2010). *Suzbijanje visokotehnološkog kriminala*, Beograd: Udruženje javnih tužilaca i zamenika javnih tužilaca Srbije.
7. *Krivični zakon Republike Srpske*, Službeni glasnik Republike Srpske, broj. 49/03, 108/04, 37/06, 70/06, 73/10.
8. Lorch S. (2001). Ermittungen im Internet:Eine Zwischenbilanz und Standortbestimung Telefonkarte”, *Kriminalistik*, No. 5, pp. 328-333.
9. Stephson, P. (2010), *Investigating Computer-Realted Crime*, Boca Rato: CRC Press.
10. Šikman, M. (2007). Krivičnoprocesni aspekti suprotstavljanja organizovanom kriminalitetu, *Pravna riječ*, *broj 12/2007*, Banja Luka: Udruženje pravnika Republike Srpske. str. 502.
11. Šikman, M. (2011). *Organizovani kriminalitet*. Banja Luka: Visoka škola unutrašnjih poslova.
12. Vetsbi DŽ. R. (2004). *Međunarodni vodič za borbu protiv kompjuterskog kriminala*, Beograd: Produktivnost.
13. Zakon o suzbijanju organizovanog i teških oblika privrednog kriminala – prečišćeni tekst, Službeni glasnik Republike Srpske, broj 112/07.
14. Zakon o unutrašnjim poslovima RS, Službeni glasnik Republike Srpske, broj: 4/12.

Summary: Recognising the need for co-operation between States in combating cybercrime and the need to protect legitimate interests in the use and development of information technologies. This paper analizes incriminations used for repressin of these forms of crime in the Republic of Serbia and Republic of Srpska and current reforms of specialized police and jurisdictional agencies. This paper also considers specific operatons of preliminary investigation and acquiring of evidence used for collections and verifyng of digital evidence and forensic analisis. The paper also points out to some existing and future probles in detecting and proving of cybercrime.

Key words: Criminal law, Council of Europe, cybercrime, police, Republic of Serbia, Republic of Srpska.

Pregledni rad - UDK 341.48: [343.326: 004.738.5

VISOKOTEHNOLOŠKI KRIMINAL I KRIVIČNOPRAVNI INSTRUMENTI SUPROTSTAVLJANJA

L[1]

Akademik prof. dr Stanko Bejatović[2]

Redovni prof. Pravnog fakulteta u Kragujevcu

Predsednik Srpskog udruženja za krivičnopravnu teoriju i praksu

Apstrakt: Problematiku krivičnopravnih instrumenata suprotstavljanja visokotehnološkom kriminalu autor je u radu obradio kroz stručno-kritičku analizu dve grupe pitanja. Prva grupa pitanja posvećena je opštim napomenama o visokotehnološkom kriminalu, stepenu njegove društvene opasnosti i instrumentima suprotstavljanja. Tri su osnovna rezultata do kojih se došlo u analizi ove grupe pitanjaa. Prvi se tiče izuzetno visokog stepena društvene opasnosti visokotehnološkog kriminala, u prilog čemu se navodi i nemali broj argumenata. Drugi rezultat je potvrda internacionalnog karaktera ove vrste kriminala i neophodnosti koordinirane međunarodne akcije u borbi protiv njega, i to kako sa normativnog tako i sa praktičnog i edukativnog aspekta. Na kraju, treći rezultat analize ovog dela rada je potvrda neophodnosti istovremenog preduzimanja više aktivnosti preventivnog i represivnog karaktera na polju borbe protv visokotehnološkog kriminala. Druga grupa pitanja posvećana je razradi krivičnopravnih instrumenata suprotstavljanja visokotehnološkom kriminalu. Posmatrano sa aspekta aktuelnosti i obima obrade, četiri su pitanja kojima je posvećena posebna pažnja u ovom delu rada. To su pitanja koja se tiču: Pretpostavki adekvatnosti krivičnog zakonodavstva kao efikasnog instrumenta borbe protiv visokotehnološkog kriminala; Vrste i načina normativnog regulisanja krivičnopravnih instrumenata suprotstavljanja visokotehnološkom kriminalu; Dosadašnjih inskustava u primeni krivičnopravnih instrumenata suprotstavljanja visokotehnološkom kriminalu i uticaju drugih faktora na stepen adekvatnosti krivičnog zakonodavstva u toj borbi (Slučaj npr. sa efikasnosti krivičnog postupka, zloupotrebom konkretne zakonske norme koja mora biti isključena ili svedena na najmanju moguću meru, organizacijom i finkcionisanjem subjekata zaduženih za primenu konkretnog zakonskog teksta i dr.). Osnovni zaključak analize ovog segmenta reagovanja protiv visokotehnološkog kriminala je stav autora da ``samo u svojoj uzajamnoj povezanosti svih ovih faktora krivično zakonodavstvo daje doprinos željenom stepenu njegovog dejstva na polju borbe protiv visokotehnološkog kriminala i time i na polju njegove prevencije.`` Odgovor na pitanje kako posetići željeni stepen dejstva krivičnog zakonodavstva u borbi protiv predmetne vrste kriminala autor daje kroz određeni broj predloga de lege ferenda.

Ključne reči: Krivično pravo, visokotehnološki kriminal, Konvencija, policija, javno tužilaštvo, sud, krivično delo, prevencija, međunarodna saradnja, instrumenti supotstavljanja, računari

---

[1] Izraz „visokotehnološki kriminal“ koji se koristi u radu i ima isto značenje kao i izraz „sajber kriminal (Cybercrime). U pitanju su samo terminološke razlike.

[2] st.bejatovic@eunet.rs

VISOKOTEHNOLOŠKI KRIMINAL, STEPEN DRUŠTVENE OPASNOSTI I INSTRUMENTI SUPOTSTAVLJANJA (OPŠTE NAPOMENE)

Posmatrano sa aspekta vremena kojem pripadamo, a u vremenu koje je pred nama to će biti svakim danom i sve izraženije, jedan od najopasnijih vidova kriminala uopšte je visokotehnološki krimnal[3]. Više je razloga koji govore u prilog ovako visokom stepenu društvene opasnosti ove vrste kriminala. Među njima poseban značaj imaju sledeći: Prvo, svakim danom njegova sve veća prisutnost, i to i u najosetljivijim institucijama društva kao celine. Primera radi, dovoljno je samo navesti činjenicu o ulasku hakera u SAD u kompjuterski sistem Pentagona, u Indiji u ministarske fajlove, u Nemačkoj u kompjuter državnog kancelara, zatim da je mnoštvo elektronskih pisama blokiralo elektronski sistem banaka i vlade i sl. S obzirom na ovo, ne čudi npr. ni upozorenje zvaničnika NATO-a da onlajn špijunaža i terorizam na internetu predstavljaju neke od najopasnijih pretnji globalnoj bezbednosti; Drugo, posledice koje za sobom povlači; Treće, njegov međunarodni karakter; Četvrto, njegova povezanost sa najtežim oblicima kriminala (slučaj pre svega sa organizovanim kriminalom i terorizmom gde on postaje ne samo moćna poluga njihovog planiranja već i ključno sredstvo izvršenja). Peto, otežan način otkrivanja i dokazivanja. Dalje, u prilog ovakvom stepenu aktuelnosti društvene opasnosti ove vrste kriminala treba istaći i činjenicu da je internetska povezanost ne samo svih zemalja na svetu već skoro i njihovih najsitnijih teritorijalnih celina danas obeležje sveta kao celine. Skoro da nema dela zemaljske kugle da nije internetom povezan sa njenim drugim delovima, bez obzira kojem kontinentu i državi on pripadao, što je dovelo do potpune kompjuterske kontrole najvažnijih društvenih procesa. S obzirom na ovo, očekivano je da iz ovako velikog procesa proističu i nemale zloupotrebe. Zatim, tu je i činjenica da se prema najnovijim podacima u tzv. sajber *(cyber)* prostoru nalazi skoro trećina čovečanstva, što uslovljava nova pravila ponašanja, nove običaje, a za sobom povlači i nove opasnosti. Dalje, načini na koje računari i računarske mreže funkcionišu postali su, zahvaljujući korisničkim programima, jednostavniji i pristupačniji najvećem broju ljudi koji se mogu bez problema za nekoliko dana obučiti za osnove rada na računaru. Na taj način se polako naziru osnovne komponente za pojavu i delovanje visokotehnološkog kriminala: lako dostupno oruđe za vršenje nezakonitih radnji, ranjivost sistema i veliki broj novih korisnika koji, osim uobičajenih ljudskih slabosti, imaju još neke, izuzetno bitne, prateće pojave za uspeh kriminalaca: neiskustvo i nedovoljno znanje određenog broja korisnika. Ako se ovome doda i činjenica da računari i računarske mreže nisu jedina oruđa koja se mogu koristiti kao sredstvo ove vrste nezakonitih radnji, problem postaje još akutniji. Gotovo svakodnevno se pojavljuju nove generacije različitih uređaja koji su originalno osmišljeni za prenos informacija, komunikaciju i zabavu. Inovacije su sa jedne strane pozitivne, jer čine nove tehnologije jeftinijim, pristupačnijim, jednostavnijim, ali imaju i lošu stranu – prosečan korisnik nema dovoljno volje, vremena i mogućnosti da se upozna sa opasnostima koje sa sobom nosi korišćenje ovih uređaja i na taj način postaje potencijalna žrtva iskusnih i

[3] O pojmu visokotehnološkog kriminala vidi: S. R. Petrović, Kompjuterski kriminal, Vojnoizdavački zavod, Beograd, 2004.

daleko bolje edukovanih pojedinaca sa nečasnim namerama. Visokotehnološki kriminal ne samo da je postao svakodnevica, već je fantastičan razvoj tehnologija uslovio i neverovatnu pojavu mnoštva vrsta nedozvoljenih dela koja se mogu izvršiti njihovim korišćenjem, od onih naivnih, do veoma opasnih ponašanja koja spadaju među teška (ponekad čak i najteža) krivična dela u mnogim nacionalnim zakonodavstvima. Rečju, visokotehnološki kriminal je postao globalni problem, a broj dela koja se mogu podvesti čak i pod najrestriktivnije i najuže definicije sajber kriminala *(Cybercrime)* gotovo se svakodnevno uvećava, a šteta koja se nanosi njegovim vrešenjem meri se na godišnjem nivou stotinama milijardi dolara.[4]

Polazeći od iznesenog i posebno transnacionalnog karaktera visokotehnološkog kriminala, kao i činjenice da se borba protiv njega ne može ni zamisliti bez uključivanja cele međunarodne zajednice, odnosno bez angažovanja najuticajnijih međunarodnih institucija, po tom pitanju u poslednjih nekoliko decenija preduzimaju se značajni napori i na međunarodnom planu. Globalni napori da se uspostavi efikasna međunarodna saradnja u borbi protiv visokotehnološkog kriminala dali su i konkretne rezultate u vidu pisanih dokumenata. Među njima poseban značaj ima Konvencija Saveta Evrope o visokotehnološkom kriminalu[5] sa Dodatnim protokolom iz 2003. godine[6] koji se bavi inkriminisanjem akata rasističke i ksenofobične prirode počinjenih putem računarskih sistema[7]. O značaju sadržaja Konvencije najilustrativnije govori činjenica da su je potpisale i države koje nisu članice Saveta Evrope. Slučaj npr. sa Kanadom, Japanom, Južnom Afrikom i SAD, koje su je i ratifikovale. Zatim, tu su i brojne organizacije koje su po prirodi svog delovanja posebno zainteresovane za ovu problematiku. Slučaj pre svega sa Interpolom kao prvom međunarodnom organizacijom koja ukazuje na potencijal visokotehnološkog kriminala i poseduje operativne priručnike sa najnovijim podacima i uputstvima za istražitelje. Zatim, tu je Preporuka Saveta Evrope br. 89 od 1989. godine, koja se tiče pitanja materijalnog krivičnog prava u vezi sa ovim kriminalom. Potom posebno vredna pažnje jeste i Preporuka Saveta Evrope od 1995. godine, koja za predmet regulisanja ima pitanja koja se tiču procesnih pravila u vezi sa informatičkim tehnologijama.[8] Dalje, Evropska organizacija za bezbednost i saradnju je 1986. godine, kroz analizu zakonodavstava zemalja članica, usvojila Preporuku za usklađivanje krivičnih zakonika u vezi sa visokotehnološkim kriminalom, i to sve u cilju stvaranja normativne osnove za efikasniju borbu protiv njega. Na spisku organizacija ovog karaktera neizostavne su *OUN, koje su* u svetlu ubrzanog i planetarnog razvoja informatičkih tehnologija preduzele napore da se na globalnom nivou ispita značaj i uloga informatičkih tehnologija, kao i opasnosti koje dolaze iz ovog „virtuelnog“ prostora a koje imaju implikacije kako na život i bezbednost svakog pojedinca, tako i na odnose među suverenim državama i regionalnim i međunarodnim organizacijama. Kroz delatnost Komisije za prevenciju kriminala i krivično pravosuđe učinjeni su napori da se promoviše

---

[4] Prlja, D., Sajber kriminal (http://www.prlja.info/;sk2008,pdf,1.5.2009)

[5] Konvencija je usvojena na Konferenciji u Budimpešti 23. novembra 2001, a stupila je na snagu 1. jula 2004.

[6] Od strane Republike Srbije, Konvencija je potpisana 2005, a ratifikovana 2009. („Sl.glasnik RS“, br. 19/09).

[7] Stupio na snagu 1. marta 2006.

[8] Preporuka Saveta Evrope No.R. (95) 13.

međunarodna saradnja u oblasti harmonizacije i primene krivičnih zakona i u oblasti borbe protiv visokotehnološkog kriminala. Rezultati ovih napora opredmećeni su u rezolucijama (br. 55/63 i 56/121) o borbi protiv zloupotrebe informatičkih tehnologija, koje je Generalna skupština UN usvojila 2001. god[9] i 2002. godine.[10] U ovom kontekstu treba istaći i da je u tzv. milenijumskoj deklaraciji, odnosno Rezoluciji br. 55/2 Generalne skupštine UN od 18. septembra 2000. godine, kao jedan od prioritetnih ciljeva utvrđena i potreba da se nove tehnologije, a naročito informatičke i komunikacione, učine bezbednim i dostupnim svima. Pored njih, tu je i Rezolucija 56/121 Generalne skupštine UN koja za predmet ima borbu protiv zloupotrebe informatičkih tehnologija. *U Rezoluciji Ekonomsko-socijalnog saveta (ECOSOC) 2007/20*[11] posebno se potencira međunarodna saradnja u oblasti prevencije, istrage, krivičnog progona i kažnjavanja privrednog kriminala i dela povezanih sa zloupotrebom identiteta. Rezolucija poziva države članice da ozbiljno razmotre potrebu za modernizacijom postojećeg nacionalnog zakonodavstva, posebno imajući u vidu dramatičan porast transnacionalnog privrednog kriminala i u vezi s tim upotrebu modernih računarskih tehnologija kao sredstva za izvršenje ovih krivičnih dela. U tom kontekstu posebno se apostrofira potreba da nacionalna krivična zakonodavstva, ukoliko to nisu učinila, predvide neovlašćenu upotrebu ili izradu identifikacionih dokumenata, kao i podataka o identitetu. S tim u vezi, podstiče se i šira i efikasna upotreba modernih tehnologija u prevenciji i suzbijanju kako privrednog kriminala, tako i kriminala povezanog sa zloupotrebom identiteta. Na kraju, zbog svesti o činjenici internacionalnog karaktera ove vrste kriminala kao i činjenice da bez kordiranih akcija na međunarodnom planu nema uspeha u borbi protiv njega, ukazuje se i na potrebu da države članice razmotre pristupanje Konvenciji Saveta Evrope o visokotehnološkom kriminalu, kao i svim drugim međunarodnim pravnim aktima koji su primenljivi kada je u pitanju privredni kriminal i zloupotreba identiteta i identifikacionih podataka. Na samom kraju istaknimo i aktivnosti *Međunarodne telekomunikacione unije kao vodeće agencije u okviru organizacije UN za pitanja komunikacionih i informatičkih tehnologija***.** Kao rezultat njenog dvogodišnjeg rada, generalni sekretar UN je maja 2007. godine predstavio dokument pod nazivom Memorandum o globalnoj sajber bezbednosti (A Global Cybersecuritu Agenda – GCA) kao okvirni (instruktivni) akt o međunarodnoj saradnji i dijalogu na pronalaženju održivih rešenja u okviru globalne informatičke zajednice. Memorandum je predstavio sedam osnovnih strateških ciljeva, a među njima jedan od prioritetnih je i princip o neophodnim zakonodavnim merama. Ovaj princip podrazumeva kritičko ispitivanje svih postojećih legislativnih instrumenata u cilju utvrđivanja opšteprihvaćenog legislativnog modela koji bi bio primenjiv i operativan u svim postojećim nacionalnim i međunarodnim okvirima.[12]

Ne ulazeći u nabrajanje nemalog broja drugih akata ovog karaktera (npr. Konvencije o zaštiti prava pojedinca u vezi sa automatskom obradom ličnih

[9] „Resolution A/res/55/63“, General Assembly of the United Nationes, 22. januar 2001.
[10] „Resolution A/res/56/121“, General Assembly of the United Nationes, 23. januar 2002.
[11] „Resolution 2007/20“, The Economic and Social Council of the Unted Nations, 26. jul 2007.
[12] Detaljnije vidi: Čvorović, D., Specifičnosti otkrivanja i dokazivanja krivičnih dela visokotehnološkog kriminala (Međunarodna pravna akta i nacionalno zakonodavstvo – Osnovna rešenja i iskustva u dosadašnjoj primeni), Tematski zbornik ”Policija, bezbednost i visokotehnološki kriminal”, Kriminalističko-policijska akademija, Beograd, 2010, str. 15–36.

podataka;[13] Konvencije o sprečavanju terorizma[14], u kojoj se, sasvim opravdano, tretira problematika veze terorizma sa visokotehnološkim kriminalom; Direktive Saveta Evropske zajednice o pravnoj zaštiti kompjuterskih programa[15] u kojoj se posebno apostrofira potreba za uniformnim rešenjima u oblasti pravne zaštite kompjuterskih programa i ističe činjenica da bi problemi visokotehnološkog kriminala mogli postati složeniji ukoliko bi se nastavilo sa praksom pojedinačnog i neusklađenog regulisanja ove materiji)[16], treba konstatovati da su tako intenzivne aktivnosti na ovom polju potvrda kako njegovog internacionalnog karaktera tako i shvatanja da nema uspeha u borbi protiv njega bez koordinirane akcije međunarodne zajednice kao celine. Ubrzan razvoj kompjuterskih tehnologija zahteva budnost zakonodavaca i neprestano praćenje promena koje se dešavaju, te takvo podešavanje pozitivnog zakonodavstva kakvo bi moglo da odgovori novim izazovima. Inertnost zakonodavaca ovde može imati teže posledice nego u bilo kojoj drugoj oblasti. Transnacionalni karakter ove vrste kriminala zahteva saradnju između država, koja mora biti na visokom nivou i zasnovana na principima koji su obostrano prihvaćeni. Brzina reakcije nakon saznanja da je krivično delo izvršeno od presudnog je značaja za otkrivanje počinilaca i za obezbeđenje dokaza, s obzirom na to da se tragovi izvršenog dela lako mogu uništiti, sakriti ili na drugi način učiniti nedostupnim ili neupotrebljivim.

I pored izuzetnog napretka, još uvek su prisutni i nemali problemi na polju efikasne međunarodne saradnje i globalnih napora u suzbijanju visokotehnološkog kriminala. Među njima poseban značaj imaju sledeći: Različito pravno definisanje radnji izvršenja i obima radnji koje predstavljaju krivična dela ovog karaktera; Nedovoljna obučenost policijskih službenika, tužilaca i sudija koji postupaju u predmetima visokotehnološkog kriminala; Neusklađenost procesnih pravila u nacionalnim zakonodavstvima u pogledu istrage krivičnih dela visokotehnološkog kriminala i neusklađenost ili odsustvo mehanizama međunarodne pravne pomoći.[17] Međutim, i pored izuzetnog značaja međunarodnog aspekta, uspešna borba i protiv ove vrste kriminala nezamisliva je bez adekvatne reakcije i na polju nacionalnog zakonodavstva. Sa stanovišta nacionalnih zakonodavstava, reakcija na opasnost od širenja visokotehnološkog kriminala trebalo bi da ide u pravcu: preduzimanja mera prevencije kako bi se sprečile ili ublažile posledice vršenja ovog kriminala i povećala svest o opasnostima koje on donosi; blagovremenog usvajanja odgovarajuće zakonodavne regulative u oblasti materijalnog i procesnog prava s ciljem stvaranja pravnih instrumenta za efikasan obračun sa njim; kadrovske i materijalne osposobljenosti nadležnih policijskih i pravosudnih organa za efikasno sprovođenje zakonskih ovlašćenja koja su im poverena. Na kraju, u vezi sa nacionalnim merama na polju borbe protiv visokotehnološkog kriminala (zbog njegove bezgraničnosti i transnacionalnosti), posebno treba apostrofirati neophodnost međunarodnog povezivanja državnih organa u celom svetu koji se

[13] Convention for the Prtection of Individuals with regard to Automatic Processing of Personal date ETS No 108, the 28. January, Entry info force: 1.10.1985.
[14] Council of Europe Convention on the Prevention of Terrorizm (CETS No.196).
[15] Objavljena u „Sl. listu Evropske zajednice“, br.L 122/42 od 17. maja 1991.
[16] Njen predmet je čuvanje podataka dobijenih prilikom pružanja javno dostupnih usluga elektronske komunikacije ili javnih komunikacionih mreža.
[17] Petrović, R. S., Kompjuterski kriminal, Vojnoizdavački zavod, Beograd, 2004, str. 51–54.

bave otkrivanjem i krivičnim progonom izvršilaca ovih krivičnih dela. Koliki je značaj ovog faktora, najbolje govori činjenica da Konvencija o visokotehnološkom kriminalu Saveta Evrope posebno insistira na obavezi osnivanja kontakt tačke, što znači da u svakoj od zemalja treba da postoji tačka kojoj se može obratiti i tražiti dostavljanje određenih podataka, i to 24 sata u toku dana, sedam dana u nedelji.[18] Duboko svesna značaja ovog faktora, Srbija je i pre ratifikovanja Konvencije posvećivala i dalje posvećuje posebnu pažnju upravo ovoj problematici. Njeni nadležni organi intenzivno rade na unapređnju međunarodne saradnje, a u okviru ove saradnje posebna pažnja se poklanja pitanjima međunarodne pravne pomoći, koja je svakim danom sve intenzivnija i svestranija. Najbolji dokaz za to su već zaključeni brojni međudržavni ugovori o međunarodnoj pravnoj pomoći[19].

KRIVIČNOPRAVNI INSTRUMENTI SUPROTSTAVLJANJA VISOKOTEHNOLOŠKOM KRIMINALU

Jedan od neizostavnih instrumenata na polju borbe protiv visokotehnološkog kriminala, kao i kriminala uopšte, jeste krivično pravo. S obzirom na tako visok stepen opasnosti ove vrste kriminala, ovom instrumentu suprotstavljanja mora se posvetiti posebna pažnja, i to kako u nacionalnim okvirima, tako i na međunarodnom planu. I u teoriji i u praksi nesporna je kako njihova funkcionalna povezanost tako i činjenica da od kvaliteta zakonske norme, njene adekvatne primene i stepena zloupotrebe prava, nemalo, zavisi i stepen uticaja ovog zakonodavstva na uspešnost ostvarivanja ciljeva kriminalne politike uopšte, a time i ciljeva kriminalne politike kod ove vrste kriminala. Ovo sve iz razloga što krivično zakonodavstvo predstavlja zakonsku osnovu za izgradnju onog dela kriminalne politike koji se realizuje na represivnom planu. No, kada je reč o krivičnopravnom reagovanju i protiv ove vrste kriminala, kao i uopšte posmatrano sa aspekta zakonske norme, reakcija na opasnost od visokotehnološkog kriminala treba da ide u dva pravca. Prvo, blagovremeno usvajanje adekvatne zakonodavne regulative u oblasti materijalnog i procesnog prava kako bi se stvorili pravni instrumenti za obračun sa visokotehnološkim kriminalom. Drugo, adekvatna primena takvih normi. Konkretni krivičnopravni propisi da bi bili u funkciji adekvatne kriminalne politike, a time i prevencije nedozvoljenog ponašanja, moraju da odgovaraju savremenim zahtevima borbe protiv kriminaliteta uopšte, da budu usklađeni sa stvarnošću i da budu primenljivi, što se posebno manifestuje na polju visoktehnološkog kriminala s obzirom na pojavu stalnog širenja kako broja tako i oblika njegovog manifestovanja, kao posledice izuzetno brzog razvoja informativne tehnike. Normativni sistem krivičnog zakonodavstva jedne države mora da bude primenljiv, društveno racionalan i pravičan. Treba da sadrži takva rešenja koja se u praksi mogu primenjivati. Subjekti zaduženi za njihovu primenu (pre svega sudovi i javna tužilaštva) treba da primenjuju norme u meri koja odgovara zakonskoj intenciji i stvarnim potrebama borbe protiv kriminaliteta. Svako odstupanje od toga dovodi do nesklada između normativnog

[18] Čl. 24/7 Konvencije.
[19] Vidi: Banović,B., Bejatović, S., Osnovi međunarodnog krivičnog prava, Pravni fakultet Kragujevac, 2011, str. 319–369.

i realnog, između onog što je zakonom propisano i onog što se dešava u praktičnoj primeni zakona. Zakon ne treba da propisuje one institute i ona rešenja koja se u praktičnoj primeni ne mogu realizovati ili nisu društveno opravdana. Sa druge strane, organi koji primenjuju zakon ne mogu da u takvom stepenu derogiraju zakonska rešenja da ih čine besmislenim i pretvaraju u deklarativne odredbe. Između normativnog i aplikativnog aspekta zakonske norme mora da se uspostavi jedna normalna i racionalna ekvivalencija, da i na jednoj i na drugoj strani postoji osećaj vrednosti o stvarnim društvenim potrebama i kriminalnopolitičkim zahtevima u propisivanju pojedinih instituta i rešenja uopšte i njihovoj primeni u praksi. Samo u takvom slučaju krivično zakonodavstvo konkretne države je u funkciji željenog stepena prevencije ne samo kriminalititeta već i svakog drugog nedozvoljenog ponašanja. Preventivna funkcija zakonske norme uopšte, a time i normi krivičnog prava, nije toliko u njenoj strogosti koliko u neminovnosti njene primene na svako lice u slučajevima kada su ispunjeni za to propisani zakonski uslovi. Uz ovo, zakonska norma da bi, po svom sadržaju, bila u ovoj funkciji, mora da je karakteriše i visok stepen preciznosti određivanja pojedinih zakonskih pojmova (izraza) i propisivanje preciznih uslova za primenu pojedinih mera i instituta. Rečju, preciznost sadržaja krivičnopravne norme mora da bude izuzetno visoka, a što poseban značaj ima upravo kod normi koje se tiču ove vrtse kriminala. [20]

U nastojanju da bude u skladu sa iznesenim zahtevima kriminalne politike, i na polju visokotehnološkog kriminala u krivičnom zakonodavstvu Srbije po pitanjima vezanim upravo za krivičnopravnu problematiku visokotehnološkog kriminala prisutne su, poslednjih godina, izuzetno intenzivne zakonodavne aktivnosti. Zakonodavna rešenja vezana za oblast visokotehnološkog kriminala u zakonodavstvu Republike Srbije kreću se u tri pravca. Prvu grupu aktivnosti čini Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala[21], kojim se vrši uspostavljanje organizacije i nadležnosti posebnih državnih organa u borbi protiv ovog vida kriminala. Donošenjem ovog zakona i osnivanjem posebnih organa za borbu protiv visokotehnološkog kriminala načinjen je veliki korak na polju borbe protiv njega. Zakon predstavlja izraz razumevanja rizika koji sa sobom nosi izvršenje krivičnih dela iz ove oblasti i doprinosi uspostavljanju visokotehnološke bezbednosti. Zakon je rezultat shvatanja da se protiv ovakve negativne društvene pojave, zbog njene prirode i njenog izrazitog transnacionalnog karaktera, ne može boriti bez adekvatne zakonske regulative nacionalnog karaktera i koordinirane međunarodne saradnje po ovim pitanjima, a normativna podloga za to je upravo ovaj zakonski tekst. Uz ovo, donošenjem ovog zakona Srbija je udovoljila zahtevima iz Konvencije Saveta Evrope o visokotehnološkom kriminalu, koja uspostavlja minimum standarda koji je neophodan, po mišljenju međunarodne zajednice, da ispune nacionalna zakonodavstva u cilju efikasne borbe protiv visokotehnološkog kriminala[22].

---

[20] Bejatović, S., Međunarodni pravni standardi u oblasti krivičnog procesnog prava i način njihove implementacije u Zakonik o krivičnom postupku, Zbornik ``Zakonodavni postupak i kazneno zakonodavstvo``, Srpsko udruženje za krivičnopravnu teoriju i praksu, Beograd, 2009, str. 114–116.

[21] Sl. glasnik RS“, br. 61/05 i 104/09.

[22] Vidi: Obrazloženje Zakona o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala, Ministarstvo pravde, Beograd, 2005.

Osnovna karakteristika ovog zakonskog teksta je uspostavljanje – osnivanje posebnih organa (policijskih, tužilačkih i sudskih) za borbu protiv visokotehnološkog kriminala. Zakonom o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala, koji je stupio na snagu 25. jula 2005. godine, osnovani su posebni organi za borbu protiv visokotehnološkog kriminala u okviru postojeće sudske i tužilačke organizacije i Ministarstva unutrašnjih poslova. U Višem javnom tužilaštvu u Beogradu formirano je posebno tužilaštvo za borbu protiv visokotehnološkog kriminala, dok je u okviru Višeg suda u Beogradu formirano Veće za borbu protiv visokotehnološkog kriminala, a u okviru Ministarstva unutrašnjih poslova osnovana je posebna služba radi obavljanja poslova organa unutrašnjih poslova u vezi sa ovim krivičnim delima. Teritorijalna nadležnost navedenih organa uspostavljena je na celoj teritoriji Republike Srbije. Iako ovakvo zakonsko rešenje pruža dobar osnov za uspešnu borbu protiv visokotehnološkog kriminala, problem nastaje s obzirom na način kako je formulisana stvarna nadležnost pomenutih organa. Naime, član 3. Zakona nakon njegovih najnovijih izmena i dopuna iz 2009. godine[23] propisuje da se ovaj zakon primenjuje radi otkrivanja, krivičnog gonjenja i suđenja za: krivična dela protiv bezbednosti računarskih podataka određena Krivičnim zakonikom; krivična dela protiv intelektualne svojine, imovine, privrede i pravnog saobraćaja, kod kojih se kao objekat ili sredstvo izvršenja krivičnih dela javljaju računari, računarski sistemi, računarske mreže i računarski podaci, kao i njihovi proizvodi u materijalnom ili elektronskom obliku, ako broj primeraka autorskih dela prelazi 2000 ili nastala materijalna šteta prelazi iznos od 1.000.000 dinara; krivična dela protiv sloboda i prava čoveka i građanina, polne slobode, javnog reda i mira i ustavnog uređenja i bezbednosti Republike Srbije, koja se zbog načina izvršenja ili upotrebljenih sredstava mogu smatrati krivičnim delima visokotehnološkog kriminala, u skladu sa članom 2. stav 1. ovog zakona. Ovako određena stvarna nadležnost posebnih organa za borbu protiv visokotehnološkog kriminala ne obuhvata sva krivična dela koja se odnose na ovu vrstu kriminala. Slučaj npr. sa krivičnim delom prikazivanja, pribavljanja i posedovanja pornografskog materijala i iskorišćavanje maloletnog lica za pornografiju iz člana 185. Krivičnog zakonika Republike Srbije i falsifikovanje i zloupotreba platnih kartica iz člana 225. KZ.[24] No, i pored ovog, može se konstatovati da je donošenjem ovog zakona uspostavljen adekvatan pravnoinstitucionalni okvir za postupanje pravosudnih i policijskih organa u ovoj oblasti.

Drugu grupu propisa u zakonodavstvu Republike Srbije koji se tiču visokotehnološkog kriminala čine propisi materijalnog karaktera. To je pre svega Krivični zakonik[25] kojim su propisana krivična dela iz oblasti visokotehnološkog kriminala. Posmatrano u odnosu na ranija zakonska rešenja ove vrste, može se konstatovati da ovaj zakonski tekst, kada je reč o visokotehnološkom krimnalu, karakterišu sledeće osobenosti. Prvo, Zakonikom su predviđena krivična dela

[23] Vidi Zakon o izmenama i dopunama Zakona o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala („Sl. glasnik“, br. 104/09).
[24] Vidi: Suzbijanje visokotehnološkog kriminala, Udruženje javnih tužilaca i zamenika javnih tužilaca Srbije, Beograd, 2010, str. 195.
[25] ”Sl. glasnik RS”, br. 85/2005 i 72/2009

vezana za oblast visokotehnološkog kriminala koja su bila predviđena i ranijim zakonima, s tim što su propisana i neka nova krivična dela koja ranije nisu postojala kao krivično delo. Slučaj npr. sa krivičnim delom neovlašćenog korišćenja računara ili računarske mreže iz člana 304. Krivičnog zakonika. Drugo, krivična dela iz glave XX Krivičnog zakonika – protiv intelektualne svojine, preuzeta su iz Zakona o autorskim i srodnim pravima, u kome su ostale kaznene odredbe za privredni prestup i za prekršaj. Treće, odredbe koje se odnose na oblast visokotehnološkog kriminala sadržane su pre svega u Opštem delu Zakonika – članu 112, u kojem je propisano značenje izraza u smislu krivičnog zakonodavstva[26]. Ovde određeni pojmovi predstavljaju deo definicija pojedinih pojmova koji se koriste u Krivičnom zakoniku i njihovo značenje u smislu odredaba ovog Zakonika, a koji su vezani za oblast visokotehnološkog kriminala, na šta upućuje i odredba člana 2. stav 2. Zakona o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala, kojim je propisano da izrazi koji se koriste u ovom zakonu imaju značenje u smislu odredaba Krivičnog zakonika. Četvrto, u Zakoniku su konkretizovana krivična dela koja spadaju u krug ove kategorije krivičnih dela. Ne upuštajući se u njihova pojedinačna nabrajanja, treba konstatovati da to nisu samo krivična dela iz XXVII glave Zakonika (čl. 298–304a) – Krivična dela protiv bezbednosti računarskih podataka, već i sva druga krivična dela koja se u smislu pozitivnopravnih zakonskih propisa smatraju krivičnim delima ovog karaktera. (Slučaj npr. sa krivičnim delima iz glave XX – Krivična dela protiv intelektualne svojine, zatim sa krivičnim delima iz glave XXII , XXXII i dr.).[27]

Zakonik o krivičnom postupku je predstavnik treće grupe propisa u zakonodavstvu Republike Srbije kada je reč o krivičnopravnoj problematici visokotehnološkog kriminala uopšte. Zakonik sadrži odredbe procesnopravnog karaktera kojima su predviđeni procesni mehanizmi i ovlašćenja svih učesnika u krivičnom postupku u pogledu otkrivanja učinilaca krivičnih dela, prikupljanja dokaza, procesuiranja i suđenja.[28] Međutim, za razliku od zakona prethodne dve grupe, ZKP ne sadrži nikakva posebna procesna pravila koja bi bila isključivo namenjena otkrivanju, dokazivanju i presuđenju ove vrste krivičnih dela. S obzirom na ovo, u postupku otkrivanja, dokazivanja i presuđenja krivičnih dela visokotehnološkog kriminala primenjuju se dve vrste odredaba Zakonika o krivičnom postupku. Prvo, to su odredbe Zakonika koje se tiču posebnog postupka za krivična dela organizovanog kriminala, korupcije i drugih izuzetno teških krivičnih dela (glava XXIXa Zakonika). Drugo, odredbe opšteg karaktera koje se odnose na sve vrste krivičnih dela, pa i krivična dela visokotehnološkog kriminala. U okviru ovih odredaba, posmatrano u odnosu na krivična dela visokotehnološkog kriminala, poseban značaj imaju odredbe kojima se reguliše prikupljanje i obezbeđivanje dokaza. U vezi sa ovim odredbama treba istaći da je Zakonik o krivičnom postupku iz 2001. godine, kao i njegove kasnije izmene i dopune, i to posebno one iz avgusta

---

[26] Reč je o značenju izraza „Računarski podatak“, „Računarska mreža“, „Računarski program“ i „Računarski virus“ – tač. 17–20. čl. 112. Zakonika.

[27] Stojanović, Z., Komentar Krivičnog zakonika, JP „Službeni glasnik“, Beograd, 2006. god., str. 485–497; Lazarević, LJ., Komentar Krivičnog zakonika Republike Srbije, Savremena administracija, Beograd, 2006. god., str. 745.

[28] Bejatović, S., Krivično procesno pravo, JP „Službeni glasnik“, Beograd, 2008. god., str. 58.

2009. godine[29] doneo nemali broj korisnih novina kada je reč o procesu otkrivanja i dokazivanja najtežih vrsta krivičnih dela, a time i krivičnih dela visokotehnološkog kriminala. Slučaj npr. sa merom nadzora i snimanja telefonskih i drugih razgovora i komunikacija, automatskog računarskog pretraživanja ličnih i drugih sa njima povezanih podataka i dr.).[30] Međutim, i pored ovog čini se da ovaj zakonski tekst još uvek ne sadrži rešenja koja su u funkciji efikasne borbe protiv visokotehnološkog kriminala. Ovde se pre svega misli na problematiku tzv. elektronskih dokaza, zatim pitanje mehanizama hitne zaštite sačuvanih računarskih podataka u smislu čl. 16. Konvencije Saveta Evrope o visokotehnološkom kriminalu i mera presretanja podataka člana 21. Konvencije. Štaviše, ni novi Zakonik o krivičnom postupku Republike Srbije[31] ne poklanja željenu pažnju ovoj problematici. Naprotiv, može se zaključiti da, načelno posmatrano, ostaje na rešenjima još uvek važećeg Zakonika kada je reč o ovim pitanjima[32]. Drugim rečima, u krivičnom procesnom zakonodavstvu Srbije još uvek nije posvećena željena pažnja adekvatnoj razradi pitanja koja su u funkciji efikasne borbe protiv visokotehnološkog kriminala. Slučaj pre svega sa pitanjima koja se tiču posebnih dokaznih radnji (npr. zakonskog okvira nadzora nad komunikacijama).

U vezi sa krivičnim zakonodavstvom kao instrumentom borbe protiv visokotehnološkog kriminala, treba imati u vidi i sledeće: zakonski tekst i njegova adekvatna primena nisu jedini preduslovi uspešnosti borbe protiv visokotehnološkog kriminala a time i njegove prevencije. Naprotiv, tu su i brojni drugi faktori. Slučaj npr. sa efikasnosti krivičnog postupka, zloupotrebom konkretne zakonske norme koja mora biti isključena ili svedena na najmanju moguću meru, organizacijom i finkcionisanjem subjekata zaduženih za primenu konkretnog zakonskog teksta i dr.[33] Samo u povezanosti svih ovih faktora krivično zakonodavstvo daje doprinos željenom stepenu njegovog dejstva na polju borbe protiv visokotehnološkog kriminala i time i na polju njegove prevencije.[34].

Na kraju, ukažimo i na neka iskustva u dosadašnjoj krivičopravnoj borbi protiv visokotehnološkog kriminala. No, u vezi sa tim pre svega treba imati u vidu činjenicu da za razliku od najvećeg broja drugih vrsta kriminala koje su

---

[29] ''Sl. glasnik RS'', br.72/2009.

[30] Vidi:Bejatović, S., Krivičnoprocesno zakonodavstvo kao instrument suprotstavljanja kriminalitetu, Zbornik „Kontrola kriminaliteta i evropski standardi: stanje u Srbiji", Beograd, Institut za kriminološka i sociološka istraživanja, 2009, str. 53–69; Grupa autora, Priručnik za istragu krivičnih dela visokotehnološkog kriminala, Savet Evrope, 2008, str. 218.

[31] ''Sl. glasnik RS'', br. 72/2011.

[32] Vidi: Nova rešenje u krivičnom procesnom zakonodavstvu –Teoretski i praktični aspekt, Srpsko udruženje za krivičnopravnu teoriju u praksu, Beograd, 2011.

[33] O pojedinačnim osobenostima svakog od ovih faktora vidi: `` Krivično zakonodavstvo, organizacija pravosuđa i efikasnost postupanja u krivičnim stvarima``, Srpsko udruženje za krivičnopravnu teoriju i praksu, Beograd, 2008.

[34] Vidi: Stojanović, Z., Krivično zakonodavstvo i teški oblici kriminaliteta, Zbornik ``Teški oblici kriminala``, Institut za kriminološka i sociološka istraživanja, Beograd, 2004,str. 54; Ignjatović, Đ., Suzbijanje najtežih oblika kriminaliteta u uslovima tranzicije i nesigurnosti, Zbornik `` Teški oblici kriminala``, Institut za kriminološka i sociološka istraživanja, Beograd, 2004, str. 52; Đurđić, V., Krivičnoprocesno zakonodavstvo kao normativna pretpostavka efikasnosti postupanja u krivičnim stvarima, Zbornik ``Krivično zakonodavstvo, organizacija pravosuđa i efikasnost postupanja u krivičnim stvarima``, Srpsko udruženje za krivičnopravnu teoriju i praksu, Beograd, 2008, str. 9–16.

već tradicionalno prisutne, kako u svetu uopšte tako i na ovim našim prostorima, iskustva u dosadašnjem krivičnopravnom reagovanju na polju visokotehnološkog kriminala nisu bogata. Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala počeo se primenjivati 25. jula 2005. godine. Međutim, i pored tako relativno kratkog vremena njegove primene, mogu se već u ovome momentu izvući i neka iskustva u vezi sa krivičnopravnim reagovanjem protiv ove vrste kriminala. Na osnovu dosadašnjih iskustava u krivičnopravnom reagovanju protiv visokotehnološkog kriminala u Srbiji, a čini se i šire, može se zaključiti sledeće:

1. Postoji nemali broj problema u procesuiranju visokotehnološkog kriminala. Oni su, u najvećem broju slučajeva, rezultat kako bića ovih krivičnih dela tako i njegovog transnacionalnog karaktera. U vezi sa ovim javljaju se pitanja od čijeg rešavanja zavisi uspeh krivičnopravnog reagovanja protiv njega. Npr. način preduzimanja krivičnog gonjenja u slučajevima istovremenog izvršenja krivičnog dela u više država. Ili, tu je i pitanje veštačenja onosno pravilne ocene njegovih rezultata od strane suda zbog specifičnosti predmeta veštačenja. Zatim, Kako uspostaviti efikasnu međunarodnu saradnju bez koje nema rezultata zbog internacionalnog karaktera visokotehnološkog kriminala? Kako postupati sa učiniocem koji nije dostigao starosnu granicu krivične odgovornosti (Posebno u slučajevima saučesništva u izvršenju krivičnog dela na prostorima država u kojima su različite starosne granice nastupanja krivične odgovornosti) ?

2. I pored vidnog napretka, tehničke mogućnosti policije i tužilaštva kao subjekata otkrivanja – procesuiranja još uvek nisu u skladu sa zahtevima efikasne borbe protiv ove vrste kriminala. Uspešno suprotstavljanje ovoj vrsti kriminala podrazumeva posedovanje adekvatne tehničke opreme i poznavanje funkcionisanja uređaja koji rade na principima visoke tehnologije, poznavanje kompjuterskih sistema i mreža i modernih telekomunikacionih tehnologija. U oblasti informacionih tehnologija neophodna su specifična znanja i iskustva, a posebno je važno stalno praćenje novih tehnologija, kako bi se u uslovima stalnog razvoja i ekspanzije održao nivo znanja potreban da se uspešno obavi postavljeni zadatak.

3. Kao izuzetno aktuelno i stalno otvoreno je i pitanje pitanje prevencije kao ključnog instrumenta sprečavanja mogućnosti ove vrste kriminala.

4. I pored značajnog napretka, još uvek su prisutni kadrovski i materijalni problemi nadležnih policijskih i pravosudnih organa za efikasno i adekvatno sprovođenje zakonskih ovlašćenja koja su im poverena u vezi sa prevencijom i represijom visokotehnološkog kriminala.

5. Statistički podaci o aktivnosti novoustanovljenih specijalizovanih organa na polju borbe protiv visokotehnološkog kriminala pokazuju njihove sve veće aktivnosti. Broj krivičnih predmeta ovog karaktera se povećava iz godine u godinu. Što se tiče krivičnih sankcija, najzastupljenije su uslovne osude, s tim što sud u osuđujućoj presudi, po pravilu, izriče mere bezbednosti oduzimanja predmeta iz člana 87. KZ i oduzimanja imovinske koristi iz čl. 91. i 92. KZ, dok se oštećeni, uglavnom, u pogledu svog imovinskopravnog zahteva upućuju na parnicu.[35]

[35] Opširnije vidi: Suzbijanje visokotehnološkog kriminala, Udruženje javnih tužilaca i zamenika javnih tužilaca Srbije, Beograd, 2010, str. 195.

LITERATURA

1. Bejatović, S., *Međunarodni pravni standardi u oblasti krivičnog procesnog prava i način njihove implementacije u Zakonik o krivičnom postupku,* Zbornik ``Zakonodavni postupak i kazneno zakonodavstvo``, Srpsko udruženje za krivičnopravnu teoriju i praksu, Beograd, 2009.
2. Bejatović, S., *Krivičnoprocesno zakonodavstvo kao instrumenat suprotstavljanja kriminalitetu*, Zbornik ``Kontrola kriminaliteta i evropski standardi: stanje u Srbiji``, Institut za kriminološka i sociološka istraživanja, Beograd, 2009.
3. Bejatović, S., *Tužilački koncept istrage kao jedno od obeležja savremenog krivičnog procesnog zakonodavstva u zemljama bivše SFRJ i Srbiji,* Zbornik ``Pravo u zemljama regiona``, Institut za uporedo pravo, Beograd, 2010.
4. Čvorović, D., *Specifičnosti otkrivanja i dokazivanja krivičnih dela visokotehnološkog kriminala (Međunarodna pravna akta i nacionalno zakonodavstvo - Osnovna rešenja i iskustva u dosadašnjoj primeni*), Tematski zbornik ”Policija, bezbednost i visokotehnološki kriminal”, Kriminalističko-policijska akademija, Beograd, 2010. god., str. 15–36.
5. Đurđević, Z., *Lisabonski ugovor: prekretnica u razvoju kaznenog prava u Europi*, Hrvatski ljetopis za kazneno pravo i praksu, Zagreb, vol. 15, br. 2/2008.
6. Fischer, T., *Strafgesetzbuch und Nebengesetze*, 56. Auflage, Verlag C. H. Beck, Muenchen, 2009.
7. Ignjatović, Đ., *Suzbijanje najtežih oblika kriminaliteta u uslovima tranzicije i nesigurnosti,* Zbornik `` Teški oblici kriminala``, Institut za kriminološka i sociološka istraživanja, Beograd, 2004.
8. Lowe-Rosenberg, *Die Strafprocessordnung und das Gerihtsverfasunggesetz,* Groskomentar, 23. Auflage, Zweiter Band , Berlin, 1988.
9. Lutz Meyer-Gossner, *Strafprocessoerdnung*, 46. Auflage, Verlag C. H. Beck, Muenchen, 2003.
10. Marinković D., Đurđević Z. *Računarsko pretraživanje i upoređivanje podataka u otkrivanju i dokazivanju krivičnih dela*, Revija za kriminologiju i krivično pravo, vol. 48, br. 3, str. 245–264, 2010.
11. Mijalković, S. Manojlović, D. *Pribavljanje listinga telefonskog pretplatničkog broja građanina – kontroverze u radu nacionalnih sistema bezbednosti*, Strani pravni život, br. 2/2008, str.154 i 15.
12. Milutinović, M., *Kriminalna politika,* Beograd, 1984.
13. Nikolić Komlen, L., Gvozdenović, R., Radulović, S., Milosavljević, A., Jerković, R., Živković, V., Živanović, S., Reljanović, M., Aleksić I., *Suzbijanje viskotehnološkog kriminala*, Udruženje javnih tužilaca i zamenika javnih tužilaca, AECID 2010, Beograd.
14. Petrović, S. R., *Kompjuterski kriminal*, Vojnoizdavački zavod, Beograd, 2004, str. 51–54.
15. *Priručnik za trening tužilaca i sudija u oblasti visokotehnološkog kriminala,* Udruženje javnih tužilaca i zamenika javnih tužilaca Srbije, ATC, Beograd, 2009. god.
16. Roxin, C., *Strafrecth*, Allgemeiner Teil, Band I, 4. AuflageVerlag C.H.Beck, Munchen, 2006.

17. Roxin, C., S*trafrecth*, Allgemeiner Teil, Band II, Verlag C. H. Beck, Muenchen, 2002.
18. Roxin, C., *Strafverfahrensrecth*, 22. Auflage, Muenchen, 2002.
19. Sieber, U., *Die Zukunft des Europaischen Strafrechts*, Sonderdruck aus Band, Zeitschrift fuer die gesamte Strafrechtswissenschaft, 121/2009.
20. Škulić, M.*, Organizovani kriminalitet* – Pojam i krivičnoprocesni aspekti, Beograd, 2003.
21. Stojanović, Z., *Krivično zakonodavstvo i teški oblici kriminaliteta,* Zbornik ``Teški oblici kriminala,`` Institut za kriminološka i sociološka istraživanja, Beograd, 2004.
22. Tanjević, N. 152 *Kompjuterski kriminal – pravna zaštita na nacionalnom nivou*, *Bezbednost* br.1–2. 2009, str. 152–167.
23. Tematski zbornik *"Policija, bezbednost i visokotehnološki kriminal",* Kriminalističko- policijska akademija, Beograd, 2010. god., str. 15–36.
24. Tiedemann, K., *Die Europaisierung des Strafrechts*, u: Kreuzer, Scheuing, Sieber; Die Europaisierung der mitgliedstaatlichen Rechtsordnungen in der Europaischen Union, Baden-Baden, 1977.

VISOKOTEHNOLOŠKI KRIMINAL [36] I KRIVIČNOPRAVNI INSTRUMENTI SUPROTSTAVLJANJA

Academician Prof. Stanko Bejatović
Full Professor. Faculty of Law
President of Serbian Association of Criminal Law and Business

Aprstakt: The problem of criminal instruments opposition Cybercrime is the author of the work through expert critical analysis of two groups of issues. The first part is devoted to general remarks on Cybercrime, its degree of social danger and the instruments of opposition. There are three main results obtained during the analysis of this group of questions insteadí. The first concerns the extremely high degree of social danger of cyber crime in favor of what is given and no small number of arguments. Another result is the confirmation of the international character of this crime and the need for coordinated international action to fight against it, both the normative and practical and educational aspects. Finally, the third result of the analysis of this work is the simultaneous confirmation of the necessity of taking more preventive and repressive actions katraktera ProTV on fighting cyber crime. The second issue is dedicated to the elaboration of instruments to counteract criminal cybercrime. From the aspect of relevance and extent of processing four issues is given special attention in this paper. These are questions concerning: Assumptions on the adequacy of criminal law as an effective instrument of combating cybercrime, types and methods of normative regulation of criminal instruments opposition visokotehnolškom crime, previous criminal inskustava in applying high-tech instruments to counteract kkriminalu and other factors influence the degree of adequacy of criminal legislation in this fight (eg Case. with the efficiency of criminal proceedings, abuse of specific legal norms that must be excluded or reduced to a minimum, the organization and functioning of the persons entrusted with the implementation of a specific legal text, etc..). The main conclusion of this segment of the analysis of reaction against high krimnala by the attitude that ``only in their mutual relationship of all these factors contributing to the criminal legislation of the desired degree of its action in the fight against cyber crime and time in the field and its prevention.`` The answer to the question to visit the desired level of effects of criminal legislation in the fight against crime by the species given by a number of proposals de lege.

Key words: Criminal law, cyber crime, the Convention, police, public prosecution, courts, crime, prevention, international cooperation, juxtaposing instruments, computers

[36] Izraz „visokotehnološki kriminal“ koji se koristi u radu i ima isto značenje kao i izraz „sajber kriminal (Cybercrime). U pitanju su samo terminološke razlike.

Pregledni rad - UDK 351.74/.75: 004.738.5

BEZBEDNOST I INTERNET

Prof. dr Radomir Milašinović
Fakultet bezbednosti, Beograd
Prof. dr Saša Mijalković
Kriminalističko-policijska akademija, Beograd
Mr Goran Amidžić
Visoka škola unutrašnjih poslova, Banja Luka

Apstrakt: Ugrožavanje bezbednosti na internetu, odnosno na određenim servisima interneta (veb-sajtovi, društvene mreže, forumi, elektronsko poslovanje) sve više uzima maha, zbog čega se ističe i kvalitativni i kvantitativni aspekt ove problematike. Ovo je, pre svega, normativno i bezbednosno, ali i tehničko-tehnološko, te globalno pitanje, oko kojeg još uvek ne postoji univerzalna usaglašenost subjekata koji na određeni način polažu ‘’pravo na internet’’. Ova problematika je uslovljena i konceptom ‘’neutralnosti mreže’’, ali i brojnim drugim konceptima, normativnog, tehnološkog, bezbednosnog, pa i kulturološkog aspekta. Usled navedenog, bezbednost u sajber-prostoru se često prenebregava, često se i podrazumeva, iako za to nema realnog osnova, ali je činjenica, pogotovo u zadnje vreme, da se na internetu svakodnevno narušava lična, kolektivna, pa i međunarodna bezbednost. Posledice narušavanja bezbednosti na internetu, usled inkorporiranosti interneta u sve pore globalnog društva, svakako su enormne. U tom kontekstu, rad se bazira na posmatranje bezbednosti na internetu sa tehničko-tehnološkog, korisničkog, normativnog i globalnog aspekta.

Ključne reči: internet, bezbednost, neutralnost mreže, ugrožavanje bezbednosti...

UVODNA RAZMATRANJA

Internet je konceptualno zamišljen kao sredstvo koje će se koristiti u zatvorenom krugu, uglavnom među učenim ljudima koji nisu opterećeni brigama za bezbednost. Oni su komunicirali otvoreno i bavili su se mogućim problemima bezbednosti na neformalan način. Sajber-bezbednost je došla u žižu interesovanja zahvaljujući nagloj ekspanziji korisničke baze interneta. Internet je ponovio onu staru istinu da tehnologija može da bude i operativna i preteća. Ono što se može iskoristiti za dobrobit društva, može se iskoristiti i na njegovu štetu. Propratni efekat nagle integracije interneta u skoro svim aspektima ljudske delatnosti jeste povećana ranjivost savremenog društva, jer je internet deo kritične globalne infrastrukture (Kurbalija, 2011: 70).

S obzirom na to da je internet poslednjih godina doživeo ekspanziju omogućujući brzu komunikaciju među korisnicima na udaljenim destinacijama, stvorila se potreba da se znatno ozbiljnije pristupi problemu bezbednosti na internetu.

U srpskom jeziku još uvek određeni termini koji su preuzeti iz engleskog jezika nisu dovoljno precizirani i terminološki prihvaćeni. Usled toga često postoji zabuna prilikom korišćenja određenih pojmova. To je slučaj i sa pojmom ‘’sajber’’, pogotovo kada se navedeni termin koristi uz imenicu bezbednost (sajber-bezbednost). Stoga treba naglasiti da se pod ovim pojmom podrazumeva bezbednost interneta, ali ne samo interneta, već i bezbednost svih aktuelnih globalnih digitalnih tokova. Ovo zbog toga što se smatra da termin internet, u aktuelnom trenutku tehničko-tehnološkog progresa neslućenih razmera i dometa, ne obuhvata dva veoma bitna segmenta koja su u vezi sa njim, a to su informaciono društvo i informaciono-komunikacione tehnologije. Drugim rečima, pod sajber-bezbednošću se podrazumeva i bezbednost interneta, ali i bezbednost (savremenog) informacionog društva, te bezbednost informaciono-komunikacionih tehnologija i njihovih korisnika.

Međutim, brzi razvoj i globalizacija otežavaju uspostavljanje valjane pravne regulative koja bi sankcionisala sve veći broj zloupotreba koje nastaju na internetu. Zbog ogromnog broja korisnika interneta u gotovo svim državama, skoro je nemoguće pronaci i kazniti učinioca određenog bezbednosnog incidenta. Mnoge vlade su donele zakone koji važe samo u njihovim zemljama, međutim, još uvek postoji veliki broj država koje nisu dovoljno svesne negativnih strana korišćenja interneta. Pri tome, donošenje ovakvih zakona i pravila nije nimalo lak zadatak. Upravo je to jedan od osnovnih razloga pojave velikog broja zlonamernih softvera koji narušavaju bezbednost korisnika interneta (internauta).

Korisnike interneta bi zato veoma trebalo da zanima šta sami mogu da učine u cilju zaštite od ovakvih pojava, pogotovo kada se radi o poslovnom okruženju gde se nameću i dodatni zahtevi vezani za osiguranje kontinuiteta poslovanja i sprečavanje krađe, oštećenja i uništenja podataka.

Prvi korak je svakako elementarna edukacija o bezbednosti na internetu.

ODNOS BEZBEDNOSTI I INTERNETA

Prilikom nastanka i razvoja interneta se svakako ne može reći da su poštovani određeni bezbednosni standardi[1], što je (delimično) i razumljivo, pogotovo ukoliko imamo u vidu koncept i sadržaj zamišljenog interneta kao nesmetanog i nesputanog ‘’auto-puta’’ informacija, ideja, podataka i ljudskih dostignuća. Međutim, s ekspanzijom interneta, koja se manifestuje i kvantitativno (uključivanjem subjekata koji koriste i koji zavise od interneta), ali i kvalitativno (kroz nove sadržaje, mogućnosti, usluge, domete), internet se sve više posmatra i kao bezbednosni problem. Ovo je svakako posledica sve učestalijih i drastičnijih narušavanja lične, ali i kolektivne bezbednosti, koja se konkretizuju korištenjem usluga interneta, preko interneta ili uz posredno korištenje (resursa) interneta.

[1] Problem bezbednosti na internetu je najčešće zanemaren. Retko gde se ima prilika uopšte učiti ili čak i upoznati se sa opasnostima interneta, kao i obezbeđivanjem sigurnosti računarskih sistema. Svi akademski kursevi posvećeni su algoritmima, programskim jezicima ili teorijskom računarstvu. Ovu temu obično i sami programeri, poznati po samoukosti, ostavljaju ‘’za kasnije’’, što obično bude nikada. Problem bezbednosti je izražen posebno danas, u uslovima poplave raznih aplikacija, od kojih je dobar deo ranjiv još ‘’izdaleka’’. U kombinaciji sa gomilom aljkavih programera, rezultati su potencijalno katastrofalani. Verovatno da jedino lenost sprečava zlonamernike da učine više štete.

S aspekta bezbednosti, internet možemo posmatrati i kao faktor ugrožavanja bezbednosti, ali i kao faktor uspostavljanja i konsolidovanja narušene bezbednosti. Međutim, usled brojnih i u zadnje vreme učestalijih, te drastičnijih oblika narušavanja bezbednosti pojedinca, ali i države[2], internet se najčešće posmatra kao faktor ugrožavanja bezbednosti. Internet se sve više postavlja kao izuzetan bezbednosni problem, gde se, primarno, ali ne i jedino posmatra pitanje odnosa interneta i kriminaliteta, odnosno kriminogeni aspekt interneta.[3]

Naime, internet u današnje vreme služi kao veoma moćno sredstvo za teroriste, kao i za vršenje krivičnih dela, ali, isto tako, internet služi i kao sredstvo propagande, širenja nemoralnih sadržaja, raznih nacionalističkih, retrogradnih i drugih društveno i globalno neprihvatljivih ideja i slično, dok, s druge strane, internet (može da) služi i kao sredstvo pronalaska izvršioca krivičnih dela, kao sredstvo suzbijanja kriminaliteta, kao način eliminisanja mogućnosti za izvođenje određenih terorističkih akata i slično.

Pored nesumnjive koristi koju pruža globalna informaciona megamreža unapređujući ogroman spektar ljudske delatnosti, ona nosi i određene opasnosti. U obilju najrazličitijih informacija iz svih oblasti, širom sveta preko interneta se emituju programi i poruke čiji su sadržaji i uticaji nepoželjni, pa čak i pogubni s

---

[2] Kao eklatantan primer može da posluži delovanje hakerske grupe ''Anonimusi''. Ovaj ''sajber-kolektiv'', čiji su članovi nepoznati, ali priznati informatički stručnjaci (s obzirom na ''rezultate'' njihovih aktivnosti), uglavnom je napadao pojedine multinacionalne korporacije, globalne organizacije nevladinog karaktera, istaknute pojedince ili pravna lica na internetu i slično, čime je direktno napadao na ličnu bezbednost korisnika na internetu. Međutim, nakon najave usvajanja antipiratskog zakona u SAD (*Stop Online Piracy Act – SOPA*), kao i nakon hapšenja rukovodstva jednog od najpoznatijih sajtova za razmenu fajlova Megaaploada, pripadnici ''Anonimusa'' su, kako su naveli, iz osvete napali, a potom i ''oborili'' sajtove Federalnog istražnog biroa i Ministarstva pravde SAD, te nekoliko sajtova muzičkih i filmskih korporacija u SAD. Navedeno obaranje sajtova se smatra jednim od prvih većih hakerskih napada na informacione resurse u SAD korištenjem internet resursa i usluga.

[3] O odnosu interneta i kriminaliteta može se govoriti sa više aspekata, od kojih je uticaj interneta na kriminalitet, odnosno posmatranje interneta kao kriminogenog faktora samo jedan.

Međutim, i kada je u pitanju povezanost interneta i kriminaliteta, treba naglasiti da postoje oprečna mišljenja, pogotovo ukoliko se uzmu u obzir istraživanja koja internet posmatraju (i) kao medij (što on, u suštini, i jeste, mada ima i druge, mnogo šire i sadržajnije aspekte), kojom prilikom se uticaj interneta na kriminalitet posmatra kao uticaj medija na kriminalitet, sa aspekta samo jednog dela medija (interneta).

Rezultati ovih brojnih istraživanja se, uslovno posmatrajući, mogu podeliti u (najmanje) tri grupe. Najbrojniji su oni teretičari koji smatraju da internet ima izrazito negativan uticaj na korisnike u smislu da podstiče agresivnost, a što je najčešće povezano sa vršenjem krivičnih dela, inspirisanih ili podstaknutih sadržajem i mogućnostima interneta. Daleko manji broj teoretičara smatra da je uticaj medija na kriminalitet predimenzioniran, nerealan, te da internet ima veoma mali ili gotovo nikakav uticaj na kriminalitet. Postoje određeni teoretičari koji smatraju da je uticaj interneta u pogledu kriminaliteta pozitivan, odnosno da internet utiče i oblikuje stavove u društvu u cilju afirmacije nekriminalnog ponašanja, odnosno na planu suzbijanja kriminaliteta. Autori koji negiraju kriminogeni uticaj interneta, ističu da njegov uticaj na osećanja, stavove i ponašanje ljudi nije uopšte dokazan, kao i da se kauzalitet između kriminaliteta i interneta ne može izolovano posmatrati, a pogotovo ne favorizovano u odnosu na druge kriminogene faktore, već da internet ima uticaj samo u odnosu na multifaktorsku etiološku dimenziju kriminaliteta. Nadalje, smatra se da je tamo i gde postoji taj uticaj, on neznatan, pod uslovom da institucije socijalizacije ličnosti i društvene kontrole funkcionišu. Određeni slučajevi krivičnih dela izvršenih na internetu ili uz pomoć interneta, posmatraju se kao izolovani slučajevi, na kojima se ne mogu graditi nikakvi relevantni opšteprihvaćeni i opštevažeći zaključci o uticaju interneta na kriminalitet.

različitih aspekata. Naime, internet danas, pored ostalog, može da posluži i služi za uputstvo kriminalcima kako da najbolje izvrše krivično delo, odnosno kako da ne budu uhvaćeni, za širenje pornografije, za propagandu političkih ideja i programa uopšte, za vršenje kriminalnih i terorističkih akata (putem interneta), za propagiranje mržnje i nasilja, za pranje novca... Prednost interneta, a koju veoma dobro koriste kriminalci i teroristi, jeste da na internetu praktično ne postoji mogućnost fizičkog ugrožavanja lica koje vrši nedozvoljene akte, pa je i mogućnost redukcije tih akata bitno smanjena.

Usled nesputane, slobodne, necenzurisane mogućnosti protoka informacija, te usled zaštite identiteta lica koja su na internetu, internet se pokazao kao pogodno sredstvo za komunikaciju lica istih ili sličnih razmišljanja, stavova, vrednosnog sistema, ponašanja, te za regrutaciju lica za određene aktivnosti, u kom smislu se ogleda i njegov kriminogeni značaj. S druge strane, na internetu se mogu pronaći konkretna i detaljna uputstva o izvršenju svakojakih krivičnih dela, sa konkretnim i istinitim primerima, što može podsticajno da utiče na vršenje krivičnih djela. Isto tako, internet se koristi i za širenje rasističke, nacionalističke i terorističke propagande, što je samo po sebi krivično delo, a takođe može da bude snažan kriminogeni faktor kod krajnjih konzumenata takvih sadržaja. Internet omogućava anonimnost, kao i krađu identiteta, a što svakako utiče i na sadržaje na internetu. Naime, korisnici interneta u sajber-prostoru imaju vlastite identitete, koje je veoma teško ‘’provaliti’’ i identifikovati sa društveno prihvatljivim i normiranim identitetom.[4] Na taj način se ostvaruje i omogućava interakcija između svih korisnika, bez mogućnosti (ili je ta mogućnost izuzetno mala) otkrivanja identiteta druge strane, ali se stiče utisak da većina korisnika i ne želi da sazna pravi identitet druge osobe, naravno, sve dok nema štete od komunikacijskog odnosa koji postoji između navedenih korisnika interneta.

Ovo je uslovilo pojavu mnoštva bezbednosnih rizika i izazova koji se postavljaju i pred pojedinca (kao korisnika interneta), ali i pred društvo (posmatrano kroz formalne ili neformalne zajednice), te pred čovečanstvo uopšte.

TEHNIČKI ASPEKTI BEZBEDNOSTI NA INTERNETU

U pogledu bezbednosti, tehničko-tehnički resursi interneta, tj. sama tehničko-tehnološka infrastruktura se posmatra kao primarna (pa čak i jedina) u narušavanju bezbednosti interneta.[5] Ovo je, svakako, samo delimično tačno.

---

[4] Niko na internetu ne zna ko je ko, šta predstavlja, šta želi, koje su mu krajnje namere i slično. Izuzetak je elektronska pošta, gde se korisnici prethodno identifikuju, ali ni ovde nema pravila. Moguće je ukrasti tuđi identitet ili jednostavno otvoriti nalog elektronske pošte na određenim besplatnim stranicama (poput stranice Jahu), te da se ne zna identitet pošiljaoca poruke.
U kontekstu ovog, potrebno je spomenuti da postoji jedna slavna karikatura na kojoj je prikazan pas kako sedi ispred računara povezanog sa internetom. Tekst ispod slike glasi: ‘’Super je što na internetu niko ne zna da si pas!’’.

[5] Delimično, ovo je posledica i određenih terminoloških nedorečenosti, pa i kontradiktornosti. Naime, često se pod tehničkim aspektom (narušavanja, ali i konsolidovanja) bezbednosti interneta podrazumeva informaciona bezbednost, odnosno ova dva pojma (tehnička bezbednost interneta i informaciona bezbednost) se posmatraju kao sinonimi, što, naravno, nije ispravno. Informaciona

U tehničko-tehnološkom smislu, pod pojmom interneta se podrazumeva veza više individualnih računara povezanih primenom protokola TCP/IP (*Transport Control Protocol/Internet Protocol*) ili HTTP (*Hyper Text Transfer Protocol*), kao i više individualnih mreža (poput *NSFnet, EARN*…) povezanih u jednu logičku mrežu u kojoj svi dele istu šemu adresiranja (Kešetović, 1996: 743). Na osnovu navedene definicije možemo konstatovati da celinu zvanu internet, u tehničko-tehnološkom smislu, čini više određenih ''entiteta''. Ti entiteti, odnosno elementi, služe vlastitoj svrsi, ali, odgovarajućim povezivanjem, služe i za potrebe interneta. Prema tome, internet čini više računara, odgovarajuća veza između tih računara, te određeni komunikacijski protokoli koji služe kao jedinstveni uniformni obrasci komuniciranja između povezanih računara. Za internet je neophodno i postojanje odgovarajućih provajdera koji korisnicima omogućavaju priključenje na internet, a zatim internet, u tehničko-tehnološkom smilu, podrazumeva i postojanje internet veze, kao i određenih internet usluga. Posmatrajući internet u tehničko-tehnološkom smislu, možemo konstatovati da suštinu tog aspekta posmatranja čini postojanje više međusobno povezanih računara ili na sličan način stvorenih računarskih mreža koje, po određenim pravilima, komuniciraju između sebe, a zbog obostrane koristi i interesa.

Dovodeći navedeno u vezu sa tehničkom kompnonentom bezbednosti na internetu, može se zaključiti da se bezbednost interneta, u tehničko-tehnološkom smislu, može narušiti kroz narušavanje bezbednosti (umreženih) računara, kroz narušavanje bezbednosti kreiranih (internih) računarskih mreža ili narušavanjem bezbednosti komunikacione veze koja povezuje računare i računarske mreže u funkcionalnu celinu znanu kao internet.

Kada je u pitanju narušavanje bezbednosti računara i računarskih mreža, navedeno se najčešće konkretizuje kroz razne oblike računarskog kriminaliteta.

Računarski kriminalitet se određuje kao skup različitih oblika delinkventnog ponašanja, gde računar predstavlja sredstvo ili cilj kažnjivog dela (pri čemu bi ovde spadala i ponašanja koja još nisu inkriminisana, ali koja bi, u slučaju da se koristilo nekim drugim ''instrumentom'', predstavljala krivično djelo), dok se, nadalje, u računarski kriminalitet uključuju i svi umišljajni kažnjivi napadi na tuđu imovinu počinjeni u vezi sa elektronskom obradom podataka (Krapac, 1992: 13). Računarski kriminalitet se posmatra i u užem i u širem smislu, pa se tako pod ovim vidom kriminaliteta u užem smislu podrazumeva svako nezakonito ponašanje usmereno na elektronske operacije sigurnosti računarskih sistema i podataka koji se u njima obrađuju, dok se u širem smislu podrazumeva svako nezakonito ponašanje vezano za računarski sistem i mrežu ili u odnosu na nju, uključujući i takav kriminalitet kakvo je nezakonito posedovanje, nuđenje i distribuiranje informacija preko računarskih sistema i mreža (Zornić, 2010). Računarski kriminalitet se definiše i kao smisleni skup krivičnih dela povezanih sa računarskim sistemima i računarskim podacima

---

bezbednost integriše i komunikacionu bezbednost i računarsku (kompjutersku) bezbednost. Konkretno, pod informacionom bezbednošću se podrazumeva zaštita informacionih sistema protiv neautorizovanog pristupa ili modifikacija informacija, bilo u skladištenju, obradi ili prenosu i protiv lišavanja usluga autorizovanih korisnika, uključujući neophodne mere detekcije, dokumentovanja i otklanjanja takvih pretnji. Preuzeto iz: *Nacional Information Systems Security Glossary,* Nacional Security Agency, Fort Meade, 2000.

ili u vezi sa sadržajem računarskih informacija, izvršenih na određenom području kroz određeno vreme (Pavlović, 2003: 629).

Brojni su modaliteti ispoljavanja računarskog kriminaliteta u smislu narušavanja tehničko-tehnološke bezbednosti interneta. Međutim, sve ih nabrojati jeste nemoguće, pogotovo jer se svakodnevno modifikuju i unapređuju, a pojavljuju se i novi. Kao najučestaliji oblici ispoljavanja računarskog kriminaliteta pojavljuju se razne internet prevare, krađe identiteta, provaljivanje u tuđe računare i računarske sisteme, krađa podataka i informacija, ‘’krađa vremena’’, razne krađe internet usluga, internet piraterija, pornografija i pedofilija, računarska sabotaža, računarska diverzija, teroristički akt realizovan (samo) uz pomoć interneta, razni oblici informacionog ratovanja...[6]

Karakteristika računarskog kriminaliteta posmatranog u ovom kontekstu narušavanja tehničko-tehnološke komponenete bezbednosti interneta, jeste u tome što se krivičnim delima računarskog kriminaliteta ili sličnim radnjama koje imaju karakteristike bezbednosnih incidenata na tehničko-tehnološkoj infrastrukturi na kojoj počiva internet, napadaju i ugrožavaju sami računari preko kojih se pristupa internetu, kao i računarske mreže sa kojih se ‘’preuzimaju’’ usluge interneta, te određeni komunikacioni kanali koji služe kao transmisija između konkretnog korisnika i interneta.

S druge strane, neophodno je napomenuti da se koncept narušavanja tehničko-tehnološke bezbednosti interneta posmatra i kroz bezbednosne incidente na određenim uslugama (servisima) samog interneta. Naime, internet se sastoji od mnoštva usluga – servisa, od kojih su najpoznatiji, svakako, veb (*World Wide Web*), elektronska pošta (*e-mail*), društvene mreže (*social network*), ćaskaonice, pretraživači, vizuelno-govorna komunikacija (Skajp), forumi, elektronsko poslovanje (elektronsko bankarstvo, trgovina, marketing...) ... U ovom slučaju, bezbednost svih servisa se može narušiti na razne načine, kojom prilikom se sam bezbednosni incident odnosi na konkretne usluge ovako parcijalizovanog interneta. Ovde se narušavanje bezbednosti interneta, odnosno usluga na internetu posmatra sa praktične (korisničke) strane, bez obzira na to da li su u ovom slučaju oštećeni ili ugroženi sami korisnici određenih usluga (npr. članovi društvenih mreža prilikom kompromitacije profila) ili su oštećeni subjekti koji imaju određeni javni, poslovni,

---

[6] Smatra se da su najčešći oblici i načini narušavanja bezbednosti računara na internetu:
skidanje elektronske pošte zaražene zlonamernim softverom koji se obično nalazi u prilogu,
otvoreni računarski portovi (kao posledica aktiviranja zlonamernog softvera) preko kojih je moguće preuzeti kontrolu nad napadnutim računarom,
poseta sumnjivim sajtovima (koji su obično postavljeni na besplatnim serverima) koji ubacuju zlonamerni softver na računar,
instalacija i startovanje ‘’sumnjivih’’ programa koji su zaraženi zlonamernim softverom,
bezbedonosni propusti u programima koji se inače koriste na računaru (operativni sistem, pretraživači...), zbog kojih je neophodno svakodnevno ažuriranje sigurnosnih dodataka,
korišćenje ‘’zakrpa’’ koje omogućavaju nelegalno korišćenje softvera,
mrežna krađa identiteta koja predstavlja prikupljanje ličnih podataka (korisničko ime, lozinka, broj platne kartice, broj telefona i dr.) od lakovernog korisnika na lažnim sajtovima,
preusmeravanje na ‘’lažni’’ ili klonirani sajt modifikacijom lokalnog DNS servera na računaru koji je prethodno zaražen zlonamernim softverom,
narušavanje bezbednosti na društvenim mrežama, poput Fejsbuka, Tvitera, Maj Spejsa... (preuzeto sa: *www.ekfak.kg.ac.rs.)*.

politički, tehnološki, lični ili neki drugi interes (npr. konkretne institucije prilikom ‘’obaranja” zvaničnih veb prezentacija).

Oblici ispoljavanja bezbednosnih incidenata na pojedinim uslugama interneta jesu mnogobrojni. Kao najučestaliji se mogu nabrojati:

- na vebu – ‘’obaranje” ličnih, zvaničnih ili komercijalnih prezentacija i drugih sajtova, zatim delimično ili potpuno menjanje sadržaja ovih sajtova, te onemogućavanje pristupa kompromitovanim stranicama...
- kod elektronske pošte, najučestaliji bezbednosni incidenti se odnose na speming (*spam*)[7] i na krađu (kompromitaciju) naloga...
- na društvenim mrežama se kao poseban problem pojavljuje kompromitacija identiteta krađama profila, zatim razni oblici nefizičkog nasilja (verbalno, seksualno), piraterija, pornografija...[8]
- širenje vjerske, nacionalne i rasne mržnje i netrpeljivosti, te pozivanje na vršenje krivičnih dela i na razne oblike antidržavnog i antidruštvenog delovanja, izuzetno su ‘’popularni” na forumima,
- elektronsko poslovanje je izuzetno kompromitovano raznim zloupotrebama u oblasti elektronskog bankarstva (fišing) i u oblasti elektronske trgovine (piraterija) ...

REGULISANJE BEZBEDNOSTI NA INTERNETU U NACIONALNIM OKVIRIMA

Kada je u pitanju normativno krivičnopravno regulisanje problematike bezbednosti interneta u nacionalnim okvirima, primarno je da se dâ osvrt na određene preporuke koje se (minimalno) moraju zadovoljiti kada je u pitanju narušavanje bezbednosti na internetu vršenjem krivičnih dela. Te osnovne preporuke su navedene u Rezoluciji o računarskom kriminalitetu usvojenoj na VIII kongresu UN-a, potom preporuke XV međunarodnog kongresa za krivično pravo, te preporuke Saveta Evrope, a posebno Preporuka o kriminalitetu vezanom za računare i Preporuka o sagledavanju problema u krivično-procesnom pravu vezanom za informatičku tehnologiju, mada postoje i druga međunarodna pravna dokumenta koja regulišu ovu oblast.

Konkretno, lista minimuma tih preporuka odnosi se na sledeće inkriminacije u nacionalnim krivičnim zakonodavstvima:

- Računarsku zloupotrebu – unos, izmena, brisanje ili potiskivanje računarskih podataka ili programa, kao i ostale vrste mešanja u obradu podataka koje utiču na njen rezultat, čime se izaziva ekonomski ili imovinski gubitak drugog lica, s namerom da se stekne nezakonita ekonomska dobit za sebe ili treće lice ili s namerom da se to lice liši imovine na nezakonit način,

---

[7] Opširnije u: Šime Pavlović, *Spaming e-poruke – Kazneno djelo ili prekršaj u hrvatskom pravnom sistemu,* Hrvatski ljetopis za kazneno pravo i praksu, Zagreb, broj 1/2004, str. 287.

[8] Više o oblicima ispoljavanja kriminalnih aktivnosti na društvenoj mreži Fejsbuk u: Božidar Banović, Aleksandar Miladinović, *Kriminološko-fenomenološki aspekt Fejsbuka,* Časopis Kriminalističko-forenzička istraživanja, Internacionalna asocijacija kriminalista, broj 1, 2010. godine, Banja Luka, str. 45–58. Dostupno i na adresi *www.iak-bl.com/images/casopis/volumen1/4.pdf.*

- Računarski falsifikat – unos, izmena, brisanje ili potiskivanje računarskih podataka ili programa, kao i ostale vrste mešanja u obradu podataka na računaru ili pod uslovima, predviđenim domaćim zakonom, koje bi predstavljalo delo falsifikata da je počinjeno u odnosu na klasičan predmet takvog krivičnog dela,
- Oštećenje računarskih podataka ili računarskih programa – bespravno brisanje, oštećenje, kvarenje ili potiskivanje računarskih podataka ili računarskih programa,
- Računarsku sabotažu – unos, izmena, brisanje ili potiskivanje računarskih podataka ili računarskih programa ili mešanje u računarski sistem s namerom da se onemogući funkcionisanje računara ili telekomunikacionog sistema,
- Neovlašćeni pristup – bespravan pristup računarskom sistemu ili mreži kršenjem mera bezbednosti,
- Neovlašćeno ometanje – bespravno ometanje tehničkim sredstvima ulazne, izlazne komunikacije ili komunikacije unutar računarskog sistema ili mreže,
- Neovlašćeno kopiranje zaštićenog računarskog programa – bespravno kopiranje, distribucija ili javno objavljivanje računarskih programa zaštićenih zakonom i
- Neovlašćeno kopiranje topografije – bespravno kopiranje zakonom zaštićene topografije, poluprovodničkog proizvoda ili bespravno komercijalno korišćenje ili uvoz u te svrhe topografije ili poluprovodničkog proizvoda napravljenog korišćenjem topografije.

Pored navedenih, ova lista miminuma preporuka kojima se inkriminišu navedene zloupotrebe računara, računarskih sistema i interneta, može se proširiti i inkriminacijom izmene računarskih podataka ili računarskih programa, računarskom špijunažom, neovlašćenim korišćenjem računara i neovlašćenim korišćenjem zaštićenog računarskog programa, pod uslovom da su učinjeni s namerom.

Indikativno je, pogotovo ako se imaju u vidu savremeni bezbednosni rizici na internetu, da inkriminacija aktivnosti poput sajber-terorizma ili izazivanja globalnog informacionog rata nije predviđena aktuelnim Krivičnim zakonom, niti navedenim preporukama.

REGULISANJE BEZBEDNOSTI NA INTERNETU NA GLOBALNOM NIVOU

U zadnje vreme su primetne mnogobrojne aktivnosti u vezi sa normiranjem bezbednosti interneta na globalnom planu. To se, pre svega, odnosi na aktivnosti na nivou UN-a i na nivou Saveta Evrope i Evropske unije, ali i drugih organizacija globalnog ili regionalnog karaktera.

Ujedinjene nacije su, u okviru rada Generalne skupštine, usvojile nekoliko rezolucija koje se bave visokotehnološkim kriminalom. Ove rezolucije nemaju obavezujuću snagu za države članice i uglavnom su deklarativnog karaktera, ali je značajno pomenuti da sadrže i poziv svim državama da što pre usaglase svoja zakonodavstva u ovoj oblasti, kako bi se eliminisale ‘’sigurne države’’ za sajber-

kriminalce, u kojima takva štetna ponašanja nisu ni inkriminisana, ni sankcionisana na odgovarajući način. Generalna skupština Ujedinjenih nacija donosi nekoliko rezolucija godišnje o ''razvoju na polju informatike i telekomunikacija u kontekstu međunarodne bezbednosti''. Posebno se ističu rezolucije 53/70 (1998), 54/49 (1999), 55/28 (2000), 56/19 (2001), 57/239 (2002) i 58/199 (2003). Od godine 1998, sve potonje rezolucije uključile su sličan sadržaj, bez bilo kakvih značajnih poboljšanja. Osim ovih rutinskih rezolucija, glavni proboj bio je u nedavnom setu preporuka za pregovore o ugovoru o sajber-bezbednosti, koje je generalnom sekretaru UN podnelo 15 država, uključujući stalne članice Saveta bezbednosti (Kurbalija, 2011: 70).

Osim toga, UN su aktivne na suzbijanju visokotehnološkog kriminala putem različitih specijalizavnih agencija i drugih tela, među kojima se posebno ističu aktivnosti Međunarodne telekomunikacione unije. Na međunarodnom nivou, unija je najaktivnija organizacija – ona je stvorila veliki broj bezbednosnih okvira, arhitektura i standarda, uključujući ''x.509'', koji obezbeđuje bazu za glavnu javnu infrastrukturu, koja se, na primer, koristi u bezbednoj verziji XTTP (hipertekstulanog transfernog protokola). Nedavno je ova unija izašla iz strogo tehničkih aspekata i pokrenula je program globalne sajber-bezbednosti. Ova inicijativa obuhvata zakonske mere, kooperativnost u sprovođenju politike i izgradnju kapaciteta.

Grupa G8 takođe ima nekoliko inicijativa na polju sajber-bezbednosti, čija je svrha poboljšanje saradnje između agencija koje sprovode zakon. Ona je formirala Podgrupu za visokotehnički kriminal, da bi se bavila uspostavljanjem neprestanih komunikacija između centara za sajber-bezbednost država članica, obukom osoblja i poboljšanjem državnih pravnih sistema za borbu protiv sajber-kriminala i unapređenje saradnje između IKT industrije i agencija za sprovođenje zakona. Podgrupa je nastala 1996. godine, kao deo tzv. Lionske grupe, koja ima za prevashodni cilj da se kroz sastanke informiše o borbi protiv različitih oblika transnacionalnog kriminala u državama-članicama G8. Podgrupa je do sada organizovala niz konferencija i edukativnih programa, a među najvažnije rezultate njenog rada se ubrajaju pisanje (neformalne) strategije borbe protiv haj-tek kriminala, kao i stvaranje mreže kontakt-osoba na nacionalnom nivou (slične službi 24-7, ustanovljene Konvencijom o visokotehnološkom kriminalu Saveta Evrope) koja trenutno funkcioniše u 40 država, i čiji je prevashodni cilj saradnja i razmena informacija u ovoj oblasti (Komlen – Nikolić i drugi, 2010: 34).

Kada je u pitanju Savet Evrope, nezaobilazno je da se pomene Konvencija o računarskom kriminalitetu, pogotovo s obzirom na to da je Savet Evrope jedino globalno telo koje je donelo (do sada) jedinu međunarodnu konvenciju iz ove oblasti na nadnacionalnom nivou. Konvencija o računarskom kriminalitetu Saveta Evrope za sada je jedini međunarodni dokument koji je otvoren za potpisivanje i za države nečlanice.[9]

---

[9] Konvencija Saveta Evrope o visokotehnološkom kriminalu je usvojena 2001. godine. Za njeno stupanje na snagu bilo je potrebno najmanje pet ratifikacija, od toga najmanje tri od strane država-članica Saveta Evrope, što se i dogodilo 1. jula 2004. godine. Do sada su je potpisale 43 zemlje-članice Saveta Evrope, od čega su je ratifikovale samo 22 države. Srbija se nalazi među državama koje su Konvenciju potpisale (2005. godine) i ratifikovale (2009. godine). Od država koje nisu članice Saveta Evrope, potpisale su je Kanada, Japan, Južna Afrika i SAD, ali su je ratifikovale samo SAD. Godine 2003. je donet Dodatni protokol uz Konvenciju, koji se bavi inkriminisanjem akata

Iako je globalna dimenzija računarskog kriminaliteta izuzetno izražena, za sada ne postoje univerzalni akti koji bi regulisali ovu oblast. Ipak, neke aktivnosti od značaja za međunarodnu saradnju i suzbijanje ovog vida kriminaliteta aktuelne su u okviru različitih globalnih i regionalnih organizacija.

Evropska unija je takođe posvetila deo svoje pažnje pitanjima vezanim za visokotehnološki kriminalitet. Prvi dokumeti, koje su 1995. i 1997. godine doneli Evropski parlament i Savet Evrope, odnosili su se na zaštitu privatnih elektronskih podataka prilikom njihove obrade i transmisije. Godine 2001. organizovan je Forum Evropske unije o sajber-kriminalu, a 2005. godine Savet je, na predlog Evropske komisije, doneo okvirnu odluku kojom su inkriminisana različita ponašanja koja se vezuju za visokotehnološki kriminal, kao što su nelegalni pristup informacionim sistemima, nelegalne izmene u računarskim sistemima i nelegalne izmene računarskih podataka (Komlen-Nikolić i drugi, 2010).

UMESTO ZAKLJUČKA

Bezbednost interneta, odnosno bezbednost na internetu se mora posmatrati kao proces, a ne kao stanje, uz uvažavanje maksime da ‘’apsolutna bezbednost nije moguća’’, ni u društvu, pa tako ni na internetu. Međutim, iako ‘’apsolutna bezbednost’’ nije moguća, to ne znači da se internet mora prepustiti stihijskim stremljenjima, kako samih korisnika i drugih subjekata na internetu, tako i određenim tehnološkim procesima od kojih zavisi tehnička bezbednost interneta. Upravo suprotno, bezbednost na internetu, shodno konceptu da je ovaj vid bezbednosti proces, a ne stanje, mora da se podvrgava određenim standardima koji se moraju zahtevati od svih korisnika interneta.

Međutim, bezbednosni standardi na internetu se, uglavnom, posmatraju kao vid narušavanja neutralnosti mreže, pa čak i kao vid cenzure interneta kroz kontrolu korisnika ili sadržaja na internetu. Ovo je i razumljivo ukoliko se ima u vidu da svi bezbednosni mehanizmi, odnosno aktivnosti koje imaju za cilj da održavaju bezbednost određenog sistema (pa bio on i internet), delimično (u većoj ili manjoj meri) narušavaju primarnu svrhu, ulogu, proces rada i suštinu tog sistema.

Razumevanje interneta, svest o postojećim opasnostima, odgovorno ponašanje i korištenje računarske zaštite nužni su kako bi ovu nesigurnu mrežu svaki korisnik za sebe učinio sigurnim mestom. Cenzura interneta je razumna opcija, ukoliko se ona izvodi na razuman način. Krajnji cilj cenzure na internetu trebao bi biti potpuno uklanjanje stranica društveno neprimerenog sadržaja, ali bi, s druge strane, internet uvek trebao ostati transparentno mesto na kojem svi korisnici mogu naći primerene i tačne informacije.[10]

Usled navedenog, bezbednost na internetu mora da bude optimalno rešenje između suprotstavljenih koncepata posmatranja interneta – s jedne strane,

---

rasističke i ksenofobične prirode počinjenih putem računarskih sistema. Dodatni protokol je stupio na snagu nakon što ga je ratifikovalo pet država, 1. marta 2006. godine. Tekst Konvencije i ostali bitni podaci mogu se naći na internet adresi: *http://conventions.coe.int/Treaty/ Commun/QueVoulezVous.asp?NT=185&CL=ENG* (Komlen – Nikolić i drugi, 2010).

[10] *Cenzura na internetu,* Centar informacijske sigurnosti, Zagreb, 2011. godine, dostupno i na: *www.cis.hr/files/dokumenti/CIS-DOC-2011-06-016%281%29.pdf.*

posmatranog kao ‘’poslednje utočište slobode’’ koje je determinisano konceptom neutralnosti mreže, odnosno uticaja formalnih ograničenja formalnih subjekata lokalne, nacionalne ili globalne zajednice, te, s druge strane, nastojanja upravo tih zajednica da na određeni način regulišu sve brojnije i frapantnije slučajeve kršenja bezbednosti kojima se narušava lični, ali i nacionalni, pa i globalni integritet korisnika interneta.[11]

LITERATURA

1. Banović, Božidar, Miladinović, Aleksandar, *Kriminološko-fenomenološki aspekt Fejsbuka,* Časopis ‘’Kriminalističko-forenzička istraživanja’’, Internacionalna asocijacija kriminalista, Banja Luka, broj 1, 2010. godine,
2. Krapac, Davor, *Kompjuterski kriminalitet*, Pravni fakultet, Zagreb, 1992. godine,
3. Kešetović, Želimir, *Izazovi Interneta: Putevi i stranputice svjetske kompjuterske mreže,* Bezbednost, Beograd, 6/96,
4. Kurbalija, Jovan, *Uvod u upravljanje internetom,* Albatros plus, Beograd, 2011. godine,
5. Pavlović, Šime, *Kompjutorska kaznena djela u Kaznenom zakoniku – osnove hrvatskog informacijskog kaznenog prava,* Hrvatski ljetopis za kazneno pravo i praksu, Zagreb, broj 2/2003,
6. Pavlović, Šime, *Spaming e-poruke - Kazneno djelo ili prekršaj u hrvatskom pravnom sistemu,* Hrvatski ljetopis za kazneno pravo i praksu, Zagreb, broj 1/2004,
7. Džemail Zornić, *Kompjuterski kriminal – Zločin i prevencija*, Zbornik radova ‘’Zloupotreba informacionih tehnologija i zaštita’’, ZITEH 2010, IT vještak, Beograd, 2010. godine,
8. Lidija Komlen Nikolić i drugi, *Suzbijanje visokotehnološkog kriminala,* Udruženje javnih tužilaca i zamjenika javnih tužilaca Srbije, ATC Beograd, 2010. godine,
9. *Cenzura na internetu,* Centar informacijske sigurnosti, Zagreb, 2011. godine,
10. *Nacional Information Systems Security Glossary,* Nacional Security Agency, Fort Meade, 2000. godine,
11. *www.iak-bl.com/images/casopis/volumen1/4.pdf,*
12. *www.cis.hr/files/dokumenti/CIS-DOC-2011-06-016%281%29.pdf,*
13. *www.ekfak.kg.ac.rs.*

[11] Nekoliko pitanja je aktuelno u vezi sa sajber privatnošću:
Prvo pitanje se odnosi na samu prirodu organizacije interneta koja pogađa njegovu bezbednost. Da li nastaviti sa sadašnjim pristupom izgradnji bezbednosti na postojećim nebezbednim temeljima ili promeniti bazu infrastrukture interneta? Kako bi se takva promena odrazila na druge karakteristike interneta, naročito na njegovu otvorenost i transparentnost? Najveći deo dosadašnjeg razvoja internet standarda imao je za cilj poboljšanje performansi ili uvođenje novih aplikacija – bezbednost nije bila prioritet.
Drugo pitanje o kojem se raspravlja jeste odnos između bezbednosti i privatnosti. Da li će dodatne mere u vezi sa sajber-bezbednošću podrazumevati izvestan gubitak privatnosti? Kakva regulativa bi trebalo da se primeni na softver kodiranja, koji se može koristiti i za legitimnu zaštitu komunikativne privatnosti i za zaštitu komunikacije od terorista i kriminalaca? Odgovori na ova i druga pitanja zavise od stalnog pomeranja balansa između sajber-bezbednosti i privatnosti.
Treće pitanje je jedno od centralnih pitanja rasprave o bezbednosti interneta, a odnosi se na kodiranje, koje se bavi sredstvima koja se mogu koristiti za zaštitu podataka komunikacije (Kurbalija, 2011: 70).

RESUME

Violating internet security or security of certain internet services (web sites, social networks, forums, e-business) has been spreading progressively, which is why qualitative and quantitative aspects of this issue come into foreground. This is, at first place, normative and security issue, but also technical/technological, and global one, that has not been agreed upon by the subjects who claim "the right to the Internet".

This issue is also conditioned by the concept of "network neutrality", but also by other ones of normative, technological, security and cultural nature. That is why the security in cyber-space has been ignored, or understood as a default, although it does not reflect the real situation. Instead of that, it is a fact that personal, collective and international security is being jeopardized on the Internet on daily basis.

The consequences of that, due to Internet incorporation in all aspects of social life, are enormous. Regarding that, this paper focuses on observing security on the Internet from the technical/technological, user's, normative and global point of view.

Pregledni rad - UDK 004.738.5: 343.341

INTERNET I TERORIZAM

Prof. dr Želimir Kešetović[1*]
Fakultet bezbednosti Univerziteta u Beogradu
Mr Marija Blagojević, istraživač saradnik[2*]
Kriminalističko-policijska akademija, Beograd

Apstrakt: Kao epohalno novi medij, internet je temeljno izmenio sve oblasti ljudske egzistencije i stvorio novu – virtuelnu stvarnost, koja ima sasvim opipljive posledice i u realnoj stvarnosti. Nastanak i razvoj svetske megamreže uticao je i na sferu bezbednosti uopšte, a posebno na terorizam. Priroda tog uticaja je ambivalentna. Internet je zbog niza kakteristika, kao što su lak pristup, raspoloživost, neregulisanost, odsustvo cenzure i vladine kontrole, potencijalno velika publika u celom svetu, anonimnost komunikacije i decentralizacija i brz protok informacija, te jeftina veb prisutnost i stalno kretanje i evazija našao višestruku primenu od strane terorista za planiranje i koordinaciju, upravljanje operacijama, propagandu, prikupljanje sredstava, publicitet, psihološki rat, prikupljanje podataka, regrutovanje i mobilizaciju itd. i time postao njihovo važno oruđe. Najvažniji otežavajući faktori u borbi protiv korišćenja interneta od strane terorista su nepostojanje (kašnjenje) legislative, odnosno njena nedorečenost i nepreciznost, te različita etička pitanja i dileme. Međutim, internet je istovremeno otvorio i nove mogućnosti u borbi protiv terorizma, jer omogućava prikupljanje informacija o teroristima, a može poslužiti i za širenje univerzalnih ljudskih vrednosti i prevazilaženje etničkih, religijskih i ideoloških predrasuda i stereotipa, podsticanje i promovisanje umerenosti u zajednicama iz kojih se regrutuju teroristi i time dovesti do svojevrsne deradikalizacije.

Ključne reči*:* terorizam, internet, komunikacija, mediji, bezbednost

1. UVOD – TERORIZAM KAO MEDIJSKI FENOMEN

Od samog nastanka terorizma pa sve do njegove savremene ekspanzije i direktnog prenosa terorističkih akcija, poput napada od 11. septembra na SAD koji je postao medijski spektakl, medij i terorizam su neodvojivi fenomeni. O tome postoji uglavnom skoro opšta saglasnost, za razliku od pitanja koja se tiču dimenzija, prirode i posledica ovog odnosa.

Odnos medija i terorizma jeste predmet interesovanja brojih naučnika iz razlitičih akademskih disciplina, ali i celog niza samoproklamovanih "eksperata" za ovu temu. Postoje različite vrste terorista i brojni oblici medija, što takođe problem čini složenijim i uslovljava različite pristupe.

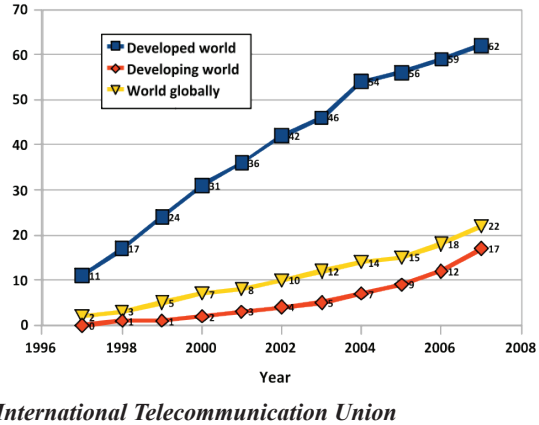
[1] * zelimir.kesetovic@gmail.com
[2] * marija.blagojevic@kpa.edu.rs

Jedan od prvih i dosta retkih pokušaja sinteze literature koja se odnosi na medije i terorizam može se naći kod Sinjorelija i Gerbera (Signorielli & Gerbner, 1988). Može se uočiti najmanje 14 različitih modela, mada će svaki spisak biti samo privremen, budući da se današnji svet veoma brzo menja. Tako iz aspekta retorike postoji pristup "propagande", u okviru sociologije "spektakl" pristup, psihološki "među-kulturni" pristup, komunikacije studije koriste "konstruktivistički" pristup, ekonomija vodi računa o "šteti", vojne studije govore o "instrumentu rata", unutrašnja bezbednost (homeland security) polazi od "rizika", studije terorizma govore o "ratu ideja", a javna politika o "upravljanju informacijama", pristup političkih nauka je "kontrola mišljenja" a humanisti prihvataju "Enigma" pristup, novinari su za pristup "praćenje medija", pravne studije "etički"pristup, i međunarodni odnosi "interkulturalni"pristup.

2. POTENCIJALI INTERNETA KAO TERORISTIČKOG ALATA

Kada su sredinom šezdesetih godina XX veka američki istraživači u eksperimentalne svrhe povezali računare putem telefonskih linija koristeći fondove Agencije za savremene istraživačke projekte (Advanced Research Project Agency – ARPA) sa ciljem razvoja mreže koja će moći da izdrži nuklearni udar, niko nije mogao ni da zamisli da je time postavljen pravac razvoja koji će iz temelja promeniti sliku savremenog sveta i uvesti novu dimenziju egzistencije – virtuelnu realnost. U 2008. godini internet dostiže punoletstvo sa oko milijardu korisnika, od čega u SAD 200 miliona, a u Kini 120 miliona, i sa oko 100 miliona sajtova. Naravno, postoje velike razlike u raširenosti interneta između razvijenih i nerazvijenih zemalja.

Internet users per 100 inhabitants 1997-2007 (Source: ITU)



Izvor:International Telecommunication Union

Na mrežu se svakog dana u proseku priključi 100.000 novih korisnika. Globalna mreža je iz temelja revolucionisala mnoge oblasti ljudskog života i rada, otvorivši neslućene i u dosadašnjoj istoriji nezabeležene mogućnosti ljudske

komunikacije i razmene informacija iz najrazličitijih oblasti ljudskog stvaralaštva. Otvaraju se nove dimenzije naučnog rada, privrednog poslovanja, državnog planiranja, ratovanja, ugrožavanja, ali i stvaranja bezbednosti. Nastaju nove mogućnosti za planiranje, pripremu i izvršenje različitih vrsta krivičnih dela, širenje opasnih ideja, ideologija i informacija, ali i mogućnosti za delovanje i saradnju organa i službi bezbednosti, podizanje bezbednosne kulture građana i ostvarivanje partnerstva svih subjekata sistema bezbednosti na različitim nivoima (Kešetović, 2008).

Ako, uz nužna ograničenja na koja upozoravaju drugi autori, prihvatimo mišljenje Pola Vilkinsona da kada neko kaže "terorizam" u demokratskom društvu, on kaže istovremeno i "mediji", pošto je po svojoj prirodi terorizam psihološko oružje koje zavisi od komunikacije pretnje prema širem društvu (Wilkinson, 2001), onda su se pojavom interneta za teroriste pojavile praktično neograničene šanse i mogućnosti. Stručnjaci koji se bave islamskim terorizmom navode da je stvaranjem interneta ostvaren jedan od glavnih ciljeva islama – stvorena je svojevrsna umma, to jest svetska zajednica vernika. Postmoderni teroristi koriste blagodeti globalizacije i moderne tehnologije da planiraju koordiniraju i izvršavaju svoje smrtonosne planove. Oni više nisu geografski ograničeni u okviru određene teritorije, politički ili finansijski zavisni od pojedinačne države, već se oslanjaju na savremene komunikacione kapacitete uključujući i internet.

Kao glavne prednosti interneta, koji od slabih pravi jake (power of the week), navode se:

- lak pristup
- raspoloživost (svaki jezik, svako vreme, e-mail, chat, diskusione grupe, blogovi, zvuk, slika, otvorena ili kodirana komunikacija)
- neregulisanost, odsustvo cenzure i vladine kontrole
- potencijalno velika publika u celom svetu
- anonimnost komunikacije – internet korisnici uživaju veliki stepen anonimnosti. Postoje brojne bezbednosne informatičke aplikacije koje omogućavaju korisnicima da sakriju svoj identitet, sadržaj svoje komunikacije ili detalje svojih transakcija. Ovo uključuje besplatne e-mail servise, steganografske i enkriptičke alate itd.
- brz protok informacija (mogućnost kompresije podataka i smanjenje vremena potrebnog za razmenu informacija)
- mogućnost prenošenja veće količine informacija,
- niski troškovi: registracija veb sajta košta manje od 50 $ a mnogi internet sajtovi omogućavaju potpuno besplatno kreiranje Web sajta. Besplatni e-mail servisi su opšte mesto, a nema troškova ni kod postavljanja poruka i newsgrupage.
- stalno kretanje i evazija (stvaranje i brisanje adresa)
- široka lepeza oružja (virusi, crvi, backdoor bombe)
- format: mogućnost kombinacije teksta, grafike, zvuka i slike, čime komunikacija postaje produbljena, dinamična i vizuelno stimulativna
- pravac: mogućnost dvosmerne interaktivne komunikacije je veoma proširena na mreži kao rezultat većeg prostora i brzine, ali takođe i usled horizontalnih i bočnih veza koje su omogućene hipertkest linkovima između sajtova.

- individualna kontrola: otvaranje mogućnosti direktne kontrole nad slanjem i primanjem informacija znači da je moć decentralizovana na individualnog korisnika koje ima izbor šta će da gleda i šta će da objavi
- kritične infrastrukture kao potencijalni ciljevi.

Ukratko, komunikacija na svetskoj računarskoj mreži je trenutna i neposredna, individualna, dinamička, produbljena, interaktivna, anonimna, necenzurisana i nepreprav ljena, jeftinija i daleko dosežna, što je čini superiornijom u odnosu na mogućnosti koje pružaju drugi mediji. Teroristi su potpuno svesni ovih mogućnosti interneta i to objašnjava zašto su ga tako žustro prihvatili. (Weimann, 2004)

3. PODRUČJA PRIMENE INTERNETA OD STRANE TERORISTA

Prema Gabrijelu Vajmanu, postoji osam osnovnih načina na koje teroristi koriste internet: to su psihološko ratovanje, publicitet i propaganda, prikupljanje podataka, prikupljanje sredstava, regrutovanje i mobilizacija, newtworking (mrežni rad), deljenje informacija i planiranje i koordinacija (Weimann, 2004, 5–11). Upoređujući Vajmanovu kategorizaciju sa onima koje su sugerisali Fred Koen (Cohen), Stiv Furnel (Steve Furnell) i Metju Voren (Matthew Warren), i Timoti Tomas (Timothy Thomas), Maura Konvej utvrđuje pet osnovnih načina na koje teroristi koriste internet: odašiljanje informacija, finansiranje, networking, regrutovanje i prikupljanje informacija. Ona objašnjava detaljnije svaku od njih. (Conway, 2006).

3.1. Odašiljanje informacija

Teroristi koriste internet da zadobiju odnosno povećaju publicitet, vrše propagandu i vode psihološki rat. internet, a posebno pojava World Wide Web je značajno povećala mogućnosti da teroristi obezbede publicitet. To može imati oblik istorijske informacije, profila lidera, manifesta itd. Međutim, internet se može koristiti i kao oružje u psihološkom ratu odnosno za širenje dezinformacija, upućivanje pretnji i diseminovanje užasnih slika, kao što je odsecanje glava taocima snimljeno i postavljeno na klipovima na internetu. Za širenje takvih slika pre pojave interneta teroristi su bili upućeni na tradicionalne medije: televiziju, radio i štampane medije koji su imali višestepene procedure i proces uredničke selekcije, pa taj "selekcioni prag" nisu mogli uvek da preskoče (Weimann, 2004: 6). Ovakve prepreke na internetu ne postoje i on daje terorističkim grupama direktnu kontrolu nad porukama koje plasiraju. Takođe se povećava njihova sposobnost da oblikuju vlastitu percepciju kod pojedinih ciljnih grupa, čak i veoma malih, i da manipulišu ne samo sopstvenim imižddžom već i imidžom svojih neprijatelja.

3.1.1. Teroristički sajtovi

Da su terorističke organizacije veoma brzo shvatile potencijale interneta govori podatak da je 1998. godine manje od polovine organizacija koje su SAD označile kao strane terorističke organizacije imalo su svoje veb sajtove, da su do kraja 1999. skoro sve ove grupe postale prisutne na internetu, a da danas sve

aktivne terorističke grupe imaju bar jedan oblik prisustva na internetu. Rezultati praćenja od 1998. do 2007. ukazuju na preko 5.000 terorističkih veb sajtova, onlajn foruma i sobe za ćaskanje (chat rooms). Neke grupe imaju više od jednog internet vebsajta . Naime, postoji jedan glavni (the "Home-page") i veći broj nezvaničnih. Opremu, tehničko znanje i podršku obezbeđuju simpatizeri terorističke grupe, dok sadržaj obezbeđuju teroristi operativci sa mesta zločina. Ma koliko pogodaka da bude na veb sajtu, ako je dobro održavan i dizajniran on daje terorističkoj grupi privid legitimnosti i privlači pažnju ostalih masovnih medija. (Conway, 2006).

Princip prezentacije je isti na skoro svim terorističkim veb sajtovima.

- osnovni ciljevi i misija
- istorijat organizacije. Retko se daju i strašne fotografije koje svedoče o njenim "podvizima". Često se široko navode argumenti koji imaju za cilj moralno opravdanje njihovog delovanja, što treba da obezbedi simpatije i podršku u delu zapadne javnosti
- deo namenjen domaćim simpatizerima sadrži teme o političkim zatvorenicima i političkoj korupciji koje dovode u pitanje legitimitet sopstvene vlade.

Prezentacije uglavnom uključuju audio i video elemente. Posebna pažnja se posvećuje logo-ima i amblemima, dok oni više sofisticirani sadrže i govore, poeziju i muziku za učitavanje. Neki imaju i falsifikovane faktografske sadržaje, a manji broj sadrži i on-line prodavnice poklona (gift shops). Pojedini internet sajtovi (http://www.awladna.net/) sadrže i kompjuterske igrice za decu sa sadržajem koji je ideološki u skladu sa ciljevima terorističke organizacije, odnosno koji može predstavljati pripremu za buduće regrutovanje novih članova. Starijima su namenjeni muzički sadržaji hip-hop i rep muzičara, čije primamljive melodije, odnosno melodične poruke sadrže pozive na nasilje kao što su pesme repera Sheikh Terra koji peva sa pištoljem u jednoj i Kur-anom u drugoj ruci.

Korišćenje interneta za terorističke svrhe uglavnom se svodi na ekstremne arapske islamističke grupe, što nije opravdano. Naime, internet koriste i čečenski teroristi, PKK (kurdska nacionalistička organizacija) i niz drugih terorističkih organizacija i grupa.

Abdul Bakier (2006) govori o elektronskom džihadu kao vrsti sajber rata u kome se napadaju antiislamistički vebsajtovi. U tom smislu posebno su zanimljivi pokušaji pridobijanja novih ideoloških sledbenika uz pomoć as-Sahab, al-Qaedinog krila zaduženog za medijsku produkciju, pre svega video materijala:

- training video – objašnjenja kako se prave bombe i eksplozivi
- operativni video – pokazuju kako je neprijatelj ranjiv
- govori – u punom trajanju, ponekad kodirani da zbune protivnika
- fotografije – često falsifikovane, na kojima su žrtve ubijene od strane neprijatelja ili sa porukom (crni turban/beli turban)

Komunikacija terorista preko interneta može biti otvorena, ali se mogu koristiti i kriptografija (kodirana informacija koji se vidi, ali se ne razume ukoliko se ne dešifruje kod) i steganografija (prekrivena informacija čiji bi najbanalniji primer bio slika preko slike u ppt. prezentaciji)[3], gde se poruka uopšte ne vidi, ali i njihova kombinacija.

[3] Postoje veoma sofisticirani oblici steganografije, u koju svrhu se koriste posebne softverske aplikacije.

3.2. Finansiranje

Poznato je da organizacija i funkcionisanje terorističkih grupa i izvođenje terorističkih akcija zahtevaju znatna finasijska sredstva. Brzina i interaktivna priroda internetske komunikacije, uz rasprostranjenost i globalnu prisutnost interneta otvaraju izvanredne mogućnosti za značajno prikupljanje finansijskih priloga.

Teroristi tragaju za novcem bilo putem veb sajtova ili korišćenjem internet infrastrukture da bi mobilisali resurse korišćenjem nelegalnh sredstava. Brojne terorističke grupe traže direktno finansijske priloge od posetilaca svojih sajtova, bilo u obliku uopštenih konstatacija o potrebi organizacije za novcem ili neposredno apeluju na svoje simpatizere da na određen bankovni račun izvrše transfer novca. Neki su, poput Ulster Loyalist Information Service, koji je povezan sa Loyalist Volunteer Force (LVF), primali sredstva pomoću PayPal servisa, ali su i pozivali pristalice kojima je neprijatno da daruju novac, da doniraju druge stvari, kao što su neprobojni prsluci. Neke grupe prikupljaju sredstva na taj način što postavljaju onlajn prodavnice u kojima prodaju knjige, audio i video trake, zastave, majice itd.

Prisutno je i iskorišćavanje kompanija, alata za elektronsku trgovinu i humanitarnih fondova. Prema Žan Fransoa Rikardu (Jean-Francois Ricard),jednom od najboljih francuskih istražitelja terorizma, mnoge islamističke terorističke akcije su finasirane pomoću prevara s kreditnim karticama. (Thomas 2003, 117). Prema holandskim ekspertima neke terorističke organizacije su veoma usavršile internet prevare, a postoje i brojni dokazi da su teroristi ili njihovi simpatizeri osnovali preduzeća da bi zaradili novac za svoje aktivnosti. Pored preduzeća, teroristi koriste i postojeće ili osnivaju svoje humanitarne organizacije. Ovo je naročito raširenо među islamističkim terorističkim organizacijama, s obzirom na to da je davanje milosrđa jedna od verskih dužnosti. Neke od "humanitarnih" organizacija koje se koriste u ove svrhe jesu Mercy International, Wafa al-Igatha al-Islamiya, Rabita Trust, Al Rasheed Trust, Global Relief Fund, Benevolence International Foundation i Help The Needy, koje se oglašavaju u novinama, na vebsajtovima i chat sobama islamističkim temama.

3.3. Rad u mreži (Networking)

Korišćenje interneta koji omogućava da pojedinci rasuti na razne strane brzo komuniciraju i efektivno koordiniraju svoje akcije po malim cenama, utiče i na **izmenu organizacione strukture terorističkih grupa**. Internet ne omogućava samo unutargrupnu komunikaciju, već i međugrupno povezivanje, povećavajući kapacitete terorista da transformišu svoje strukture i izgrade veze zahvaljujući alternativnom prostoru koji se stvara za komuniciranje i dogovore i hipertekstualnoj prirodi veba koja omogućava grupama da povežu svoje unutrašnje podgrupe i eksterne organizacije širom planete sa svog centralnog veb sajta.

Arkvila i saradnici ukazali su na pojavu novih oblika terorističkih organizacija prilagođenih informatičkom dobu, navodeći da će oni nastaviti da se pomeraju od hijerarhijske ka mrežnoj strukturi. Veći napori će biti uloženi u izgradnju niza transnacionalnih grupa povezanih Internetom nego u izgradnju čvrstih samostalnih grupa.

Radi se o vrsti organizacione strukture koja je kvalitativno različita od tradicionalnog hijerarhijskog dizajna. Teroristi će sve više biti organizivani u

potpuno mrežnom, decentralizovanom i "višekanalnom" maniru u kome ne postoji pojedinac, centralno rukovodstvo, komanda ili štab. U okviru mreže kao celine postoji malo hijerarhije i može biti više lidera, u zavisnosti od veličine grupe. Nema, dakle, glave ili srca u koje bi trebalo ciljati. Ovakva grupa, da bi ostvarila svoj potencijal, mora koristiti najsavremenije informacione i komunikacione tehnologije, a internet postaje njihova integralna komponenta. (Arquilla et al,1999:41).

Internet se takođe koristi za **planiranje, odlučivanje i koordiniranj**e akcija. Mnogi od terorista koje su SAD optužile za 11. 9. komunicirali su imejlom. U optužnici četvorice članova Oružane islamske grupe (Gama'a al-Islamiyya) navodi se da su kompjuteri bili korišćeni za prenos i distribuciju poruka, komunikacija i informacija između lidera i članova grupe u SAD i širom sveta.[4] Omogućena je i komunikacija između različitih grupa, tako da teroristi iz Čečenije, Palestine, Indonezije, Avganistana, Turske i Iraka mogu razmenjivati ideje, sugestije i sasvim praktične informacije u pripremanju napada.

Korišćenje interneta **smanjuje i rizik** za teroriste koji su pod sve većim pritiskom policije. Informacione tehnologije daju teroristima globalnu moć i domašaj, pri čemu oni ostaju nevidljivi (Tibbetts, 2002: 5). One stvaraju distancu između planera napada i njihovih ciljeva i omogućavaju teroristima da planiraju bez rizika koji nosi upotreba mobilnih telefona (Thomas, 2003: 119).

3.4. Regrutovanje

Veb komunikacija je olakšala i regrutaciju odnosno mobilizaciju simpatizera da aktivnije podrže terorističke ciljeve ili aktivnosti. Potencijalni regruti lakše i brže dolaze do informacija u multimedijalnom formatu, dok globalni doseg mreže omogućava grupama da objavljuju događaje i da ih vidi veći broj ljudi, a povećane su i mogućnosti za interaktivnu komunikaciju, pomaganje grupi i kontaktiranje sa njom. Konačno korišćenje diskusionih foruma omogućava kako simatizerima tako i protivnicima da se angažuju u debati. Ovo može pomoći terorističkoj grupi u prilagođavanjeu njene pozicije i taktike i povećanju opšte podrške. Tvrdi se da je onlajn regrutovanje dosta raširenо. Vajman sugeriše da oni koji regrutuju teroriste mogu koristiti interaktivnu Internet tehnologiju da tragaju po čet sobama za pojedincima, pre svega mladim ljudima. U tu svrhu mogu poslužiti i elektronski bilteni (Weimann, 2004:8).

3.5. Prikupljanje podataka

Internet omogućava korisnicima pristup ogromnoj količini informacija do kojih je ranije bilo veoma teško doći, budući da su bile uskladištene u veoma različitim formatima i na različitim lokacijama. Danas postoji na hiljade internet alata koji pomažu u prikupljanju informacija. Teroristi koriste mrežu za traganje za podacima ('data mining') tj. prikupljanje i sređivanje podataka o potencijalnim metama, ali i o antiterorističkim merama i strategijama i za deljenje podataka ('information sharing'). Zbog ovoga se u SAD povela ozbiljna rasprava o dostupnosti podataka

4 Indictment, United States v. Sattar, No. 02-CRIM-395, 11 (S.D.N.Y Apr. 9, 2002). Available onlajn at http://news.findlaw.com/hdocs/docs/terrorism/ussattar040902ind.pdf.

na sajtu Ministarstva odbrane, kao i podataka o kritičnim infrastrukturama poput nuklearnih elektrana, a policijske agencije su zabrinute zbog proliferacije veb strana na temu "kako da" (napravim bombu kod kuće, vodimo biološki rat i sl.).

4. INTERNET KAO ORUĐE U BORBI PROTIV TERORIZMA

Internet kao novi globalni medij nije isključivo oruđe terorista. On je jednostavno tehničko sredstvo u rukama ljudi, i kao takav nije ni dobar ni loš. Od ljudi zavisi kako će ga i u koje svrhe koristiti. U tom smislu on je i novo oruđe koje stoji na raspolaganju službama koje su zadužene za suzbijanje i kontrolu terorizma. Preko interneta snage bezbednosti mogu dosta saznati o verovanjima, vrednostima, planovima i aktivnostima i ponašanju terorističkih organizacija. Ove informacije se mogu koristiti za sprečavanje terorističkih napada. Kao znaci ranog upozorenja mogu poslužiti sumnjive aktivnosti i signali:

- povećana frekvencija poruka – (prve poruke AQ u maju, a poslednje 9. 9, dok je najveća frekvencija bila u avgustu)
- povećan saobraćaj na bratskim sajtovima – logističke informacije i drugi podaci se postavljaju u kodiranom obliku na sajtove ideološki bliskih organizacija
- u planiranju 11. 9. pripadnici Al-Q razmenili su međusobno na hiljade poruka na delu islamističkog veb sajta koji je zaštićen lozinkom
- u ratu protiv Izraela Hamas je primio novac prikupljen preko veb sajta fondacije Svete zemlje za spas i razvoj stacionirane u SAD
- na veb sajtu TV stanice AL Manar Hezbolah je proturio antijevrejsku glasinu da 11. 9. oko 4.000 Jevreja nije došlo na posao u STC, jer su upozoreni na predstojeći napad.

U pretpolju terorističkih aktivnosti korišćenje interneta je značajno u smislu širenja univerzalnih ljudskih vrednosti i prevazilaženja etničkih, religijskih i ideoloških predrasuda i stereotipa, podsticanja i promovisanja umerenosti u zajednicama iz kojih se regrutuju teroristi i svojevrsne deradikalizacije (http://www.islamnet.eu/).

U operativnom smislu, među prilikama koje pruža mreža valja navesti mogućnost praćenja terorističkih aktivnosti, infiltraciju u forume, pravljenje falš veb sajtova da se zavaraju i namame teroristi i simpatizeri, međunarodna saradnja organa i službi bezbednosti u smislu transfera tehnologije, znanja i informacija, te mobilizacija što šireg kruga subjekata za borbu protiv terorizma (http://www.antiteror.ru).

5. UMESTO ZAKLJUČKA

Kao što primećuje DŽefri Simon, teroristi su uvek koristili poslednju reč medijske tehnologije svog vremena. U budućnosti teroristi neće koristiti medije samo za oblikovanje javnog mnjenja, već i za uticaj na izbore, javnu politiku, spoljnu politiku i ponašanje potrošača. (Simon, 1994).

Teroristi menjaju startegiju i napadaće preko interneta, tvrdi direktor FBI Robert Miler. Stručnjaci iz Biroa veruju da je skori napad na kompjuterizovane

sisteme u Americi neminovan. Direktor je upozorio Kongres da teroristi menjaju startegiju i da će napasti putem interneta. Neki stručnjaci iz Biroa veruju da je veliki napad na kompjuterizovane sisteme u Americi neminovan već u narednih nekoliko meseci. "Zaista verujem da će u doglednoj budućnosti pretnja od kibernetičkih napada biti ista ili veća od pretnje klasičnog terorizma", kaže Miler. Budući da su svi veliki sistemi u Americi, uključujući kontrole leta, električne mreže, kontrole vozova i tokova novca, kompjuterizovani i umreženi, članovi Kongresa ozbiljno su shvatili upozorenje. Predsednik Komiteta za obaveštajni rad Majk Rodžers ističe da se kompjuterski napad već sprema. "Katastrofa koja će nas pogoditi je neminovna, a časovnik otkucava", kaže Rodžers. Stručnjaci upozoravaju da Amerikancima, ali i stanovnicima drugih razvijenih zemalja, ne preti samo opasnost da ostanu u mraku, bez gasa, vode ili u nekontrolisanom vozu ili avionu. Na udaru će se naći i poslovanje firmi, a samim tim i radna mesta. Kibernetički detektiv Kevin Mandia kaže da najveća opasnost preti velikim svetskim kompanijama." Da ja imam firmu koja je među 500 najuspešnijih sa Forbsove liste, zabrinuo bih se za bezbednost svojih sistema", upozorava Mandia. Samo sajt američkog Ministarstva odbrane svakog dana pretrpi oko 500 hakerskih napada iz celog sveta, a padaju i sajtovi ostalih državnih institucija i velikih firmi. Veruje se da su se i kopije mnogih američkih proizvoda u svetu pojavile pošto su njihove karakteristike i način proizvodnje ukradeni upadom preko interneta. Očekuje se da, posle svedočenja prvog čoveka FBI, Kongres odobri veća sredstva za službe koje se bave zaštitom informatičkih sistema (Brkić, 2012).

Najvažniji otežavajući faktori u borbi protiv korišćenja interneta od strane terorista jesu nepostojanje (kašnjenje) legislative, odnosno njena nedorečenost i nepreciznost u vrlo važnim pitanjima: šta su nova krivična dela, kako ih dokazivati, procesuirati i kažnjavati. Takođe postoje ozbilje pravne i moralne dileme: može li država da koristi internet za dezinformisanje, propagandu, uništavanje terorističkih sajtova i sl. Često nije jasno ko je neprijatelj, i postoji rizik pogrešne identifikacije. Postavlja se pitanje kako država da odgovori (razlog za rat?). Takođe ne postoji ni međunarodna saglasnost, budući da su različiti pristupi u odnosu na slobodu širenja informacija. Tako je, recimo, zakonodavstvo u Ujedinjenom Kraljevstvu veoma strogo, pa se u određenim slučajevima može kažnjavati i učitavanje terorističkog materijala sa interneta, odnosno njegovo posedovanje u personalnom računaru, dok se u SAD, usled Prvog amandmana ne sme vršiti cenzura sadržaja na internetu. Nacionalni subjekti sistema bezbednosti nisu spremni da se otvore u meri u kojoj je to potrebno za efektivnu međunarodnu saradnju u ovoj oblasti. Najzad, jasno je da je radikalizacija pojedinaca i grupa proces, ali nisu sasvim jasne i istražene opcije deradikalizacije. Veoma su osetljiva i pitanja korišćenja Interneta za kontrapropagandu, koja, ukoliko je isuviše umerena, nema efekta, a ukoliko je agresivna, može imati i kontraefekte.

U poređenju sa razvijenim zemljama, stepen korišćenja računara u Srbiji je relativno mali[5], kao i procenat korisnika interneta. Pojavio se, međutim, jedan broj nacionalističkih pa i rasističkih internet sajtova koji propagiraju radikalne ideje i

[5] Prema podacima iz istraživanja Centra za proučavanje informacionih tehnologija Beogradske otvorene škole taj procenat se kreće oko 24%. Vidi http://www.bos.org.yu/arhiva.php?subaction=showfull&id=1161000047&archive=&start_from=&ucat=9&

ideologije. Ova oblast je dobrim delom i normativno neregulisana, a i napori na izgradnji adekvatnih kapaciteta u organima i službama bezbednosti i pravosuđa za suprotstavljanje kompjuterskom kriminalitetu uopšte, pa i potencijalnom korišćenju interneta od strane terorista, nalaze se na samom početku. U tom smislu korisno je izučavanje dobre prakse i relevantnih stranih iskustava kako bi se bezbednosne strukture blagovremeno pripremile za sprečavanje korišćenja svetske mreže od strane terorista.

LITERATURA:

1. Arquilla, John, David Ronfeldt & Michele Zanini. 1999. 'Networks, Netwar and Information-Age Terrorism.' In Ian O. Lesser, Bruce Hoffman, John Arquilla, David F. Ronfeldt, Michele Zanini & Brian Michael Jenkins, Countering the New Terrorism. Santa Monica, Calif.: Rand. http://www.rand.org/publications/MR/MR989/MR989.chap3.pdf
2. Bakier, A. (2006). "Electronic Jihad" [available onlajn] and "Website Recruitment for Jihad" [available onlajn
3. Brkić, B. (2012), "Sajbernapadi-novastrategija"http://www.rts.rs/page/stories/ci/story/2/%D0%A1%D0%B2%D0%B5%D1%82/1039064/%D0%A1%D0%B0%D1%98%D0%B1%D0%B5%D1%80+%D0%BD%D0%B0%D0%BF%D0%B0%D0%B4%D0%B8+-+%D0%BD%D0%BE%D0%B2%D0%B0+%D1-%81%D1%82%D1%80%D0%B0%D1%82%D0%B5%D0%B3%D0%B8%D1%98%D0%B0.html pristup 02.04.2012.
4. Kešetović, Ž. (2008). „Internet kao oruđe terorista", *Revija za bezbednst*, No. 4, str. 37–41
5. Signorielli, N. & Gerbner, G. (1988). *Violence and terror in the mass media: An annotated bibliography*. Westport, CT: Greenwood Press.
6. Simon, J. (1994). *The Terrorist Trap* – America's Experience with Terrorism. John Wiley & Sons
7. Tibbetts, P. (2002). Terrorist Use of the Internet and Related Information
8. Technologies. [Unpublished Paper]. Fort Leavenworth, Kansas: United States Army Command and General Staff College. http://stinet.dtic.mil/cgi-bin/fulcrum_main.pl?database=ft_u2&searchid=0&keyfieldvalue=ADA403802&filename=%2Ffulcrum%2Fdata%2FTR_fulltext%2Fdoc%2FADA403802.pdf
9. Thomas, T. 2003. 'Al Qaeda and the Internet: The Danger of "Cyberplanning."' Parameters Spring. http://carlisle-www.army.mil/usawc/Parameters/03spring/thomas.htm
10. Weimann, G. (2004) *How Modern Terrorism Uses the Internet*, Washington,DC:UNITED STATES INSTITUTE OF PEACE.
11. Wilkinson, R. (2001) *Terrorism Versus Democracy.*London: Frank Cass.
12. http://www.antiteror.ru
13. http://www.awladna.net/
14. http://www.islamnet.eu/

Prethodno saopštenje - UDK 004.738.5: 341.48 (4-672 EU)

BORBA PROTIV SAJBER KRIMINALA U EVROPSKOJ UNIJI SA OSVRTOM NA REPUBLIKU SRPSKU

***Mr Stevo Ivetić*[1],**
Ministarstvo unutrašnjih poslova Republike Srpske
stevoi@mup.vladars.net
Gojko Pavlović*[2], *MA
Visoka škola unutrašnjih poslova Banja Luka
gojko.pavlovic@education.muprs.org

Apstrakt: U prvom dijelu rada autori daju opšti osvrt na međunarodnopravni okvir u borbi protiv sajber kriminala. Potom ukazuju na aktivnosti Evropske unije u borbi protiv ovog vida kriminala, a posebno na Evropsku unutrašnju strategiju bezbjednosti, odnosno na jedan od ciljeva ove strategije koji govori o podizanju nivoa bezbjednosti za građane i preduzeća u sajber okruženju. Nadalje, autori u radu obrazlažu korake koje Evropska unija planira da sprovede radi ostvarenja ovoga cilja, a posebna pažnja se poklanja prvom i trećem koraku, koji govore o uspostavljanju centra za sajber kriminal u EU i mreže CERT. Takođe, dio rada odnosi se i na pravni i institucionalni okvir u borbi protiv sajber kriminala u Republici Srpskoj, odnosno ukazuje se na trenutna rješenja, dosadašnje rezultate, te se daju konkretni prijedlozi autora u cilju daljnjeg usaglašavanja sa standardima Evropske unije i njihovih primjena u praksi.

Ključne riječi: sajber kriminal, evropska unutrašnja strategija bezbjednosti, pravni i institucionalni okvir borbe u Republici Srpskoj

UVODNA RAZMATRANJA

Visokotehnološki kriminal je novi oblik kriminaliteta transnacionalnog karaktera. Inače izrazi „visokotehnološki kriminal“ i „sajber kriminal“ imaju isto značenje, u pitanju je samo terminološka razlika s obzirom na to da Konvencija Savjeta Evrope koristi izraz sajber kriminal, dok se na našem govornom području koristi izraz visokotehnološki kriminal (Komlen-Nikolić i dr., 2010: 30).

Sajber kriminal kao savremena prijetnja doživljava svoju ekspanziju, a kao vrste ove prijetnje u literaturi se uglavnom navode: državno-sponzorisani sajber napadi; ideološki i politički ekstremizam; organizovani sajber kriminal[3] i sajber

[1] Autor je načelnik Službe ministra unutrašnjih poslova i predavač na policijskoj grupi predmeta na Visokoj školi unutrašnjih poslova u Banjoj Luci. Takođe, autor je doktorand na Fakultetu za bezbjednost i zaštitu u Banjoj Luci.

[2] Autor je viši stručni saradnik za bezbjednosnu grupu predmeta na Visokoj školi unutrašnjih poslova u Banjoj Luci. Takođe, autor je doktorand na Pravnom fakultetu Univerziteta Union u Beogradu.

[3] O povezanosti organizovanog i sajber kriminala vidi: Brenner, S. (2002). *Organized Cybercrime? How Cyberspace May Affect the Structure of Criminal Relationships*. North Carolina Journal of Law & Technology,Volume 4, Issue 1. North Carolina: UNC School of Law; EUROPOL Public Information, (2011). *Threat assessment: internet facilitated organised crime – iOCTA*. The Hague: EUROPOL.

kriminal na nivou pojedinaca (Cornish, P., Hughes, R., Livingstone, D., 2009: 3–11). Takođe, sajber kriminal pokriva širok spektar krivičnih djela, uključujući hakovanje kompjutera, podataka i sistema, kompjuterske prevare, te krivična djela vezana za sadržaj kao što su dječija pornografija i autorska prava (Schreier, Weekes, Winkler, 2010: 9).

Međunarodnopravni okvir borbe protiv ovog vida kriminala ogleda se u brojnim dokumentima, rezolucijama i konvencijama koje su usvojile Ujedinjene nacije, Savjet Evrope, Evropska unija i druge organizacije, a koje za cilj imaju upravo borbu protiv sajber kriminala i drugih oblika kriminala povezanih sa njim. S tim u vezi Generalna skupština Ujedinjenih nacija je usvojila dvije rezolucije koje se odnose na borbu protiv zloupotrebe informatičkih tehnologija, i to: Rezoluciju br. 55/63 od 22. januara 2001. godine i Rezoluciju br. 56/121 od 23. januara 2002. godine. Takođe, Ekonomsko-socijalni savjet Ujedinjenih nacija je u julu 2007. godine usvojio Rezoluciju 2007/20, koja govori o međunarodnoj saradnji u oblasti prevencije, istrage, krivičnog progona i kažnjavanja privrednog kriminaliteta i djela povezanih sa zloupotrebom identiteta. [4] Nadalje, kao rezultat napora Međunarodne telekomunikacione unije (*ITU*), generalni sekretar Ujedinjenih nacija je u maju 2007. godine predstavio dokument pod nazivom Memorandum o globalnoj sajber bezbjednosti (*A Global Cybersecuritu Agenda – GCA*).[5]

Što se tiče Savjeta Evrope, on je, takođe, usvojio mnogo preporuka i konvencija koje se tiču uspostavljanja pravnog okvira u borbi protiv sajber kriminala. Tako je još 1976. godine, u Strazburu, održana Evropska konferencija o kriminološkim aspektima privrednog kriminala, na kojoj je prvi put ukazano na nekoliko različitih vrsta računarskog kriminaliteta.[6] Potom, 28. januara 1981. godine donijeta je Konvencija o zaštiti prava pojedinca u vezi sa automatskom obradom ličnih podataka, koja je na snagu stupila 1. oktobra 1985. godine, a čiji je cilj usvajanja bio jačanje pravne regulative na ovom polju zbog porasta upotrebe računarske tehnologije u administrativne svrhe. Nadalje, 1989. godine usvojena je Preporuka o kriminalnim aktivnostima povezanim sa upotrebom računara, a potom 1995. godine još jedna Preporuka koja je za predmet regulisanja imala pitanja koja se tiču procesnih pravila u vezi sa informatičkim tehnologijama. Trenutno najvažniji pravni akt u borbi protiv ovog kriminala jeste Konvencija Savjeta Evrope o visokotehnološkom kriminalu usvojena na Konferenciji u Budimpešti 23. novembra 2001. godine, a koja je stupila na snagu 1. jula 2004. godine.[7] Godine 2003. donijet je i Dodatni protokol uz Konvenciju, koji se bavi inkriminisanjem

[4] Vidi: „Resolution A/res/55/63“ General Assembly of the United Nations, 22. januar 2001; Resolution A/res/56/121“, General Assembly of the United Nations, 23. januar 2002; „Resolution 2007/20“, The Economic and Social Council of the United Nations, 26. jul 2007;

[5] Vidi: „ITU Global Cybersecurity Agenda (GCA): Framework for International Cooperation in Cybersecurity“. Dostupno na: *http://www.ifap.ru/library/book169.pdf*

[6] „Criminological Aspect of Economic Crime“, Strasbourg, 15–18. novembar 1976.

[7] Koju je BiH potpisala 09. 02. 2005. godine, ratifikovala 19. 05. 2006. godine, a koja je stupila na snagu 01. 09. 2006. godine. (Konvencija je objavljena u „Službenom glasniku BiH“, broj 6/06 – Međunarodni ugovori). Vidi listu zemalja članica Savjeta Evrope koje su pristupile konvenciji, dostupno na: http://www.conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=11&DF=09/02/2012&CL=ENG .

akata rasističke i ksenofobične prirode počinjenih putem računarskih sistema, koji je stupio na snagu 1. marta 2006. godine. Od strane Savjeta Evrope usvojene su još i Konvencija o zaštiti djece od seksualne eksploatacije i seksualnog zlostavljanja, 25. oktobra 2007. godine i Konvencija o sprečavanju terorizma 2005. godine, a koja je stupila na snagu 01. juna 2007. godine.[8]

Od pravnih instrumenata koji su nastali u okvirima Evropske unije[9], u oblasti borbe protiv visokotehnološkog kriminala, mogu se izdvojiti Direktiva o pravnoj zaštiti kompjuterskih programa i Direktiva o čuvanju podataka koji su dobijeni ili obrađeni prilikom pružanja javno dostupnih usluga elektronske komunikacije ili javih komunikacionih mreža.[10] Takođe, kao bitnu u borbi protiv savremenih bezbjednosnih prijetnji i izazova, potrebno je istaći Evropsku strategiju bezbjednosti koja je usvojena 12. decembra 2003. godine pod nazivom „Bezbjedna Evropa u boljem svijetu“ .[11] Ovom strategijom su po prvi put uspostavljeni principi i postavljeni jasni ciljevi za unapređenje Evropskih bezbjednosnih interesa.[12] Strategija je organizovana u tri poglavlja, i to: analiza bezbjednosnog okruženja, u kojem su predstavljeni globalni izazovi i ključne prijetnje[13], definisanje tri strateška cilja, od kojih je jedan upravo borba protiv navedenih prijetnji i procjena političkih implikacija za Evropu.[14]

U izvještaju Havijera Solane pod nazivom „Pružanje bezbjednosti u svijetu koji se mijenja“, podnesenom Evropskom savjetu, od 11. decembra 2008. godine, koji u stvari predstavlja Izvještaj o implemenataciji Evropske strategije bezbjednosti[15]

---

[8] Vidi: Savjet Evrope, Preporuka No. R. (89) 9; Savjet Evrope, Preporuka No. R. (95) 13; *Convention on Cybercrime*, Budapest 23. XI 2001. (ETS No. 185); *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (ETS No. 108, the 28 January 1981, Entry into force: 1. 10. 1985); *Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse*, Lanzarote, 25. 10. 2007; *Council of Europe Convention on the Prevention of Terrorism* (CETS No. 196).

[9] Vidi: Direktiva Savjeta Evropske zajednice o pravnoj zaštiti kompjuterskih programa od 17. maja 1991. godine sa obavezom primjenjivanja u državama članicama od 1. januara 1993. godine. „*Council Directive of 14 may 1991 on the Legal Protection of Computer Programs*“, Directive 91/250/EEC, Official Journal no L 122/42; „*Directive 2006/24/EC of the European Parliament and of the Council: on the retention of data generated or processed in connection with provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC*“, Official Journal of the European Union, 13. 4. 2006.

[10] O svim ovim prethodno navedenim dokumentima, odnosno preporukama, konvencijama i rezolucijama detaljnije vidi: Komlen-Nikolić i dr., 2010: 32-68.

[11] Vidi: Javier, S. (2003). *A safer Europe in a better world, European security strategy*. Brussels: European Commission. Prevod djela na srpskom jeziku: Havijer, S. (2006). *Bezbedna Evropa u boljem svetu, Evropska strategija bezbednosti.* Beograd: ISAC Fond.

[12] O evropskim bezbjednosnim principima, ciljevima i interesima vidi: Royal Institute for International Relations, (2004). *A European Security Concept for the 21st Century*. Brussels: IRRI-KIIB. Egmont paper 1. Dostupno na: http://www.egmontinstitute.be/paperegm/ep1.U560.pdf

[13] Kao globalni izazovi u strategiji se ističu: siromaštvo, bolesti, migracije, ekološki problemi, nadmetanje za prirodne resurse, posebno vodu, energetska zavisnost i dr., a kao glavne prijetnje se navode: terorizam, profilerizacija oružja za masovno uništenje, regionalni sukobi, neuspjeh država i organizovani kriminalitet. Navedeno prema: Havijer, 2006: 5–9.

[14] Vidi šire: Biscop, S. (2004). „The European Security Strategy, Implementing a Distinctive Approach to Security“. In: *Sécurité & Stratégie*. Brussels: Royal Defence College. Paper No. 82. Dostupno na: http://www.egmontinstitute.be/papers/Artikel.ESS.pdf, 25.07.2011. godine.

[15] Glavna karakteristika ove strategije jeste davanje prednosti nevojnim sredstvima rješavanja sukoba, kao načinu da se bezbjednost osigura u dužem vremenskom periodu. Radi prevencije prijetnji koje je identifikovala, EU namjerava da razvija tzv. „stratešku kulturu“. „Potreban nam je razvoj strateške

iz 2003. godine, naglašava se da izazovi i prijetnje koji su tada identifikovani nisu nestali, već naprotiv, da su postali još složeniji, a pored starih su se javili i neki novi, među kojima je i sajber kriminalitet (Javier, 2008: 3–6). Takođe, navodi se i da su navedene prijetnje u posljednjih nekoliko godina postale složenije i međusobno povezane. Evropa bi u vezi sa tim, dakle da bi bila aktivnija i sposobnija da se nosi sa tim prijetnjama, morala da razvije podstrategije i akcione planove za borbu protiv navedenih prijetnji (Vasconcelos, 2009: 57). Upravo na bazi toga, a kao odgovor na sve složenije bezbjednosne izazove i prijetnje, usvojen je najprije tzv. Štokholmski program 2009. godine, a zatim i Strategija unutrašnje bezbjednosti početkom 2010. godine.[16] Nakon toga, krajem 2010. godine, Evropska komisija je u saradnji sa Evropskim parlamentom i Savjetom Evropske unije izradila dokument pod nazivom „*The EU Internal Security Strategy in Action: Five steps towards a more secure Europe*“,[17] odnosno "*Evropsku unutrašnju strategiju bezbjednosti u akciji: pet koraka ka bezbjednijoj Evropi*" (European Commission, 2010).

U ovoj unutrašnjoj strategiji bezbjednosti identifikovani su najurgentniji izazovi i prijetnje za bezbjednost Evropske unije, te predloženo pet strateških ciljeva i nekoliko konkretnih koraka za svaki od ovih ciljeva za period 2011–2014. godina, koji bi trebali da, pored tekućih napora i inicijativa, pomognu da Evropska unija bude bezbjednija. Pet strateških ciljeva koji su definisani ovom strategijom jesu (European Commission, 2010: 4–15):

- poremetiti međunarodne kriminalne mreže;
- prevencija terorizma, radikalizacije i regrutovanja terorista;
- *podizanje nivoa zaštite za građane i poslovna preduzeća u sajber prostoru*;
- jačanje bezbjednosti kroz bolje upravljanje granicama i
- povećanje evropske otpornosti na krize i katastrofe.

KORACI EVROPSKE UNIJE U BORBI PROTIV SAJBER KRIMINALA

Dakle, jedan od strateških ciljeva Evropske unutrašnje strategije bezbjednosti, a samim time i Evropske unije, jeste borba protiv sajber kriminala, definisana u ovoj strategiji kao podizanje nivoa zaštite za građane i poslovna preduzeća u sajber prostoru.

U strategiji se ističe da je bezbjednost IT mreže jedan od ključnih faktora za dobro funkcionisanje informacionog društva. Naglašava se da su brzi razvoj i primjena novih informacionih tehnologija stvorili nove oblike kriminalnih aktivnosti. Sajber, odnosno visokotehnološki kriminal je globalni fenomen, koji izaziva značajnu štetu unutrašnjem tržištu Evropske unije. Dok sama struktura

---

kulture koja podrazumijeva odlučnu, jaku i, kad je potrebno, robusnu intervenciju“. Navedeno prema: Havijer, 2006: 17–18.

[16] O pozadini usvajanja Evropske strategije unutrašnje bezbjednosti, kao i o tzv. Štokholmskom programu vidi: Nikodinovska-Stefanovska, S. (2010). The EU internal security strategy. u Zborniku radova: Nikač, Ž. (Ur.). *Suzbijanje kriminala i Evrpopske integracije* (str. 321–328). Beograd: Kriminalističko policijska akademija i Hans Zajdel Fondacija.

[17] Dostupno na: http://ec.europa.eu/commission_2010-2014/malmstrom/archive/internal_security_strategy_in_action_en.pdf, 25. 07. 2011. godine.

interneta, kao takvog, ne poznaje granice, nadležnost za krivično gonjenje sajber kriminala i dalje se zaustavlja na nacionalnim granicama. S toga se pozivaju države članice, ali i druge zemlje, da udruže svoje napore u borbi protiv ovog vida kriminaliteta. Takođe, ističe se da kriminalistički centar za visoke tehnologije pri Europolu već sada igra veoma važnu ulogu koordinatora za sprovođenje zakona, ali da su i dalji napori neophodni (European Commission, 2010: 9).

Koraci koji su predviđeni za ispunjavanje ovoga cilja kao i rokovi za njihovo provođenje, te odgovorni subjekti prikazani su u sljedećoj tabeli.
[18]

Tabela 1: Koraci Evropske unije u borbi protiv sajber kriminaliteta

Cilj i koraci	**Odgovorni subjekt**	**Vrijeme**
Cilj 3: Podizanje nivoa bezbjednosti za građane i preduzeća u sajber prostoru		
Korak 1: Izgradnja kapaciteta za primjenu zakona i u pravosuđu		
- osnivanje Evropskog centra za sajber kriminal;	Subjekti iz studije izvodljivosti Evropske komisije iz 2011. godine	2013.
- razvijanje kapaciteta za istrage i krivično gonjenje počinilaca sajber kriminala;	Države članice u saradnji sa CEPOLOM, Europolom i Eurojustom	2013.
Korak 2: Rad sa industrijom radi osnaženja i zaštite građana		
- uspostavljanje rješenja vezanih za izvještavanja o incidentima povezanim sa sajber kriminalom i pružanje smjernica građanima o sajber bezbjednosti i sajber kriminalu.	Države članice, Evropska komisija, Europol, ENISA i privatni sektor	2010.
- smjernice o saradnji u rukovanju ilegalnim online sadržajima	Evropska komisija sa državama članicama i privatnim sektorom	2011.
Korak 3: Poboljšati sposobnost za suočavanje sa sajber napadima		
- uspostavljanje mreže tzv. Computer Emergency Response Teams u svakoj državi članici i jednog tima za institucije Evrpopske unije, kao i nacionalnih rezervnih planova, te vježbi za odgovore i oporavak.	Države članice i institucije Evropske unije sa ENISA[18]	2012.
- uspostavljanje Evropskog sistema za razmjenu informacija i upozorenja – European information sharing and alert system (EISAS).	Države članice sa Evropskom komisijom i ENISA	2013.

Izvor: European Commission, (2010). *The EU Internal Security Strategy in Action: Five steps towards a more secure Europe*. Brussels: COM(2010) 673. p. 20.

[18] ENISA – European Network and Information Security Agency.

Prema tome, kao što se iz Tabele 1. može vidjeti, EU planira da sprovede čitav niz aktivnosti vezanih za suprotstavljanje sajber kriminalu. Tako će, do 2013. godine, u okviru postojećih struktura, osnovati centar za sajber kriminal[19], putem kojeg će države članice i institucije Evropske unije biti u mogućnosti da izgrade operativne i analitičke kapacitete za sprovođenje istraga i saradnju sa međunarodnim partnerima. Ovaj centar bi trebao da unaprijedi procjenu i praćenje postojećih preventivnih i istražnih mjera, da podrži dalji razvoj obuke, kao i da uspostavi saradnju sa Evropskom agencijom za bezbjednost mreža i informacija (ENISA – European Network and Information Security Agency), te da sarađuje sa mrežom nacionalnih timova za računarske incidente (Computer Emergency Response Teams – CERTs). Centar za sajber kriminal bi trebao postati centralna tačka u borbi Evropske unije protiv sajber kriminala (European Commission, 2010: 9).

Trenutno se očekuje donošenje odluke o tome da li će ovaj centar biti pri Europolu[20]. Što se tiče nadležnosti koje će imati, one se mogu svesti na tri, i to: izrada strategija, sprovođenje istraživanja i pružanje operativne podrške. Međutim, ono što je potrebno posebno naglasiti, vezano za poslednju nadležnost, jeste to da ovaj centar nema nadležnost da vrši istrage u pojedinim zemljama članicama Evopske unije, osim, naravno, ukoliko to neka država članica želi, tj. na njen izričit zahtijev će moći sprovoditi istragu (Hagemeijer, 2012). U strategiji se dalje pozivaju sve države članice Evropske unije da na nacionalnim nivoima obezbijede zajedničke standarde postupanja za policiju, sudije, tužilaštva i forenzičke istražioce u istragama i gonjenju krivičnih djela sajber kriminala. Takođe, u saradnji sa Eurojust-om, CEPOL-om i Europolom, države članice se podstiču da do 2013. godine razviju svoje nacionalne centre za sajber kriminal, koji bi trebalo da blisko sarađuju sa akademskim krugovima i sa industrijom.

Nadalje, svaka država članica, kao i institucije EU moraju u ovoj godini uspostaviti svoj CERT (*Computer Emergency Response Team*), tj. tim za računarske incidente. S tim u vezi, naglašava se da nakon što budu uspostavljeni, potrebno je da blisko sarađuju sa policijskim agencijama na prevenciji, otkrivanju i reakciji, tj. odgovoru na sajber napade. Zajedno bi svi ovi timovi trebali da povećaju spremnost Evrope da se nosi sa rizicima vezanim za sajber kriminal. Kao rezultat svih ovih aktivnosti, do kraja 2013. godine, planira se razviti Evropski sistem za razmjenu informacija i upozorenja – EISAS (*European information sharing and alert system*), odnosno uspostavljanje mreže kontakata između država članica i drugih relevantnih tijela. I na kraju, ističe se da države članice, zajedno sa Evropskom agencijom za bezbjednost mreža i informacija, treba da razviju nacionalne planove za nepredviđene situacije, kao i da sprovode redovne vježbe za odgovore na računarske incidente, kao i vježbe za oporavak od tih incidenata (European Commission, 2010: 9–10).

---

[19] O nadležnosti i ovlašćenjima centra vidi: Council of the European Union, (2010). *Council conclusions concerning an Action Plan to implement the concerted strategy to combat cybercrime.* Luxembourg: 3010th GENERAL AFFAIRS Council meeting. p. 4.

[20] Za borbu protiv sajber kriminala u Evropskoj uniji zadužen je upravo Europol. Odlukom Savjeta o osnivanju Kancelarije evropske policije (Europola) od 06. aprila 2009. godine, a koja se primjenjuje od 01. januara 2010. godine, u skladu sa članom 4 stav 1. Aneksom su nabrojane nadležnosti Europola, a između ostalih, naveden je i sajber kriminal. Vidi: Council of European Union (2009). *COUNCIL DECISION of 6 April 2009 establishing the European Police Office (Europol).* (2009/371/JHA). Official Journal of the European Union, L 121, pp. 37 – 66.

BORBA PROTIV SAJBER KRIMINALA U REPUBLICI SRPSKOJ

U Bezbjednosnoj politici BiH iz 2006. godine, naglašeno je da je od posebnog značaja da organi izvršne vlasti, na svim nivoima, preuzmu odgovornost za sopstveni razvoj i stabilnost kroz uvažavanje prihvaćenih evropskih standarda[21], Republika Srpska, prvenstveno kroz aktivnosti Ministarstva unutrašnjih poslova Republike Srpske (MUP RS), ali i drugih entiteskih organa i institucija, kontinuirano radi na jačanju svojih kapaciteta i unapređenju kvaliteta rada u svim segmentima iz djelokruga svojih nadležnosti. U tom kontekstu velika pažnja se posvećuje i praćenju novih trendova i pojavnih oblika kriminaliteta, među kojima je i sajber kriminalitet. Stoga je i potreba za pravnim i institucionalnim okvirima radi efikasne borbe protiv ovog vida kriminaliteta odavno prepoznata. Još su zakonodavnom reformom iz 2003. godine u krivično zakonodavstvo Republike Srpske uvedena određena krivična djela iz ove oblasti, i to: neovlašćeno ulaženje u zaštićenu kompjutersku bazu podataka (član 238), proizvodnja i prikazivanje dječije pornografije (član 200), neovlašćeno fotografisanje (član 175), neovlašćeno korištenje ličnih podataka (član 176), iskorišćavanje djece i maloljetnih lica za pornografiju (član 199), upad u kompjuterski sistem (član 271).[22]

S tim u vezi činjeni su određeni napori da se adekvatno odgovori na ovu savremenu prijetnju, pa je tako MUP RS preduzeo niz koraka, od organizovanja seminara do pokretanja zakonodavnih i institucionalnih promjena u pravcu jačanja kapaciteta za borbu protiv sajber kriminala. Naime, MUP RS je u martu 2009. godine, uz podršku TAIEX instrumenta Evropske komisije, radi uspostavljanja saradnje i obezbjeđivanja odgovarajuće podrške organizovao regionalni seminar pod nazivom „Borba protiv kompjuterskog kriminala“ za sve predstavnike policijskih agencija, tužilaštava i Internet provajdera iz BiH i zemalja iz regiona. Nakon toga je u aprilu iste godine, na inicijativu MUP RS, uslijedio sastanak predstavnika Savjeta Evrope i policijskih tijela i tužilaštava iz BiH, u organizaciji Ministarstva pravde BiH, na kojem je izvršena analiza zakonodavstva u BiH i donesene preporuke u vezi sa sajber kriminalom, tj. u vezi sa usklađivanjem zakonodavstva sa Konvencijom o sajber kriminalu. Kao rezultat toga uslijedile su izmjene i dopune Krivičnog zakona Republike Srpske[23] kojima je u uvedena posebna glava posvećena krivičnim djelima protiv bezbjednosti računarskih podataka, odnosno inkriminisano je sedam novih krivičnih djela, i to: oštećenje računarskih podataka i programa (član 292a), računarska sabotaža (član 292b), izrada i unošenje računarskih virusa (član 292v), računarska prevara (član 292g), neovlašćeni pristup zaštićenom računaru, računarskoj mreži, telekomunikacionoj mreži i elektronskoj obradi podataka (član 292d), sprečavanje i ograničavanje pristupa javnoj računarskoj mreži (član 292đ) i neovlašćeno korišćenje računara ili računarske mreže (član 292e). Takođe, izmijenjen je i član 200, koji se odnosi na proizvodnju i prikazivanje dječije pornografije, na način da je sada inkriminisano i posjedovanje materijala koji su u vezi sa dječijom pornografijom.

---

[21] Vidi: Predsjedništvo BiH. (2006). *Bezbjednosna politika Bosne i Hercegovine*. Sarajevo: Predsjedništvo BiH. str. 20.

[22] Vidi: *Krivični zakon Republike Srpske*, („Službeni glasnik Republike Srpske“, broj 49/03, 108/04, 37/06, 70/06).

[23] Vidi: *Zakon o izmjenama i dopunama Krivičnog zakona Republike Srpske*, („Službeni glasnik Republike Srpske“, broj 73/10).

Pararelno, MUP RS je radio i na institucionalnoj izgradnji, te je u okviru Uprave kriminalističke policije kao unutrašnja organizaciona jedinica formirana Jedinica za operativnu i tehničku podrašku, u okviru koje djeluje posebno Odjeljenje za sprečavanje visokotehnološkog kriminaliteta.[24] U sprečavanju visokotehnološkog kriminaliteta Odjeljenje koristi specijalne metode za izvođenje istražnih radnji kada ne postoje drugi načini za prikupljanje dokaza, čime se stvaraju uslovi za njihovu primjenu u skladu sa Zakonom o krivičnom postupku RS, a protiv lica za koja postoje osnovi sumnje da učestvuju u izvršenju prvenstveno gore navedenih, ali i svih drugih krivičnih djela predviđenih Krivičnim zakonom RS.

Nadalje, u kontekstu unapređenja sopstvenih kapaciteta, MUP RS je organizovao i druge seminare, radionice, konferencije i studijske posjete na ovu temu. Nakon seminara iz marta 2009. godine, u novembru iste godine uslijedila je studijska posjeta Centralnoj kancelariji MUP Francuske za borbu protiv kriminala vezanog za informacione i komunikacione tehnologije. Potom su u 2011. godini organizovana još dva seminara u Banjoj Luci, na temu „Izazovi dječije pornografije na internetu“ i seminar posvećen „Konvenciji o sajber kriminalu“. Tokom 2012. godine MUP RS nastavlja sa aktivnostima vezanim za međunarodnu razmjenu iskustava u vezi sa borbom protiv sajber kriminala, te je u februaru organizovan regionalni seminar na temu „Borba protiv sajber terorizma“, a već u martu Međunarodna naučnostručna konferencija pod nazivom „Suzbijanje kriminala i evropske integracije, s osvrtom na visokotehnološki kriminal“, u saradnji sa Hans Zajdel Fondacijom. Pored toga, predstavnici MUP RS aktivno učestvuju u projektu Savjeta Evrope za borbu protiv sajber kriminala, pod nazivom „Cybercrime@IPA“, u koji su uključene i druge zemlje Jugoistične Evrope i Turska.

Uporedo s tim Narodna skupština Republike Srpske je krajem juna 2011. godine usvojila Zakon o informacionoj bezbjednosti[25], kojim se obezbjeđuje primjena mjera i standarda informacione bezbjednosti u Republici Srpskoj. Prema zakonu, pod informacionim mjerama bezbjednosti podrazumijeva se: fizička zaštita[26], zaštita podataka[27] i zaštita informacionog sistema[28]. Takođe, zakonom je predviđeno uspostavljanje CERT, tj. posebne organizacione jedinice u okviru Agencije za informaciono društvo Republike Srpske, za djelovanje u hitnim slučajevima. CERT će imati zadatak koordinacije u prevenciji i zaštiti od računarskih incidenata na internetu, kao i usklađivanje rada organa i drugih pravnih i fizičkih lica radi zaštite njihovih informacionih sistema.

---

[24] Vidi: *Izmjene i dopune Pravilnika o unutrašnjoj organizaciji i sistematizaciji radnih mjesta u MUP RS*, („Službeni glasnik Republike Srpske“, broj 116/09), koji je u primjeni od 7. januara 2010. godine.
25 Vidi: *Zakon o informacionoj bezbjednosti,* („Službeni glasnik Republike Srpske“, broj 70/11).

[26] Fizička zaštita obuhvata zaštitu objekta, prostora i uređaja u kojem se nalaze podaci – Član 7 Zakona o informacionoj bezbjednosti.

[27] Zaštita podatka obuhvata prevenciju i otklanjanje štete od gubitka, otkrivanja ili neovlašćene izmjene podataka, a odnosi se na: pravila za postupanje sa podacima, sadržaj i način vođenja evidencije o izvršenim pristupima podacima i nadzor koji se tiče bezbjednosti podataka – Član 8 Zakona o informacionoj bezbjednosti.

[28] Zaštita informacionog sistema obuhvata zaštitu podataka koji se obrađuju, skladište ili prenose u informacionom sistemu, kao i zaštitu povjerljivosti, cjelovitosti i dostupnosti informacionog sistema u procesu planiranja, projektovanja, izgradnje, upotrebe, održavanja i prestanka rada tog sistema – Član 9 Zakona o informacionoj bezbjednosti.

ZAKLJUČAK

Evropska unija kao i druge regionalne organizacije, ali i organizacije koje djeluju na globanom nivou, odavno je prepoznala potrebu da se adekvatna pažnja posveti pravnoj i institucionalnoj borbi protiv sajber kriminala.[29] S tim u vezi, Evropska unija je krajem 2010. godine usvojila tzv. Evropsku unutrašnju strategiju bezbjednosti, u kojoj je kao jedan od ključnih ciljeva navedena upravo institucionalna izgradnja kapaciteta u okviru EU, ali i država članica, u vidu osnivanja centara za sajber kriminal i tzv. CERT, odnosno timova za djelovanje u hitnim slučajevima. U vezi sa njihovim uspostavljanjem potrebno je istaći razliku između ovih organa i tzv. Mreže 24/7, uspostavljene u skladu sa obavezom svake zemlje potpisnice Konvencije Savjeta Evrope o sajber kriminalu da u vezi sa članom 35. Konvencije uspostave tačku za kontakt[30]. Dakle, riječ je o različitim organima, različitih regionalnih organizacija, Evropske unije i Savjeta Evrope.

Bosna i Hercegovina je 2008. godine imenovala predstavnika iz Državne agencije za istrage i zaštitu kao kontakt tačku 24/7, ali je uspostavljanjem Direkcije za koordinaciju policijskih tijela BiH, koja je preuzela dio njihovih nadležnosti, za kontakt tačku određen predstavnik iz Direkcije, odnosno iz Odsjeka - NCB Interpol Sarajevo. Imajući u vidu da se ova vrsta kriminala reguliše entitetskim zakonima (osim dijela koji se tiče autorskih prava definisanih Krivičnim zakonom BiH), mišljenja smo da je potrebno sačiniti Memorandum o uspostavljanju mreže kontakt tačaka 24/7 za sajber kriminal unutar BiH, i to između Direkcije za koordinaciju policijskih tijela BiH, MUP RS, MUP FBiH i Policije Brčko Distrikta kojim bi se definisale same kontakt tačke u pomenutim institucijama i način funkcionisanja sistema u skladu sa bezbjednosnom strukturom i zakonskim nadležnostima policijskih agencija u BiH.

S tim u vezi, potrebno je naglasiti da Republika Srpska ni u jednom momentu ne zaostaje za aktivnostima drugih evropskih zemalja, naprotiv, usvojen je i pravni okvir za borbu protiv ovog vida kriminaliteta, ali i institucionalno se Republika Srpska prilagodila borbi protiv ove savremene prijetnje.

Naime, u Sporazumu o stabilizaciji i pridruživanju, potpisanom između BiH i EU 06. 06. 2008. godine u Luksemburgu, u poglavlju VII. Pravda, sloboda i sigurnost, u članu 84. Sprečavanje i borba protiv organizovanog kriminala i drugih nezakonitih aktivnosti, stav 1. tačka (j) kompjuterski kriminal je taksativno naveden kao oblast zajedničke saradnje u sklopu koje će se promovisati regionalna saradnja i poštovanje međunarodnih standarda, a koji su predmet ovoga rada. Realizujući

---

[29] O budućim trendovima u vezi sa sajber kriminalom, na međunarodnom, nacionalnim, institucionalnim i individualnim nivoima, vidi: Rush, H., Smith, C., Kraemer-Mbula, E., Tang, P. (2009). *Crime online: Cybercrime and illegal innovation.* London: National Endowment for Science Technology and the Arts (NESTA), pp. 80 – 87.

[30] Dostupnu 24 sata na dan, sedam dana u sedmici, kako bi osigurala pružanje trenutne pomoći u svrhu istraga ili postupaka u pogledu krivičnih djela vezanih za kompjuterske sisteme i podatke, ili u svrhu prikupljanja dokaza o krivičnom djelu u elektronskom obliku. Takva pomoć će obuhvatati omogućavanje ili, ako to domaći zakoni i praksa dozvoljavaju, direktno izvršavanje slijedećih mjera: davanja tehničkih savjeta, zaštite podataka i prikupljanja dokaza, davanja pravnih informacija i lociranja osumnjičenih. Tačka za kontakt jedne strane imat će mogućnost i ovlaštenje da hitno komunicira s tačkom za kontakt druge strane. Kako bi se olakšao rad mreže, svaka strana će se postarati da raspolaže obučenim i opremljenim osobljem. – Član 35 Konvencije Savjeta Evrope o sajber kriminalu.

prethodnu navedenu obavezu Republika Srpska je svoje zakonodavstvo usaglasila sa odredbama Konvencije Savjeta Evrope o sajber kriminalu.[31] Tako je, 2010. godine izmjenama i dopunama krivičnog zakona, u krivičnopravni sistem uvedena posebna glava posvećena krivičnim djelima protiv bezbjednosti računarskih podataka. Takođe, u 2011. godini usvojen je i Zakon o informacionoj bezbjednosti.

Nadalje, potrebno je istaći da je MUP Republike Srpske, u vidu institucionalne izgradnje, u odnosu na ostale bezbjednosne strukture u Bosni i Hercegovini napravio značajan iskorak i napredak u oblasti borbe protiv sajber kriminala, i to formiranjem Jedinice za operativnu i tehničku podršku, a u okviru nje i posebnog Odjeljenja za sprečavanje visokotehnološkog kriminaliteta, koje već sada ima ulogu respektabilnog centra za borbu protiv sajber kriminala u Republici Srpskoj, ali i šire.

U narednom periodu planira se nastaviti sa razvojem kapaciteta u ovoj oblasti, a posebno pažnju posvetiti dodatnoj edukaciji, usavršavanju i opremanju visokosofisticiranom opremom koja može zadovoljiti tehničke standarde i uslove za borbu protiv ovog vida kriminaliteta (Pravci razvoja MUP RS za period 2012–2016. godina, 2012: 19). Takođe, očekuje se i osnivanje tzv. CERT Republike Srpske.

Jedna od oblasti koja će se morati dodatno unaprijediti u budućnosti jeste svakako pravni sistem. Naime, s obzirom na to da su već sada mnoge policijske agencije, širom svijeta, a među njima i policija Republike Srpske, posvetile ljudstvo i druge resurse istragama sajber kriminala, potrebno je i da pravni sistem pruži odgovarajuću podršku. Pod ovom podrškom prvenstveno podrazumijevamo propisivanje novih, različitih, krivičnih djela sajber kriminala, kao i sankcija za njih, te usaglašavanja pravne prakse sudova u primjeni zakona na krivična djela ove vrste. Takođe, neophodno je i daljnje usaglašavanje sa Konvencijom Savjeta Evrope vezano za procesna pitanja, a posebno u vezi sa vremenom čuvanja podataka na serverima provajdera internet usluga, u vezi sa kojim je MUP RS već pokrenuo odgovarajuće inicijative prema Ministarstvu pravde RS i Regulatornoj agenciji za komunikacije BiH.

LITERATURA:

1. Biscop, S. (2004). „The European Security Strategy, Implementing a Distinctive Approach to Security“. In: *Sécurité & Stratégie*. Brussels: Royal Defence College. Paper No. 82.
2. Brenner, S. (2002). *Organized Cybercrime? How Cyberspace May Affect the Structure of Criminal Relationships*. North Carolina Journal of Law & Technology,Volume 4, Issue 1. North Carolina: UNC School of Law.
3. *Convention on Cybercrime*, Budapest 23. XI 2001. (ETS No. 185).
4. Cornish, P., Hughes, R., Livingstone, D. (2009). *Cyberspace and the National Security of the United Kingdom – Threats and Responses*. London: Royal Institute of International Affairs.Chatham House Report.
5. Council of the European Union. (2010). *Council conclusions concerning an Action Plan to implement the concerted strategy to combat cybercrime.* Luxembourg: 3010th GENERAL AFFAIRS Council meeting.

[31] Vidi: Vanjskopolitička inicijativa BH. (2011). *Monitoring procesa evropskih integracija Bosne i hercegovine. Godišnji izvještaj za 2011*. Sarajevo: VPI BH. str. 72.

6. Council of European Union. (2009). *COUNCIL DECISION of 6 April 2009 establishing the European Police Office (Europol)*. 371/JHA. Luxembourg. Official Journal of the European Union, L 121, pp. 37–66.
7. European Commission, (2010). *The EU Internal Security Strategy in Action: Five steps towards a more secure Europe*. Brussels: European Commission. *COM(2010)673*.
8. EUROPOL Public Information, (2011). *Threat assessment: internet facilitated organised crime – iOCTA*. The Hague: EUROPOL.
9. Hagemeijer, M. (2012). *Workshop on Combating Cyber terrorism.* Banja Luka: MUP RS & TAIEX.
10. Javier, S. (2003). *A safer Europe in a better world, European security strategy*. Brussels: European Commission.
11. Javier, S. (2008). *Report on the Implementation of the European Security Strategy, Providing Security in a Changing World (S407/08)*. Brussels: European Council.
12. Havijer, S. (2006). *Bezbedna Evropa u boljem svetu, Evropska strategija bezbednosti.* Beograd: ISAC Fond.
13. *Konvencija Savjeta Evrope o sajber kriminalu*, („Službeni glasnik BiH“, broj 6/06 – Međunarodni ugovori).
14. *Krivični zakon Republike Srpske*, („Službeni glasnik Republike Srpske“, broj 49/03, 108/04, 37/06, 70/06).
15. Komlen-Nikolić, L., i dr. (2010). *Suzbijanje visokotehnološkog kriminala*. Beograd: Udruženje javnih tužilaca i zamenika javnih tužilaca Srbije.
16. Moore, R. (2005). *Cybercrime: Investigating High – Technology Computer Crime*. Cincinnati: Anderson Publishing.
17. Nikodinovska-Stefanovska, S. (2010). The EU internal security strategy. u Zborniku radova: Nikač, Ž. (Ur.). *Suzbijanje kriminala i Evrpopske integracije* (str. 321–328). Beograd: Kriminalističko policijska akademija i Hans Zajdel Fondacija.
18. Predsjedništvo BiH. (2006). *Bezbjednosna politika Bosne i Hercegovine*. Sarajevo: Predsjedništvo BiH.
19. Royal Institute for International Relations, (2004). *A European Security Concept for the 21st Century*. Brussels: IRRI-KIIB. Egmont paper 1.
20. Rush, H., Smith, C., Kraemer-Mbula, E., Tang, P. (2009). *Crime online: Cybercrime and illegal innovation.* London: National Endowment for Science Technology and the Arts (NESTA).
21. Schreier, F., Weekes, B., Winkler, T. (2010). *Cyber Security:The Road Ahead*. Geneva: DCAF.
22. Vasconcelos, Á. ed., (2009). *The European security strategy 2003–2008, Building on common interests*. Paris: European Union Institute for Security Studies. Report No. 05.
23. Vanjskopolitička inicijativa BH. (2011). *Monitoring procesa evropskih integracija Bosne i Hercegovine. Godišnji izvještaj za 2011*. Sarajevo: VPI BH.
24. *Pravci razvoja Ministarstva unutrašnjih poslova Republike Srpske za period 2012–2016. godina*, („Službeni glasnik Republike Srpske“, broj 10/12).
25. *Zakon o izmjenama i dopunama Krivičnog zakona Republike Srpske*, („Službeni glasnik Republike Srpske“, broj 73/10).
26. *Zakon o informacionoj bezbjednosti*, („Službeni glasnik Republike Srpske“, broj 70/11).

SUMMARY

In the first part of the paper, the authors provide the general overview of the international framework of the fight against cyber-crime. In addition, they point out to European Union activities in the fight against this type of crime, especially to European internal security strategy, that is, to one of the objectives of this strategy that deals with the improvement of the citizens' and enterprises' security in the cyber environment. Furthermore, the authors also pay attention to the steps European Union plans to take in order to implement this objective, whereby these steps imply establishment of EU Cyber Crime Center and CERT network. A part of the paper refers to the legal and institutional framework of the fight against cybercrime in the Republic of Srpska, that is, it is pointed out to the current solutions, previous results, and are given authors' concrete suggestions in order to keep harmonizing with the European Union standards and their implementation in practice.

Pregledni rad - UDK 343.326: 004.738.5

SECURITY-CRIMINALISTIC DIMENSIONS OF CYBER-TERRORIST ATTACKS

БЕЗБЕДНОСНО-КРИМИНАЛИСТИЧКЕ ДИМЕНЗИЈЕ САЈБЕР-ТЕРОРИСТИЧКИХ НАПАДА

Dr. Zlate Dimovski, PhD
Professor and Associate Dean on the Faculty of security – Skopje
Idrizovo, bb, Gazi Baba, 1000 Skopje
University "St. Kliment Ohridski" – Bitola
e-mail: zdimovski@fb.uklo.edu.mk
Ice Ilijevski, MSc
Assistant and PhD student on the Faculty of security – Skopje
Idrizovo, bb, Gazi Baba, 1000 Skopje
University "St. Kliment Ohridski" – Bitola
e-mail: iilijevski@fb.uklo.edu.mk
Kire Babanoski, MSc
PhD student on the Faculty of security – Skopje
University "St. Kliment Ohridski" – Bitola
e-mail: kbabanoski@gmail.com

Abstract: Cyber terrorism is a new, modern form of terrorism that its violent aims, motives and ideology, seek to achieve through the exploitation of information and computer systems, specifically the use of computers as weapons or as targets of attacks. In today's modern information-communication era of life, terrorists are increasingly adapting to the new conditions, taking them to perform so-called cyber terrorist attacks.

The main scientific object of the paper is detailed elaboration of security and criminalistic dimensions of such attacks, which appear as a new global real security threat to mankind (although they are secondary to the physical terrorism). For this purpose, it is given an analysis of various aspects of these phenomena, such as planning, organizing, training, motivation, trends, risks, threats, vulnerabilities, advantages and disadvantages, sources, targets of attack, consequences. In criminalistic characteristics of cyber terrorist attacks are given wider and more detailed response to the main issues of criminalistic, for clearer understanding of these negative behaviors. At the end of the paper, the authors try to give some recommendations for more effective security response by the law enforcement agencies, regarding the ways and measures to prevent and detect cyber terrorist attacks. The scientific value of the paper consists in exposing the most important dimensions of these attacks, emphasizing the need for scientific perceiving, precise definition and a broader range of preventive action to protect the national and global security.

Key words: cyber terrorism, cyber terrorist attacks, security dimensions, criminalistic dimensions

INTRODUCTION

Tremendous achievement and development of high technology and sophisticated computer systems have opened a new «cyber space», which constantly destroys old traditional forms of organization, behaviour and belief. Cyber information led to the cyber revolution and the emergence of information society, in which dominated the race for information and communication technologies, along with the global liberalization and free circulation of people, goods and ideas. Today, thirty years after the introduction of the term, the concept of cybernetics, it inevitably became a primary component of many important terms: cyber society, cyber policy, cyber economy, cyber war, cyber terrorism, cyber crime, which essentially the most precious crown represents cyber information.

The development and dissemination of information technique and technology in the world, despite its advantages, however, has certain disadvantages: it opens the door to antisocial and criminal behavior in a way that was impossible before. The computer systems are new and highly sophisticated opportunities for breaking the law, and creating the potential to commit traditional types of crime in non-traditional ways. However, despite the economic consequences of cyber crime, society relies on computer systems, for almost everything in life, by air, rail and bus traffic control to coordination of medical services and national security. If there is a small error in the operation of these systems a lot of lives will be put in danger. Rapid expansion of large computer networks and the ability to access many systems through regular telephone line increases the vulnerability of these systems and open up the possibility for abuse and criminal activity. Consequences of cyber crime can contribute to serious economic crises, and violation of national and global security.

CYBERTERRORISM AS A MODERN TYPE OF TERRORISM

No single definition of the term "terrorism" has yet gained universal acceptance. Likewise, no single definition for the term "cyber terrorism" has been universally accepted. Labelling a computer attack as "cyber terrorism" is problematic because of the difficulty determining the identity, intent, or the political motivations of an attacker with certainty.[1]

Cyber terrorism can be viewed as an independent notion from cyber crime. Cyber crime is prejudiced as the concept that encompasses cyber terrorism. On the contrary though, these two concepts cover different areas. Cyber crime is a problem faced by the nation. This is a violation on the set law of a particular nation. Although this is the case this issue can also have detrimental effect in the international scene. Cyber terrorism is an issue that encompasses national and regional boundaries. This is due to the utilisation of the computer technology that operates through the international network, which does not recognise the territorial and geographical

[1] Wilson, C., Computer Attack and Cyber terrorism: Vulnerabilities and Policy Issues for Congress, CRS Report for Congress, 2005, p. 5-6, downloaded from http://fpc.state.gov/documents/organization/45184.pdf [retrieved on the 20.01.2012]

boundaries set by every nation. Although cyber terrorism is a worldwide issue, it has detrimental effects to the people of every nation. Effects can also be seen in the national and regional leadership and also commerce.[2]

Cyber-terrorism is a complex issue that is vital for information security specialists and to some extent the society to recognize. One must be conscious of all of its characteristics in order to better evaluate how and where the "terrorists" are likely to attack our approach. What makes this subject significant is that a cyber terrorist attack is comparatively very easy and economical to instigate. For that reason, it can from any where in the world, at anytime, and, more importantly, the stakes of this cat and mouse game are can be quite high. In view of the fact that it is only a matter of time before a system is attacked, one must stay alert and share the knowledge obtained so that we can help protect ourselves at a personal, business, and national level.[3]

By combining the above concepts of intent and effects, "cyber terrorism" may be defined as the use of computers as weapons, or as targets, by politically motivated international, or sub-national groups, or clandestine agents who threaten or cause violence and fear in order to influence an audience, or cause a government to change its policies.[4]

In many ways the Internet and similar networked systems are ideal for terrorist activities and operations. At the most general level, they provide capabilities for worldwide communications and security at exceedingly low cost. This concept is certainly no secret, and recent evidence demonstrates widespread net use by various terrorist organizations worldwide. The analysis below is focused on terrorist use (and abuse) of the Internet in four major areas[5]:

1. Use of the Internet for terrorist communications, essentially covert communications, and as a means for a new command and control infrastructure.
2. Access to information via the Internet and world wide web (WWW) including for such requirements as information on potential targets as well as technical data in areas such as weapons construction
3. Use of the Internet as a platform for the dissemination of propaganda on terrorist groups and causes, and the related objective of recruiting individuals into these organizations
4. Terrorist attacks on the Internet, and capabilities connected to the net - commonly known as cyber warfare, as yet another avenue for terrorist attack.

---

[2] Nagpal, R. Defining Cyber Terrorism, Asian School of Cyber Laws, 2004 [retrieved on the 04.06.2006] downloaded from http://www.asianlaws.org/cyberlaw/library/cc/def_ct.htm

[3] Saint-Claire, S., Overview and Analysis on Cyber Terrorism, School of Doctoral Studies (European Union) Journal, 2011, p. 97, downloaded from http://www.iiuedu.eu/press/journals/sds/SDS_2011/DET_Article2.pdf [retrieved on the 10.01.2012]

[4] Wilson, C., Computer Attack and Cyber terrorism: Vulnerabilities and Policy Issues for Congress, CRS Report for Congress, 2005, p. 7, downloaded from http://fpc.state.gov/documents/organization/45184.pdf [retrieved on the 20.01.2012]

[5] Wagner, A., R., *Fighting* Terror *in Cyberspace*, Terrorism and the internet: use and abuse, p.7, downloaded from http://www.worldscibooks.com/etextbook/5934/5934_chap1.pdf [retrieved on the 01.02.2012]

SECURITY DIMENSIONS OF CYBER TERRORIST ATTACKS

In security-legal sense, cyber terrorism is a deliberate misuse of digital information system, network or components that wrap or complete terrorist struggle and activity. Result from the misuse of the system will be directly violence against people (not included also crash, chaos in hospitals and the like), but still can cause fear, increased the world crime with the fastest pace, the greatest strategic vulnerability of all the vital social functions, enormous human suffering and casualties as "collateral damage". In this context, even scarier is the fact that these subtle effects can initiate cyber war or "set" certain countries to launch a classic war, in response to cyber actions "taken by the other side". According to the U.S. certain considerations it is only a matter of time before the U.S. can experience the "cyber Pearl Harbour" that would have devastating results, the theft of electronic funds data that would supported the terrorist information, forwarding, redirection of shipments of weapons, etc. But probably the most dangerous is the ultimate simulation of "cyber Chernobyl" accident.

There are many forms of terrorism on the Internet. Some are not dangerous enough to be deemed a simple spread of information instead of terrorism. They are simple show of skill and are harmless. Acts of cyber-crimes may involve stealing of money, company secrets, or attacking country's infrastructure and causing real damage.

Extensive planning and pre-operational surveillance by hackers are important characteristics that precede a cyber attack directed at an organization. Some experts estimate that advanced or structured cyber attacks against multiple systems and networks, including target surveillance and testing of sophisticated new hacker tools, might require from two to four years of preparation, while a complex coordinated cyber attack, causing mass disruption against integrated, heterogeneous systems may require 6 to 10 years of preparation. This characteristic, where hackers devote much time to detailed and extensive planning before launching a cyber attack, has also been described as a "hallmark" of previous physical terrorist attacks and bombings launched by Al Qaeda.[6]

A difference should be made between terrorists who make use of available technology and the pure "cyber terrorist". Traditional terrorists may increase their arsenal of more conservative methods, such as bombings, hijackings, and murders, with new methods such as computer viruses, Radio Frequency Weapons, , and "denial of service" attacks. However, the pure cyber-terrorist may also exist.

This variety of terrorist may do without the conventional approach of terrorism, instead exploiting computer technology to put into effect demands, gain ransoms, or generally cause destruction upon the world population. Additionally, the cyber-terrorist can achieve these objectives without exposing himself to actual harm. Although the pure cyber-terrorist has not appeared in the news yet, current hacker and denial of service attacks may provide a peek as to what the pure cyber-terrorist can accomplish.

---

[6] Wilson, C., Computer Attack and Cyber terrorism: Vulnerabilities and Policy Issues for Congress, CRS Report for Congress, 2005, p. 17, downloaded from http://fpc.state.gov/documents/organization/45184.pdf [retrieved on the 20.01.2012]

The largest threat associated with cyber terrorism and the biggest advantage to the pure cyber-terrorist) is the "detached" sort of attacks. Borders are not crossed, bombs are not smuggled and placed, hostages are not captured, and terrorists do not surrender their lives. Openly stated, "tomorrow's terrorist may be able to do more with a keyboard than with a bomb."

Cyber terrorism is an impending threat to the United States, or any other technologically advanced country. Even nations with more primitive technology can be negatively affected by the "ripple effect". With the excess of technology increasing at an tremendous rate, the threat of cyber terrorism will only get worse.[7]

In societies of the third technological revolution there are two basic methods by which terrorists may commit terrorist attacks.

The first method is when the information technology represents a target of terrorist attacks. By performing certain sabotage (electronic and physical) on the information system, they will try to kill or to commit an interruption in the functioning of information system and information infrastructure, depending on the particular purpose.

The second method is when information attack represents a mean-step implementation of a larger operation. This act implies that terrorists will make efforts to manipulation and exploitation of information system, theft of information as an alternative or forcing - "programming" of the system to perform the function for which intended.

The definition of computer attack includes any actions directed against computer systems to disrupt equipment operations, change processing control, or corrupt stored data. Different attack methods target different vulnerabilities and involve different types of weapons. Several of these methods may be within the current capabilities of some terrorist groups.[8] Three different methods of attack are identified, based on the effects of the weapons used. However, as technology evolves, distinctions between these methods may begin to blur. These methods are the following:

- A physical attack involves conventional weapons directed against a computer facility or its transmission lines;
- An electronic attack (EA) involves the use the power of electromagnetic energy as a weapon, more commonly as an electromagnetic pulse (EMP) to overload computer circuitry, but also in a less violent form, to insert a stream of malicious digital code directly into an enemy microwave radio transmission; and
- A computer network attack (CNA), usually involves malicious code used as a weapon to infect enemy computers to exploit a weakness in software, in the system configuration, or in the computer security practices of an

[7] Saint-Claire, S., Overview and Analysis on Cyber Terrorism, School of Doctoral Studies (European Union) Journal, 2011, p. 85-86, downloaded from http://www.iiuedu.eu/press/journals/sds/SDS_2011/DET_Article2.pdf [retrieved on the 10.01.2012]

[8] All methods of computer attack are within the current capabilities of several nations. See CRS Report RL31787, *Information Warfare and Cyber war: Capabilities and Related Policy Issues.* Noted in: Rodriguez, C., A., Cyber terrorism – A rising treath in the Western hemisphere, Fort Lesley J. McNair Washington DC, 2006, downloaded from http://www.library.jid.org/en/mono45/Rodriguez,%20Carlos.pdf [retrieved on the 15.01.2012]

organization or computer user. However, CNA may also occur when an attacker uses stolen information to enter restricted computer systems.

Attack with help of the information technology is easily feasible, using cheap tools that are easy to hide and are virtually intangible. If it is known that terrorists are "crazy" about their media promotion, if it is known that the preferred target of terrorists in the media, then we can conclude that the possibilities of terrorists for intrusion into sensitive information technology enormously increases the possibilities of "information warfare". It is just a perfect weapon in the rich arsenal of weapons of terrorists who tirelessly follow all the modern trends in this important area.

If today there are an enormous number of objective and subjective obstacles to starting a cyber wars of larger scale (e.g. international economic dependence, escalation and response from the other side in a military conflict, lack of technological readiness), then for the new "terrorists" there are neither obstacles nor the "red line" for launching cyber terrorism globally.

Invisible enemy armed only with a laptop computer connected to the global computer network, "armed" with great human knowledge transformed into a digital code that determines an enormous destructive power and fiery desire to achieve their dark goals, sails into attack with severe recognizable direction, but with the sole objective: electronic attack on national information network of great strategic importance for the smooth functioning of all vital social functions.

It's an evil face of cyber terrorists and cyber terrorism, a dangerous threat to national security in certain states, a death threat to global security in the future. That danger is close to an atomic bomb. The invasion of cyberspace continues with tremendous speed, the speed of development of a powerful offensive computer technology. The world again is facing with another new and very dangerous security challenge of the greatest evil - terrorism.

Cyber terrorism is an attractive option for modern terrorists for several reasons[9]:

- First, it is cheaper than traditional terrorist methods. All that the terrorist needs is a personal computer and an online connection. Terrorists do not need to buy weapons such as guns and explosives; instead, they can create and deliver computer viruses through a telephone line, a cable, or a wireless connection.
- Second, cyber terrorism is more anonymous than traditional terrorist methods. Like many Internet surfers, terrorists use online nicknames—"screen names"—or log on to a website as an unidentified "guest user," making it very hard for security agencies and police forces to track down the terrorists' real identity. And in cyberspace there are no physical barriers such as checkpoints to navigate, no borders to cross, and no customs agents to outsmart.
- Third, the variety and number of targets are enormous. The cyber terrorist could target the computers and computer networks of governments,

[9] Weimann, G., Cyber terrorism. How Real Is the Threat?, Special report 119, United States Institute of Peace, Washington, DC, 2004, p. 6, downloaded from http://www.usip.org/files/resources/sr119.pdf [retrieved on the 20.12.2011]

individuals, public utilities, private airlines, and so forth. The sheer number and complexity of potential targets guarantee that terrorists can find weaknesses and vulnerabilities to exploit. Several studies have shown that critical infrastructures, such as electric power grids and emergency services, are vulnerable to a cyber terrorist attack because the infrastructures and the computer systems that run them are highly complex, making it effectively impossible to eliminate all weaknesses.

- Fourth, cyber terrorism can be conducted remotely, a feature that is especially appealing to terrorists. Cyber terrorism requires less physical training, psychological investment, risk of mortality, and travel than conventional forms of terrorism, making it easier for terrorist organizations to recruit and retain followers.
- Fifth, as the I LOVE YOU virus showed, cyber terrorism has the potential to affect directly a larger number of people than traditional terrorist methods, thereby generating greater media coverage, which is ultimately what terrorists want.

CRIMINALISTIC DIMENSIONS OF CYBER TERRORIST ATTACKS

One model[10] describes the anatomy of cyber terrorism. It is descriptive and should not be confused as a prescriptive model. In order to fully understand cyber terror, one must first understand the cyberspace environment and its unique attributes. Then by analyzing the various components of the cyber terror anatomy, we can grasp the answers to basic questions: who, what how, where, why, and when. Only after one understands these basic pillars, can one fully understand the whole of cyber terrorism. In this model there are

- Cyber terror Actors – Who? - State Supported, Non-State Supported, Sub-State Actor, Hacker, Insiders
- Tools and Techniques - What? - It Is Getting Easier, Modification, Fabrication, Interception, Interruption
- Cyber Tactics, Techniques, and Procedures (TTPs) - How? - Social Engineering/Dumpster Diving/Trashing, Polymorphic Viruses/Code, Worms, Viruses, Denial of Service Attacks
- Categories of Information Targets - Where? - Information and Communications, Physical Distribution, Energy, Banking and Finance, Vital Human Services, The Weakest Link
- Motives - Why? - Cyber Attack, Effects/Results, Advantages, Disadvantages
- Timing is Critical - When? - Stand Alone/Isolated Attack, Coordinated/ Compound Attack.

History has shown that computer crime is carried out by different groups of people: students, amateurs, terrorists and members of organized criminal groups. The only thing that differs is the nature of the crime. Individuals accessing a computer

[10] Ashley, B., K., Anatomy of cyber terrorism: Is America vulnerable? Air University, Maxwell AFB, AL, 2003, downloaded from http://www.au.af.mil/au/awc/awcgate/awc/ashley.pdf [retrieved on the 01.02.2012]

system without further criminal intent differ from employees of a financial institution that transferred money to his account from foreign accounts. Criminal behavior covers a wide range of ages of people in society: from 10 to 60 years, with skills from amateurs to professionals. Computer criminals are average people, not super criminals with unique abilities and talents. Any person of any age, motivated by technical challenges, and some of their ideological beliefs, is a potential criminal. According to some previous studies, employees represent the greatest threat, and indeed computer crime is called an internal crime. According to one document, 90 % of economic crime is committed by employees of damaged companies. An investigation in North America and Europe showed that 73 % of criminal activities were derived from internal sources, and only 23 % of external. As technique of remote processing of data is developed, so will increase the danger from external sources. In recent times are beginning to create criminal groups, composed of members from all around the world. Rapidly it is improved their mutual cooperation. The internet can be found so-called computer-crime communities where are exchanged stolen access codes and software.[11]

Cyber terrorist[12] prefer using the cyber attack methods because of many advantages for it:

- It is Cheaper than traditional methods.
- The action is very difficult to be tracked.
- They can hide their personalities and location.
- There are no physical barriers or check points to cross.
- They can do it remotely from anywhere in the world.
- They can use this method to attack a big number of targets.
- They can affect a large number of people.

According to the tools[13], there are an almost uncountable number of ways that the terrorist can use the computer as a tool. Facilitating identity theft, computer viruses, hacking, use of malware, destruction or manipulation of data all fall under this category. These uses of the computer, when combined with 'computer as target' form the 'traditional' picture of cyber terrorism.

According to the target[14], there are a large number of potential targets that involve, either directly or indirectly, computers. Consider, for example, the impact of Personal Identity Theft. While the incidence of identity theft is comparatively low, the impact of theft upon the unfortunate soul whose ID is stolen can be large: terrorists could use the stolen identity to mask their work, carrying out certain operations under their target's name, not their own.

This would help evade detection by authorities, as well as potentially acting as a 'signal' that an identity or operation had been compromised. The Internet,

---

[11] Shushlevski, Z., Computer crime, downloaded from http://www.ii.edu.mk/predmeti/filozofija/Pdf/konvertirani/%CA%EE%EC%EF%BC%F3%F2%E5%F0%F1%EA%E8%20%EA%F0%E8%EC%E8%ED%E0%EB.pdf [retrieved on the 05.02.2012]

[12] Elmusharaf, M., M., Computer Crime Research Center, Cyber Terrorism: The new kind of Terrorism, 2004, downloaded from http://www.crime-research.org/articles/Cyber_Terrorism_new_kind_Terrorism [retrieved on the 01.02.2012]

[13] Gordon, S., Ford, R., Cyberterrorism?, Symantec Security Response, White paper, Symantec, USA, 2003, p. 7, downloaded from http://www.symantec.com/avcenter/reference/cyberterrorism.pdf [retrieved on the 15.01.2012]

[14] ibid

especially the essentially useless authentication provided by email, provides the perfect breeding ground for identity theft.

Similarly, the rise of online stock trading and stock message boards has created an environment in which it is possible to deliberately manipulate a stock price (perhaps via a stolen identity). A terrorist could use such techniques as a funding source, or even attempt to move the markets towards chaos.

Thus, a well organized virtual attack upon a bank or corporation's stock rather than the bank or corporation itself, could in fact prove to be highly effective.

All of the attacks mentioned above are more likely to be successful when carried out against individual users or corporations rather than governments. However, governmental control currently relies heavily on the stability of the overall economy; thus economic destabilization is a viable attack against a government as well as the attacked third-party entity.

Their wide range of activities includes the use of private information for the purpose of extortion same forms of cyber crime by entering into networks, as well as physical and electronic destruction of digital information system. Already there is not a digital device that can not become a victim of computer vandals and terrorists. All devices connected to computers can become a target of hackers, who through a global computer network can bring a digital code that will disrupt their regular and normal operation. For each device that connects to the network can send a series of digital commands that make the device work as the creator of those commands wishes. Classic protection systems are almost helpless in terms of methods used by today's hackers and cyber terrorists.

SECURITY RESPONSE TO THE CYBER TERRORIST ATTACKS

Modern terrorism significantly differs from the classical terrorism. It is also clear that conventional anti-terrorist methods simply do not work against modern terrorism, at least in the cyber terrorism. Through asymmetrical access of the non-state actors who employing terrorism, and particularly al-Qaeda, have imposed new standards in the war. This means that contemporary terrorism is no longer just purely criminal or security problem. It is a problem that flies through political, military, social, economic, cultural and religious heritage. Therefore, for such a phenomenon that has a global prefix that quickly adapts and adjusts to the appropriate region, one of the possible ways of coping is through regional cooperation.

Regional cooperation supported by an entity like the EU, which has developed mechanisms for its support, can successfully develop an effective medium for security response. Regional cooperation, arguably, may be appropriate security response to threats of modern terrorism because it contains conditions which rests and through which operates the threat. Indeed, more than clear is that the countries of a given region share similar security, political, economic, social, cultural and historical perspectives and challenges. The EU has built a number of mechanisms that play a significant role in dealing with modern terrorism. In this context, for example, are efforts and activities for integrated border management. Through a centralized database for data exchange is ensured an effective flow of information. It may be suitable remedy for past inaction and bureaucratic procedures that hamper the proper response to terrorism.

Greatly facilitate regional cooperation comes because of the fact that certain countries, despite being only aspiring to join the EU through the process of standardization and harmonization are subject to acceptance of a number of mechanisms which the EU has in its operative part. It relates to traffic safety, preventing financing of terrorism and humanitarian assistance, which is especially landmark in the new position that is built with EU on terrorism.

Thinking about the transformation of international relations on the planet as a country without borders, the challenges in the field of international terrorism, organized crime, cyber challenges, environmental degradation, natural and other disasters, has become more evident that it is necessary to strengthen the partnership between NATO and the EU. Alliance needs the European Union, but Europe has indispensable necessity of NATO.

Laws, systems of criminal justice and international cooperation did not keep pace at which technology was changing. Only a few countries have adequate laws to address this problem, and none of them failed to resolve all legal, regulatory and preventive issues.

When this question is evaluated on the international scene, the problems with inappropriate measures are discovered. Computer crime is a new form of international crime and is necessary international cooperation to consider effective. This can only happen if there is a basis of understanding what the problem is and which can be solutions.

Some of the problems of international cooperation in computer crime and criminal law may be:

1. Lack of global consensus on what types of behavior will fit the computer crime;
2. Lack of global consensus on definitions of criminal behavior;
3. Lack of expertise in the areas of police, prosecutors and courts in this field;
4. Lack of agreement among different national procedural laws concerning the investigation of computer crime;
5. International character of cybercrime;
6. Lack of extradition and mutual assistance and synchronized mechanisms for law enforcement on the international field.[15]

The Interpol, with its 178 member countries, is doing a great job in fighting against cyber terrorism. They are helping all the member countries and training their personnel.

The Council of Europe Convention on Cyber Crime, which is the first international treaty for fighting against computer crime, is the result of 4 years work by experts from the 45 member and non-member countries including Japan, USA, and Canada. This treaty has already enforced after its ratification by Lithuania on 21st of March 2004.[16]

---

[15] Shushlevski, Z., Computer crime, downloaded from http://www.ii.edu.mk/predmeti/filozofija/Pdf/konvertirani/%CA%EE%EC%EF%BC%F3%F2%E5%F0%F1%EA%E8%20%EA%F0%E8%EC%E8%ED%E0%EB.pdf [retrieved on the 05.02.2012]

[16] Elmusharaf, M., M., Computer Crime Research Center, Cyber Terrorism: The new kind of Terrorism, 2004, downloaded from http://www.crime-research.org/articles/Cyber_Terrorism_new_kind_Terrorism [retrieved on the 01.02.2012]

CONCLUSION

Further, the next generation of terrorists will grow up in a digital world, with ever more powerful and easy-to-use hacking tools at their disposal. They might see greater potential for cyber terrorism than do the terrorists of today, and their level of knowledge and skill relating to hacking will be greater. Cyber terrorism could also become more attractive as the real and virtual worlds become more closely coupled, with automobiles, appliances, and other devices attached to the Internet. Unless these systems are carefully secured, conducting an operation that physically harms someone may be as easy as penetrating a Web site is today.

At least for now, hijacked vehicles, truck bombs, and biological weapons seem to pose a greater threat than cyber terrorism. However, just as the events of September 11 caught us by surprise, so could a major cyber assault. We cannot afford to shrug off the threat.[17]

BIBLIOGRAPHY

- Ashley, B., K., Anatomy of cyber terrorism: Is America vulnerable? Air University, Maxwell AFB, AL, 2003, downloaded from http://www.au.af.mil/au/awc/awcgate/awc/ashley.pdf [retrieved on the 01.02.2012]
- Denning, D., E., Social science research council/After sept. 11, Is Cyber Terror Next?, downloaded from http://essays.ssrc.org/sept11/essays/denning_text_only.htm [retrieved on the 05.02.2012]
- Elmusharaf, M., M., Computer Crime Research Center, Cyber Terrorism: The new kind of Terrorism, 2004, downloaded from http://www.crime-research.org/articles/Cyber_Terrorism_new_kind_Terrorism [retrieved on the 01.02.2012]
- Gordon, S., Ford, R., Cyberterrorism?, Symantec Security Response, White paper, Symantec, USA, 2003, p. 7, downloaded from http://www.symantec.com/avcenter/reference/cyberterrorism.pdf [retrieved on the 15.01.2012]
- Nagpal, R. Defining Cyber Terrorism, Asian School of Cyber Laws, 2004 [retrieved on the 04.06.2006] downloaded from http://www.asianlaws.org/cyberlaw/library/cc/def_ct.htm
- Rodriguez, C., A., Cyber terrorism – A rising treath in the Western hemisphere, Fort Lesley J. McNair Washington DC, 2006, downloaded from http://www.library.jid.org/en/mono45/Rodriguez,%20Carlos.pdf [retrieved on the 15.01.2012]
- Saint-Claire, S., Overview and Analysis on Cyber Terrorism, School of Doctoral Studies (European Union) Journal, 2011, p. 97, downloaded from http://www.iiuedu.eu/press/journals/sds/SDS_2011/DET_Article2.pdf [retrieved on the 10.01.2012]
- Shushlevski, Z., Computer crime, downloaded from http://www.ii.edu.mk/predmeti/filozofija/Pdf/konvertirani/%CA%EE%EC%EF%BC%F3%F2%E5%F0%F1%EA%E8%20%EA%F0%E8%EC%E8%ED%E0%EB.pdf [retrieved on the 05.02.2012]

[17] Denning, D., E., Social science research council/After sept. 11, Is Cyber Terror Next?, downloaded from http://essays.ssrc.org/sept11/essays/denning_text_only.htm [retrieved on the 05.02.2012]

- Wagner, A., R., *Fighting* Terror *in Cyberspace*, Terrorism and the internet: use and abuse, p.7, downloaded from http://www.worldscibooks.com/etextbook/5934/5934_chap1.pdf [retrieved on the 01.02.2012]
- Weimann, G., Cyber terrorism. How Real Is the Threat?, Special report 119, United States Institute of Peace, Washington, DC, 2004, p. 6, downloaded from http://www.usip.org/files/resources/sr119.pdf [retrieved on the 20.12.2011]
- Wilson, C., Computer Attack and Cyberterrorism: Vulnerabilities and Policy Issues for Congress, CRS Report for Congress, 2005, p. 5-6, downloaded from http://fpc.state.gov/documents/organization/45184.pdf [retrieved on the 20.01.2012]

SUMMERY

Cyber terrorism is a new, modern form of terrorism that its violent aims, motives and ideology, seek to achieve through the exploitation of information and computer systems, specifically the use of computers as weapons or as targets of attacks. In today's modern information-communication era of life, terrorists are increasingly adapting to the new conditions, taking them to perform so-called cyber terrorist attacks. In many ways the Internet and similar networked systems are ideal for terrorist activities and operations. At the most general level, they provide capabilities for worldwide communications and security at exceedingly low cost. This concept is certainly no secret, and recent evidence demonstrates widespread net use by various terrorist organizations worldwide.

Tremendous achievement and development of high technology and sophisticated computer systems have opened a new "cyber space", which constantly destroys old traditional forms of organization, behaviour and belief. Cyber information led to the cyber revolution and the emergence of information society, in which dominated the race for information and communication technologies, along with the global liberalization and free circulation of people, goods and ideas. Today, thirty years after the introduction of the term, the concept of cybernetics, it inevitably became a primary component of many important terms: cyber society, cyber policy, cyber economy, cyber war, cyber terrorism, cyber crime, which essentially the most precious crown, represents cyber information. There are many forms of terrorism on the Internet. Some are not dangerous enough to be deemed a simple spread of information instead of terrorism. They are simple show of skill and are harmless. Acts of cyber-crimes may involve stealing of money, company secrets, or attacking country's infrastructure and causing real damage. History has shown that computer crime is carried out by different groups of people: students, amateurs, terrorists and members of organized criminal groups

Modern terrorism significantly differs from the classical terrorism. It is also clear that conventional anti-terrorist methods simply do not work against modern terrorism, at least in the cyber terrorism. Through asymmetrical access of the non-state actors who employing terrorism, and particularly al-Qaeda, have imposed new standards in the war. This means that contemporary terrorism is no longer just purely criminal or security problem. It is a problem that flies through political, military, social, economic, cultural and religious heritage. Therefore, for such a phenomenon that has a global prefix that quickly adapts and adjusts to the appropriate region, one of the possible ways of coping is through regional cooperation.

Pregledni rad – UDK 004.738.5: 343.326

STRATEŠKE KONCEPCIJE U SUPROTSTAVLJANJU VISOKOTEHNOLOŠKOM KRIMINALU[1]

U[1]*prof. dr Goran Bošković*[2]
doc. dr Zvonimir Ivanović[3]
Kriminalističko-policijska akademija, Beograd

***Apstrakt**:* Pravilan izbor adekvatne strategije u suprotstavljanju kriminalu krucijalna je polazna tačka i osnovni preduslov za efikasno suprotstavljanje svakom obliku kriminala, a posebno visokotehnološkim kriminalnim aktivnostima. Štaviše, zbog svojih osnovnih karakterisitka, efikasno suprotstavljanje visokotehnološkom kriminalu, kao uslov svih uslova, ima organizovanje i angažovanje svih kapaciteta, na različitim nivoima, koji uključuju strateške koncepcije, međudržavnu i međuagencijsku saradnju. U oblasti kreiranja strategiskih koncepata suprotstavljanja visokotehnološkom kriminalu veoma se daleko otišlo na svim nivoima od globalnih inicijativa i strateških koncepcija do lokalnih usklađenih policijskih pristupa. Autori u radu, koristeći se komparativnim analitičkim pristupom, pružaju pregled globalnih, regionalnih i lokalnih koncepata rešavanja problema suprotstavljanja visokotehnološkom kriminalu i ukazuju na osnovna strateška stremljenja u ovoj oblasti. Globalne i regionalne koncepcije u radu su prikazane blago evrocentrično, dok se kao lokalni primeri daju SAD, Australija i Srbija.

Ključne reči: strateški koncepti, visokotehnološki kriminal, organizovani kriminal, preventivne koncepcije, međunarodne organizacije.

UVOD

Osnovne polazne koncepcije u suprotstavljanju visokotehnološkom kriminalu[4] iziskuju kao neophodno ustanovljavanje i regulisanje strateških odbrambenih i ofanzivnih nivoa suprotstavljanja ovoj pojavi. Verovatno najnezahvalnija predviđanja u strateškim oblastima organizovanja vlasti tiču se visokotehnoloških kriminalnih aktivnosti i preventivnih delatnosti u borbi protiv istih.[5] Nivo i značaj priprema i

---

[1] Ovaj rad je rezultat realizovanja naučnoistraživačkog projekta pod nazivom *Razvoj institucionalnih kapaciteta, standarda i procedura za suprotstavljanje organizovanom kriminalu i terorizmu u uslovima međunarodnih integracija*. Projekat finansira Ministarstvo prosvete i nauke Republike Srbije (br. 179045), a realizuje Kriminalističko-policijska akademija u Beogradu (2011−2014). Rukovodilac projekta je prof. dr Saša Mijalković.

[2] goran.boskovic@kpa.edu.rs.
[3] zvonimir.ivanovic@kpa.edu.rs.

[4] Zakonom o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnoloskog kriminala iz 2005. godine, u članu 2 uvodi se novi termin *visokotehnološki kriminal* i određuje kao vršenje krivičnih dela kod kojih se kao objekat ili sredstvo izvršenja krivičnih dela javljaju računari, računarske mreže, računarski podaci, kao i njihovi proizvodi u materijalnom ili elektronskom obliku.

[5] Strateško planiranje ostvaruje se donošenjem kratkoročnih, srednjoročnih i dugoročnih planova, definisanjem vizije, misije, ciljeva, učesnika, njihovih prava i obaveza, postupaka evaluacije. (Simonović, 2006: 185).

planiranja u suprotstavljanju visokotehnološkom kriminalu različitih struktura vlasti u mnogim državama je veoma raznolik.[6] U tom kontekstu neophodno je na nivou strateških razmatranja ukazati na incijative, aktivnosti i napore globalnih i regionalnih međunarodnih organizacija u kreiranju strateških opredeljenja u suprotstavljanju visokotehnološkim kriminalnim aktivnostima.

Na globalnom planu organizacija Ujedinjenih nacija kroz rad svojih specijalizovanih tela i radnih grupa aktivno se uključila u rešavanje problema bezbednosti u današnjem informatičkom društvu. Jedno od naznačajnijih specijalizovanih tela Ujedinjenih nacija jeste *Međunarodna telekomunikaciona unija*[7] (International Telecommunication Union – ITU), čiji se rad odvija kroz sledeće specijalizovane ogranke: Sektor za razvoj telekomunikacija, Sektor za telekomunikacione standarde, Sektor radiokomunikacija, Strateška jedinica (Strategy & Policy Unit – SPU)[8]. Dva najveća dostignuća ITU u oblasti kreiranja strateških opredeljenja u suprotstavljanju visokotehnološkom kriminalu jesu *Plan globalne kiber bezbednosti* i *Kiber bezbednosna kapija* – izvor informacija onlajn na internetu kao rezultat nacionalne i međunarodne inicijative. Koristeći ovaj onlajn resurs, korisnici mogu dobiti informacije vezane za različite inicijative u odnosu na svaku zemlju u nekoliko različitih oblasti kao što su: razmena informacija, nadzora i upozoravanja, industrijskih standarda i rešenja, zakona i zakonodavstava kao i privatnosti i zaštite.

Ujedinjene nacije su u još nekim svojim organizacijama kao što su *Kancelarija UN za kontrolu narkotika i prevenciju kriminala* (United Nations Office on Drugs and Crime – UNODC)[9] i *Kancelarija UN za poslove razoružanja* (United Nations Office for Disarmament Affairs – UNODA)[10] veoma intenzivno razvijale kapacitete za borbu protiv visokotehnološkog kriminala. UNODC je fokusiran na kriminalnu zloupotrebu identiteta, promovisanje legislative o visokotehnološkom kriminalu, obuku pripadnika policije i drugih organa gonjenja. UNODA je u poslednje vreme proširila svoju delatnost na informacioni rat i kiber terorizam.[11]

---

[6] Deo procesa strateškog planiranja suzbijanja kriminala obuhvata i procene objekta kriminalističke obrade koje se odnose na snage, slabosti, mogućnosti i pretnje. U stranoj literaturi ovaj postupak je poznat pod nazivom „SWOT"– *Strength, Weaknesses, Opportunities, Threats* (Lowenthal, 2002: 87).

[7] Prvobitno određena kao Međunarodna telegrafska unija, osnovana od mrežnih operatera u cilju omogućavanja međupovezivanja i međuoperativnosti nacionalnih ustanova i usluga. Sada su joj glavni ciljevi standardizacija, alociranje radio spektruma i organizacija sporazuma o povezivanju među državama u cilju omogućavanja međunarodnih telefonskih poziva. Od aprila 2008. godine okuplja 191 članicu i preko 700 privatnih kompanija i drugih organizacija. Osnovni cilj joj je da izgradi sigurnost i poverenje u korišćenje međunarodnih komunikacionih tehnologija, omogućavanje saradnje između privatnih i javnih organizacija i stvaranje inicijativa za obrazovanje i obuku.

[8] Bavljenje pitanjima kiber bezbednosti ove jedinice se ogleda i kroz konjunkciju sa otvorenom platformom *Partnerstva za globalnu kiberbezbednost* (Partnerships for Global Cybersecurity – PGC).

[9] Oformljena 1997. godine u cilju rešavanja međunarodnih problema i pitanja zabranjene trgovine narkoticima, prevencije kriminala i međunarodnog terorizma. Šire videti u – *United Nations Office of Drugs and Crime* (2008), About UNODC. Internet: http://www.unodc.org/unodc/en/about-unodc/index.html.

[10] Osnovana 1982. godine, reformisana 1998. godine, za cilj ima promociju nuklearnog razoružavanja i zabrane proliferacije i podrške razoružanju dugih oružja masovnog uništenja, hemijskog ili biološkog oružja.

[11] Detaljnije, u: Chellany. B (2001), *Revolution in Information Technology and its Impact on Security. The Asian Pacific Region: Evolution of the Scope of Security and Disarmament in the 21st Century*, United Nations Conference on Disarmament Issues. Internet: http://disarmament.un.org/RCPD/pdf/plen2b.pdf.

NATO (North Atlantic Treaty Organization –NATO)[12] pruža svojim kapacitetima prostor za razmatranje različitih nivoa bezbednosne problematike, od kojih, pitanje kiber bezbednosti ima veoma značajnu ulogu, čija aktuelnost raste. Još je daleke 1969. godine NATO je ustanovio *Komitet za izazove modernog društva* (Committee on the Challenges of Modern Society – CCMS) koji je trebao uvesti „nevojni ugao gledanja u savezu", kako bi se sagledale „socijalne slabosti dolazeće izvan tradicionalnih bezbednosnih okvira".[13] Tako, već od 1970. godine NATO igra značajnu ulogu u razvoju kompjuterskih internet komunikacija zajedno sa Ministarstvom odbrane SAD odnosno njegovom *Agencijom za napredna istraživanja* (U.S. Defence Advanced Research Projects Agency – DARPA), obuhvatajući i dostignuća u kiber sigurnosti, infrastrukturi i tehnologiji tokom 90-tih.[14] Primarni organ NATO–a za podršku praktične saradnje u nevojnom naučnom sektoru i inovacijama, uključujući i inicijative u vezi s mrežnom bezbednosti i kiber terorizmom jeste *Komitet nauke za mir i bezbednost* (The Science for Peace and Security Committee).[15] Ministri odbrane NATO-a su se saglasili da agresivnije intenziviraju napore u proučavanju prevencije visokotehnološkog kriminala nakon incidenata u javnom kiber prostoru Estonije 2007. godine.[16] Ovaj incident je ukazao na internacionalizaciju ove vrste kriminala i potrebu da se u okvirima NATO na širem osnovu primenjuju internet bezbednosne procedure. Kao posledica ovih dešavanja javlja se stvaranje *Centra Kiber Odbrane*[17] u Estoniji 2008. godine.

U okvirima Grupe 8 najrazvijenijih zemalja[18] i Rusije osnovana je *24/7 Mreža kontakata za visokotehnološki kriminal*, a u okviru NATO – *Tehnički Centar za brze reakcije na kompjuterske incidente* (NATO Computer Incident Response Capability-Technical Centre – NCIRC-TC), te su kroz ove institucije stvoreni centri za kontakte u vezi s incidentima visokotehnološkog kriminala. Na kraju i Interpolove regionalne radne grupe pružaju mogućnost obuke u pogledu problematike visokotehnološkog kriminala u najrazličitijim oblastima sveta.[19]

---

[12] Savez koji je bio pandan Varšavskom paktu u doba hladnog rata, i koji je neformalno iz tog rata izašao kao pobednik, okuplja dvadeset šest država članica, osnovni cilj mu je sada održanje mira u regionu i svetu.

[13] North Atlantic Treaty Organization (2002) *Vulnerability of the Interconnected Society*. NATO CCMS Short-Term Project: Final Report. Oslo, Norway. Internet: http://www.nato.int/science/publication/nation_funded/doc/262-VIS%20Final%20 RepOct%202002.pdf.

[14] Detaljnije, u: Cerf, V.; Kahn, R. (1999). *What Is The Internet (And What Makes It Work)*. Corporation for National Research Initiatives. Internet: http://www.cnri.reston.va.us/what_is_internet.html.

[15] Ovaj komitet je 2006. godine u Sofiji (Bugarska) organizovao istraživačku radionicu na temu *Kiber terorizam kao nova bezbednosna pretnja* na kojoj su učestvovali stručnjaci zemalja članica, partnerskih zemalja i zemalja koje nisu članice NATO –a. Osnovni cilj ove radionice jeste razmatranje pitanja dalje potrebe za istraživanjima oblasti kao što su interakcija među kiber terorizmom i organizovnim kriminalom, ulozi vlada i međunarodsnih organizacija u borbi i sprečavanju kiber terorizma, ali i merama bezbednosti, kao što su biometrijske mere, kriptografija, bezbednosne mere bežičnih mreža (vajerlesa) i računarske forenzike.

[16] U ovom napadu kriminalci locirani u više od 50 država onemogućili su svakodnevne rutinske aktivnosti u celoj Estoniji.

[17] Sedam zemalja članica NATO koje su izrazile želju učešća u ovom centru su na samitu 2008. godine u Rumuniji u Bukureštu trebale da dobiju i formalnu inauguraciju kroz jedno telo *Menadžmenta kiber odbrane*, koje bi preuzelo primat u daljim aktivnostima NATO na ovom polju.

[18] Zemlje članice su: Kanada, Francuska, Japan, Nemačka, Italija, Velika Britanija i SAD.

[19] Naša zemlja ima dva sertifikovana trenera za ovu oblast, čija je obuka ostvarena preko saradnje sa Interpolom.

REGIONALNE INCIJATIVE ZA KREIRANJE STRATEŠKIH OPREDELJENJA U SUPROTSTAVLJANJU VISOKOTEHNOLOŠKOM KRIMINALU

Regionalne međuvladine organizacije značajno doprinose globalnim naporima za strateško suprostavljanje visokotehnološkom kriminalu i obezbeđenju kiber prostora (Kjaerland, 2005). U ovom smislu kao deo fronta u suprostavljanju ovoj pošasti pojavljuje se i Organizacija za evropsku bezbednost i saradnju – OEBS (Organization for Security and Co-operation in Europe – OSCE). Ona je oformila *Radnu grupu za bezbednost informacija i privatnost* (Working Party on Information Security and Privacy –WPISP) koja je primarno angažovana na edukaciji i prikupljanju podataka iz ove oblasti i prezentaciju novih dometa u suprotstavljanju visokotehnološkom kriminalu kroz časopis *Smernice za bezbednost informacionih sistema i mreža*. Ova radna grupa godišnje sprovodi i ankete u državama članicama u primeni ovih smernica i izdaje i vodič *Privatnost onlajn: OEBS-ov vodič za policiju i praksu*, kojim pokušava da ukaže na aktuelne probleme i trendove u kiber prostoru. WPISP je ustanovila sajt[20] posvećen bezbednosnoj kulturi u kiber prostoru s ciljem razmene ideja o politici suprotstavljanja visokotehnološkom kriminalu i promociji bezbednosne kulture u ovoj oblasti. Pored pomenutog, WPISP se bavio i različitim istraživanjima i analizom aktivnosti vezanih za pretnje kiber bezbednosti, kreiranjem smernica u ovoj oblasti, stvaranjem zajedničkih okvira za primenu bezbednosti informacija i zaštitu privatnosti[21], edukacijom i razmenom informacija u krugu zemalja članica cilju boljeg obezbeđenja kiber prostora.

Parlament EU je doneo veći broj deklaracija, rezolucija i ostvario više oblika međunarodnih kontakata, dok je Savet Evrope doneo jednu od najpoznatijih i najpriznatijih konvencija u pogledu politike borbe protiv visokotehnološkog kriminala – *Konvenciju o visokotehnološkom (kiber) kriminalu*. U oblasti suprotstavljanja visokotehnološkom kriminalu i druge evropske institucije svojim radom značano doprinose kiber bezbednosti, a najvažnije su: *Evropski institut telekomunikacionih standarda* (European Telecommunications Standards Institute – ETSI), Evropski *komitet za stadardizaciju* (European Committee for Standardization – CEN), *Odbor za informacione i komunikacione standarde* (Information and Communications Technologies Standards Board – ICTSB. U Evropi se koordinacija u pogledu bezbednosnih pretnji visokotehnološkog kriminala većinom sprovodi od strane *Evropske jedinice timova za brze reakcije na kompjuterske incidente* (European Task Force on Computer Security Incident Response Teams – TF-CSIRT) i Europolovog *Centra za visokotehnološki kriminal*.

U regionu Pacifika se veoma dobro napreduje u pogledu kreiranja okvira za suprotstavljanje visokotehnološkom kriminalu kroz rad organizacije *Azijskopacifičke ekonomske saradnje* (Asia Pacific Economic Cooperation – APEC) i njenih radnih tela *Grupe za telekomunikacije i infomatiku* i *Grupe za bezbednost i napredak* (Security and Prosperity Steering Group – SPSG), koje aktivno podstiču aktivnosti vezane za pretnje kiber bezbednosti. U ovom regionu održano je niz

[20] Internet: http://www.oecd.org/site/0,3407,en_21571361_36139259_1_1_1_1_1,00.html.
[21] Internet: http://www.oecd.org/document/33/0,3343,en_21571361_36139259_36306849_1_1_1_1,00.html.

konferencija i radionica na temu kiber terorizma i mrežne bezbednosti. *Association of Southeast Asian Nations – ASEAN* je preko organizacije *Ministara za IT i telekomunikacije* (Telecommunications and IT Ministers – TELMIN) fokusirala svoj rad na promociju, saradnju i harmonizaciju politike bezbednosti kroz kreiranje i podršku u stvaranju *timova za brze reakcije na kompjuterske hitne slučajeve* (Computer Emergency Response Team – CERT) u ovom regionu. Na kraju treba pomenuti i da su: *Azijskopacifička telekomunikaciona unija*, *Ekonomsko-socijalna komisija UN za Aziju i Pacifik* (United Nations Economic and Social Commission for Asia and the Pacific – UN ESCAP) kao i Kina, Japan i Koreja dosta doprineli kreiranju okvira za efikasniju borbu protiv visokotehnološkog kriminala u ovoj oblasti. [22]

Sa druge strane okeana, *Organizacija američkih država* (Organization of American States –OAS) i *Latinoamerička saradnja razvijenih mreža* (Latin American Cooperation of Advanced Networks – CLARA) ušle su u brojne programe i inicijative u cilju poboljšanja američke kiber bezbednosti. Ovu ulogu je na sebe preuzela u najvećem delu *Međuamerička telekomunikaciona komisija* (Inter American Telecommunication Commission – CITEL) kroz aktivno promovisanje razvoja bezbednosti telekomunikacija i borbe protiv prevara. U okviru CLARA postoji *Jedinica za bezbednost* (Security Task Force – GT-Seg), a u okviru OAS *Međuamerički komitet protiv terorizma* (Inter – American Committee Against Terrorism –CICTE), koji su zajedničkim snagama preuzeli ulogu regionalnog koordinatora za saradnju *Timova za brzu reakciju na kompjuterske incidente i ugrožavanje bezbednosti*. OAS-ov tim vladinih stručnjaka za visokotehnološki kriminal podržava i promoviše saradnju organa gonjenja u regionu kroz različite oblike obuke i edukacije.

Nevladine organizacije i privatno finansirane organizacije od javnog interesa aktivno participiraju u zaštiti kiber prostora od različitih oblika visokotehnološkog kriminala. Neke od njih su: *Spamhaus*, *The London Action Plan, CAUCE* i *StopSpamAlliance*. Njihove aktivnosti se uglavnom ogledaju u podizanju nivoa javne svesti o problemima zaštite kiber prostora i saradnje na sprečavanju pojedinih oblika visokotehnološkog kriminala. Takođe, slično ovome imamo *Anti Phasing Working Group, International Bonnet Task Force*, *Anti-Spy ware Coalition,* koji su postali lideri u borbi protiv socijalnog inženjeringa, fišinga, farminga, botnetova i zloćudnih programa.

Na planu prevencije visokotehnološkog kriminala deluje oko 537 organizacija neke od njih su: Authentication & Online Trust Alliance – AOTA, International Chamber of Commerce – ICC, World Information Technology and Services Alliance (WITSA) i druge. Ove organizacije su sponzorisale veći broj akcija sa ciljem promocije politike bezbednosti i povišenja javne svesti u pogledu suprotstavljanja visokotehnološkom kriminalu. U ovim pravcima se globalna, i sa njom ukomponovana regionalna, strategija kreće i putem istraživanja, razvoja i standardizovanja kiber bezbednosnih proizvoda[23] kao i protokola. To se naročito

[22] Vidi, u: *Organisation for Economic Co-operation and Development* (2007) *OECD Workshop on Digital Identity Management (IDM)*. Internet: http://www.oecd.org/sti/security-privacy/idm.

[23] Što bi predstavljalo ukupnost programskih, protokolarnih i sistemskih rešenja u sprečavanju i odvraćanju od napada kiber kriminala.

može videti kroz saradnju javnih i privatnih sektora u ovoj oblasti i realizaciju različitih zajedničkih aktivnosti kao što su *3rd Generation Partnership Project* – 3GPP i *European Research and Education Networking Association* – TERENA. Pomenute organizacije se bave razvojem naprednih bezbednosnih tehnologija, uključujući standarde autentifikacije, kriptografije, biometrije.

Ono što je veoma bitno razumeti jeste da se neke od ovih organizacija pojavljuju tek u poslednjih nekoliko godina, da do tog momenta, uopšte, nisu postojale, te da su kreirane samo kako bi se ostvario ovaj njihov cilj. Strateška orijentacija ima svoju osnovnu projekciju da od najviših nivoa prelazi ka osnovnom frontu, pri čemu svaka od linija ima vrlo značajnu ulogu u ukupnom rešavanju problema, na šta ukazuju ovi pozitivni primeri aktivnosti navedenih organizacija.

OSNOVNA STRATEŠKA OPREDELJENJA SAD I AUSTRALIJE U SUPROSTAVLJANJU VISOKOTEHNOLOŠKOM KRIMINALU

Strateškom koncepcijom u nacionalnim okvirima najdalje su otišle *SAD*. Već vrlo brzo posle terorističkih akata 11. septembra, država je, haotično pokušavajući da se odbrani od novih mogućih akata preduzela mnoge korake zadiranja u privatnost, vršenja prospektivnog i drugih vrsta nadzora. Kasnije su se ovakvi, možda i prenagljeni, koraci pretvorili u konceptualne potrebe i sistemske, strukturisane i projektovane zahteve organa suprotstavljanja različitim oblastima visokotehnološkog kriminala. Uz date koncepte na mnogim nivoima državne uprave predstavljene su i strategije u borbi protiv ovog oblika kriminala, pa tako skoro sve važnije državne agencije u SAD imaju ustanovljene i usklađene koncepte strategija u ovoj oblasti.

Jedna o značajnih aktivnosti koje je preduzeo predsednik SAD na ovom planu jeste ustanovljavanje posebne *Jedinice za borbu protiv krađe identiteta*[24]i donošenje posebne strategije suprotstavljanja visokotehnološkom kriminalu.[25] U strateškom planu jedinica je postavila ukupno 31 preporuku, koje su date u rasponu od minornih koraka do široke promene politike u cilju podizanja nivoa bezbednosti kiber prostora. Generalno, skoro svaka instanca u javnoj vlasti je, od ovog trenutka, preduzela niz značajnih koraka u pogledu zaštite svojih domena, pa tako, na primer, *Odbor za federalne rerzerve SAD*, *Federalna komisija za osiguranje depozita* (Federal Deposit Insurance Corporation – FDIC), *Kancelarija za nadzor krađa* i još neke agencije su ustanovile baze podataka praćenja incidenata vezanih za sigurnost elektronskih podataka. *Specijalna tajna služba SAD* (USA Secret service – USS) uključila je svoje resurse u ovu kampanju proširivanjem svojih kapaciteta i linkova sa zvaničnog sajta. *Poreska služba u SAD* je preko svog sajta i linkova i obaveštenja na njima u konstantnom pružanju podrške i informacija svojim obveznicama; ovaj oblik podrške obuhvata i *fišing,* pored krađe identiteta (Bidwell, 2002).

---

[24] Koja je rezultat nove doktrine u bezbednosnim oblastima, uvezivanja u obaveštajno-bezbednosne zajednice; videćemo da je svaki segment ove jedinice u stvari zasebna orgaizacija, organ ili agencija u SAD.

[25] Strateški plan je bio rezultat aktivnosti ove jedinice i 11. 04. 2007. godine je predstavljen predsedniku u cilju odobravanja. Strategija je obuhvatila više organizacija i dalekosežnim predviđenim merama ukazala na buduća efikasna rešenja. Internet: www.idtheft.gov/reports/StrategicPlan.pdf.

Strateški koncept u globalu nije moguć bez upliva privatnog sektora u akcije i različite oblike preventivnih i reperesivnih mera i radnji. Jedan od oblika uključivanja privatnog sektora je fizički otelotvoren u postavljanju edukativnog sajta *www.LooksTooGoodToBeTrue.com.* Ključni učesnici ovog projekta sa strane privatnog sektora su *Nacionalni centar za borbu protiv kriminala belog okovratnika*, Monster.com, kao i članovi *Saveta rizika trgovaca*.

Sve navedeno je prikazano u smislu funkcionisanja različitih poluga vlasti na višem nivou. Ova strategija ne ostavlja po strani ni lokalne organe reda, smatrajući da je već od prvog momenta kontakta žrtava sa oblicima visokotehnološkog kriminala bitno da ukažu na pojedine korake, koje žrtve mogu preduzeti kako bi započele postupak restitucije dobara i sredstava oduzetih putem izvršenog dela i eventualno osujetile dalje nastupanje štete. U tom smislu, kao rezultat primene smernica strateškog plana u cilju obuke lokalnih policijskih stanica održano je više od 900 savetovanja za pripadnike organa gonjenja više od 250 agencija.

Ministarstvo odbrane SAD[26] sa *Federalnom komisijom za trgovinu* (Federal Trade commission – FTC) kreiralo je nacionalni kurs obuke savetnika za žrtve ovog oblika kriminala. Takođe, *Ministarstvo odbrane SAD* vodi i radionicu o krađi identiteta kao oblik konstantnog vida obuke.[27] Kao deo širokog fronta u borbi protiv ove *pošasti* pojavljuje se i *Američka advokatska komora,* čija je *Sekcija za administraciju zakona i regulaciju prakse* predložila rezoluciju kojom bi se urgiralo na nacionalne, federalne, državne, teritorijalne, plemenske i lokalne advokatske komore u saradnji sa državnim i lokalnim za pružanje subvencionisanih oblika pravne pomoći ugroženim kategorijama stanovništva, kako bi se ustanovio program predstavljanja i zastupanja pomoći žrtvama krađe identiteta.

Australija je strateški pokušala da se postavi u pogledu borbe protiv visokotehnološkog kriminala. Već se u preliminarnim strateškim konceptima[28] prepoznaju nacrti strateškog cilja kreiranja sigurnog i bezbednog elektronskog operacionalnog okruženja za javni ali i privatni sektor. Preporuke koje su predstavljale okvire strateškog plana razvoja australijskog pristupa problemu mogu se svesti na sledeće:

- Ustanovljavanje okruženja ili zajednice u kiber prostoru koja je u najmanju ruku bezbedna i sigurna kao i u fizičkoj sredini;
- Razumevanje suštine i prirode problema, što je jako teško ako se imaju u vidu okviri visokotehnološkog kriminala i nemogućnosti registrovanja svih njegovih oblika, ali i tamne brojke ovog kriminaliteta;
- Izrada sveobuhvatnog plana na kreiranju politike i zakonodavnog okruženja koje pruža šansu i privatnom sektoru da učestvuje u kreiranju pravila i ostvarivanju „mekog mešanja“ države u ove oblasti;
- Hvatanje u koštac sa značajnim pitanjima, kao što je pitanje anonimnosti na internetu;
- Rešavanje pitanja ustanovljavanja i potvrđivanja idetiteta (istovetnosti);
- Ustanovljavanje preventivnog odgovora, uključujuči i kiber etiku, kao

[26] Kancelarija za žrtve kriminala ovog ministarstva.
[27] Internet: *www.ovcttac.org/calendar* .
[28] Detaljnije, u: *Embracing the Future Together*, Commonwealth Investigations Conference 10 September 2002, Critical issues in hi-tech crime.

i efektivna protektivna dejstva usmerena na smanjenje viktimizacije, promovisanje adekvatnih aktivnosti i postupanja u kriznim situacijama i strateška razmatranja bezbednosnih pitanja u okvirima javnog i privatnog sektora u pogledu ove tehnologije;
- Određivanje odgovarajućih uloga i prioriteta organa gonjenja, uz obzire neadekvatnih postojećih resursa;
- Uticaj na politiku informacione ekonomije na nacionalnom nivou, kao i doprinos ključnim procesima regionalnog i međunarodnog karaktera;
- Kreiranje realne strateške i „neomeđene“ obaveštajne službe, uključujući i razmatranje uloge koju Australijska kriminalistička komisija može imati u ovom smislu;
- Omogućavanje da reforma zakonodavstva prati brzi razvoj novih tehnologija kao i da se uniformnost ali i komparativnost postigne na najvišem mogućem nivou, bez prihvatanja najnižih mogućih standarda (uz mogućnost držanja adekvatnog nivoa);
- Ustanovljavanje i održavanje efektivnih parterstava sa lokalnom zajednicom, drugim organima i organizacijama, obaveštajnim i odbrambenim strukturama, provajderima internet usluga, privatim sektorima i akademskim naučnim ustanovama;
- Utvrđivanje odnosa između prevencije visokotehnološkog kriminala i represivne delatnosti u ovom sektoru, kao i inicijativa za zaštitu kritičnih infrastruktura;
- Razvoj modela za multiagencijski Australijski centar visokotehnološkog kriminala koji bi imao ulogu jedinstvenog kontaktnog i operativnog centra;
- Razvoj operativnog odgovora kojim se umanjuju opasnosti kiberterorizma;
- Razvoj koordiniranog sistema prijavljivanja incidenata od zajedničke koristi za policiju, vladu i privatni sektor;
- Ujednačenje i smanjenje obima postojećih inicijativa, i na teritoriji Australije ali i šire, uz razvoj modela kojim bi se osigurale najefikasnije i najefektivnije strategije koordinacije i saradnje u primeni resursa;
- Menadžment sa medijima podizanje svesnosti zajednice ali i marketinško promovisanje rezultata sposobnosti i kapaciteta policije;
- Angažovanje značajnih kapaciteta na razvoju novih oblika odgovora na pretnje;
- Efektivno rešavanje pitanja kadrova uključujući i obezbeđivanje ili davanje pristupa specijalističkim resursima, adekvatnim i kontinualnim obukama, i zadržavanjem kritičnog osoblja kao i
- Preispitivanje tradicionalnih metoda rada.

U okvirima razmatranja strateških koncepata autralijski kreatori kriminalne politike u oblasti suprotstavljanja visokotehnološkom kriminalu uvideli su određena krucijalna operativna pitanja:
- Nacionalna regionalna i međunarodna koordinacija i saradnja;
- Doprinos zaštiti kritičnih infrastruktura kroz prikupljanje obaveštajnih podataka;
- Dejstvovanje preko graničnih linija i u okvirima različitih jurisdikcija i političkih režima;
- Preispitivanja troškova i prioriteta istraga;

- Pronalaženje, utvrđivanje i izuzimanje elektronskog dokaznog materijala od strane policije;
- Obuka policije u oblasti visokotehnološkog kriminala u pogledu gorućih problema – privremenog oduzimanja elektronskih dokaza, istragama oko mrežnih krivičnih dela, izvođenje ovih dokaza;
- Ostvarivanje efektivnog, ekonomičnog i pravovremenog forenzičkog odgovora na ove izazove, uključujući savremene tehnološke resurse;
- Razvoj strateških i taktičkih obaveštajnih odeljenja na osnovu informacija (i obaveštajnih podataka) iz različitih izvora, uključujući i privatni sektor;
- Pitanje pronalaženja tragova u kiber prostoru, drugim rečima, mogućnost traganja (uključujući i pitanja zadržavanja i očuvanja podataka, internet-kafea, anonimizatora, rajeva podataka);
- Rešavanje problema povećane incidence kriminaliteta identiteta, od kojih je većina upravo omogućena razvojem informacione i komunikacione tehnologije i interneta;
- Rad u realnom vremenu, ili internet vremenu, i vođenje onlajn istraga;
- Rešavanje pitanja enkripcije ili pribavljanje podataka sigurnim putem;
- Pristup skladištenoj elektronskoj pošti bez potrebe pribavljanja naredbe;
- Pribavljanje ovlašćenja za sprovođenje prekograničnih pretraga u vezi s bazama podatka;
- Praćenje procesuiranja ovih oblika kriminala i pronalaženje novih pojavnih oblika pranja novca;
- Posedovanje adekvatnih mogućnosti nadzora i presretanja;
- Ustanovljavanje standarda i smernica za borbu protiv visokotehnološkog kriminala;
- Dejstvovanje u okvirima ustanovljenih i potvrđenih režima privatnosti;
- Adekvatno postupanje sa pitanjima viktimologije, naročito vezano za elektronsku krađu identiteta (prevaru) i
- Stvaranje i usavršavanje stručnosti i iskustva u dejstvovanju sa velikom količinom različitih jurisdikcionih pitanja u okvirima izvršenja dela visokotehnološkog kriminala.

Australijska policija je u jednom trenutku prepoznala značajno povećanje moguće opasnosti od elektronskih incidenata vezanih za računarsku bezbednost i ukazala da je primarna meta visokotehnološkog krminala bio australijski bankarski i finansijski sistem i da postoji direktna korelacija između povećane zavisnosti za sofisticiranim internet tehnologijama i rastućeg nivoa ranjivosti na potencijalne napade.[29] Sve ovo je ukazalo da se težište rada u suprotstavljanju visokotehnološkom kriminalu mora usmeriti na: prevazilaženje više jurisdikcionih nadležnosti i granica; pribavljanje, zadržavanje i očuvanje tragova kao dokaznog materijala; pribavljanje adekvatnih ovlašćenja; dešifrovanje enkripcije; dokazivanje istovetnosti (identiteta); znanja gde tragati za dokazima; odgovor na oblike ove vrste kriminala u realnom vremenu; koordiniranje istražnih aktivnosti; poboljšanje stepena obuke na svim nivoima; razvijanje strateških partnerstava i saveza i unapređivanje razmene informacija i obaveštajnih podataka.

[29] Detaljnije, u: Police Commissioners' Conference Electronic Crime Working Party 2000, pp. 25–28; Rees 2000, pp. 16–19.

Na osnovu iskustava i potreba uspostavljanja temelja australijske strateške orijentacije u borbi protiv visokotehnološkog kriminala, identifikovano je pet oblasti koje bi bile fokus za delovanje: prevencija, partnerstvo, edukacija i osposobljavanje, sredstva na raspolaganju i logistika, zakonodavna i normativna rešenja. Integralo tretiranje navedenih oblasti je krucijalno zbog međusobnih nerazdvojnih veza i ukoliko bi se koristio pojedinačni pristup same aktivnosti borbe protiv visokotehnološkog kriminala, imale bi ograničen domašaj.

Ove strateške temelje je pretekla nacionalna spremnost na nove pristupe u ovoj oblasti. Naime, ranije su počeli da se donose komplementarni radni planovi, koji su se odnosili na pomenute oblasti, kako bi se primenjivala politika prioritetizovanja određenih zadataka, koliko to dozvoljavaju raspoloživi resursi. Preduzeti su svi mogući koraci kako bi se osiguralo da strateška koncepcija bude adekvatno i principijelno primenjena na svim nivoima. Šta više na Konferenciji policijskih komesara osnovana je *Radna grupa za zakonodavne reforme u vezi sa elektronskim kriminalom* (E-Crime Law Reform Working Party – ECLRWP). Posebno se radilo na određenim pitanjima pravne prirode, kao na primer: presretanje i nadzorne mogućnosti elektronskog saobraćaja, pristup policije skladištenim (zapamćenim) elektronskim porukama, legislativnim odgovorima na opasnost od kriminaliteta identiteta, pitanja zadiranja u privatnost i zadržavanja i konzerviranja podataka.

Evidentno je da strateška razmena esencijalnih (hardverskih i softverskih) resursa, povišen nivo nacionalnih i internacionalnih oblika kooperacije i koordinacije, izgradnja sigurnih partnerstava, naročito između organa gonjenja i privatnog sektora, moraju biti esencijalni pitanja sa kojima će se rešavati problem visokotehnološkog kriminala ubuduće.

OSNOVNA STRATEŠKA OPREDELJENJA U SUPROTSTAVLJANJU VISOKOTEHNOLOŠKOM KRIMINALU U REPUBLICI SRBIJI

Značaj definisanja strateških opredeljenja u suprotstavljanju visokotehnološkom kriminalu prepoznat je i u našoj zemlji kroz aktivnosti nadležnih državnih organa, prvenstveno *Odeljenja za borbu protiv visokotehnološkog kriminala* Službe za borbu protiv organizovanog kriminala – SBPOK i *Posebnog odeljenja javnog tužilaštva za visokotehnološki kriminal*. U daljem tekstu predstavićemo osnovne odrednice strategije koja je u postupku donošenja u okviru *Odeljenja za borbu protiv visokotehnološkog kriminala*.[30] Strategija *Odeljenja za borbu protiv visokotehnološkog kriminala* osmišljena je kao kratak opis ciljeva i zadataka koje ovo odeljenje u savremenim uslovima mora ostvariti, pravac u kome će se rad odeljenja kretati, jasnu viziju koja se želi postići, a ujedno predstavlja i idejnu konstrukciju koja bi trebala da omogući razvijanje detaljnijih planova za svaku oblast visokotehnološkog kriminala pojedinačno (kriminal u oblasti intelektualne svojine, elektronskog kriminala i drugo).

Strategija predstavlja pažljivo razmotrene stavove policijskih službenika i eksperata iz ove oblasti i osmišljena je kao vodič za druga odeljenja u okviru Ministarstva unutrašnjih poslova, druga ministrastva sa kojima po pitanju sprečavanja

[30] Ovom prilikom se zahvaljujemo ovom odeljenju na ustupanju materijala za ovaj rad.

visokotehnološkog kriminala ovo odeljenje sarađuje, kao i druge zainteresovane institucije. Interno, ova strategija, u okviru Ministarstva unutrašnjih poslova predstavlja baznu osnovu i smernicu na osnovu koje policijski stručnjaci iz ove oblasti mogu da sagledaju svoju ulogu u okviru Ministarstva, zatim u okviru partnerstva sa drugim organima i organizacijama u državnom, javnom i privatnom sektoru, kao i u odnosu sa stanovništvom. Ovom strategijom predstavljaju se principi koji su ključni za uspeh jednog društva u suzbijanju visokotehnološkog kriminala.

Cilj strategije jeste i da se ne dozvoli da delovi teritorije Republike Srbije postanu pogodno mesto za izvršioce krivičnih dela iz oblasti visokotehnološkog kriminala i organizovanih kriminalnih grupa koje se bave izvršenjem krivičnih dela iz oblasti visokotehnološkog kriminala. Posebna pažnja se poklanja fenomenu smišljenog korišćenja elementa inostranosti i anonimnosti na internetu pri izvršenju krivičnih dela radi izbegavanja otkrivanja identiteta izvršioca i sprečavanja organa unutrašnjih poslova da obezbede dokaze.

Strategija je zasnovana i osmišljena na temelju sledećih principa:

- Visok nivo koordinacije: u okviru postojeće strukture na nacionalnom nivou uključuju se sve postojeće raspoložive snage i uvažavaju sve postojeće inicijative;
- Visokotehnološki kriminal je globalna pojava i zahteva efikasnu i dvosmernu saradnju između Republike Srbije i međunarodnih institucija u okviru bilateralne i multilateralne saradnje, kao i koordinaciju i visoku operabilnost u postupanju koje po zahtevima realizuje ovo Odeljenje;
- Prevencija je bolja od represije; Odeljenje za borbu protiv visokotehnološkog kriminala sarađuje sa partnerskim institucijama kako bi se vršila efikasna prevencija, efikasno otkrivali učinioci ovih krivičnih dela i razrešila krivična dela iz oblasti visokotehnološkog kriminala;
- Uvažavanje privatnog sektora; Odeljenje za borbu protiv visokotehnološkog kriminala sarađuje sa preduzećima čija tehničko-tehnološka rešenja i iskustva mogu pomoći u efikasnoj borbi protiv visokotehnološkog kriminala;
- Edukacija policijskih službenika i podizanje javne svesti o problemima koji se pojavljuju u savremenom informacionom društvu, podrazumeva praćenje trendova i razvoja novih formi visokotehnološkog kriminala;
- Reforma zakonodavnih rešenja u skladu sa međunarodnim sporazumima i konvencijama uz uvažavanje nacionalnih potreba i specifičnosti;
- Razvoj kapaciteta i mogućnosti u cilju uspešnog prevazilaženja problema koji se javljaju zbog brzog tehnološkog razvoja i narastajuće informacione infrastrukture;
- Razmena podataka i informacija (taktičkih i strateških) između ministarstava, partnerskih agencija i društva uopšte;
- Konsultacije, monitoring i evaluacija strategije kako bi se osigurala relevantnost i efikasnost.

Strategija ukazuje na prioritete *Odeljenja za borbu protiv visokotehnološkog kriminala,* koji se mogu identifikovati kao:

- Usklađivanje strategije Odeljenja za borbu protiv visokotehnološkog kriminala sa strategijama koje su razvile druge institucije koje se bave upravljanjem, regulisanjem i bezbednosnim pitanjima u vezi s elektronskim okruženjem;

- Obezbeđivanje vođstva i ohrabrivanje partnerstva i saradnje u vezi s pitanjima koja se tiču visokotehnološkog kriminala;
- Razvoj tehničko-tehnoloških, namenskih policijskih sredstava i povećanje kapaciteta kako bi se sadašnje i buduće istrage u oblasti visokotehnološkog kriminala uspešno realizovale;
- Uključivanje privatnog sektora u cilju efikasnije reakcije na krivična dela u oblasti elektronske trgovine i bankarstva, efikasne prevencije i smanjenja stope elektronskog kriminala;
- Doprinos reformi zakonodavstva i pružanje argumenata za poboljšanje pravne regulative kojom se reguliše odgovornost i nadležnost za istrage u oblasti visokotehnološkog kriminala na teritoriji Republike Srbije.

Strategija ima pet fokusnih tačaka pomoću kojih se mogu identifikovati ciljevi koje Odeljenje za borbu protiv visokotehnološkog kriminala želi ostvariti. Cilj je postizanje proaktivne prevencije i efikasnog odgovora na izazov koji postavlja pojava visokotehnološkog kriminala. One su povezane i jedino zajedno mogu dati pozitivne rezultate. Te fokusne tačke su: prevencija, partnerstvo i saradnja, edukacija, jačanje resursa i kapaciteta i pravna regulativa. Svaka fokusna tačka je dalje razrađena u cilju preciznog definisanja aktivnosti u realizaciji ove strategije i za svaku oblast interesovanja strategije sačinjen je i plan rada kojim se planira preduzimanje akcija na strateškom nivou.

Odeljenje za borbu protiv visokotehnološkog kriminala mora razmotriti šta sve treba da učini kako bi se izašlo u susret potrebama države, privatnog sektora i društva uopšte, kroz obezbeđivanje adekvatne zaštite od kriminala u okviru svojih kapaciteta, a koji su adekvatni novoj, informacionoj eri. Postoji i potreba da se usklade potrebe državnih institucija u borbi protiv visokotehnološkog kriminala i opšteg, javnog interesa, kao što su ljudska prava. U okruženju gde se ne koriste informacione tehnologije, sprovođenje krivičnog zakonodavstva i prevencija kriminala nisu samo u domenu rada policije, već predstavljaju i odgovornost podeljenu između privatnog, javnog sektora i nevladinih organizacija.

Izazovi elektronskog kriminala su veliki, a njihovo vreme izvršenja u najvećem broju slučajeva jednovremeno sa nastupanjem posledica izvršenih krivičnih dela, zbog toga se ne može očekivati da jedna nacija i jedna država, ili neki pojedinačni državni organ, sami reše ovaj problem. Upravo iz ovog razloga Odeljenje za borbu protiv visokotehnološkog kriminala mora biti povezano sa širim kontekstom preventivnih i represivnih akcija sa uključivanjem tužilaštva i suda, kao i da bude upoznato sa radom međunarodnih institucija i njihovim inicijativama, kao i sa novim inicijativama u privatnom sektoru, kako bi se zaštitila osetljiva informaciona infrastruktura i društvo učinilo bezbednijim.

ZAKLJUČAK

Može se zaključiti na osnovu datog pregleda da se i naša zemlja polako uključuje u date tokove aktuelnih oblika suprotstavljanja visokotehnološkom kriminalu. Sve pomenute inicijative predstavljaju aktivne i aktuelne koncepte pokušaja rešavanja problema *pošasti* zvane visokotehnološki kriminal. Naša zemlja nije dovoljno bogata da bi se sa ovim problemom mogla nositi kao što je prikazano

u slučaju SAD, ali i u ovom pogledu treba biti realan i prepoznati svoju ulogu i značaj u mogućem ešalonu braniku od ovog bezbednosnog izazova.

Strateški koncepti u suprotstavljanju visokotehnološkom kriminalu prikazani u ovom tekstu doveli su nas do ovog momenta kada možemo sagledati i rezultate napora većine zemalja kako se ostvaruju i u našem podneblju, naročito sa aspekta onoga što je naša zemlja do ovog momenta prošla. Kao određene korake koje smo morali da napravimo, ovo predstavlja deo puta koji moramo da savladamo, ono čini jedan segment, kao što je to činilo u slučaju donošenja Nacionalne strategije i Akcionog plana za borbu u protiv korupcije i Strategije suprostavljanja organizovanom kriminalu. Nadamo se da će sledeći korak biti i donošenje Nacionalne strategije za suprotstavljanje visokotehnološkom kriminalu, kao dela integralnog odgovora naše države na izazove visokotehnoloških kriminalnih aktivnosti.

Naravno, ovi strateški pristupi čine bazu na čijoj osnovi treba razvijati dalje koncepcijske aktivnosti, pregledno prikazani pristupi mogu predstavljati neke vrste putokaza koji se mogu pratiti. Strateški pristupi predstavljaju okvire, šablone, ali tu se ne može zaustaviti, neophodno je da svaka država u okviru svojih mogućnosti, ali i raspoloživih okolnosti, prema sopstvenoj problematici razradi dalje, na praktičnim problemima i rešenjima zasnovane metode. Upravo to se može i primetiti u razrađenim opisanim strateškim opredeljenjima pomenutih država. Komparativno posmatrano, na ovim osnovama se prema prikazanom dobrano, i već duže vreme, radi u našoj zemlji.

LITERATURA

1. Bidgoli, H. (2006). *The handbook of information security*, New Jersey: John Wiley & Sons, Inc Hoboken.
2. Bidwell, T. (2002). *Hack Proofing Your Identity in the Information Age*. London: Syngress Publishing, Inc.
3. Cerf, V.; Kahn, R. (1999). *What Is The Internet (And What Makes It Work)*. Corporation for
4. Denning, D. (1998). 'Cyberspace Attacks and Countermeasures', in Denning, D. E. and Denning, P. J. *Internet Beseiged: Countering Cyberspace Scofflaws*, pp. 29-55, New York: ACM Press.
5. Chellany, Brahma (2001). *Revolution in Information Technology and its Impact on Security. The Asian Pacific Region: Evolution of the Scope of Security and Disarmament in the 21st Century*. United Nations Conference on Disarmament Issues. Videti na http://disarmament.un.org /RCPD/pdf/plen2b.pdf dostupan 20.05.2009.
6. Ghosh, R. (2002). 'The Cybercrime Act 2001: Implementing the European Union's Cybercrime Convention', San Jose: *RSA Conference*.
7. Kjaerland, M. (2005). Classification of computer security incidents based on reported attack data. *Journal of investigative psychology and offender profiling*, Oxford: John Wiley & Sons.
8. Lowenthal, M. (2002). *Intelligence: From Secrets to Policy*, 2d ed., Washington: CQ Press.

9. Portnoy, M.; Goodman, S. (2009). *Global Initiatives to Secure Cyberspace An Emerging Landscape*, Berlin: Springer Science Business Media, LLC.
10. Simonović, B. (2006). *Rad policije u zajednici (Community Policing)*, Banja Luka: Visoka škola unutrašnjih poslova.
11. Smith, R.; Grabosky, P.; Urban, G. (2004). *Cyber criminals on trial, defining and mesuring cyber crime*. Cambridge: Cambridge University Press.

STRATEGIC CONCEPTS IN COMBATING HI-TECH CRIME

***Abstract**:* Strategically aspects in combating crime represent the beginning point and sine qua non condition in fighting any form of crime; it is also the case for the hi-tech crime. Moreover, because of its core features effectively countering cybercrime, as a prerequisite, have the organization of the capacity and commitment of all, at various levels, including strategic planning, intergovernmental and interagency cooperation. In the area of hi-tech crime strategic concepts are very sophisticated on any level, as this problem deserves, from global initiatives and strategic concepts down to local and basic police approaches. In this article authors are trying to connect all of the operational levels, through representing global, regional and local concepts in problem solving and strategic aspirations. Global and regional concepts in this paper are displayed as Eurocentric, while local examples are given for the USA, Australia and Serbia through analytical and comparative approach.

Key words: strategic concepts, hi-tech crime, organized crime, preventive concepts, international organizations.

Prethodno saopštenje - UDK 343.3/.7: 004.7

ZNAČAJ DIGITALNIH DOKAZA U KRIVIČNOM POSTUPKU

Doc. dr Uroš Pena
Direkcija za koordinaciju policijskih tijela BiH
E-mail: urospena@hotmail.com
Dragan Mitrović
direkcija za koordinaciju policijskih tijela BiH
E-mail: drmitrovic@blic.net

Apstrakt: Razvoj informacione tehnologije stvorio je nove izazove u obavljanju policijskih aktivnosti. Većina profesija morala je da se prilagodi digitalnom dobu, a policijska profesija trebalo bi da bude naročito prilagodljiva, pošto digitalne tehnologije u službi kriminaliteta zahtjevaju nove tipove kriminalističkih istraga. Sve više i više informaciona tehnologija postaje instrument u kriminalnim aktivnostima. Istraživanje ovog sofisticiranog kriminaliteta i obazbjeđenje potrebnih dokaza za prezentaciju na sudu postaće značajan policijski zadatak.

S dostignućima tehnike i tehnologije razvile su se i nove mogućnosti i metodi njihove zloupotrebe, među kojima posebno mjesto zauzima kompjuterski kriminalitet. Razvoj informacione tehnologije karakteriše izuzetno velik protok digitalnih podataka u vidu elektronskih (računarskih) zapisa, a koji se nalaze u računaru ili se prenose putem računara, a mogu da budu ključni dokaz u otkrivanju i dokazivanju najraznovrsnijih zloupotreba informacione tehnologije, prije svega zloupotrebe računara i računarskih mreža (među kojima su i kompjuterska krivična djela).

Ključne riječi: kompjuter, kompjuterski kriminalitet, digitalni dokaz, obezbjeđenje dokaza, dokazna vrijednost...

UVOD

Savremeni pojavni oblici kriminaliteta zahtijevaju novu metodiku otkrivanja krivičnih djela, koja podrazumijeva i pribavljanje dokaza u elektronskoj formi, odnosno elektronskih, softverskih ili kompjuterskih dokaza, kako ih nazivaju u teoriji i još uvijek nedovoljno izgrađenoj praksi. Budući da se kriminalitet koji se vrši putem visokih tehnologija odvija na raznim poljima, kompjuter i drugi uređaji i sredstva visoke tehnologije mogu se u odnosu na ovaj kriminalitet pojaviti bilo kao predmet krivičnog djela odnosno objekat napada, bilo kao sredstvo izvršenja krivičnog djela. Ovo je prisutno ne samo u oblasti kompjuterskog, već i oblasti opšteg, ali i finansijskog i ekonomskog kriminaliteta, to jest u svim kriminalnim slučajevima gdje se kao sredstvo izvršenja, ili kao sredstvo za prikrivanje krivičnog djela ili učinioca pojavljuje bilo koji uređaj čije je funkcionisanje zasnovano na visokoj informatičkoj tehnologiji, odnosno elektronskoj tehnologiji.

Život je daleko ispred mogućnosti zakonodavca da inkriminiše sve potencijalno opasne društvene pojave, koje su vezane za savremene tehnologije. Broj

djela koja se mogu podvesti čak i pod najrestriktivnije i najuže definicije *cybercrime*-a gotovo svakodnevno se uvećava. Klasifikacija takvih ponašanja je teška, zato što se ne mogu utvrditi kriterijumi koji će određena djela svrstati isključivo u jednu kategoriju, dok sa druge strane pojave novih načina zloupotrebe nužno iziskuju i proširenje pomenute liste kriterijuma. Sa druge strane, više je nego potrebno identifikovati i na sistematičan način razdvojiti poželjna i dozvoljena ponašanja od onih koja zloupotrebom tehnologije nanose ogromnu štetu pojedincima, organizacijama i preduzećima širom svijeta svake godine.[1]Pavan Dugal, predsjednik međunarodne organizacije koja se bavi izučavanjem visokotehnološkog kriminaliteta *Cyberlaws*, iznio je jednostavnu podjelu koja zadovoljava osnovne pretpostavke analize. Dugal dijeli sva krivična djela iz ove grupe na: djela protiv ličnosti, djela protiv imovine i djela protiv države (www.crime-research.org).

Kriminalno ponašanje u ovoj oblasti odvija se u vrlo specifičnoj – elektronskoj sredini. Stoga uspješno suprotstavljanje ovoj vrsti kriminaliteta podrazumijeva poznavanje funkcionisanja uređaja koji rade na principima visoke tehnologije, poznavanje kompjuterskih sistema i mreža i modernih telekomunikacionih tehnologija. Osnovna funkcija kompjuterskog sistema je obrada i distribucija podataka u elektronsku sredinu. Podatke koji se nalaze u formi pogodnoj za ljudsko opažanje i razumijevanje, operater korišćenjem računara prebacuje u formu pogodnu za automatsko obrađivanje, dakle oni se kroz interaktivni odnos čovjeka i uređaja pretvaraju u podatke u elektronskoj formi. Elektronski podaci sami po sebi sada predstavljaju niz magnetskih tačkica na stalnoj ili privremenoj memoriji računara i oni mogu predstavljati primarni dokaz. U takvom obliku ne mogu se čulno opaziti, ali mogu se koristiti kao dokaz. Moguće ih je presnimiti na drugi oblik elektronske memorije: tvrdi ili meki disk (flopi disketu), optički kompakt disk, eksternu memoriju (izmjenljivi disk) i tako obezbijediti u neizmijenjenom obliku, a da bi se čulno opazili, pretvaramo ih pomoću uređaja i programa u tekst, fotografiju, video zapis, zvuk ili drugi oblik koji je pogodan za ljudsko opažanje i razumijevanje (Suzbijanje visokotehnološkog kriminala, 2010: 217).

Prikupljanje validnih dokaza u pojedinačnim slučajevima često je veoma otežano. Jedan od osnovnih principa u prikupljanju digitalnog forenzičkog materijala jeste da poslije izvršenog krivičnog djela ne treba ništa mijenjati, što se u praksi veoma rijetko dešava. Podaci, datoteke i programi koji su objekat izvršenja ovog krivičnog djela služe oštećenima za svakodnevno poslovanje, knjigovodstvenu evidenciju, održavanje poslovnih kontakata ili su u njima sadržani lični podaci koji imaju samo afekcionu vrijednost. Oštećeni najčešće sami pokušavaju da otklone štetu koja im je nanijeta ili angažuju lica koja imaju veći ili manji fond znanja iz informacionih tehnologija, kako bi povratili izbrisane podatke. Ovakvim djelovanjem se gotovo uvijek uništavaju neposredni dokazi koji bi mogli dovesti do izvršioca, a tužiocu na raspolaganju ostaju samo posredni dokazi, koji uglavnom nisu dovoljni kako bi izvršilac bio otkriven i osuđen.

---

[1] Procjena je da šteta od različitih djelovanja visokotehnološkog kriminaliteta – ne uzimajući u obzir njegove potencijalne veze sa organizovanim kriminalitetom – na godišnjem nivou iznosi oko 200 milijardi dolara. Dragan Prlja, *Sajberkriminal*, predavanje održano na Pravnom fakultetu Univerziteta u Beogradu, 28. 12. 2008. godine. Tekst predavanja može se naći na internet adresi: http://www.prlja.info/sk2008.pdf, 01.05.2009.

U policijskoj praksi se sve više kriminalističkih istražilaca susreće sa digitalnim dokazima, jer su prisutni u sve više krivičnih djela. Da bi se što bolje prikupili i analizirali takvi dokazi, policijski službenici morali bi posjedovati osnovna znanja o pojmovima i načinu rada samog računara, računarske opreme ili drugog uređaja koji sadrži digitalne dokaze, te bi morali biti upoznati sa pravilnim načinom prikupljanja i obezbjeđenja takvih dokaza.

KOMPJUTERSKI KRIMINALITET I DIGITALNI DOKAZI

Korištenje ICT (eng. Information and communication technologies) tehnologija u kriminalne svrhe zahtijeva posebne metode za vođenje kriminalističkog istraživanja. Digitalni dokazi su osjetljivi, lako se brišu i mijenjaju, a time i kompromituju. Specijalni forenzički alati omogućavaju povrat i analizu i obrisanih, skrivenih i privremenih datoteka koje u svakodnevnom normalnom radu nisu vidljive. S obzirom na to da se kompjuter može koristiti kao oruđe za izvršenje krivičnog djela, on može, odnosno mora sadržavati dokaze koji se odnose na bilo koje krivično djelo.

Kako se zloupotreba može izvršiti nad svim oblicima elektronskog signala, koji predstavlja materijalni ekvivalent nematerijalne informacije, potrebno je da se pojam digitalnog dokaza proširi u pojam elektronskog dokaza. *Elektronski dokaz* je svaka informacija u elektronskom obliku koja ima dokazujuću vrijednost, a koja može biti uskladištena ili prenesena u elektronskom obliku. Pojam *digitalnog dokaza* je uži od pojma elektronskog dokaza, i u digitalnoj forenzičkoj nauci obuhvata kompjuterski uskladištene i generisane dokaze, digitalne audio i video signale, digitalni zapis sa mobilnog telefona, zapis sa digitalne fax mašine ili drugih digitalnih uređaja. Međunarodna organizacija za kompjutersku registraciju (International Organization of ComputerEvidence – IOCE) propisala je opšte *principe i procedure* koje se odnose na digitalne dokaze, za usaglašavanje metoda i praktičnih rješenja među nacijama, i koje garantuju međunarodnu razmjenu digitalnih dokaza. Nažalost, nigdje u svijetu još ne postoji verifikacija zvaničnih istražnih organa, forenzičkih analitičara i pravosudnih organa, podjednako kvalifikovanih u svojim oblastima, da objektivno i tačno vode istragu, forenzičku akviziciju, analizu, dokazni postupak i prezentaciju digitalnih dokaza na sudu. Istraga incidentnog kompjuterskog događaja zahtijeva uvijek timski rad. Za poslove akvizicije i forenzičke analize uvijek treba angažovati kvalifikovanog eksperta za informacione tehnologije (IT), specijalistu za konkretni operativni sistem (OS), program, platformu, mrežu, itd.

Dokaz je ono što razdvaja hipotezu od neosnovane tvrdnje. Dokazi mogu potvrditi ili oboriti hipotezu, pa je njihov integritet ključna stvar u njihovom prihvatanju odnosno odbacivanju pred sudom. Postoji nekoliko specijalnih karakteristika digitalnog dokaza koje ih čine posebno izazovnim. Prije svega, potrebno je jasno i precizno definisati digitalni dokaz. Digitalni dokaz je informacija uskladištena ili prenošena u digitalnoj formi koja učestvuje u sudskom procesu ili nekom drugom sporu. Digitalna forma po svojoj prirodi podrazumijeva da se radi o nekom elektronskom ili magnetnom uređaju, pa to mogu biti podaci u operativnoj memoriji, na hard disku, *flash* karticama, ali i podaci koji se nalaze

u transmisiji, npr. radio talasi. Digitalni dokaz nije nešto što ljudi mogu na prvi pogled protumačiti. U bukvalnom smislu digitalni dokaz predstavlja niz nula i jedinica koje neki elektronski uređaj prevodi u ljudima razumljivu formu koju oni mogu koristiti kao potkrepljenje svojoj hipotezi u okviru nekog sudskog slučaja (www.ecdlcentar.com).

Da bi se dokazalo neko krivično djelo, neophodno je prikupiti dokaze. Međutim, kada je rječ o kompjuterskom kriminalitetu, mora se imati u vidu da „digitalni dokazi" često nisu jednaki ostalim oblicima fizičkih dokaza u odnosu na koje su osjetljiviji i podložni mijenjanju strukture i sadržaja, te se prema njima treba posebno odnositi.

Policijski službenik koji prikuplja dokaze s kompjutera ili kompjuterske mreže, mora znati pravila postupanja kod prikupljanja tih podataka, jer ako on prikupi te podatke nezakonito, ti podaci se neće moći koristiti u sudskom postupku. Digitalni dokaz označava bilo koji kompjuterski podatak koji može potvrditi da je izvršeno krivično djelo, ili koji može ukazati na povezanost između krivičnog djela i žrtve, ili krivičnog djela i njegovog izvršioca. Digitalni dokazi su vrlo važni, jer predstavljaju kombinaciju različitih informacija, poput teksta, slike, audiosnimka i videosnimka. Ponekad informacija koja je pohranjena na kompjuter može biti jedini trag koji će kriminalističko istraživanje dovesti na pravi put.

Postoji cijeli niz digitalnih dokaza koji nas okružuju u svakodnevnom životu, a kojih smo skoro u potpunosti nesvjesni. Tvrdi disk može sadržavati cijelu biblioteku informacija, digitalna kamera u svojoj memoriji može pohraniti hiljade fotografija, a kompjuterska mreža može sadržavati još više informacija o licima i njihovom ponašanju. Brojevi bankovnih računa, novčane transakcije, povjerljivi dokumenti i drugi različiti podaci putuju oko nas kroz zrak ili putem žičanih vodova, a svaki od njih predstavlja potencijalni izvor digitalnog dokaza. Samo mali postotak digitalnih dokaza moguće je otkriti ''klasičnim alatima'', dok je ostatak digitalnih dokaza moguće otkriti samo posebnim alatima (bilo komercijalnim bilo freeware/eng. Freeware–besplatni alati/) (Protrka, 2011: 2).

Digitalni dokazi su jedna vrsta materijalnih dokaza, bez obzira na činjenicu što ih je teže evidentirati. Oni predstavljaju spoj magnetskog polja i elektronskih tehnika koje se skupljaju i analiziraju uz pomoć specijalnih tehnika i alata. U odnosu na materijalne dokaze, digitalni dokazi imaju nekoliko prednosti. Od digitalnih dokaza je moguće napraviti tačnu kopiju koja se naknadno može istraživati kao da se radi o originalu, dok je kod materijalnih dokaza to gotovo nemoguće. Prilikom ispitivanja kopije, a ne originala, izbjegavaju se oštećenja koja bi mogla nastati na originalu prilikom istraživanja. Pomoću pravilnih alata moguće je vrlo lako odrediti je li digitalni dokaz modifikovan ili uništen, jednostavno upoređujući ga sa originalom. Digitalni dokaz je vrlo teško uništiti: čak i onda kada su ''obrisani'', digitalni dokazi se mogu povratiti na kompjuterski disk ili neki drugi medij za pohranu podataka. Digitalni dokaz je jednostavno pohraniti, a zbog lakoće izrada kopija, gotovo ih je nemoguće uništiti ili izgubiti. Zbog toga što se digitalnim dokazima može lako manipulisati i prenositi ih, istražitelji koji se bave kompjuterskim kriminalitetom nailaze na nove izazove u radu s ovakvom vrstom dokaza.

Digitalni dokazi mogu biti bilo kakav niz bitova i bajtova na disku računara ili drugom memorijskom sistemu, i to su najčešće neki: *sistemski* (swap fajl, log

fajl, konfiguracijski fajlovi i folderi…), *korisnički* (dokumenti i tekstualni fajlovi, tabele, slike, baze podataka, audio-video, arhivirani fajlovi, privremeni fajlovi, backup, sakriveni i šifrovani fajlovi, obrisani i preimenovani fajlovi ...) ili *internet* (Internet adrese, e-mail, cookies, bookmark, history…).

Potrebno je razmotriti još jedno pitanje koje proističe iz same prirode funkcionisanja računara i procesa zapisivanja i brisanja podataka sa hard diska. Poznato je da se računarski podaci uobičajenim načinom brisanja – smještanjem fajla u „kantu za đubre" (eng. recyclebin) i davanjem komande za njeno „pražnjenje" fizički ne brišu sa hard diska. Za trajno i nepovratno brisanje podataka potrebno je upotrijebiti neki od vajper (eng. whipe) programa, koji vrše „prepisivanje" hard diska. Razvojem digitalne forenzike nastaju sve savršeniji programi za povraćaj (eng. recovery) podataka, koji su u stanju da izvrše povraćaj podataka čak i poslije više „prepisivanja" hard diska. Smatramo da je za postojanje krivičnog djela *Oštećenje računarskih podataka i programa* dovoljno sprovesti uobičajen način brisanja podataka, a da kasniji povraćaj podataka ne može biti tretiran kao okolnost koja eliminiše postojanje krivičnog djela (Suzbijanje visokotehnološkog kriminala, 2010: 90).

Dakle, treba sakupljati sve posredne dokaze sa lica mjesta, ne samo ono što digitalni forenzičar misli da treba, nego i sve ono što može potencijalno indicirati šta se stvarno desilo. U procesu akvizicije digitalnih dokaza treba generalno snimiti listu datoteka i logova kao dokaze, čak i bez ikakve ideje šta se stvarno dogodilo. Treba imati u dokaznom materijalu svaku datoteku koja potencijalno može sadržavati dokaz, prije nego što nestane ili bude promijenjena. Nakon inicijalne istrage (bez zapljene računara), treba se okrenuti prvobitnoj hipotezi i dograditi je detaljnije sa prikupljenim dokazima. Velika je vjerovatnoća da je propušten neki važan dokaz, što je dobar argument da se kompjuter zaplijeni dok traje istraga (što nije uvek lako). Sve posredne dokaze, koji zajedno čine dokazni materijal, treba tretirati kao da direktno vode ka nepobitnom dokazivanju izvršene kriminalne radnje i kao da su svi jednako važni i kritični za konkretni slučaj. Tek tada počinje proces izgradnje dokaza bez tzv. pukotina, odnosno, izgradnja neoborivog dokaza. Potrebno je, dakle, mnogo posrednog dokaznog materijala za jedan mali čvrsti dokaz (Petrović, 2010: 3).

ANALIZE DIGITALNIH DOKAZA

Digitalna ili kompjuterska istraga obuhvata postupak dolaženja do podataka (digitalnih dokaza) i utvrđivanja vremena kada su bili unijeti, modifikovani, distribuirani, korišćeni, uskladišteni, sklonjeni, kao i vremena kada su fajlovi bili kreirani, postavljeni, punjeni, modifikovani ili kada im se pristupilo. Digitalnim dokazom se smatra svaka informacija koja ima dokazujuću vrijednost i koja je uskladištena ili prenesena u binarnoj formi i na koju se sud može osloniti. Nakon sakupljanja, akvizicije i validacije podataka sa ''osumnjičenog/korumpiranog'' računara, koriste se forenzički alati za identifikaciju i analizu digitalnih podataka. U fazi akvizicije i analize, podaci se ispituju radi identifikacije i otkrivanja dokaza.

Analiza digitalnih dokaza je proces koji uključuje analizu i korelaciju više vrsta podataka na različitim nivoima. Svrha i vrijednost analize jeste ta da

proučimo različite tipove podataka i zatim ih pretvorimo u korisne informacije. Kod prikupljanja digitalnih dokaza potrebno je odrediti kompjutere ili medije koji su predmet istraživanja, sačuvati originalne medije i spriječiti bilo kakve izmjene sadržaja medija, ako je računar upaljen preuzeti sadržaj radne memorije (RAM – Random Access Memory), ugasiti računar bilo redovnim putem bilo isključivanjem napajanja, napraviti kopiju svih bitnih medija, te obaviti forenzičku analizu na kopijama – slikama medija (Protrka, 2011: 4).

Nauka o digitalnim dokazima je standardizovana u ISO/IEC 27037 (www.iso27001security.com)(prikupljanje i čuvanje digitalnih forenzičkih dokaza) i kroz: *SWGDE – ScientificWorkingGroup on Digital Evidence*i *IOCE – International Organization on ComputerEvidence* (www.theiai.org). U okviru njih su izdate preporuke za osnovne principe forenzičke analize digitalnih dokaza, kriterijumi, standardne radne procedure za: zapljenu računara, forenzičku akviziciju i analizu, čuvanje, kopiranje originalnih digitalnih dokaza, i dr.

Za dobijanje digitalnih dokaza u forenzičkom postupku postoji mnogo razvijenih *tehnika* i *alata* koji se danas koriste, a njihov prevelik značaj povezan je sa činjenicom „da danas preko 90 posto svih novih informacija je proizvedeno u digitalnom obliku“, i da se takvo bogatstvo mora na adekvatan način kontrolisati, nadgledati i čuvati.

Razvoj forenzičkih alata usavršavao se kroz tri generacije. Prvu generaciju su sačinjavali razni alati za: slike, dokumenta, pretraživanje i oporavak sistema; drugu generaciju su činili posebno dizajnirani i razvijeni profesionalni alati (*Encase, SANS, Helix* itd.), kao i veliki broj besplatnih alata otvorenog koda koji se mogu naći i preuzeti sa interneta; treću generaciju čine inteligentni alati koji u realnom vremenu, bezbjedno i efikasno nadgledaju cjelokupan mrežni saobraćaj.

Naravno, svi destruktivni korisnici pokušavaju da prikriju i uklone tragove, tako da su najkvalitetniji digitalni dokazi po pravilu uvijek nevidljivi za standardne alate iz operativnog sistema. Ono što je potrebno da bi se neki forenzički alat koristio u istrazi, jeste da bude sertifikovan i priznat od državnih sudskih organa, kako bi digitalni dokazi bili validni u sudskom procesu. Preporuka *profesionalaca* je da se forenzički alati i tehnike ne primjenjuju na „živim“ podacima, već da se naprave njihove kopije, i da nikad, baš nikad, ne eksperimentišu korisnici koji nisu za to obučeni, jer će skoro sigurno oštetiti ili izgubiti potrebne digitalne dokaze.

Ako je krivično djelo počinjeno u stvarnom fizičkom svijetu i ako postoji kompjuter s mrežnim pristupom na mjestu izvršenja krivičnog djela, istražitelj će izvršiti pretraživanje računara i računarske mreže u potrazi za digitalnim dokazima koji mogu poslužiti u istrazi. Slično tome, ako je kriminalni čin zabilježen na računaru ili računarskoj mreži, kriminalistički istražitelji mogu utvrditi mjesto gdje se nalazi taj računar, te na taj način pokušati locirati mjesto izvršenja djela. Nepohranjivanjem digitalnih dokaza istražitelj se dovodi u opasnost od gubitka tih dokaza, te nemogućnost nastavka daljeg procesa istraživanja.

Istraživanje najviše zavisi o poznatim činjenicama koje istražitelji imaju o djelu. Ako je kompjuter rezultat ili posljedica kompjuterskog kriminaliteta, istražitelji se trebaju fokusirati na hardver, a ako djelo uključuje protivzakonite informacije i podatke, istražitelji trebaju potražiti bilo šta što je povezano s tim informacijama i podacima, uključujući tu i medije, odnosno softvere na kojima se ti podaci i informacije nalaze. Ako su informacije i podaci koji se nalaze na računaru

pravno relevantni, a istražitelji znaju šta traže, biće moguće u vrlo kratkom roku prikupiti potrebne dokaze, a ako istražitelji ne znaju šta traže, potrebno je proširiti opseg istraživanja i u njega pri tom uključiti svu računarsku opremu kako bi se prikupili i istražili materijali koji bi mogli poslužiti kao dokaz. Bez obzira na sve, istražitelji moraju biti u stanju dokazati autentičnost i integritet prikupljenih dokaza (Protrka, 2011: 5).

Policijski istražitelji su prva ‘’stručna linija’’ koja obrađuje ovakve slučajeve. Pomoć tokom obrade mjesta događaja i prikupljanja digitalnih dokaza, mogu im pružiti stručna lica. Sud će vještačenje digitalnih dokaza prepustiti sudskom vještaku iz područja informatike, elektronike, elektrotehnike ili komunikacija, koji može sudu na jednostavan način pojasniti komplikovane tehničke sadržaje vezane za izvršeno djelo iz područja kompjuterskog kriminaliteta.

Tokom analize, vještak mora odgovoriti na postavljena pitanja, što nije uvijek jednostavno. Zapisi na optičkim medijima, ukoliko ih ima, prilično su nedvosmisleni. No, zapisi na tvrdim diskovima sadrže samo stanje u trenutku privremenog oduzimanja, dok se pitanja često odnose na događaje iz prošlosti, a na koja nije moguće odgovoriti jer o njima jednostavno više nema raspoloživih tragova. Vještak se mora orijentisati primarno na činjenice iz svoje struke, ne iznoseći bilo kakve činjenice ili stavove koji nisu dio njegovog stručnog područja. Tokom krivičnog postupka vještačenje može biti prihvaćeno kao meritorno pri donošenju odluke, ukoliko je napravljeno stručno, sudu prihvatljivo jasno i nedvosmisleno.

U većini slučajeva tokom provođenja istražne radnje pretresanja stana i drugih prostorija, sudija ne želi uključiti i pretragu računara i računarske opreme, uz obrazloženje da je za izdavanje naloga potrebno detaljno opisati računar ili druge digitalne dokaze koji su predmet preduzimanja istražne radnje pretresa, odnosno, potrebno je navesti bar marku ili model predmetnog računara ili računarske komponente. Vrlo su rijetki pretresi stana u kojima su prije početka pretresa poznate karakteristike računara, kako bismo ga detaljno opisali radi dobivanja sudskog naloga za pretragu računara, a ponekad se kod samog pretresa stana dođe do saznanja da se materijalni dokazi izvršenja krivičnog djela nalaze na računaru ili drugim računarskim komponentama.

Radi pribavljanja materijalnih dokaza da je baš tim sredstvom izvršeno krivično djelo, odnosno da se na/u njemu kriju dokazi koji su proizvod krivičnog djela, računar je potrebno pretražiti, odnosno potrebno je učiniti uvid u sadržaj podataka koji se nalaze na tvrdom disku računara. Prepoznavanje digitalnih dokaza predstavlja proces koji se mora odvijati u dva stadija. U prvom stadiju istražitelj mora prepoznati hardver koji sadrži informacije, a nakon čega istražitelji moraju biti u mogućnosti razlikovati nevažne informacije i digitalne podatke koji su u vezi sa izvršenim djelom ili mogu pružiti vezu između djela i žrtve ili djela i izvršioca. Policijski službenici trebaju imati u vidu da postoji veliki broj različitih dijelova hardvera koji mogu sadržavati digitalne dokaze, a isto tako postoji i veliki broj različitih medija za pohranu podataka, a uz sve to treba voditi i računa o medijima za prenos podataka.

Sudska praksa prihvata kompjuterski generisane i memorisane digitalne dokaze pod adekvatnim uslovima. Transformacija digitalnih podataka, koji se sastoje iz niza kodiranih bita, u sudski dokaz, jeste apstraktan proces, koji može navesti sudiju da dovede u pitanje autentičnost i integritet kompjuterski generisanog

dokaza. U tom smislu, moraju se na nacionalnom nivou (na nivou zakona ili podzakonskog akta) propisati odgovarajuće procedure, koje obuhvataju: proceduru rukovanja i čuvanja digitalnih dokaza i proceduru za forenzičku akviziciju i analizu digitalnih dokaza. Pojam akvizicije i analize je u ovom radu korišćen u smislu otkrivanja, izvlačenja i dokazivanja digitalnih dokaza u dokaznom postupku (Petrović, 2010: 3).

Očekuje se da forenzička analiza digitalnih dokaza otkrije najviše potrebnih podataka za izgradnju čvrstog, neoborivog digitalnog dokaza bez tzv. pukotina. Postoji velika razlika između kompjuterskog digitalnog dokaza u računaru (*computerevidence*) i čvrstih, neoborivih dokaza (*proof*) prihvatljivih na sudu. Neoborivi, čvrsti dokaz nepobitno uspostavlja činjenice, ali je to i subjektivna interpretacija kompjuterskog digitalnog dokaza koji izvodi vještak za informacione tehnologije. Kompjuterski digitalni dokaz u računaru je objektivan digitalni podatak i može se koristiti u mjeri u kojoj se može dokazati da nije izmijenjen, npr. ulazna log datoteka je uvijek ulazna log datoteka.

MOGUĆNOSTI POLICIJE I TUŽILAŠTVA

Prilikom preduzimanja radnji obezbjeđivanja i zapljene digitalnih[2] i drugih materijalnih dokaza, primjenjuju se odredbe ZKP-a koje se odnose na pretresanje stana i lica i privremeno oduzimanje predmeta, za pregled računarske opreme na licu mjesta, odredbe ZKP koje se odnose na uviđaj, a u pogledu vještačenja tako oduzete opreme i njenog digitalnog sadržaja, opšte odredbe o vještačenju.

S obzirom na maršrutu kriminalnog akta iz oblasti visokotehnološkog kriminaliteta koja se u kiber prostoru nerijetko pruža i preko teritorije nekoliko kontinenata, pitanje pravilnog postavljanja mjesne nadležnosti može biti od prvorazrednog značaja. Ovakve slučajeve višestruke nadležnosti sudova različitih država, isključivo specifične za cyber[3] crime, svojim odredbama nisu regulisali ni KZ, ni ZKP.[4]

Nadnacionalni i transnacionalni karakter visokotehnološkog kriminaliteta u praksi ne implicira isključivo probleme u pogledu pravilnog određivanja mjesne nadležnosti. Prikupljanje dokaza u cilju rasvjetljivanja kriminalnog akta koji je svoje tragove „ostavio“ na globalnoj računarskoj mreži i računarskim sistemima

---

[2] Postojeći ZKP ne daje ni elementarnu definiciju dokaza, a kamoli elektronskog, koji se pojavljuje u vezi sa izvršenjem krivičnih djela visokotehnološkog kriminaliteta. Elektronski dokaz je informacija ili podatak od značaja za istragu koji je smješten ili prenijet putem računara. Ima istu vrijednost kao i svi drugi materijalni dokazi i za njega važe potpuno ista procesna pravila kao i za sve ostale dokaze. Međutim, pri ovome treba imati u vidu specifičnost elektronskih dokaza koja proizilazi iz njihove prirode, a to je da su veoma osjetljivi, da se vrlo lako mogu izmijeniti, obrisati ili na bilo koji drugi način uništiti, što zahtijeva posebnu pažnju i pristup u postupku pribavljanja i obezbjeđivanja ovakvih dokaza.

[3] Engleska riječ izvedena od *grčke* Κυβερνήτης / kybernetes – uravljač, pilot, kormilar. U duhu srpskog jezika pravilno je izgovarati „kiber“.

[4] Takva situacija, gdje bi više od jedne države moglo da zahtijeva nadležnost, može biti posebno česta u slučajevima napada na informacione sisteme, kao što su na primjer napadi virusa i drugih malicioznih programa koji istovremeno mogu da nanesu štetu velikom broj informacionih sistema na globalnom nivou.

više kontinenata ili država, jedino je moguće u postupku pružanja međunarodne pravne pomoći.

Zbog neprimjereno dugog trajanja ovog postupka, u praksi se često odustajalo od primjene odgovarajućih odredbi ZKP-a, čak i u situacijama kada je pružanje takve pomoći bilo od neprocjenjive važnosti za ishod samog postupka.

Čekanje odgovora po upućenim zamolnicama u trajanju od po dvije i više godina obesmišljavalo je, ne samo korišćenje ovog pravnog instituta, već i same krivične postupke u kojima je trebao biti primijenjen.

Zakon o pružanju međunarodne pravne pomoći u krivičnim stvarima, čijim su donošenjem stavljene van snage odredbe ZKP-a koje se tiču postupka za pružanje međunarodne pravne pomoći i izvršenje međunarodnih ugovora u krivičnopravnim stvarima, propustio je da reguliše specifične aspekte pružanja međunarodne pravne pomoći u krivičnim stvarima iz oblasti visokotehnološkog kriminaliteta u kojoj je, više nego u bilo kojoj drugoj, brzina[5] u postupanju od presudnog značaja za uspješno vođenje krivičnog postupka.

Osim što je previdio postojanje mreže 24/7,[6] zakon je propustio da predvidi i upotrebu modernih načina komuniciranja,[7] uključujući E-mail i faks, za upućivanje zahtjeva (*za kojima bi uslijedila zvanična pisana molba*) u hitnim postupcima pružanja međunarodne pravne pomoći, kao što su uzajamna pomoć u pogledu prikupljanja podataka o saobraćaju u realnom vremenu, zapljena i dostava sačuvanih računarskih podataka za potrebe druge države itd.

U tom smislu praksa je pokazala da je zaobilaženje ovako „tromih" zakona i sporih procedura jedino moguće uspostavljanjem neformalnih kontakata i saradnje, što nažalost implicira pitanje pravne validnosti na ovaj način prikupljenih dokaza.

Izvršioci se služe pogodnošću da im internet pruža skoro potpunu anonimnost, kao i činjenicom da je digitalne finansijske tokove, koji obično vode preko više država, veoma teško pratiti i utvrditi krajnju destinaciju sredstava. Sociološki profili oštećenih se veoma razlikuju, a žrtva prevare izvršene putem interneta može postati gotovo svako, zbog čega je neophodno uvijek biti na oprezu, jer izvršioci ovakvih krivičnih djela usavršavaju načine obavljanja svojih kriminalnih aktivnosti i mijenjaju ciljne grupe svog djelovanja. Grupe ovih kriminalaca su veoma dobro organizovane, specijalizovane su za odeđene regione, a da bi internet prevare bile uspješne, služe se najrazličitijim metodama za pribavljanje podataka o potrencijalnim žrtvama i sklapanje njihovog sociološkog profila. Najbolji izvor informacija predstavljaju sami oštećeni, koji posjetom lažnim reklamnim sajtovima, ili odgovorom na posebnu vrstu reklamnih e-mail poruka tzv. spam ostavljaju svoje lične podatke, a na osnovu prikupljenih materijala se pravi mehanizam prevare.

Kada operater može da identifikuje i kontroliše podatak, može se smatrati da je takav podatak materijalni objekat, kao što je to, na primjer, podatak

---

[5] Priroda podataka relevantnih u visokotehnološkom kriminalitetu je izuzetno nestabilna i čuva se veoma ograničen vremenski period (ponekad samo par minuta). Stoga je brzo reagovanje od ključnog značaja u izvršenju uzajamne pomoći.

[6] Autori Konvencije o VT kriminalitetu su uvidjeli da postojeći modaliteti policijske saradnje i uzajamne pomoći iziskuju dodatne kanale radi efikasne borbe u računarskoj eri. Takvo mjesto za kontakt bi trebalo da bude u stanju da obezbijedi momentalnu pomoć u istragama i sudskim postupcima.

[7] Do stepena koji garantuje odgovarajuće nivoe bezbjednosti i autentičnosti (uz korišćenje enkripcije, elektronskog potpisa i sertifikata).

zabilježen na tvrdom (hard) disku, izmjenljivom disku – popularnoj fleš memoriji (USBflashdisc), disketi (flopydisc), na kompakt disku (CD), magnetnoj traci i dr. Takav podatak je moguće i čulno opaziti u vidu slike na monitoru, zvuka, pisanog taksta ili slika odštampanih pomoću kompjuterskih štampača, ili kombinacije svega navedenog. Ovo je veoma važno sa aspekta pribavljanja, obezbjeđivanja i korišćenja dokaza koje na uređaju pronađemo u elektronskoj formi, jer podatak koji je obrađivan u kompjuterskom sistemu, ne može se više identifikovati i kontrolisati od strane operatera bez poznavanja i poštovanja određenih postupaka i korišćenja specifičnih tehničkih sredstava. Informacioni sistem automatski prebacuje podatke od jednog mjesta na memoriji do drugog. U kompjuterskim mrežama za osobu koja kontroliše podatke je nemoguće da fizički locira obrađene podatke, bilo u cjelini ili djelimično, bez posebnih procedura i tehničkih sredstava. Pošto takvi podaci mogu biti kontrolisani samo uz pomoć "logičkih" operacija, a ne uz pomoć fizičkih, bilo bi teško tretirati ih kao definisanje objekta.

Problem je da li elektronski dokaz i pod kojim uslovima može da se smatra kao materijalni, u istom smislu kao dokument, knjiga, spis, magnetofonska i video traka, fotografija i nesporni potpis. Na primjer, da bi se dokazalo krivično djelo iz oblasti ekonomskog i finansijskog kriminaliteta, potrebno je pribaviti određenu poslovnu dokumentaciju (fakture, otpremnice, izvode promjena na žiro-računu kod poslovne banke i dr.). Moderno poslovanje podrazumijeva vođenje kompjuterskog knjigovodstva, koje omogućava brzinu i tačnost formiranja knjigovodstvenih dokumenata, neuporedivo veću brzinu računskih operacija koje se vrše pri knjiženju, daje mogućnosti za brže i efikasnije pretraživanje poslovne dokumentacije, ali s druge strane stvara i mogućnost zloupotreba u smislu formiranja lažne dokumentacije, koja ima sve karakteristike intelektualnog falsifikata. Dakle, dokazi za osnovno krivično djelo koji se prikrivaju tim falsifikatima moraju se pronaći u kompjuteru ili kompjuterskoj mreži pravnog lica prilikom vršenja uvida u određenu poslovnu dokumentaciju. Ovaj uvid se umjesto na klasičan način, listanjem i pregledanjem dokumenata, sada vrši izlistavanjem kompjuterski formiranih dokumenata, koje treba pronaći u memoriji uređaja na kojem se knjigovodstvo vodi. Dakle, otkrivanje i pronalaženje ovakve dokumentacije kao i utvrđivanje da li je ona autentična ili naknadno mijenjana, zahtijeva poznavanje procedura i načina rada kompjuterskog knjigovodstva, ali i posebna informatička znanja koja uz upotrebu specijalnih softvera za pronalaženje podataka i ponovno izazivanje brisanih podataka, odnosno utvrđivanje izmjena podataka u memoriji uređaja ili na dokumentima, kao i komunikacije koja je vršena kroz mrežu, treba da obezbijede pribavljanje i fiksiranje kvalitetnih dokaza.

Postavlja se pitanje da li radi obezbjeđivanja dokaza treba izvršiti i privremeno oduzimanje uređaja na kojem se vodi knjigovodstvo, odnosno hard diska na kojem se relevantni podaci čuvaju, ili se dokazom može smatrati kopija tih podataka koja je napravljena na licu mjesta po određenoj proceduri. U dosadašnjoj praksi, privremeno je oduzimana samo dokumentacija koja se odštampa na papiru, a zatim je potpisom i pečatom ovjeri odgovorno lice. U određenim slučajevima to je možda dovoljno, ali je to metodološki pogrešan pristup. U memoriji uređaja, osim dokumenta u obliku koji je dostupan, nalaze se i drugi relevantni podaci, kao na primjer skriveno, "crno" knjigovodstvo, ili brisani podaci, koji se određenim postupcima i uz korišćenje posebnih softverskih alata mogu restituisati.

Tri su osnovne kategorije digitalnih podataka koji mogu činiti digitalne dokaze u komjuterskoj ekscesnoj situaciji (Petrović, 2010: 4):

- *Prelazni podaci* ili informacije koje se gube nakon isključivanja računara, kao što su veze sa otvorenom radnom memorijom (RM), rezidentni memorijski programi, itd. Ovi podaci se mogu izgubiti u toku procesa isključivanja računara. Otuda je veoma važno do kraja precizno sprovoditi proceduru akvizicije. Prije isključivanja računara treba odmah ispitati, locirati i izvući osjetljive i šifrovane podatke, jer se može desiti da se poslije isključivanja ne može doći do njih (npr. vlasnik ključa ili smart kartice za pristup je nekooperativan ili mrtav, itd.).
- *Osjetljivi podaci* ili podaci uskladišteni na hard disku (HD) koji se lako mogu izmijeniti, kao što je, npr., posljednje vrijeme pristupa login datoteci itd.
- *Privremeno pristupačni podaci* ili podaci uskladišteni na HD kojima se može pristupiti samo u određeno vrijeme (npr. šifrovani podaci).

Ukoliko ne postoji mogućnost da se dokazi pribave odmah i direktno na licu mjesta, neophodno je kompjutersku opremu ili druge uređaje bezbjedno isključiti, zapečatiti i privremeno oduzeti na način koji obezbjeđuje da ne dođe do uništenja, brisanja ili izmjene dokaza koji se u elektronskoj formi nalaze na tim uređajima. Ovi dokazi se mogu fiksirati kasnije u laboratorijskim ili drugim pogodnim uslovima, uz obavezno prisustvo osumnjičenog ili lica od kojeg su ovi uređaji oduzeti ili pak odgovornog lica u pravnom licu ili državnom organu. Ukoliko je fizički nemoguće oduzeti uređaje i opremu, ili dijelove uređaja, treba obezbijediti i zapečatiti prostoriju u kojoj se oni nalaze, a prethodno onemogućiti ne samo fizički pristup, već i pristup uređaju sa daljine žičnim ili bežičnim putem, odnosno isključiti ga iz mreže, kako bi se dokazi sačuvali u neizmijenjenom obliku.

U oblasti suzbijanja kompjuterskog kriminaliteta potrebno je primjenjivati i specijalne istražne tehnike kao što su elektronsko praćenje, presretanje elektronskih komunikacija ili druge oblike nadzora. Ovo mogu biti i tajne operacije za potrebe borbe protiv organizovanog kriminaliteta. Za primjenu ovih tehnika neophodno je najprije stvoriti zakonski i institucionalni okvir, kao i izvršiti edukaciju i osposobljavanje pripadnika policije za elektronsko praćenje, a što bi posebno predstavljalo utvrđivanje lokacije lica preko IP adresa, bez čega neće biti moguće ostvariti efikasno gonjenje učinilaca, koji se prilikom izvršenja krivičnog djela koriste kompjuterskom tehnologijom (Suzbijanje visokotehnološkog kriminala, 2010: 266).

Kada je u pitanju unapređenje tehničkih mogućnosti državnih organa koji se bore protiv VT kriminaliteta, svakako da je najznačajnije unapređenje tehničkih mogućnosti policije, posebno njihovog specijalizovanog odjeljenja.

Fiksiranje, prikupljanje, čuvanje i obrada digitalnih dokaza nalažu visoku tehničku opremljenost Posebnog odjeljenja MUP-a, pri čemu potreba za hitnim i neodložnim vještačenjima nalaže potrebu posjedovanja najsavremenijih hardverskih i softverskih alata kojima je moguće „ući u trag“ izvršiocima ovih krivičnih djela, koji se nerijetko regrutuju iz reda veoma promućurnih ljudi, sa multidisciplinarnim znanjima iz IT-a, često stečenim na samom webu.

Kompjuterski kriminalitet je unio poseban problem u oblast sudskog vještačenja i svjedočenja. Pravilo klasičnog svjedočenja kaže da svjedok može svjedočiti samo ako je očevidac, odnosno samo o onome što je lično iskusio (čuo, vidio, zna), a ne iz druge ruke, što se smatra posrednim dokazom, poznatim u žargonu kao “rekla – kazala”.

Međutim, kod računara imamo upravo slučaj da se sve što se nalazi u njemu može svesti pod kategoriju "rekla – kazala" dokaze. Naime, ništa direktno vezano za događaj se ne vidi u računaru, jer se login datoteka može naknadno izmijeniti, promijeniti datum datoteke, izbrisati ili izmijeniti dokument, što praktično znači da samo osoba koja je izazvala kompjuterski incident (kompjuterski kriminalac) ima direktno saznanje o tome i jedini je očevidac, odnosno neposredan svjedok. Dakle, kompjuterski podaci se mogu koristiti kao dokazi za svjedočenje samo ako su veoma pažljivo preuzeti i ako zadovoljavaju neke specifične kriterijume u sudskom vještačenju (forenzičkoj akviziciji i analizi). Ovi su kriterijumi kritični u pogledu sposobnosti forenzičkog analitičara da sakupi što više posrednih dokaza pomoću kojih se dolazi do neoborivog dokaza. Praktično, posredni su svi dokazi u kompjuterskom kriminalnom aktu koji se sakupe analizom samog softvera, računara i/ili računarske mreže. Da bi posredni dokaz bio prihvatljiv za sud, mora biti takav da potvrđuje hipotezu o čvrstom dokazu, ili da je pobija. Drugo, mora postojati dokaz da je login datoteka, kao posredni dokaz, nastala u normalnom radnom procesu, pa je, npr. potrebno imati čvrste dokaze da je počinilac bio logovan kada je server pao. Ovo je dovoljno čvrst dokaz i opravdava postupak da nadležni organ istrage službeno zahtijeva prisluškivanje linije osumnjičenog te da se snimi vrijeme pristupa serveru, koje se kasnije upoređuje sa login podacima u log datotekama računara i aktivnostima drugih mrežnih uređaja i utvrđuje kao neoboriv dokaz pristupa serveru (Petrović, 2010: 4).

Postojanje *contactpoint*-a u okviru „mreže 24/7"[8], predviđene Konvencijom o visokotehnološkom kriminalitetu[9], nezamislivo je bez sigurnog *online* pristupa svim vrstama telekomunikacionih mreža.

Sve to podrazumijeva postojanje redundantnog računarskog sistema[10] implementiranog na heterogenim platformama (Windows/Linux), sa visokom propusnom moći mreže, koja bi cjelokupnim perfomansama obebijedila sigurnost i brzinu u obavljanju poslova.

Kako suzbijanje VT kriminaliteta podrazumijeva i preventivnu stranu djelovanja, smatramo da je od posebnog značaja izrada kvalitetne web prezentacije koja bi svojim sadržajima edukovala njene posjetioce, ne samo u pogledu potencijalnih opasnosti koje ih vrebaju na mreži, već i u pogledu mjera koje mogu preduzeti u cilju sigurnosti i zaštite sopstvenog integriteta. Takođe, iznoseći primjere iz tužilačke i sudske prakse, uvjereni smo da bi takvi sadržaji mogli odvratiti izvjestan broj lica od izvršenja krivičnih djela koja su planirali, ili namjeravali da izvrše.

---

[8] „Da bi rad mreže bio olakšan, svaka strana ugovornica treba da obezbijedi obučeno i opremljeno osoblje" – član 35. Konvencije.

[9] Svaka strana ugovornica treba da odredi mjesto za kontakt, koje je dostupno 24 sata, 7 dana u nedjelji, da bi omogućila pružanje trenutne pomoći istragama ili postupcima u vezi sa krivičnim djelima koja se odnose na računarske sisteme i podatke, ili radi prikupljanja dokaza u elektronskom obliku o krivičnom djelu, (član 35. Konvencije).

[10] Redundantan sistem– u kojem za sve segmente sistema postoje alternativni, koji se u slučaju otkazivanja primarnog automatski aktivira, omogućujući tako neprekidan rad.

ZAKLJUČAK

Problem primarnog i sekundarnog dokaza izražen je u ovoj oblasti. Naime, u zakonodavstvima nekih zemalja sekundarni dokazi se mogu prihvatiti samo u slučaju da se ne raspolaže primarnim dokazima. Proceduru dolaženja do dokaza u elektronskoj formi neophodno je materijalizovati sačinjavanjem zapisnika, u kojima se detaljno opisuju primijenjene procedure, fotografisanjem, audiovideo dokumentovanjem, prisustvom svjedoka i stručnih lica u postupku. Sve ovo se radi u cilju da se otkloni sumnja da su dokazi pribavljeni na zakonit način i da se potvrdi da su u potpunosti fiksirani u obliku u kojem su i zatečeni na licu mesta. Organi otkrivanja i krivičnog gonjenja moraju da poštuju ovu metodiku i procedure da u kasnijoj fazi postupka dokazi ne bi bili osporeni.

Neophodno je u što kraćem roku izvršiti dopunu pozitivnih zakonskih propisa vezano za mogućnost da kao dokaze u postupku treba prihvatiti i elektronske dokaze izvedene na magnetskim medijima, optičkim diskovima i drugim vrstama elektronskih memorija, kao i ostalih medija iz kojih mogu da se posredno i neposredno izvedu elektronski dokazi.

Elektronski dokazi zavise od načina izvršenja konkretnog krivičnog djela koje je direktno ili posredno povezano sa kompjuterom i kompjuterskim mrežama. Kao relevantni dokazi mogu da posluže sve vrste memorija na kojima se skladište elektronske informacije (hard diskovi, fleš memorije, optički kompakt diskovi i dr.), tekuće i neko prethodno (back-up) stanje podataka, svi elektronski dnevnici (log-ovi), štampani izveštaji izvedeni sa svih vrsta elektronskih memorija, izvorna (Source) i izvršna (exe, com) verzija programa, hardverska i telekomunikaciona oprema.

Prave probleme pribavljanja, obezbjeđivanja i korišćenja elektronskih dokaza, odnosno dokaza u elektronskoj formi, ili kako ih neki nazivaju, digitalnih dokaza, definisaće praksa otkrivanja i gonjenja krivičnih djela za čije su dokazivanje potrebni takvi dokazi. Praktične probleme potom treba iz života prenijeti u zakonsku regulativu i nova zakonska rješenja efikasno primjenjivati od strane dobro ostručenih specijalista u ovoj oblasti.

Dinamika razvoja IT zahtijeva kontinuiranu, neprekidnu obuku svih učesnika u borbi protiv VTK, a odgovarajući tehnička opremljenost samo je preduslov primjene tako stečenih znanja i vještina.

S obzirom na toliko puta pominjani karakter visokotehnološkog kriminaliteta koji ne priznaje nacionalne boje i obilježja, nameće se logičan zaključak da su tehnička sredstva neophodna za njegovo otkrivanje i suzbijanje jedinstvena, te kao takva i univerzalna, za sve države i pravne sisteme.

Da li će i u kom obimu takva tehnička sredstva biti i upotrijebljena, u velikoj mjeri zavisi od ekonomske moći države, te je u tom smislu izlišno davati poređenja i uporedne analize u odnosu na tehničku opremeljnost tužilaštava iz regiona, pa i šire.

LITERATURA:

1. **Bača, M., Kesić, T.**: *Digitalni dokazi i standardizacija njihove primene u krivičnim stvarima*, Zbornik radova Suzbijanje kriminala i evropske integracije, Kriminalističko-policijska akademija i Hans Zajedel Fondacija, Beograd, 2010.
2. **Banović, B.**: *Elektronski dokazi*, Revija za kriminologiju i krivično pravo, vol. 44, br. 3, 2006.
3. **Đokić, Z., Živanović, S.**: *Problemi pribavljanja, obezbeđivanja i korišćenja dokaza u elektronskoj formi, od značaja za krivični postupak*, Teški oblici kriminala, Budva, Beograd, 2004.
4. **Kostić, Z., Grubor, G.**: *Alati za digitalnu forenzičku istragu*, Računarstvo i informatika, Beograd, 2008.
5. **Petrović, D. L.**: *Digitalni dokazi*, Ziteh, Beograd, 2010.
6. **Protrka, N.**: *Računalni podaci kao elektronički (digitalni) dokazi*, Policijska sigurnost, Zagreb, broj 1, 2011.
7. *Suzbijanje visokotehnološkog kriminala*, Udruženje javnih tužilaca i zamjenika javnih tužilaca Srbije, 2010.
   - http://www.crime-research.org/analytics/702, 01.05.2009.
   - http://www.ecdlcentar.com/baza/ecdl_informacije/it-vestak-cd2009/ZBORNIK%20RADOVA%20ZITEH%2006
   - http://www.iso27001security.com/html/27037.html
   - http://www.theiai.org/disciplines/digital_evidence/index.php
   - http://www.albany.edu/crccp/resources.html

THE IMPORTANCE OF DIGITAL EVIDENCE IN CRIMINAL PROCEEDINGS

Assistant professor Uroš Pena, PhD
Directorate for coordination of law enforcement organizations and agencies of BIH
E-mail: urospena@hotmail.com
Dragan Mitrović
directorate for coordination of law enforcement organizations and agencies of BIH
E-mail: drmitrovic@blic.net

Abstract: The development of information technology has created new challenges in carrying out police activities. Most professions have had to adapt to the digital age, and the police profession should be particularly flexible, since digital technology in the service of crime require new types of criminal investigations. More and more, information technology is becoming an instrument of criminal activity. The study of this sophisticated criminal activity and providing the necessary evidence for presentation in court will become a significant police task.

With the achievements of technics and technology, there have been developed new opportunities and methods of their mistreatment, among which special place takes computer crime. The development of information technology is characterized by a very large flow of digital information in form of electronic (computer) records, which are located within a computer or transmitted via computer. They can be crucial evidence in identifying and proving in the most diverse misuse of information technology, especially abuse of computer and computer networks (including computer crimes).

Keywords: computer, computer crime, digital evidence, securin-gevidence, the probative value ...

Prethodno saopštenje - UDK 004.738.5+343.326(497.7)

IZRADA I UPOTREBA LAŽNIH PLATEŽNIH KARTICA KAO MASOVNI OBLIK KOMPJUTERSKOG KRIMINALA U REPUBLICI MAKEDONIJI

Doc. dr Svetlana Nikoloska
Fakultet bezbednosti – Skoplje
svetlananikoloska@hotmail.com
snikoloska@fb.uklo.edu.mk

Apstrakt: Kompjuterski kriminal predstavlja kriminal koji je uslovljen informatičkom tehnologijom i primenama tehnoloških dostignuća u ostvarivanju kriminalnih ciljeva izvršilaca. Kriminalci koriste svoja stručna znanja u cilju ostvarivanja svojih motiva, a dominira motiv sticanja imovinske koristi, najčešće novca. Kako da kriminalci ,,ukradu,, novac sa bankovnog računa, a da to nije razbojništvo. Zadnjih godina u Republici Makedoniji kompjuterski kriminal je prepoznatljiv u više pojavnih oblika, a najizraženiji su izvršena krivična dela s elementima izrade i upotrebe lažnih platežnih kartica. Kriminalci deluju organizovano, u kriminalnim grupama domaćih i stranih kriminalaca koje povezuje ,,kriminalni biznis,, koji se odvija u pravcu nabavljanja opreme, materijala, podataka i izrade platežnih kartica i njihove upotrebe na bankomatima i u platnom prometu u cilju izvlačenja ,,tuđeg novca,,. Kriminalci imaju podijeljene uloge u kriminalnoj realizaciji, jedni nabavljaju opremu i stručni su u izradi, drugi postavljaju sredstva za snimanje podataka – skimere, a treći upotrebljavaju falsifikovane kartice i izvlače novac sa tuđih računa, a ima i grupa kriminalaca – kontrolora. Analizom modusa operandi i instrumentuma operandi krivičnog dela izrade i upotrebe lažnih platežnih kartica, gradi se model istraživanja i prevencije ovog kriminala.

Ključne reči: kompjuterski kriminal, informatička tehnologija, platežna kartica, kriminalni biznis, novac.

UVOD

Uvođenjem kompjuterske tehnologije u finansijske institucije – banke i širenje novih metoda u radu banaka omogućava se, s jedne strane, brz i jednostavniji pristup finansijskim sredstvima – novcu kojim fizička i pravna lica raspolažu na svojim bankarskim računima, ali sa druge strane, povećava se mogućnost i opasnost od zloupotrebe tehnologije u cilju prisvajanja novca sa tuđih računa u bankama. Kriminalci se sve više organizuju i rade na usavršavanju kriminalnog delovanja i koriste sve više novih metoda za kriminalne operacije u cilju ostvarivanja visoke kriminalne dobiti sa smanjenjem opasnosti njihovog otkrivanja i krivičnog gonjenja.

Kompjuterski kriminal predstavlja oblik kriminalnog ponašanja gde kriminalci koriste svoja znanja i umeća, ali i tehnička sredstva u izrađivanju sredstava kriminalnog napada (instrumentum operandi) koja im olakšavaju način kriminalog delovanja (modus operandi), ali im omogućavaju i širi spektar kriminalnog delovanja (radius operandi) u vreme koje je pogodno za kriminalno

delovanje (tempus operandi), a nanose imovinsku štetu licima koje i ne poznaju fizički, ali imaju podatke o njihovim ,,debelim,, bankarskim računima. Bankarske račune napadaju kriminalci koji, korišćenjem tehničkih sredstava ,,kradu,, podatke o licima koja imaju račun u banci, a raspolažu finansijskim sredstvima korišćenjem platežnih kartica. Falsifikovanjem platežnih kartica omogućava se njihova upotreba i izvlačenje tuđih finansijskih sredstava, pri čemu su tragovi kriminalnog delovanja nevidljivi, dokazi "sakriveni", a kriminalci zadovoljni i uživaju u kriminalnom bogatstvu.

U Republici Makedoniji zadnjih godina ovaj oblik kompjuterskog kriminaliteta je sve više zastupljen, a kriminalističko istraživanje ukazuje na organizovan način kriminalnog ponašanja u kriminalnim operacijama koje uključuje i lica iz susednih i drugih zemalja, a kriminalno se operiše u više država. Nadležni organi, policija i javno tužilaštvo suočavaju se sa više problema u procesu istraživanja, a to su obezbeđivanje dokaza i njihovo povezivanje sa izvršiocima kriminalnih dela i pronalaženje i hapšenje kriminalaca, a kao najveći problem se javlja utvrđivanje visine štete od kriminalnog delovanja i zaplena kriminalne dobiti u cilju obeštećenja žrtava komjuterskog kriminaliteta sa elementima izrade i upotrebe lažnih platežnih kartica.

POJAM KOMPJUTERSKOG KRIMINALITETA

Kompjuterski kriminalitet je opšti pojam, koji obuhvata krivična dela koja su izvršena posredstvom kompjutera i kompjuterskog sistema i mreža i krivična dela koja su usmerena ka napadu i oštećivanju kompjuterskog sistema i mreža. Postoji više definicija kompjuterskog kriminaliteta, a skoro svaka od postojećih obuhvata kompjuter kao sredstvo kompjuterskog napada ili kompjuter, kompjuterski sistem ili kompjutersku mrežu kao cilj kriminalnog napada i neophodno znanje iz oblasti informatičke tehnologije. Prva definicija kompjuterskog kriminaliteta definiše ovaj pojam kao "bilo koji nezakonski akt za čije je uspešno izvršenje presudno poznavanje kompjuterske tehnologije."[1] Potom je nastajalo sve više definicija autora koji su istraživali kompjuterski kriminalitet u njegovim pojavnim oblicima. ,,Kompjuterski kriminal obuhvata krivična dela kod kojih se kompjuter pojavljuje kao sredstvo (oruđe), predmet ili objekt napada, za čije je izvršenje ili pokušaj neophodno izvesno znanje iz računovodstava ili informatike,,[2]

Kompjuterski kriminalitet je opšta formulacija koja obuhvata različite oblike kriminalnog delovanja, odnosno, to je kriminalitet koji je usmeren protiv bezbednosti informacionog (kompjuterskog) sistema u celini ili u njegovom pojedinačnom delu, različitim načinima i različitim sredstvima u nameri da se za sebe ili za nekog drugog pribavi neka korist ili da se drugome nanese neka šteta.[3]

Znanje iz oblasti kompjuterske tehnologije danas se stiče od malih nogu, još dok su deca u osnovnoj školi, a kompjuterska tehnologija je ušla u sve oblasti

---

[1] Computer Crime:Criminal Justice Resurce Manual, 1979.

[2] Brvar B. , Pojavne oblike zlorabe računalnika, Revija za kriminalistiko in kriminologijo, 2-1982, str. 93.

[3] Јовашевиќ Д., *Лексикон кривичног права*, ЈП Службени лист СРЈ, Београд, 2002 године.

poslovanja, tako da je to znanje neophodnost za svakog građanina na planeti, a neki to znanje iskorišćavaju za kriminalne ciljeve. Nekad se nedozvoljena ponašanja u sferi kompjuterske mreže vrše i zbog radoznalosti, radi testiranja znanja, ali se sve više znanje koristi i u destruktivne, kriminalne svrhe. Definicija nemačkog autora Ulricha Siebera obuhvata protivpravne povrede imovine, kod kojih se računarski podaci s predumišljajem menjaju (kompjuterska maniulacija), uništavaju (kompjuterska sabotaža), neovlašćeno zahvataju i iskorišćavaju (kompjuterska špiujnaža) ili se koriste zajedno sa hardverom (krađa vremena).[4] Ovo je jedna od definicija koja je bliža komjuterskom kriminalitetu koji ima elemente sticanja protivzakonite imovinske koristi, a u tom pravcu ide i definisanje Dona Parkera koji kompjuterski kriminal definiše kao: "zloupotreba kompjutera je svaki događaj u vezi sa upotrebom kompjuterske tehhologije u kome žrtva trpi ili bi mogla da trpi gubitak, a učinilac deluje u nameri da sebi pribavi ili bi mogao da pribavi korist".[5] Đorđe Ignjatović pod kompjuterskim kriminalitetom podrazumeva poseban vid inkriminisanih ponašanja kod kojih se računarski sistem (shvaćen kao jedinstvo hardvera i softvera) pojavljuje ili kao sredstvo izvršenja ili kao objekt krivičnog dela, ukoliko se delo na drugi način, ili prema drugom objektu, ne bi moglo izvršiti ili bi ono imalo bitno drugačije karakteristike.[6]

Ignjatovićeva definicija je prihvatljiva za kompjuterski kriminalitet sa elementima izrade i upotrebe lažnih platežnih kartica u delu da je ovo krivično delo kombinacija krađe, prevare i falsifikovanja isprava, ali kriminalno delovanje je vezano za kompjuter u delu izrade falsifikovane platežne kartice, a sama upotreba je napad na kompjuterski sistem, ili bankarski kompjuterski sistem koji sadrži finansijske podatke. Kod ovog krivičnog dela kompjuter je sredstvo izvršenja i objekt kriminalnog napada, sredstvo je kompjuter pomoću koga se izrađuju falsifikovane platežne kartice, a kriminalni napad je napad na finansijski račun u banci, upotrebom te kartice. Krivično delo je moguće izvršiti samo u slučaju da je izrađena lažna platežna kartica, ali i da bi se ona napravila potrebni su kompjuterski podaci koji su u bazama bankarskog kompjuterskog sistema, kao i podaci o kodovima koji su neophodni da se aktivira kartica, ili da bankomat ,,iskeširа,, novac.

,,Kompjuter kao sredstvo izvršenja krivičnog dela, gde se učinilac služi kompjuterom da bi izvršio određeno krivično delo, najčešće prevaru, krađu, proneveru, ali i druga tradicionalna krivična dela, koja su izvršena na specifičan način, uz korišćenje kompjutera, što i predstavlja osnov za njihovo odvajanje od tradicionalne podele kriminaliteta i svrstavanje pod pojam kompjuterskog kriminaliteta u širem smislu. Kompjuter kao objekt napada, gde su kompjuter, ili kompjuterska mreža i informacije koje ona sadrži krajnji cilj kriminalnog napada, bilo da je sam kompjuter, ili mreža objekt oštećenja, onesposobljavanja ili uništenja, ili se želi neovlašćeno doći do informacija koje su u njemu sadržane, iz raznih motiva".[7]

---

[4] Sieber U., Kompjuterski kriminal i krivično pravo, Kőln, 1977, str. 188.

[5] Parker D., Computer Abuse, str. 14.

[6] Ignjatović, Đ, Pojmovno određenje kompjuterskog kriminaliteta, Anali pravnog fakulteta, Beograd, 1991, br. 1–3, str. 142.

[7] Бановић, Б., Обезбеђење доказа у криминалистичкој обради кривичних дела привредног криминалитета, Београд, стр. 138–139.

Kompjuterski kriminalitet obuhvata deo tradicionalnog kriminaliteta za čije je izvršenje neophodan kompjuter ili je cilj napada kompjuterski sistem, ali kompjuterski kriminalitet obuhvata i druge pojavne oblike, i ima shvatanja kriminologa da je kompjuterski kriminalitet deo ekonomskog kriminaliteta, ali i shvatanja da se radi o imovinskom kriminalitetu i da je kompjuterska zloupotreba po svom karakteru najbliža imovinskom kriminalitetu.[8] Cilj kriminalnog delovanja jeste sticanje imovinske koristi kroz korišćenje informacija i podataka u kompjuterskim sistemima. Informacije su postale jedan od strateških resursa, a veliki broj naučnih, ekonomskih, bezbednosnih, ličnih i drugih podataka je sačuvan u kompjuterima i može imati visoku cenu, ukoliko se koristi u nedozvoljene svrhe. Kvantitet i vrednost informacija u elektronskoj bazi podataka, nesumnjivo predstavljaju istinsku metu za one koje se bave kriminalnim aktivnostima. Kriminalci nesumnjivo prate razvoj savremenih informatičkih tehnologija i prilagođavaju svoja kriminalna delovanja tom razvoju. [9]

U definisanju kompjuterskog kriminala i definisanju nekih značajnih pojmova koji se koriste u inkriminacijama kompjuterskih krivičnih dela, svoje preporuke nacionalnim zakonodavstvima daje i Konvencija o kompjuterskom kriminalu Saveta Evrope, donesena 23. novembra 2001. godine u Budimpešti. Konvencija je donesena u svrhu toga da zemlje potpisnice ovog dokumenta vode zajedničku politiku usmerenu ka zaštiti društva od kompjuterskog kriminala, pored ostalog i kroz usvajanje adekvatnog zakonodavstva i negovanje međunarodne saradnje. Konvencija o kompjuterskom kriminalu definiše ovaj kriminalitet u četiri kategorije, od kojih je značajan kriminal s elementima izrade i upotrebe lažnih platežnih kartica, u koji spadaju prve dve kategorije, i to:

1) Dela protiv tajnosti, integriteta i dostupnosti kompjuterskih podataka i sistema – njih čine nezakonski pristup, presretanje, uplitanje u podatke ili sisteme;
2) Korišćenje uređaja (proizvodnja, prodaja, uvoz i distribucije), programa i pasvorda i
3) Dela čije je izvršenje vezano za kompjuter (među kojima je falsifikovanje i krađa, koji predstavljaju najtipičnije oblike kriminalnog napada).

Konvencijom su definisani i pojmovi kompjuterskog sistema i kompjuterskih podataka, koji su bitni termini u inkriminisanju kompjuterskih krivičnih dela. Kompjuterski sistem podrazumeva bilo kakav uređaj ili grupu međusobno povezanih uređaja koji – jedan ili više njih – vrše automatsku obradu podataka prema određenim programima. Pojam kompjuterski podaci označava prezentiranje činjenica, informacija ili koncepta u obliku pogodnom za obrađivanje preko kompjuterskog sistema, uključujući i program pogodan da se kompjuterski sistem stavi u funkciju. Konvencija je dosta bitna za razne inkriminacije u nacionalnim zakonodavstvima, harmonizaciju nacionalnih zakonodavstva država potpisnica Konvencije, čime se stvaraju i uslovi za međusobnu saradnju i razmenu informacija i podataka u borbi protiv kompjuterskog kriminala. Imajući u vidu da kompjuterski kriminal karakteriše i to da se kriminalci udružuju zbog kriminalnog delovanja i ostvarivanja kriminalnog cilja, tako da se kriminalno delovanje vrši na teritoriji više država, ili se jedan deo kriminalne operacije vrši u jednoj državi, a drugi, treći ili bilo

[8] Konstantinović-Vilić, S. i Nikolić-Ristanović, V., Kriminologija, Niš, 2003, str. 161.
[9] Тупанчевски, Н. и Кипријановска, Д., Основи на македонското информатичко казнено право, МРКПК бр. 2–3, 2008. година, стр. 524.

koji u nizu kriminalnih aktivnosti vrše se na teritoriji više država. Međusobna saradnja u procesu istraživanja kompjuterskog kriminaliteta jeste neminovnost svih država na čijoj teritoriji kriminalci deluju i gde nastaje kriminalna posledica.

IZRADA I UPOTREBA LAŽNIH PLATEŽNIH KARTICA

Republika Makedonija je prihvatila preporuke Konvencije o kompjuterskom kriminalu i u 2009. godini je napravila veliki korak u inkriminisanju novih kompjuterskih krivičnih dela, ali su i redefinisane postojeće inkriminacije novim stavovima u kojima je predviđeno da delo može biti izvršeno kompjuterom ili kompjuterskim sistemom ili mrežom, koji su objekt ili cilj kriminalnog napada. Sama praksa u Republici Makedoniji poslednjih godina je ukazala na potrebu inkriminisanja novog krivičnog dela koje sadrži elemente izrade i upotrebe lažne platežne kartice, koja dela su ranije postojala kao kriminalni slučajevi koji su otkriveni i rasvetljeni tako što su klasifikovani kao kompjuterska prevara.

Inkriminacija se odnosi na kriminalne situacije u kojima je učinilac (predviđeno je da učinilac može biti fizičko i pravno lice) napravio lažnu platežnu karticu s namerom da je upotrebi kao stvarnu, ili da nabavi lažnu karticu s takvom namerom, ili da je da drugome da je upotrebi, ili je sam već upotrebio lažnu platežnu karticu kao stvarnu. Zakonodavac je predvideo nekoliko načina izvršenja ovog dela, i to:

1. Izrada lažne platežne kartice,
2. Nabavljanje lažne platežne kartice i
3. Upotreba lažne platežne kartice.

Namera je jedna od bitnih subjektivnih karakteristika ovog dela, a znanje je činjenica koju treba dokazati u procesu rasvetljavanja; samim tim što koristi tuđu karticu, učinilac treba da zna za mogućnost da je ta kartica lažna.

Kao jedan od načina izvršenja ovog dela predviđeno je i pribavljanje bankarskih podataka o stvarnim platežnim karticama i podacima o nosiocima tih platežnih kartica s namerom da se iskoriste u izradi i upotrebi lažnih platežnih kartica, ili se bankarski podaci daju drugome da izradi i upotrebi lažne platežne kartice. Predviđeno je da ovo krivično delo može biti izvedeno i od strane člana grupe, bande ili drugog zločinačkog udruženja kao kvalifikovani oblik krivičnog dela.

Izrada i upotreba lažne platežne kartice jeste složeno krivično delo gde kriminalci rade na pripremi i obezbeđivanju sredstva za izradu platežnih kartica kao i na prikupljanju podataka o fizičkim i pravnim licima koja poseduju platežne kartice, a na računima imaju veću količinu novca. Predviđeno je da je kao kriminalno ponašanje sankcionisano i samo prikupljanje bankarskih podataka o stvarnim platežnim karticama i njihovim sopstvenicima u nameri da se zloupotrebe u cilju izrade lažnih platežnih kartica kojima bi se ,,izvukao,, tuđi novac. Za izvršenje ovog krivičnog dela najčešće se kriminalci organizuju u trajne ili labave kriminalne organizacije ili grupe čiji članovi imaju konkretne kriminalne uloge. Organizovane kriminalne grupe predstavljaju skup pojedinaca koji imaju zajedničke interese, koji su najčešće skup pojedinačnih interesa, i koji u njihovoj realizaciji zajednički deluju. Organizovane grupe variraju od labavih udruženja sa zajedničkim interesima do čvrsto usklađenih organizacija sa dobro definisanim ciljevima. Kriminalne organizacije predstavljaju najviši organizacioni oblik kriminalaca, karakterističan

po organizacionoj čvrstini, hijerajhijskim odnosima, strogoj disciplini, poslušnosti i ličnoj lojalnosti, uz izgrađenu dugoročnu strategiju i detaljno razrađenu taktiku.[10]

Izrada i upotreba lažne platežne kartice jeste kompjutersko krivično delo koje ima široki dijapazon kriminalnih aktivnosti koje su povezane i međusobno uslovljene, tako da je najpre neophodno pribavljanje podataka o platežnim karticama, njihovim osobenostima, kodovima i skrivenim brojčanim kombinacijama kako bi se omogućilo njihovo izrađivanje. Pribavljanje podataka najćešće je povezano sa postavljanjem specijalnih tehničkih instrumenata – skimera i mikrokamere na bankomatima kako bi kriminalci snimili podatke. Kasnije se tako snimljeni podaci prenose na kompjuter, gde se obrađuju i onda se štampaju lažne platežne kartice na specijalno za to obezbeđenoj plastici. Lažne platežne kartice se upotrebljavaju na bankomatima i na prodajnim mestima koja imaju aparate za elektronsko plaćanje. Sam kriminalni proces je složen i u njemu učestvuju lica koja imaju informacijsko znanje, a to su oni koji nabavljaju, postavljaju i koriste snimljene podatke u izradi lažnih kartica, a licima koja ih koriste i ne treba informacijsko znanje. Najčešće je organizator onaj koji ima stručnost i znanje, njegova kriminalna uloga je najvažnija. Kriminalna dobit je u rukama onih koji upotrebljavaju kartice, ali je njihov zadatak da novac sakupe i predaju organizatoru koji deli kriminalni „plen„ srazmerno kriminalnim ulogama. To su tradicionalno grupe organiziranog kriminala koje imaju hijerahijsku organizovanost i podelu kriminalnih uloga u pripremi i izvršenju krivičnih dela.

Ove organizirane kriminalne grupe dobijaju i naziv sajber mafije, koja ima svoja pravila, način komuniciranja i ponašanja koji se razlikuje od konvencionalne kriminalne mafije, njihovo oruđe je kompjuter i stručno znanje, ali u pripremi kriminalnih dela im je potreban novac kojim nabavljaju skupu opremu za izradu kriminalnih sredstava, lažna kartica je sredstvo izvršenja krivičnog dela, ali je i sama oprema sredstvo izvršenja krivičnog dela – instrumentum operadi.

U cilju izvršenja ovog krivičnog dela kriminalci nabavljaju uređaje namenjene snimanju podataka o licima koja poseduju platežne kartice. Najpoznatiji uređaj je skimer, koji se postavlja na bankomatima i ima određeni kapacitet snimanja podataka koji su na skrivenom delu platežne kartice, a snimaju i kodove koje koriste građani koji su koristili svoje platežne kartice u periodu dok je bio postavljen skimer.

Slika br. 1 i 2 Platežne kartice

[10] Petrović, S., Policijska informatika, Kriminalističko-policijska akademija, Beograd, 2007, str. 128.

Slika br. 3 Kritična mesta podataka na platežnim karticama

Slika br. 4 Bankomat na kojem je postavljen skimer

Zakonom o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala uređuje se obrazovanje, organizacija, nadležnost i ovlašćenja posebnih organizacionih jedinica državnih organa radi otkrivanja, krivičnog gonjenja i suđenja za krivična dela visokotehnološkog kriminala. Visokotehnološki kriminal u smislu ovog zakona predstavlja vršenje krivičnih dela kod kojih se kao objekat ili sredstva izvršenja krivičnih dela javljaju računari, računarske mreže, računarski podaci, kao i njihovi proizvodi u materijalnom ili elektronskom obliku. Pod proizvodima u elektronskom obliku se podrazumevaju računarski programi i autorska dela koja se mogu upotrebiti u elektronskom obliku.[11]

Internacionalnost, transnacionalnost i multidimenzionalnost su samo neka od svojstava kriminalne sajber mafije, čija organizacijska formula nije tako jednostavna, uobičajena i jednoobrazna, što predstavlja i problem organima progona koji otkrivaju, raznjašnjavaju i obezbeđuju dokaze o izvršenim krivičnim delima i dokaze i činjenice koje povezuju kriminalce sa krivičnim delima i elektronskim dokazima.

IZRADA I UPOTREBA LAŽNE PLATEŽNE KARTICE U REPUBLICI MAKEDONIJI

Kompjuterski kriminal u Republici Makedoniji je realan problem koji zadaje muku organima progona u procesu njegovog otkrivanja, razjašnjavanja i obezbeđivanja dokaza, a još više sama obrada elektronskih dokaza i njihovo pripremanje u formi koja je prihvatljiva sudskim organima. Ono što je bilo problem, jeste nedostatak posebne inkriminacije krivičnog dela „Izrada i upotreba lažne platežne kartice„ tako da su kriminalna ponašanja klasifikovana kao kompjuterska prevara ili oštećenje i neovlašćeno ulaženje u kompjuterski sistem ili kompjuterski falsifikat. Kao nova inkriminacija je uvedena izmenom Krivičnog zakonika u 2009. godina[12], a na snazi je od marta 2010. godine.

Marta 2010. godine Ministarstvo unutrašnjih poslova Republike Makedonije[13] otkrilo je kriminalni rad dve organizovane kriminalne grupe koje su vršile kompjuterska krivična dela, tačnije krivično delo „Izrada i upotreba lažne platežne kartice„. Jedna kriminalna grupa ima međunarodni karakter, gde kriminalno deluje pet makedonskih i troje bugarskih državljana, koji su, lažnim platežnim karticama nabavljenim u Bugarskoj, izvršili više nelegalnih transakcija na više bankomata u Republici Makedoniji. Druga kriminalna grupa je sastavljena od osam članova koji su kriminalno delovali u nacionalnim granicama države. Izrada kartica se odvijala u Bugarskoj, kriminalci su nabavili skimer u Bugarskoj, postavili ga na bankomatima u Makedoniji, a onda su skimerom skinuli podatke koji su iskorišćeni pri izradi lažnih platežnih kartica kod stručnjaka u Bugarskoj, pa su potom te kartice upotrebljavali u Makedoniji. Lice iz Bugarske naplatilo je

[11] Puača, D., ,Mandić, I. , Vasić, Ž. i Žorić, A., Organizacija i nadležnost tužilaštva i sudova u borbi protiv kompjuterskog kriminala, Infoten Jahorina, br. 7, mart 2008.

[12] Измена и дополнување на Кривичниот законик, Сл. весник на РМ бр. 114/09, Чл. 274 - б.

[13] Statistički podaci iz analitičke službe MUP-a Republike Makedonije.

izradu kartica pre nego što su bile upotrebljene. Ove dve kriminalne grupe izvršile su devet krivična dela, a prijavljeno je 16 izvršilaca, koji su stekli protivpravnu imovinsku koristi u visini od 3,4 miliona denara ili 55 hiljada eura. Krivična dela su izvršena u Skoplju i Kumanovu.

U 2011. godini u Republici Makedoniji javnom tužiocu su podnete prijave za 13 krivičnih dela ,,Izrada i upotreba lažne platežne kartice,, , a prijavljeno su 23 izvršioca, od kojih je i dvoje Bugara, jedan Grk i jedan Srbin. Stečena je protivpravna imovinska korist u visini od 1,1 milion denara ili 17 hiljada eura. Krivična dela su vršena u Skoplju, Vinici i Đevđeliji. I u 2011. godini krivična dela su izvršila dve organizirane kriminalne grupe, jedna međunarodna, a druga nacionalna. Prva grupa je sastavljena od troje makedonskih i jednog srpskog državljanina, a način kriminalog delovanja je obezbeđenje bankarskih podataka nosioca bankarskih računa i platežnih kartica upotrebom specijalnog uređaja za snimanje u Makedoniji i Srbiji; lažne kartice su upotrebljene za kupovinu zlatnog nakita u Republici Makedoniji, ali kriminalno je delovano i u drugim, susednim državama.

U Republici Makedoniji pre 2010. godine otkriveni su slučajevi kriminalnog delovanja sa identičnim kriminalnim ponašanjem, ali su krivična dela kvalivifikovana pod drugim nazivima, tako da je u 2008. i 2009. godini razjašnjen slučaj kriminalnog delovanja međunarodne kriminalne grupe makednoskih državljana koji su kriminalno sarađivali sa kriminalcima iz Bugarske, Italije, Srbije, a otkriveni su pri izlasku na makedonsko-grčkoj granici. U jednoj od kriminalnih grupa učestvovao je i poznati pevač iz Makedonije. U 2009. godini kriminalci su stekli 22 miliona denara ili 340 hiljada eura, a kriminalno su delovali u više makedonskih gradova: Skoplje, Kumanovo, Strumica, Tetovo, Gostivar, Kavadarci i Ohrid.

U procesu razjašnjavanja, operativni radnici obezbedili su dokaze o kriminalnoj povezanosti kriminalnih grupa i pored osnovnog dela ,,Izrada i upotreba lažne platežne kartice,, , izvršioci su osumnjičeni i za krivično delo ,,Zločinačko udruživanje,,.

Oštećena lica ovim krivičnim delom najčešće su domaći, ali i strani državljani, i to najčešće lica koja imaju registrovani biznis u Republici Makedoniji, ali i druga strana fizička i pravna lica.

REFERENCE

1. Banović, B., Obezbeđenje dokaza u kriminalističkoj obradi krivičnih dela privrednog kriminaliteta, Beograd.
2. Brvar, B., Pojavne oblike zlorabe računalnika, Revija za kriminalistiko in kriminologijo, 2-1982.
3. Computer Crime:Criminal Justice Resurce Manual, 1979.
4. Ignjatović, Đ., Pojmovno određenje kompjuterskog kriminaliteta, Anali pravnog fakulteta, Beograd, 1991, br. 1–3.
5. Јовашевиќ Д. , *Лексикон кривичног права*, ЈП Службени лист СРЈ, Београд, 2002 године.
6. Konstantinović-Vilić S. i Nikolić-Ristanović V., Kriminologija, Niš, 2003.

7. Parker, D., Computer Abuse.
8. Petrović, S., Policijska informatika, kriminalističko policijska akademija, Beograd, 2007.
9. Puača, D., Mandić, I., Vasić, Ž. i Žorić, A., Organizacija i nadležnost tužilaštva i sudova u borbi protiv kompjuterskog kriminala, Infoten Jahorina, br. 7, mart. 2008.
10. Sieber, U., Kompjuterski kriminal i krivično pravo, Kȍln, 1977.
11. Тупанчевски, Н. и Кипријановска, Д., Основи на македонското информатичко казнено право, МРКПК бр. 2–3, 2008 година.
12. Кривичен законик на РМ, Сл. весник на РМ бр. 114/09.
13. Статистички податоци од МВР на РМ.

SUMMARY

Criminal offense, making and using false payment cards, is a form of computer crime, where criminals use knowledge and technical means to achieve criminal profits. Criminals acting in organized criminal groups who know exactly criminal task and criminal profits of each of the offenders, the organizers of the direct perpetrator, one who uses false payment cards. Prosecution authorities no choice but to ostruče and adapt their operational work, a combination of operational measures and the special investigative measures in order to provide electronic evidence.

Prethodno saopštenje - UDK 341.48: [343.326: 004.738.5] (497.6 RS)

PRAVNI I INSTITUCIONALNI OKVIR SUPROTSTAVLJANJA VISOKOTEHNOLOŠKOM KRIMINALITETU U REPUBLICI SRPSKOJ

Doc. dr Nevenko Vranješ
Mr Srđan Rajčević, dipl. inž. rač.
Agencija za informaciono društvo Republike Srpske
nvranjes@blic.net
srajcevic@gmail.com

Apstrakt: Visokotehnološki kriminalitet predstavlja negativnu društvenu pojavu modernog doba koja bilježi značajan rast. Zbog specifičnog objekta (predmeta) i sredstva za izvršenje, ovaj oblik kriminaliteta nema geografsku, vremensku i nacionalnu limitiranost. Kao takav, on zahtijeva energičan, snažan i kontinuiran odgovor stručnih i osposobljenih službi. U tom smislu moraju postojati adekvatni nacionalni i internacionalni subjekti koji mogu odgovoriti izazovima visokotehnološkog kriminaliteta. Pri tome, takvi subjekti ne mogu funkcionisati samostalno i kao izolovane jedinke, te je međunarodna saradnja u ovoj oblasti neminovna i uglavnom se odvija kroz sistem CERT (Computer Emergency Response Team). Treba napomenuti da postojanje ovakvih struktura predstavlja i obavezu države na putu međunarodnih integracija.

Republika Srpska ima uspostavljen pravni i institucionalni okvir suprotstavljanja visokotehnološkom kriminalitetu koji se intezivno gradi i razvija i koji je u poređenju sa drugim entitetom i zemljama okruženja na zavidnom nivou. U radu se, s pravnog stanovišta, predstavljaju i analiziraju formalnopravni i materijalno–institucionalni kapaciteti Republike Srpske u borbi protiv visokotehnološkog kriminaliteta.

Ključne riječi: visokotehnološki kriminalitet, Zakon o informacionoj bezbjednosti, standardi informacione bezbjednosti, Agencija za informaciono društvo Republike Srpske i Odjeljenje za informacionu bezbjednost.

UVODNA RAZMATRANJA

Vrijeme u kojem živimo karakteriše snažna podrška informacionih tehnologija ljudskom mišljenju i razmišljanju te samim tim i odlučivanju. Danas, informacione tehnologije predstavljaju ne samo sredstvo za ostvarivanje ambicioznih ciljeva već i aparat bez kojeg je nezamisliv moderan ljudski život u svim njegovim sferama, od ekonomije, privrede i politike pa do sporta i nauke. Fundamentalna činjenica koja egzistira u „informatičkom dobu“ jeste da informacije imaju znatno veći značaj nego u prethodnim periodima ljudske istorije. U tom smislu, teoretičari i stručnjaci su već odavno pristupili izučavanju termina informatičko ratovanje. U važećim vojnim doktrinama razvijenih zemalja, informacioni prostor ili „infosfera“ podrazumijeva se kao peti borbeni prostor, zajedno sa kopnom, vodom, vazduhom i kosmosom. Nime, vojni stručnjaci smatraju da je „infosfera“ prostor

gdje bi se mogle voditi primarne borbe, i uveliko se pripremaju za takav koncept vođenja ratova. (Džigurski, 2002: 140–141). U tom smislu, a shodno zaključcima Lisabonskog samita, buduća dva ključna pravca NATO sastojaće se u izgradnji raketnog štita, ali i u uspostavljanju *smart defense*, svojevrsnog oblika „pametne odbrane", koja će se ogledati u zaštiti informacionih sistema. (Iklódy, 2010: 4).

Nažalost, kao što je već napomenuto, informatička dostignuća i tehnologije mogu biti sredstvo (subjekat) ali i objekat (predmet) različitih ugrožavanja, koja se najčešće ispoljavaju u vidu visokotehnološkog kriminaliteta. U tom smislu, pojavljuje se i jedna relativno nova (posebna) kategorija kriminala – visokotehnološki kriminal.

Visokotehnološki kriminal obuhvata skup krivičnih djela gdje se kao objekat izvršenja i kao sredstvo za izvršenje krivičnog djela javljaju računari, računarske mreže, računarski podaci, kao i njihovi produkti u materijalnom i elektronskom obliku. Ova definicija uključuje veliki broj zloupotreba informacionih tehnologija, kao i oblast zloupotreba u radio-difuznim tehnologijama. Tako se razlikuju krivična djela gdje su računari pojavljuju kao sredstvo izvršenja (Computer Related Crime) i kao objekat izvršenja (Computer Crime), kao i krivična djela u čijem se načinu izvršenja pojavljuju elementi nezakonitog korišćenja interneta. Broj i vrste krivičnih djela iz oblasti visokotehnološkog kriminala, kao i ekonomsku štetu koja nastaje izvršenjem ovih krivičnih djela, veoma je teško procijeniti. Međutim, broj izvršenja krivičnih djela i ekonomska šteta koja je do sada registrovana iz godine u godinu u stalnom je porastu. Načini izvršenja krivičnih djela, zbog same prirode savremenih informacionih tehnologija, veoma su raznoliki i sve sofisticiraniji.[1]

Visokotehnološki kriminal je našao svoje mjesto i u krivičnom zakonodavstvu u Bosni i Hercegovini i to prvenstveno u Krivičnom zakonu Republike Srpske, a u okviru krivičnih djela protiv privrede i platnog prometa, ali i u okviru posebne kategorije krivičnih djela. Tako, glava 24 Krivičnog zakona Republike Srpske tretira Krivična djela protiv privrede i platnog prometa. U navedenoj grupi krivičnih djela pronalazimo krivično djelo upad u kompjuterski sistem, koje u stavu 1 glasi: „Ko u privrednom poslovanju u namjeri da sebi ili drugom pribavi protivpravnu imovinsku korist ili drugog ošteti, neovlašćeno unese izmjene, sakrije, objavi, izbriše ili uništi tuđe kompjuterske podatke ili programe, kazniće se zatvorom do tri godine".[2] Nadalje, u stavu 2 istog člana definiše se iznos pribavljene imovinske koristi odnosno prouzrokovane imovinske štete, od čije visine zavisi dužina trajanja zatvorske sankcije. Tako, ukoliko je upadom u kompjuterski sistem pribavljena imovinska korist odnosno pričinjena materijalna šteta koja prelazi 10. 000 KM, učinilac će se kazniti zatvorom od šest mjeseci do pet godina, a ako taj iznos prelazi 50. 000 KM, kazniće se zatvorom od jedne do deset godina. Najzad, sam pokušaj izvršenja djela Upad u kompjuterski sistem kažnjiv je prema odredbama stava 3 navedenog člana, za šta zakon (začuđujuće) ne propisuje konkretnu sankciju.

---

[1] *http://www.mup.rs/cms_lat/saveti.nsf/saveti-sajber-kriminal.h*, 17. 02. 2012. godine. O konkretnom primjeru napada na kompjuterski sistem države vidjeti: Aaviksoo, Jaak, 2010. *Cyberattacks Against Estonia Raised Awarness of Cyberthreats*, in Kibaroğlu, Mustafa (edit.), *Defence Against Terrorism Review*, Centre of Excellence-Defence Against Terrorism, Ankara.

[2] *Čl. 271 Krivičnog zakona Republike Srpske*, Službeni glasnik Republike Srpske, br. 49/2003.

Krivična djela protiv bezbjednosti računarskih mreža propisana su glavom dvadeset četiri a., pod naslovom: „Krivična djela protiv bezbjednosti računarskih podataka“. Navedena djela obuhvataju slijedeće: (1) oštećenje računarskih podataka i programa: (2) računarsku sabotažu; (3) izradu i unošenje računarskih virusa; (4) računarsku prevaru; (5) neovlašćeni pristup zaštićenom računaru, računarskoj mreži, telekomunikacionoj mreži i elektronskoj obradi podataka; (6) sprečavanje i ograničavanje pristupa javnoj računarskoj mreži i (7) neovlašćeno korišćenje računara ili računarske mreže.[3]

Analizom navedenih krivičnih djela uočavamo jedan sveobuhvatan pristup koji je ovakvo zakonsko rješenje približio modernim evropskim standardima te napravio inkriminaciju danas frekventinih djela iz oblasti cyber kriminala. Posebnu pažnju privlači i visina propisanih sankcija, koje za krivično djelo računarskih prevara kojima se pribavlja imovinska korist veća od 30.000 KM dosežu do 10 godina zatvora.[4]

AGENCIJA ZA INFORMACIONO DRUŠTVO REPUBLIKE SRPSKE

Agencija za informaciono društvo Republike Srpske osnovana je krajem 2007. godine na osnovu odluke vlade Republike Srpske kao javna ustanova.

Agencija je ovlaštena i zadužena da obavlja sledeće poslove: (1) koordinaciju razvoja informatike i interneta u saradnji sa drugim nadležnim organima u javnoj upravi, školstvu i zdravstvu; (2) predlaže i sprovodi mjere izgradnje informacionih sistema organa lokalne samouprave (skupštine gradova i opština) koje obezbjeđuju komunikaciju sa republičkim organima i primjenu unificiranih programskih rješenja u što većoj mjeri; (3) licenciranje sertifikacionih tijela u infrastrukturi javnih ključeva; (4) izdavanje licenci i sertifikata, konsalting i obuku kadrova državne uprave i davanje stručne ocjene informatičke osposobljenosti istih; (5) koordinira rad na formiranju jedinstvene baze podataka državnih organa i organa lokalne uprave u Republici Srpskoj; (6) definiše koncept interkonekcijskih pravila za informatičku međuoperativnost; (7) stručnu verifikaciju projekata iz oblasti IKT u javnom sektoru, prvenstveno u upravi; (8) razvoj zakonodavstva i pripremanje nacrta propisa i opštih akata u oblasti primjene informatike i interneta u javnoj upravi, poslovnom okruženju i školstvu, i preduzima mjere za njihovo sprovođenje (eLegaslativa); (9) utvrđivanje tehnoloških standarda i standarda procesa rada u oblasti primjene informatike i interneta i preduzima mjere za njihovo sprovođenje; (10) promociju primjene novih tehnologija i kreiranje novih poslova u informacionom sektoru; (11) monitoring propisivanja akata i implementaciju regulative u području infrastrukture i ePoslovanja; (12) prati i savjetuje u vezi s međunarodnim ugovorima koji se odnose na IKT, strana ulaganja u oblasti IKT i sl.; (13) pruža savjetodavnu podršku u oblastima borbe protiv “Cyber” kriminala;

---

[3] *Čl. 56 Zakona o izmjenama i dopunama Krivičnog zakona Republike Srpske*, Službeni glasnik Republike Srpske, br. 73/2010.

[4] *Čl. 292g Krivičnog zakona Republike Srpske,* Službeni glasnik Republike Srpske br. 49/2003, te izmjene i dopune u Službenom glasniku Republike Srpske br. 73/2010.

(14) inicira i koordinira stvaranje razvojnih centara, tehno-parkova i klastereske povezanosti proizvodnje u oblasti IKT; (15) promociju informacionog društva u okviru reforme obrazovnog sistema i koordinaciju implementacije državnih projekata vezanih za učešće IKT u obrazovnom procesu; (16) akreditovanje edukacijskih i ispitnih centara, u saradnji sa Ministarstvom prosvjete i kulture, koji omogućuju sertifikovanje građana u IKT oblasti kroz formu postobrazovanja i doživotnog učenja; (17) utvrđivanje standarda i procedura i davanje saglasnosti za nabavku opreme i programskih rješenja, izvođenje radova i pružanje usluga iz oblasti informatike i interneta za potrebe javne uprave i javnog sektora; (18) razvoj zajedničke računarsko-telekomunikacione mreže državnih organa i drugih informatičkih i internet resursa u vlasništvu Republike Srpske; (19) praćenje razvoja interneta u svijetu, usaglašavanje naših potreba kao i svakodnevna primjena interneta u državnoj upravi, javnom sektoru i poslovanju; (20) razvijanje metodologije, tehnologije i organizacije razvoja informacionih sistema republičkih organa; (21) utvrđivanje standarda i procedura i preduzimanje mjera za obezbjeđenje i zaštitu podataka informacionih sistema; (22) unapređenje dugoročnog planiranja i upravljanja informatičko-telekomunikacionom i internet infrastrukturom; (23) implementaciju i koordinaciju projekata usmjerenih na umanjenje "tehnološkog raskoraka" između BiH i razvijenog svijeta, unutar BiH po entitetima i regionima, kao i između različitih socijalnih grupa u RS; (24) praćenje dostignuća u drugim zemljama ili asocijacijama zemalja iz svog djelokruga i vršenje odgovarajuće harmonizacije; (25) praćenje i podsticanje razvoja industrije informacionih i komunikacionih tehnologija (softver, inženjering, hardver, konsalting), specijalno malih i srednjih preduzeća; (26) promovisanje ravnomjernog razvoja informacionog društva, uključujući udaljena (ruralna) područja i (27) pomaganje dostizanja uslova za evropske i regionalne integracije u području IKT i izgradnje informacionog društva.

Radom i poslovanjem Agencije rukovodi direktor. Za rad Agencije i svoj rad direktor je odgovoran Upravnom odboru i osnivaču. Organizacija Agencije definisana je „Pravilnikom o unutrašnjoj organizaciji i sistematizaciji radnih mjesta". Ovim pravilnikom utvrđuju se unutrašnja organizacija, organizacione jedinice i način njihovog rada, broj zaposlenih, njihove dužnosti i uslovi za vršenje poslova i zadataka, način rukovođenja, kao i ostala pitanja vezana za organizaciju i upravljanje Agencijom. U tom smislu Agencija je strukturirana u četiri odjeljenja, i to: (1) Odjeljenje za razvoj i primjenu elektronskih servisa; (2) Odjeljenje za inženjering i tehničku podršku; (3) Odjeljenje za razvoj, standardizaciju i primjenu informatičkih projekata i (4) Odjeljenje za statističku analizu i praćenje razvoja informacionog društva.

Shodno odredbama Zakona o informacionoj bezbjednosti, te Uredbe o mjerama informacione bezbjednosti, predviđeno je formiranje i petog odjeljenja u sklopu Agencije, tj. Odjeljenja za informacionu bezbjednost (OIB) koje bi formiralo CERT, te u svom radu težišno vršilo poslove zaštite od ugrožavanja i brzih odgovora na ugrožavanja informacione bezbjednosti i kompjuterskih sistema uopšte.

Agencija u vršenju svojih funkcija poštuje i provodi principe zakonitosti, javnosti, odgovornosti, ekonomičnosti, efikasnosti i profesionalne nepristrasnosti.

ZAKON O INFORMACIONOJ BEZBJEDNOSTI

Zakon o informacionoj bezbjednosti predstavlja novinu u pravnom sistemu Republike Srpske. Po svojoj prirodi, nomotehničkom pristupu i strukturi predstavlja jasan, precizan i koncizan organski okvir za uspostavljanje i održavanje informacione bezbjednosti, kako u organima javne uprave Republike Srpske tako i drugim relevantnim subjektima koji za ovim vidom bezbjednosti ispolje potrebu. Treba naglasiti da je zakon prošao punu proceduru od nacrta, javne rasprave i predlaganja do usvajanja u Narodnoj skupštini Republike Srpske, te da je akademska, stručna i ostala javnost imala priliku da učestvuje u njegovom kreiranju. Najzad, usvajanjem ovog zakona prestao je sa važenjem Zakon o onformacionom sistemu Republike Srpske („Službeni glasnik Republike Srpske", broj 38/98) koji je predstavljao arhaičan pravni propis.

Zakon o informacionoj bezbjednosti definiše informacionu bezbjednost kao bezbjednost koja se obezbjeđuje primjenom mjera i standarda informacione bezbjednosti.

Informaciona bezbjedniost preciznije se zakonski određuje članom 2, stav1 Zakona o informacionoj bezbjednosti kao stanje povjerljivosti, cjelovitosti i dostupnosti podataka. Sljedstveno navedenoj definiciji, zakon daje određenje i njenih strukturalnih pojmova: podatak, povjerljiv podatak, cjelovitost podataka i dostupnost podataka.

Pod podatkom se podrazumijeva informacija, poruka i dokument sačinjen, poslat, primljen, zabilježen, skladišten ili prikazan elektronskim, optičkim ili sličnim sredstvom, uključujući prenos putem interneta i elektronske pošte.

Povjerljiv podatak je podatak koji je dostupan samo licima koja su ovlašćena da ostvare pristup ili dalje postupaju sa tim podatkom.[5]

Cjelovitost podatka podrazumijeva očuvanje postojanja, tačnosti i kompletnosti podatka, kao i zaštitu procesa ili programa koji sprečavaju neovlašćeno mijenjanje podatka.

Dostupnost podatka podrazumijeva mogućnost da ovlašćeni korisnici mogu pristupiti podatku uvijek kada za tim imaju potrebu.

Ono što je posebno važno s aspekta informacione bezbjednosti jeste i definisanje pojma CERT. CERT (Computer Emergency Response Team) je međunarodno priznat termin, a podrazumijeva posebnu organizacionu jedinicu za djelovanje u hitnim slučajevima, čiji je zadatak koordinacija prevencije i zaštite od računarskih bezbjednosnih incidenata na internetu i drugih rizika bezbjednosti informacionih sistema organa i drugih fizičkih i pravnih lica.[6]

Posebnu pažnju zakon posvećuje mjerama informacione bezbjednosti, pri čemu propisuje tri vrste mjera informacione bezbjednosti: (1) fizičku zaštitu, (2) zaštitu podataka i (3) zaštitu informacionog sistema.

Fizička zaštita obuhvata zaštitu objekata, prostora i uređaja u kojem se nalaze podaci.

Zaštita podataka obuhvata prevenciju i otklanjanje štete od gubitka, otkrivanja ili neovlašćene izmjene podataka. U tom smislu, propisuju se pravila za

---

[5] Šire vidjeti: *Čl. 4, stav b Zakona o zaštiti tajnih podataka*, Službeni glasnik BiH br. 54/05.

[6] Uporedi: *http://www.businessdictionary.com/definition/computer-emergency-response-team-CERT.html*, 20. 02. 2012. godine.

postupanje s podacima, sadržaj i način vođenja evidencije o podacima i nadzor koji se tiče bezbjednosti podataka.

Zaštita informacionog sistema obuhvata zaštitu podataka koji se obrađuju, skladište ili prenose u informacionom sistemu, kao i zaštitu povjerljivosti, cjelovitosti i dostupnosti informacionog sistema u procesu planiranja, projektovanja, izgradnje, upotrebe, održavanja i prestanka rada tog sistema.

Vezan za primjenjivost Zakona o informacionoj bezbjednosti jeste princip pozitivne i negativne enumeracije primjenjivosti. Tako, odredbe Zakona o informacionoj bezbjednosti primjenjuju: republički organi, organi jedinica lokalne samouprave, pravna lica koja vrše javna ovlašćenja i druga pravna i fizička lica koja ostvaruju pristup ili postupaju sa podacima u elektronskom obliku republičkih organa, organa jedinica lokalne samouprave i pravnih lica koja vrše javna ovlašćenja.

Principom negativne enumeracije odredbe Zakona o informacionoj bezbjednosti ne primjenjuju se u onim slučajevima gdje se drugim zakonima propisuje upotreba dokumenta na papiru i u pogledu podataka čija se informaciona bezbjednost obezbjeđuje u skladu sa propisima kojima se uređuje tajnost podataka.

UREDBA O MJERAMA INFORMACIONE BEZBJEDNOSTI

Uredbom o mjerama informacione bezbjednosti utvrđuju se mjere informacione bezbjednosti kojima se obezbjeđuje osnovna zaštita podataka na fizičkom, tehničkom i organizacionom nivou.

Uredba, kao što je i pravilo, razrađuje cjelokupan zakon.[7] Sljedstveno tome, uredebom se bliže razrađuju zakonom propisane vrste zaštite, i to: fizička zaštita, zaštita podataka i zaštita informacionih sistema.

Mjere informacione bezbjednosti fizičke zaštite sprovode se radi sprečavanja neovlašćenog ili nasilnog ulaska lica u objekte i prostorije u kojima se nalaze podaci odnosno uređaji sa podacima, sprečavanja i otkrivanja zloupotreba podataka od strane zaposlenih kao i otkrivanja i reagovanja na rizike. Mjere informacione bezbjednosti fizičke zaštite obuhvataju: (1) uspostavljanje administrativne zone; (2) izradu plana fizičke zaštite; (3) procjenu efikasnosti mjera fizičke zaštite; (4) kontrolu lica; (5) skladištenje podataka i (6) fizičku zaštitu informacionih sistema.

U pogledu zaštite podataka, uredbom je uređeno da računar za vođenje baze podataka i centralni računar informacionog sistema (server) moraju biti

[7] Suštinski, uredba je podzakonski akt. To je generički naziv za propise slabije pravne snage od zakona, te ih donose, po pravilu, nezakonodavni izvršni i upravni organi, a ukoliko ih donose zakonodavni organi, onda ih donose po postupku različitom od inače složenijeg postupka donošenja zakona. Specifičnost uredbi sa zakonskom snagom ogleda se u tome što one imaju samostalnu egzistenciju, tj. deluju nezavisno od samog zakona. Nastaju u situacijama kada zakonodavna vlast svoju zakonodavnu nadležnost prenosi *de iure* na organe izvršne vlasti. Konkretno, u slučaju SAD, Kongres daje ovlašćenja predsjedniku da ne samo u vanrednim, već i u uobičajenim situacijama donosi ovakve akte. O uredbama sa zakonskom snagom, šire vidjeti: Savić, S.: *Osnove prava*, PPGP «Komes grafika», Banjaluka, 2005, str. 278–279. Takođe vidjeti: Danić, D.: *O uredbama*, Arhiv za pravne i društvene nauke, Beograd 1–6/1939, str. 121, i Dmičić, M.: *Ustavnost i zakonitost i uredbodavna ovlašćenja izvršne vlasti*, Pravna riječ, Časopis za pravnu teoriju i praksu, br. 22/2010, Udruženje pravnika Republike Srpske, Banjaluka, 2010, str. 27–43.

opremljeni: (1) sistemom za bezbjedno prijavljivanje za rad sa mogućnošću evidentiranja ostvarenih pristupa, kako bi se pristup serveru mogao kontrolisati i ograničiti; (2) mehanizmom za sprečavanje neovlašćenog iznošenja i unošenja podataka upotrebom prenosivih informatičkih medija, komunikacionih priključaka i priključaka za ispis podataka i (3) mehanizmom zaštite od računarskih virusa i drugih štetnih programa. Pored navedenog, pristup bazi podataka dozvoljen je samo licima zaduženim za održavanje i razvoj informacionog sistema dok je pristup telekomunikacionom, računarskom i aplikativnom sistemu za obradu podataka, dozvoljen uz upotrebu odgovarajućeg korisničkog imena i pripadajuće lozinke. Najzad, korisničko ime i pripadajuća lozinka ne smiju se otkriti i dati na upotrebu drugom licu.

Zaštita informacionih sistema, prema Uredbi o mjerama informacione bezbjednosti nalaže da računar za vođenje baze podataka i centralni računar informacionog sistema (server) i računarsku mrežu postavlja i ugrađuje stručno lice, u skladu sa projektnom dokumentacijom, važećim normama, standardima i tehničkim uputstvima. U tom pogledu, posebno je važan stav da kontrola upotrebe informacionog sistema podrazumijeva evidentiranje aktivnosti korisnika informacionog sistema, kao i mjere za sprečavanje zloupotrebe informacionog sistema kroz instaliranje sistema za otkrivanje neovlašćenog upada u računarsku mrežu, definisanje, pregledanje i analiziranje zapisa rada informacionog sistema i sprovođenje analiza ranjivosti informacionog sistema.

Pored navedenih mjera informacione bezbjednosti, pomenuta uredba razrađuje i upravljanje rizikom informacione bezbjednosti što podrazumijeva planiranje, organizovanje i usmjeravanje aktivnosti radi obezbjeđivanja uslova da rizici ne ugroze neprekidno funkcionisanje, odnosno poslovanje organa, pravnih i fizičkih lica.

Uredbom o mjerama informacione bezbjednosti prestala je da važi Uredba o mjerama zaštite podataka i informacija u informacionom sistemu republičkih organa i organizacija (Službeni glasnik Republike Srpske", broj 25/04).

ZAKLJUČAK

Republika Srpska ima dosta upotpunjen pravni (zakonski i podzakonski) kao i institucionalni okvir za prevenciju, suprotstavljanje i otklanjanje posljedica visokotehnološkog kriminala. Takođe, bitno je napomenuti da su uspostavljeni kapaciteti kompatibilni sa evropskim zahtjevima i da znatno prednjače u odnosu na Federaciju BiH i zemlje iz okruženja.

Kao ključna institucija zadužena za oblast informatike pojavljuje se Agencija za informaciono društvo Republike Srpske, koja je glavni nosilac informacione bezbjednosti u smislu standarda informacione bezbjednosti, zaštite podataka i odgovora na eventualna ugrožavanja. Institucionalno zaokruživanje ove materije nastupiće skorašnjim formiranjem CERT-a, za šta su stvorene sve zakonske pretpostavke.

Pored Agencije za informaciono društvo, Ministarstvo unutrašnjih poslova Republike Srpske raspolaže posebnom organizacionom jedinicom koja se namjenski bavi problematikom visokotehnološkog kriminala, provodeći Krivični zakon i

druge srodne zakone iz ove oblasti. Tužilaštvo Republike Srpske i Tužilaštvo Bosne i Hercegovine kao i nadležni sudovi, takođe, predstavljaju nezaobilazne subjekte u ostvarivanju informacione bezbjednosti.

U narednom periodu potrebno je uspostaviti čvršću koordinaciju između svih subjekata zaduženih za informacionu bezbjednost, izvršiti edukaciju korisnika podataka, te formirati CERT koji će u što kraćem roku postati dio šire integracije evropskih CERT-ova.

LITERATURA

1. Aaviksoo, Jaak, 2010. *Cyberattacks Against Estonia Raised Awarness of Cyberthreats*, in Kibaroğlu, Mustafa (edit.), *Defence Against Terrorism Review*, Centre of Excellence-Defence Against Terrorism, Ankara.
2. Džigurski, Ozren, 2002. *Informatika*, Fakultet civilne odbrane Univerziteta u Beogradu, Beograd.
3. Iklódy, Gábor, 2010. *The New Strategic Concept and the Fight Against Terrorism: Challenges &* Opportunities, in Kibaroğlu, Mustafa (edit.), *Defence Against Terrorism Review*, Centre of Excellence-Defence Against Terrorism, Ankara.
4. *Krivični zakon Republike Srpske*, Službeni glasnik Republike Srpske br. 49/2003 i 70/2010.
5. *Uredba o mjerama informacione bezbjednosti*, nacrt, 2012.
6. *Zakon o informacionoj bezbjednosti*, Službeni glasnik Republike Srpske, br. 70/2011.

Associate Professor Nevenko Vranješ, PhD
MSc Srđan Rajčević
Agency for Information Society of the Republic of Srpska

LEGAL AND INSTITUTIONAL FRAMEWORK OF CONFRONTING TO CYBER CRIME IN REPUBLIC OF SRPSKA

CONCLUSION

Republic of Srpska has completed a few of legal (law and regulations) and institutional framework to prevent, counter and remove the consequences of cyber crime. Also, it is important that the established capacity compatible with European requirements, and significantly ahead in relation to the Federation of BiH and neighboring countries.

As a key institution responsible for the field of information technology appears to the Agency for Information Society of the Republic of Srpska, which is the main carrier of information security standards in terms of information security, data protection and response to possible threats. Institutional completion of this subject will perform recent establishment of a CERT for what they have created all the legal requirements.

In addition to the Information Society Agency, Ministry of Internal Affairs of the Republic of Srpska has a separate organizational unit that deals with a dedicated cyber crime by implementing the Criminal Law and other related laws in this area. Prosecution of the Republic of Srpska and Prosecution of the Bosnia and Herzegovina, as well, as the responsible courts too, are indispensable actors in achieving information security.

In the future, it is necessary to establish closer coordination between all entities in charge of information security, to educate the users and establish the CERT, which will as soon as possible become a part of a wider European integration CERT.

Prethodno saopštenje - UDK 341.48: 004.738.5(497.11)

EKONOMSKI SAJBER KRIMINAL U SRBIJI – ASPEKT ZAŠTITE INTERNET POTROŠAČA

Doc. dr Branislav Radnović
Univerzitet Educons, Sremska Kamenica, Republika Srbija
Mr Milena Ilić
JP „Gradsko stambeno“, Beograd, Republika Srbija
Nemanja Radović
Srednja škola unutrašnjih poslova – Centar za osnovnu policijsku obuku, Sremska Kamenica, Republika Srbija

Apstrakt: Nastanak i razvoj interneta i kompjutera doneo je brojne prednosti, kako fizičkim, tako i pravnim licima. Međutim, uporedo sa razvojem interneta i kompjutera, razvijali su se i maliciozni programi, i različiti vidovi internet prevara, te je stoga internet doneo sa sobom i veliki broj bezbednosnih rizika. Danas se moderno društvo suočava sa sve većim sajber kriminalom, koji obuhvata različita krivična dela u sajber prostoru protiv pojedinaca, privrednih institucija i države. Sajber kriminal obuhvata široku lepezu protivpravnih aktivnosti, od širenja virusa, neovlašćenog pristupa računarskoj mreži, preko piraterije, zloupotrebe platnih kartica i maloletničke pornografije, ali i ostalih krivičnih dela u kojima se koriste kompjuteri i kojima se narušava bezbednost internet potrošača. Podaci koji se neovlašćeno pribavljaju zloupotrebom informacionih sistema mogu na razne načine poslužiti za sticanje protivpravne koristi. Borba protiv sajber kriminala podrazumeva pre svega veću zaštitu internet potrošača i zahteva jedan ozbiljan pristup, stalni razvoj znanja, različite obuke, praćenja i nabavke savremene bezbednosne opreme potrebne za suzbijanje ove vrste kriminala. Korisnici internet usluga, odnosno internet potrošači, nisu više isključivo mladi ljudi, te se stereotipi o tipičnim korisnicima kao isključivo mladim ljudima menjaju, profil korisnika je sve raznovrsniji, internet više nije elitistički, već populistički medij, te je s tim u vezi borba za zaštitu internet potrošača sve teža. Rad se bavi kategorijom ekonomskog *cyber* kriminala u Srbiji, i aspektom zaštite internet potrošača, određujući i komparirajući profil internet potrošača, u svetu, i u Srbiji, kao i obrađujući najčešće vidove prevara i načinom na koji se domicilno zakonodavstvo sa njima bori.

Ključne reči: visokotehnološki kriminal, internet potrošači, zaštita potrošača, internet prevare

INTERNET POTROŠAČI

Pojam potrošač upotrebljava se da opiše i razgraniči dve vrste potrošačkih jedinica: ljude (građane) kao potrošače i organizacije (preduzeća, institucije) kao potrošače. Postoji i klasifikacija potrošača na individualne i kolektivne, u zavisnosti od toga da li je njihovo ponašanje usmereno na zadovoljavanje ličnih potreba ili se radi o ponašanju od kojeg koristi ima više ljudi ili šira zajednica. Postoji i klasifikacija potrošača na finalne i industrijske kupce.[1]

[1] Milisavljević, M.; Maričić, B.; Gligorijević, M. (2007). Osnovi marketinga, 3. izdanje, Ekonomski fakultet, Beograd.

Potrebe ljudi, odnosno potrebe potrošača se mogu smatrati osnovom savremenog marketinga, odnosno suštinom marketing koncepta, a samim tim ključ za opstanak i rast svake tržišno orijentisane organizacije jeste njena sposobnost da identifikuje i zadovolji nezadovoljene potrebe potrošača, bolje i brže od svojih konkurenata. Organizacije moraju da shvate potrebe i želje potrošača tržišta koje segmentiraju. Činjenica je da ljudi imaju raznolike i brojne potrebe.

Internet prate brojne prednosti, ali i brojni nedostaci.[2] Samo poslovanje na internetu, prema pojedinim autorima, uglavnom se obavlja kroz sledeće procese[3]:

- Prikupljanje informacija
- Marketing i
- Elektronska trgovina

Prikupljanje informacija predstavlja jednu od najznačajnijih poslovnih aktivnosti na internetu. Obavlja se kroz onlajn istraživanja, prikupljanjem primarnih i sekundarnih informacija korišćenjem Interneta i ostalih elektronskih resursa. "Onlajn" istraživanja mogu biti primarna i sekundarna. Primarno istraživanje predstavlja prikupljanje primarnih podataka u *cyber* prostoru (onlajn ankete, praćenje diskusionih grupa, *chat*, virtualne fokus grupe). Sekundarno istraživanje se odnosi na pronalaženje i prikupljanje podataka koji se već nalaze negde na mreži.

Postoji posebna debata između specijalista i akademskih sredina koje se bave e-trgovinom u vezi s odnosom između elektronske trgovine i elektronskog poslovanja. Po jednima, elektronska trgovina obuhvata celokupnu elektronski podržanu aktivnost jedne organizacije, uključujući i sveukupnu infrastrukturu njenog informacionog sistema. Druga strana u ovoj raspravi zastupa stav da e-poslovanje obuhvata sve interne i eksterne elektronski podržane aktivnosti jedne organizacije uključujući i e-trgovinu. Imajući u vidu definiciju elektronske trgovine u kojoj presudnu ulogu ima razmena vrednosti izvan granica jedne organizacije, što nije primarna odlika elektronskog poslovanja, autor ovog rada je bliži stavu da elektronsko poslovanje u opštem slučaju ne obuhvata elektronsku trgovinu. Preciznije, e-poslovne aplikacije se transformišu u e-trgovinu onda kada se u okviru njih pojavljuje razmena vrednosti.

Poseban segment potrošača jesu internet ili tzv. onlajn potrošači. Na samom početku razvoja interneta, korisnici su bili malobrojni, a zabluda o internetu bila je da je on akademski i istraživački alat. Rast novih korisnika kretao se po stopi 60–85%. Danas preko milijardu ljudi ima pristup internetu. Prema podacima najvećeg svetskog internet pretraživača Gugla, Kinezi su prestigli Amerikance po broju korisnika mreže. Tako je krajem 2007. godine Kina imala 219 miliona korisnika interneta, a SAD 216 miliona. Predviđanja su da će kupovina putem interneta u sledećih deset godina dosegnuti 30 posto ukupnih kupoprodajnih transakcija u maloprodaji, što će se odraziti i na poslovanje i tržišni udeo kreditnih kompanija.

Glavne potrošačke onlajn aktivnosti jesu: povezivanje, uživanje, saznavanje i trgovanje. Najčešći predmeti kupovine na internetu jesu putovanja i smeštaj, odeća i sportski rekviziti, knjige, magazini i „*e-learning*" materijali.

Bez obzira o kojoj vrsti poslovanja na internetu je reč, potrošači su sastavni, nezaobilazni segment, koji trpi različite vidove ugrožavanja i zloupotreba.

---

[2] Ilić, M.; Radnović, B.; Radnović, V, (2008). Opasnost slabljenja Internet kapaciteta i upravljanje potencijalnim rizicima", YUPMA 2008. Zlatibor, 231–243.

[3] Filipović, V.; Kostić-Stanković, M. (2007). Marketing menadžment, FON, Beograd, str. 139.

POJAM I OBLICI SAJBER KRIMINALA

Jedan od najvećih izazova modernog društva jeste sajber kriminal. Pod sajber kriminalom podrazumevamo kriminal počinjen uz upotrebu kompjutera ili sličnog sredstva i interneta. Reč je o protivzakonitim aktivnostima koje pojedinac ili grupa koristi za pribavljanje dobara i uvećanje sopstvene koristi. Sajber kriminal obuhvata krivična dela u sajber prostoru protiv ličnosti, protiv imovine i protiv države. Pod sajber prostorom podrazumeva se prostor koji kreiraju kompjuterske mreže. Termin sajber prostor prvi je upotrebio Vilijam Džibson u naučnofantastičnoj noveli *Neuromancer* 1984. godine. Postoji više naziva za sajber kriminal; među njima se posebno ističu termini: internet kriminal, eKriminal, kriminal visokih tehnologija i mrežni kriminal. Sajber kriminal obuhvata široku lepezu protivpravnih aktivnosti, od širenja virusa, neovlašćenog pristupa računarskoj mreži, preko piraterije, do maloletničke pornografije i pljački banaka, zloupotrebe platnih kartica, ali i svih ostalih krivičnih dela u kojima se koriste kompjuteri. Što se tiče sajber prostora, važno je naglasiti da je tu reč o veštačkoj tvorevini koja zahteva visoku tehničku opremljenost i dobru informacionu strukturu. U sajber prostoru paralelno postoje virtuelno i realno, komunikacija je kolektivna. Zato je veoma teško govoriti o nacionalnim razmerama sajber kriminala, koji se, zbog toga, svrstava u oblik transnacionalnog kriminala.

Kod sajber kriminala *cilj napada* su servisi, funkcije i sadržaji koji se nalaze na kompjuterskoj mreži. Reč je o krađi podataka ili identiteta, uništavanju ili oštećenju delova ili celih mreža i kompjuterskih sistema. Cilj počinilaca je mreža u koju se ubacuju virusi, obaraju sajtovi, upadaju hakeri i vrši „odbijanje usluga“. Kada je reč o *alatu*, sredstvima koje moderni kriminalci koriste, važno je naglasiti da oni ne „prljaju“ ruke koristeći mrežu u činjenju dela. Nekada ova upotreba mreže predstavlja potpuno novi alat, dok se u drugim prilikama toliko usavršava da ju je teško i prepoznati. Spominju se i dve varijante: nova dela sa novim alatima i stara dela sa novim alatima. Korišćenje ovog novog oružja naročito je popularno kod dečje pornografije, zloupotreba intelektualne svojine i onlajn prodaje nedozvoljene robe (droge, ljudskih organa, dece, nevesta, oružja i sl.). Kada govorimo o okruženju u kojem se napadi realizuju, to okruženje služi za prikrivanje kriminalnih radnji. Najviše uspeha u tome imaju pedofili, ali ni drugi kriminalci nisu ništa manje uspešni. Što se tiče dokaznih sredstava kod sajber kriminala, tu se kao dokaz kriminalnih radnji mogu pojaviti mreža i ICT.

Kompjuteri i kompjuterska tehnologija se mogu zloupotrebljavati na razne načine, a sam kriminalitet koji se realizuje pomoću kompjutera može imati oblik bilo kog od tradicionalnih vidova kriminaliteta, kao što su krađe, utaje, pronevere, dok se podaci koji se neovlašćeno pribavljaju zloupotrebom informacionih sistema mogu na razne načine koristiti za sticanje protivpravne koristi.

Pojavni oblici kompjuterskog kriminaliteta jesu:

1. *Protivpravno korišćenje usluga* – Podrazumeva neovlašćenu upotrebu kompjutera ili njegovu ovlašćenu uporebu ali za ostvarivanje potreba nekog neovlašćenog korisnika. Primer neovlašćene upotrebe kompjutera jeste kada se kompjuter koristi u bilo koje druge svrhe osim onih koje predstavljaju deo njegove namene u informatičkom sistemu.

Primeri ovlašćene upotrebe kompjutera, ali za potrebe neovlašćenog korisnika, ili radi ostvarenja drugih nedopuštenih ciljeva jesu npr. slučajevi kad

zaposleni u jednoj firmi pribave podatke za budućeg poslodavca ili kad raspoloživo kompjutersko vreme koriste za obavljanje nekih svojih poslova.

2. Neovlašćeno pribavljanje informacija – Ovde je reč o krađi podataka sadržanih u kompjuterskim sistemima, s ciljem ostvarivanja protivpravne imovinske koristi. Neovlašćeno pribavljanje informacija je sa pojavom interneta postalo još veće, tako da mete mogu biti i lični PC računari ali i bilo koji povezani ili izolovani kompjuterski sistem.

3. Kompjuterske krađe – Krađe zauzimaju visoko mesto u oblasti kompjuterskog kriminaliteta i tu je krađa identiteta najzastupljenija. Ova vrsta krađe predstavlja opasnu radnju, jer podriva poverenje u integritet komercijalnih transakcija i ugrožava individualnu privatnost. Krađa identiteta raste sa povećanjem elektronske trgovine. Kradljivci identiteta, snabdeveni individualnim personalnim informacijama, mogu da otvore račune u bankama, obavljaju kupovinu, a u zemljama u kojima su automatizovane servisne usluge za građane mogu da dobiju sertifikate o rođenju, pasoš, kredit... sve to u ime osobe o čijim podacima se radi. Lažnim identitetom kriminalac može da dobije pozajmicu u banci, kupi stan i na taj način finansijski optereti žrtvu. U nekim slučajevima može da joj napravi i kriminalni dosije. Žrtva u većini slučajeva ne zna da se njen identitet koristi sve dok ne dobije račun za naplatu.

4. Kompjuterske prevare – Vrše se u nameri pribavljanja za sebe ili drugog protivpravne imovinske koristi, s tim što se ovde u zabludu ne dovodi neko lice, već se ta zabluda odnosi na kompjuter u koji se unose netačni podaci, ili se propušta unošenje tačnih podataka, ili se na bilo koji drugi način računar koristi za ostvarivanje prevare u krivičnopravnom smislu. Kompjuterske prevare su najrašireniji oblik kompjuterskog kriminaliteta i one daleko dopiru zbog veličine interneta kao tržišta. Kompjuterski prevaranti zloupotrebljavaju upravo one karakteristike sajber prostora koje doprinose rastu elektronske trgovine: anonimnost, distanca između prodavca i kupca i trenutna priroda transkacija. Uz to, oni koriste prednost činjenice da prevara preko interneta ne zahteva pristup do nekog sistema za isplatu, kao što to zahteva svaka druga vrsta prevara i što je digitalno tržiste jos uvek nedovoljno uređeno i kao takvo konfuzno za potrošače, što za njih predstavlja skoro idealne uslove za prevaru.

5. Kompjuterske sabotaže i kompjuterski terorizam – Kompjuterske sabotaže koriste se u uništenju ili oštećenju kompjutera i drugih uređaja za obradu podataka, ili brisanju, menjanju, odnosno sprečavanju korišćenja informacija sadržanih u memoriji informatičkih uređaja. Najčešći vidovi kompjuterske sabotaže jesu oni koji deluju destruktivno na operativno-informativne mehanizme i korisničke programe, najčešće one koji imaju funkciju čuvanja podataka.

Kad je reč o kompjuterskom terorizmu danas, postoji realna opasnost da informatički resursi a posebno globalne informatičke mreže postanu i veoma efikasno sredstvo u rukama terorista. U vremenu koje dolazi teroristi će sve više koristiti visoku tehnologiju za špijunažu i sabotažu, a tako i za propagiranje svojih ideja. Njihovi ciljevi mogu biti banke podataka, računarski resursi, vladini komunikacioni sistemi, rafinerije nafte. Iskustva sa *Al-Quaidom* pokazuju da se pripadnici ove terorističke organizacije služe sofisticiranim tehnikama zaštite svojih kanala komunikacije na internetu, stalno postavljaju nove veb lokacije na kojima propagiraju svoje fundamentalističke ideje, a kod nekih od uhapšnih terorista

pronađeni su kompjuteri sa šifrovanim fajlovima. Ono što povećava opasnost kad je reč o tome da će teroristi u narednom periodu sve više koristiti visoku tehnologiju za ostvarenje svojih destruktivnih ciljeva jesu izvori "talenata" koji mogu da obezbede stručnjake ili specijaliste koji su sposobni da vrše računarsku sabotažu i špijunažu visokog nivoa, da od terorista preuzimaju zadatke po ugovoru, ili da obučavaju teroriste za tajne akcije putem visoke tehnologije.

6. *„Provaljivanje" u kompjuterski sistem* – podrazumeva neovlašćen elektronski upad u centralni kompjuterski sistem i njegovu bazu podataka. Ovakva dela vrše hakeri, koji se preko svojih personalnih računara uključuju u druge informativne sisteme. Hakeri spretno zaobilaze zaštitne mehanizme, a dela ne vrše iz zlonamernih pobuda, već nastoje da javno demonstriraju informatičku veštinu kojom raspolažu ili da ukažu na postojeće slabosti u mehanizmu zaštite kompjuterskih sistema. Na meti hakera najčešće su one kompjuterske mreže za koje se očekuje da su maksimalno zaštićene od elektronskih provala, kao što su: vojne kompjuterske komunikacije, informatički sistemi obaveštajnih službi i državnih institucija. Ovakvi upadi proizvode potencijalnu opasnost prouzrokovanja nepopravljivih šteta na vitalnim kompjuterskim mrežama. U krivičnopravnom smislu, ovakvim se delima vrši povređivanje službene ili vojne tajne, kroz uvid u zaštićene kompjuterske banke informacija.

7. *Kriminal vezan za kompjuterske mreže* – Oblik kriminalnog ponašanja kod koga je sajber prostor okruženje u kome se kompjuterske mreže pojavljuju u trostrukoj ulozi. Prvo kao *sredstvo* ili alat, zatim kao *cilj,* ili *okruženje* izvršenja krivičnog dela. Kompjuterske mreže kao cilj napada – napadaju se servisi, funkcije i sadržaji koji se na mreži nalaze. Kradu se usluge i podaci, oštećuju ili uništavaju delovi ili cela mreža. Kompjuterske mreže kao sredstvo ili alat – moderni kriminalci koriste kompjuterske mreže kao sredstvo za realizaciju svojih namera. Korišćenje ovog sredstva naročito je popularno kod dečje pornografije, zloupotrebe intelektualne svojine ili onlajn prodaje nedozvoljene robe (droga, ljudski organi...).

Različiti dokumenti na različite načine klasifikuju oblike *cyber* kriminala. Tako je na Desetom kongresu UN o sprečavanju zločina i postupanju sa prestupnicima (*Tenth United Nations Congress on the Prevention of Crime and the treatment of Offenders*) održanom 2000. godine, konstatovano da postoje dve supkategorije sajber kriminala.

a) **Sajber kriminal u užem smislu –** kao svako nezakonito ponašanje usmereno na elektronske operacije sigurnosti kompjuterskih sistema i podataka koji se u njima obrađuju;

b) **Sajber kriminal u širem smislu –** kao svako nezakonito ponašanje vezano za ili u odnosu na kompjuterski sistem i mrežu, uključujući i takav kriminal kakvo je nezakonito posedovanje, nuđenje i distribuiranje informacija preko kompjuterskih sistema i mreža.

Od dela sajber kriminala u širem smislu najčešće se pojavljuju: kompjuterski falsifikati, kompjuterske krađe, tehničke manipulacije uređajima ili elektronskim komponentama uređaja, zloupotrebe sistema praćenja kao što su manipulacije i krađe elektronskih kreditnih kartica ili korišćenje lažnih šifri u nezakonitim finansijskim aktivnostima.

Evropska konvencija o sajber kriminalu (*European Union Convention on Cybercrime*) usvojena 2001. godine u Budimpešti predviđa četiri grupe dela:

a. *Dela protiv poverljivosti, integriteta i dostupnosti kompjuterskih podataka i sistema* – nezakoniti pristup, presretanje, uplitanje u podatke ili sisteme, korišćenje uređaja, programa, pasvorda.

b. *Dela vezana za kompjutere* – falsifikovanje i krađe, kao najtipičniji oblik napada.

c. *Dela vezana za sadržaje* – dečja pornografija je najčešći sadržaj koji se pojavljuje u ovoj grupi obuhvatajući posedovanje, distribuciju, čuvanje ili činjenje dostupnim i raspoloživim ovih materijala.

d. *Dela vazana za korišćenje autorskih i srodnih prava* – obuhvataju reprodukovanje i distribuciju neautorizovanih primeraka dela kompjuterskim sistemima.

Sajber kriminal u zavisnosti od tipa počinjenih dela može biti:

1. *Politički* – Tu spadaju sajber špijunaza i sajber sabotaža, haking, sajber terorizam i sajber ratovanje.

2. *Ekonomski* – Sajber prevare (Nigerijska podvala ili pranje novca), krađa internet vremena, krađa internet usluga, piratstvo softvera i mikročipova, sajber industrijska špijunaža, prevarne internet aukcije (neisporučivanje proizvoda, lažna prezentacija proizvoda, lažna procena, trgovina robom sa crnog tržišta, višestruke ličnosti)

3. *Proizvodnja i distribucija nedozvoljenih i štetnih sadržaja:* dečja pornografija, pedofilija, verske sekte, širenje rasističkih, nacističkih i sličnih ideja i stavova, zloupotreba žena i dece.

4. *Manipulacija zabranjenim proizvodima, supstancama i robom*: drogom, ljudskim organima i oružjem.

5. *Povrede sajber privatnosti*: nadgledanje e-pošte, spam, *phiching*, prisluškivanje, praćenje e-konferencija.

Štete nastale vršenjem kompjuterskih delikata, zavisno od pojavnog oblika kompjuterskog kriminaliteta, mogu se podeliti na:

1. *Finansijske* – nastaju kada učinilac vrši delo u cilju sticanja protivpravne imovinske koristi, pa tu korist zaista stekne, ili je ne stekne ali svojim delom objektivno pričini određenu finansijsku štetu.

2. *Nematerijalne* – neovlašćeno otkrivanje tuđih tajni ili drugo indiskretno štetno postupanje.

3. *Kombinovane* – kada se otkrivaju određene tajne, ili povredom autorskih prava, putem zloupotrebe kompjutera ili informatičke mreže naruši nečiji ugled, odnosno povredi moralno pravo a istovremeno prouzrokuje i konkretna finansijska šteta.

INTERNET PREVARE

Najčešći način prevara jeste putem zloupotrebe imejl poruka. Slanjem velikog broja imejl poruka pronalazi se zainteresovana osoba. Posle uspostavljanja prvog kontakta, prevarant sa različitih imejlova šalje poverljive poruke koje treba da uvere potencijalnu žrtvu u opravdanost investicije.

Drugi najčešći način prevara jeste preko onlajn oglasnih tabli. To se čini tako što se u grupe koje komuniciraju na ovaj način ubacuje neko ko „ima informacije“ ili šalje „poverljive poruke“ i na taj način pokušava da podigne cenu akcija.

Kod trećeg načina prevare, sam posrednik, koji vam nudi hartije od vrednosti, nije svestan da je žrtva manipulacije. Manje firme angažuju posrednike da u njihovo ime kontaktiraju s potencijalnim investitorima i da im ponude hartije od vrednosti. To se čini preko vebsajtova, „*chat room*“, diskusionih grupa i onlajn oglasnih tabli. Tako se može dogoditi da firma bude lažna.

Falsifikovani čekovi – plaćanje preko interneta falsifikovanim čekovima. Ovi čekovi često imaju veću vrednost od robe koja se kupuje. Kupac – prevarant šalje falsifikovani ček i traži od prodavca da mu vrati suvišnu sumu na račun u stranoj državi.

Spoofing – tehnika kojom se služe prevaranti koji se predstavljaju preko imejla ili vebsajta koji pripada nekom drugom. Oni najčešće preko imejla šalju link do lažnog vebsajta. Lažni vebsajt izgleda isto kao i orginalni, na kojem je žrtva prijavljena. Prevaranti preko lažnog vebsajta skupljaju šifre za nalog na orginalnom vebsajtu ili brojeve kreditnih kartica.

Lažno predstavljanje – prevarant prisvaja lične podatke neke osobe bez njenog znanja. Prevarene osobe često misle da svoje lične podatke npr. broj kreditne kartice prosleđuju legitimnom servisu. U nekim slučajevima odgovaraju na imejl u kojem su im zatraženi lični podaci radi nastavljanja neke pretplate i slično. Ovo se može izbeći tako što nikada ne upisujete lične podatke ukoliko adresa ne počinje sa https://, i ukoliko sajt ne uliva poverenje.

Prevare s kreditnim karticama – neovlašćeno korišćenje kreditne kartice od strane prevaranta. Do broja kartice je moguće doći preko nesigurnih vebsajtova na kojim se čuvaju brojevi kreditnih kartica od kupaca. Poznat je i *Card-Skimming*, a to je kopiranje podataka sa kreditne kartice na lažnu kreditnu karticu.

Valentino prevare – oblik internet prevara sa najvećom stopom rasta. Sama prevara povezana je s uslugama koje se pružaju usamljenim osobama i imaju za predmet sklapanje brakova ili drugi vid druženja.

Lančana pisma – ovde je reč o takvoj vrsti imejlova u kojima se od vas traži da dobijeni imejl prosledite određenom broju vaših prijatelja. U nekim pismima se navodi da će osobu koja ne prosledi pismo pratiti nesreća, dok se u drugima navodi da će se određenoj osobi (najčešće detetu sa određenom telesnom deformacijom) isplatiti određena suma donacije za svaki imejl koji prosledite. Ova pisma najbolje je uopšte ne čitati, odnosno treba ih brisati, jer ona sadrže kriptovane informacije koje će licu koje je poslalo lančano pismo omogućiti da zloupotrebi vaše lične podatke ali i podatke svake osobe koja pročita lančano pismo.

Veliki broj preduzeća koristi u svom poslovanju internet servise koji pružaju ono što je poznato kao ’softver kao usluga’ (*Software as a Service – SaaS*). Ovakvi servisi pružaju kompanijama priliku da uštede novac i resurse korišćenjem softvera koji su instalirani na veb serverima trećih lica putem interneta. Na ovaj način preduzeća su pošteđena kupovine servera, kao i projektovanja mrežne arhitekture, i omogućeno im je da svoje poslove obavljaju pomoću internet pretraživača. Međutim, i visokotehnološki kriminal se kreće u istom pravcu. Kriminalci iz ove oblasti danas koriste internet servise koji nude upotrebu zloćudnih programa po modelu poznatom kao *Crimeware as a Service (CaaS*), kako bi izvršili krivična dela u virtuelnom okruženju. Oni ne moraju da kupuju i razvijaju svoje servere kako bi koordinisali napade. Umesto toga, oni koriste infrastrukturu koja već postoji. Kriminalci će radije da plaćaju nadoknadu

za korišćenje usluga na ovakvim servisima, nego da gube vreme i troše svoje resurse na razvijanje potrebne infrastrukture. Kao i legalna preduzeća koja plaćaju trećim licima za upotrebu internet servisa koji nude 'softver kao uslugu', i kriminalci iz oblasti visokotehnološkog kriminala plaćaju drugim kriminalcima koji su već razvili mrežnu infrastrukturu i zlćudne programe, kako bi koristili te programe kao uslugu na ovakvim internet servisima. Ti internet servisi pružaju im mogućnost da usmere svoj trud na pojedince ili preduzeća koja žele da napadnu i zbog toga ih kriminalci koji vrše krivična dela iz oblasti visokotehnološkog kriminala sve češće koriste.[4]

EKONOMSKI SAJBER KRIMINAL U SRBIJI

Kada je reč o kompjuterskom kriminalu u Srbiji, treba spomenuti da su najizraženije pojave piraterija, zloupotreba platnih kartica i internet pedofilija. U oblasti borbe protiv ove vrste kriminala u Srbiji, najznačajniji pomak učinjen je osnivanjem specijalizovanih organa na nivou policije, tužilaštva i suda. Zakonom o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala, koji je stupio na snagu 25. jula 2005. godine, osnovano je *Posebno tužilaštvo* u okviru Višeg javnog tužilaštva u Beogradu, *posebno sudsko odeljenje* u Višem sudu u Beogradu i *Služba za borbu protiv visokotehnološkog kriminala* u okviru Ministarstva nadležnog za unutrašnje poslove. Nadležnost navedenih specijalizovanih organa uspostavljena je na celoj teritoriji Republike Srbije, dok je stvarna nadležnost propisana članom 3. navedenog zakona i odnosi se na:

1. krivična dela protiv bezbednosti računarskih podataka određena Krivičnim zakonikom,
2. krivična dela protiv intelektualne svojine, imovine, privrede i pravnog saobraćaja kod kojih se kao objekat ili sredstvo izvršenja javljaju računari, računarski sistemi, računarske mreže i računarski podaci, kao i njihovi proizvodi u materijalnom ili elektronskom obliku, ako broj primeraka autorskih dela prelazi 2.000 ili nastala materijalna šteta prelazi iznos od 1.000.000 dinara,
3. krivična dela protiv sloboda i prava čoveka i građanina, polne slobode, javnog reda i mira i ustavnog uređenja i bezbednosti Republike Srbije, koja se zbog načina izvršenja ili upotrebljenih sredstava mogu smatrati krivičnim delima visokotehnološkog kriminala.[5]

Od kompjuterskog kriminala u Srbiji najizraženija je povreda prava intelektualne svojine. Nove tehnologije, osim značajnog doprinosa unapređenju samih proizvoda, olakšale su mogućnosti kopiranja i izrade plagijata. Značaj zaštite intelektualne svojine intenzivira se ubrzanim razvojem tehnologije i obuhvata pitanja u vezi sa zaštitom autorskog prava, prava na dizajn, patenta, žiga i poslovne tajne.

Intelektualna svojina kao intelektualni kapital svojih nosilaca dobija jednu apsolutno novu dimenziju sa razvojem interneta, a kompjuterski kriminal danas,

[4] Urošević, V. (2009). 'Nigerijska prevara' u Republici Srbiji. Bezbednost, Beograd, 51(3), 145–157.
[5] Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala, "Službeni glasnik RS" br. 61/05, 104/09.

najćešće u različitim vidovima eksponiranja, fokusiran je ka intelektualnoj svojini. Izvršioci ovih krivičnih dela umišljajno postupaju sa namerom da ostvare enormnu protivpravnu imovinsku korist.

Svesni vrednosti intelektualne svojine, potencijala interneta i sofisticiranosti kompjuterskih tehnologija, oni nezakonitim radnjama uslovljavaju egzistiranje krivičih dela koja su po svojoj pravnoj prirodi specifična i zahtevaju studiozni pristup.

Uspešnost borbe protiv kompjuterskog kriminala fokusirane ka pravima intelektualne svojine podrazumeva osnivanje specijalizovane asocijacije koja bi okupila kako informatičke kadrove tako i specijalizovane stručnjake za prava intelektualne svojine, pravne eksperte za kompjuterski kriminal koji će delovati u pravcu studioznog pristupa i urgentnih akcija sprečavanja i borbe protiv kompjuterskog kriminala koji ugrožava prava intelektualne svojine. Glavni dokaz u borbi protiv piraterije jeste forenzičko veštačenje računara, čija je stopa u Srbiji čak 74 odsto.[6]

Globalna rasprostranjenost platnih kartica, njihovog korišćenja i laka dostupnost modernih tehnologija, učinile su ih izuzetno atraktivnim objektom napada kriminalaca. Na meti su nova i nedovoljno razvijena tržišta, bez dovoljno iskustva i u kojima ne postoji sistem za prepoznavanje i sprečavanje zloupotreba. Takvo tržište je potencijalni lak plen za iskusne kriminalce i kriminalne grupe.

Ubrzani razvoj kartičarstva doneo je u Srbiju i kriminal zloupotreba platnih kartica. Na osnovu stanja i kretanja kriminaliteta u ovoj oblasti, Srbiju je uveliko uhvatio talas ovog oblika kriminala.

Osnovni oblici falsifikovanja i zloupotreba platnih kartica jesu:

1. Zloupotreba ukradenih ili izgubljenih kartica;
2. Zloupotreba neuručenih platnih kartica;
3. Neovlašćena upotreba tuđe platne kartice;
4. Pravljenje i korišćenje lažnih platnih kartica;
5. Pribavljanje podataka za pravljenje lažne platne kartice.

Republika Srbija je 16. 4. 2005. godine u Hesinkliju potpisala Konvenciju o visokotehnološkom kriminalu. Takođe je od 2005. godine pa do 2009. godine usvojeno više propisa. Godine 2005. u „Službenom glasniku Republike Srbije“ donet je Ukaz o proglašenju Zakona o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala. Ovim zakonom utvrđuje se obrazovanje, organizacija, nadležnost i ovlašćenja posebnih organizacionih jedinica državnih organa radi otkrivanja, krivičnog gonjenja i suđenja za ova krivična dela. Za postupanje u predmetima nadležno je Više javno tužilaštvo u Beogradu za teritoriju Republike Srbije. U Višem javnom tužilaštvu obrazuje se posebno odeljenje za borbu protiv visokotehnološkog kriminala. Radom posebnog tužilaštva rukovodi posebni tužilac za visokotehnološki kriminal. Takođe, po ovom zakonu u okviru ministartva nadležnog za unutrašnje poslove obrazuje se služba za borbu protiv visokotehnološkog kriminala.

U Beogradu su otvorene dve specijalno opremljene sudnice za sajber kriminal u Višem sudu. Sudnice raspolažu i kabinama za zaštićene svedoke, video-bimom, kao i kabinama za prevodioce i prostorom za novinare.

---

[6] *www.singipedia.com/attachment.php?attachmentid=671&d..*

Srbija je postala još jedna od zemalja u Evropi koja na ovaj način počinje da se bori protiv kompjuterskog kriminala. To su bili sami počeci borbe protiv sajber kriminala. Postojao je samo jedan registrovani veštak za IT tehnologije. Cilj tužilaštva je bio da se uspostavi tzv. centralizacija podataka. Takođe se radilo na proširenju saradnje kako sa policijom, tako i sa provajderima internet usluga.

Iako je Krivični zakonik Republike Srbije zvanično dopunjen i usvojen, tako da može da tereti sajber kriminal, nadležni prebacuju odgovornost i nespremnost za suočavanje sa ovim problemom jedni na druge. Tako, u MUP-u tvrde da su počeli ozbiljno da se bave internet kriminalom, iako još nemaju planiranu jedinicu koja bi se s tim uhvatila u koštac, a za to nisu spremne ni sudske ni izvršne vlasti. Samim sudijama treba mnogo vremena samo da bi savladali osnovnu tehnologiju.

Tek u martu 2009. godine Narodna skupština Republike Srbije je konačno ratifikovala Konvenciju o visokotehnološkom kriminalu i dodatni protokol uz Konvenciju o visokotehnološkom kriminalu koji se odnosi na inkriminaciju dela rasističke i ksenofobične prirode izvršenih preko računarskih sistema.

Godine 2009. reforma pravosuđa u Srbiji dovela je do novih problema, jer je broj tužilaštava prepolovljen. Uspostavljanjem nove pravosudne mreže potvrđeno je da se visokotehnološkim kriminalom bave dva zamenika višeg tužioca u Beogradu koji će biti nadležni za celu Srbiju. U isto vreme, broj krivičnih dela iz ove oblasti se kontinuirano povećava.

U Krivičnom zakoniku Republike Srbije[7] definisani su sledeći pojmovi od značaja za visokotehnološki kriminal:

- računar je svaki elektronski uređaj koji na osnovu programa automatski obrađuje i razmenjuje podatke;
- računarski sistem je svaki uređaj ili grupa međusobno povezanih ili zavisnih uređaja od kojih jedan ili više njih, na osnovu programa, vrši automatsku obradu podataka;
- računarska mreža je skup međusobno povezanih računara, odnosno računarskih sistema koji komuniciraju razmenjujući podatke;
- računarski podatak je svako predstavljanje činjenica, informacija ili koncepta u obliku koji je podesan za njihovu obradu u računarskom sistemu, uključujući i odgovarajući program na osnovu koga računarski sistem obavlja svoju funkciju;
- računarski program je uređeni skup naredbi koji služi za upravljanje radom računara, kao i za rešavanje određenog zadatka pomoću računara;
- računarski virus je računarski program ili neki drugi skup naredbi unet u računar ili računarsku mrežu koji je napravljen da sam sebe umnožava i deluje na druge podatke u računaru ili računarskoj mreži dodavanjem tog programa ili skupa naredbi jednom ili većem broju računarskih programa ili podataka;

U Krivičnom zakoniku u glavi dvadeset sedam, navedena su sledeća dela koja se smatraju krivičnim delom protiv bezbednosti računarskih podataka:

1. oštećenje računarskih podataka i programa – neovlašteno brisanje, izmena, oštećenje, prikrivanje ili drugo delovanje koji čini računarski podatak ili program neupotrebljivim;

[7] Krivični zakonik Republike Srbije, "Službeni glasnik RS" br. 85/05, 88/05, 107/05, 72/09, 111/09.

2. računarska sabotaža – unošenje, uništenje, brisanje, izmena, oštećenje, prikrivanje ili drugo delovanje koje čini da se računarski podatak ili program uništi ili ošteti računar ili drugi uređaj za elektronsku obradu i prenos podataka, sa namerom da onemogući ili znatno omete postupak elektronske obrade i prenosa podataka koji su od značaja za državne organe i druge službe i subjekte;
3. pravljenje i unošenje računarskih virusa;
4. računarska prevara – unošenje netačnih podataka, propust unošenja tačnog podatka ili na drugi način prikrivanja ili lažnog prikazivanja podataka i na taj način uticanja na rezultat elektronske obrade i prenosa podataka, u nameri da sebi ili drugom pribavi protivpravnu imovinsku korist i time drugom prouzrokuje imovinsku štetu;
5. neovlašćeni pristup zaštićenom računaru, računarskoj mreži i elektronskoj obradi podataka;
6. sprečavanje i ograničavanje pristupa javnoj računarskoj mreži;
7. neovlašćeno korišćenje računara ili računarske mreže;
8. pravljenje, nabavljanje i davanje drugom sredstava za izvršenje krivičnih dela protiv bezbednosti računarskih podataka;

Prema Krivičnom zakoniku Republike Srbije, kazne za ovakav oblik kriminala su od novčane kazne do kazne zatvora do 10 godina.

U poslednjih par godina na teritoriji Srbije zaplenjeno je više od sto hiljada diskova pirata.

Krađa identiteta postala je jedna od omiljenih aktivnosti organizovanog kriminala, jer olakšava obavljanje drugih krivičnih dela, od šverca droge preko trgovine oružjem do finansijskih prevara.

Sajber kriminalci kradu novac sa platnih kartica, šire viruse po kompjuterskim sistemima, prave neovlašćene kopije platnih kartica, itd.

Među domaćim sajber kriminalcima veoma su popularne takozvane libijske klopke. To su štipaljke, žabice koje su iste boje kao i automat i koje se gurnu u otvor na bankomatu u koji ulazi kreditna kartica. Kada građanin ubaci karticu da podigne novac, ona u stvari ne uđe u automat, već upada u žabicu. Pošto automat ne registruje karticu, korisnik ne uspeva da podigne novac, ali ni da izvadi karticu. Tada uglavnom prilazi lice koje je i postavilo žabicu, obraćajući se građanima rečima da se to i njemu dogodilo, tražeći pin kod vlasnika kartice. Nakon ukucavanja pin koda, pošto se ništa nije desilo, ovaj upućuje vlasnika kartice da ode do centrale banke i tamo zatraži pomoć. Nakon toga, vadi karticu, ubacuje je u automat i uzima novac.

ZAKLJUČAK

S obzirom na ubrzan razvoj tehnike i tehnologije, a s tim i povećanje broja korisnika računara i interneta kao medija komuniciranja, dolazi i do kvantitativnog i kvalitativnog rasta sajber kriminala. Štete u svetu zbog ovih dela mere se milionima dolara. Dakle, ekonomske posledice sajber kriminala su iz dana u dan sve veće. Ono što je posebno za brigu, jeste da se jedna od grana sajber kriminala odnosi na dečiju pornografiju i pedofiliju, koja je uzela maha i raste iz dana u dan. Sve je više

korisnika ovih sajtova, a žrtve su pre svega deca. Ovde sem ekonomskih, imamo i velike socijalne, psihološke, kulturne i opšte društvene posledice.

Značajna uloga je u pre svega preventivnom delovanju državnih organa i institucija, koje moraju kontinuirano da apeluju na oprez prilikom korišćenja interneta, posebno naglašavajući roditeljima kako uputiti decu na bezbednu upotrebu računara i interneta, kao i da stimulišu kontinuiranu edukaciju o tom pitanju.

Što se tiče borbe protiv sajber kriminala u Srbiji, može se reći da je ona još u razvoju i tek se treba uhvatiti u koštac s ozbiljnim problemima i štetama koje prouzrokuje sajber kriminal, sa svim njegovim varijatetima.

Borba protiv sajber kriminala zahteva ozbiljan pristup celokupnoj tematici, stalni razvoj bezbednosnog znanja, program različitih obuka, praćenje i nabavku savremene tehnologije i opreme i to ne samo od nadležnih organa i institucija koje su uključene u borbu protiv ovog vida kriminala, već i od strane korisnika računara, odnosno internet potrošača.

LITERATURA

1. Filipović, V.; Kostić-Stanković, M. (2007). Marketing menadžment, FON, Beograd
2. Ilić, M.; Radnović, B.; Radnović, V, (2008). Opasnost slabljenja Internet kapaciteta i upravljanje potencijalnim rizicima“, YUPMA 2008. Zlatibor, 231–243
3. Krivični zakonik Republike Srbije, “Službeni glasnik RS” br. 85/05, 88/05, 107/05, 72/09, 111/09
4. Milisavljević, M.; Maričić, B.; Gligorijević, M. (2007). Osnovi marketinga, 3. izdanje, Ekonomski fakultet, Beograd
5. Urošević, V. (2009). ‘Nigerijska prevara’ u Republici Srbiji. Bezbednost, Beograd, 51(3), 145–157.
6. Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala, “Službeni glasnik RS” br. 61/05, 104/09.

RESUME

Because of all the benefits that entails, it has truly changed the way business is done today and the way we communicate. It is because of the diversity and breadth of information offered on the one hand and the way thanks to the development of technology to change this information comes the traditional concepts of education, traditional business, and traditional ways of spending free time.

Disadvantages of the Internet are reflected in the increasing congestion necessary and unnecessary information, which is increasingly occupied by leisure users. Internet is often criticized that information with him sometimes incorrect or socially unacceptable. Also, the internet is an important way of communication in personal and professional life, but it can be misused. One way to misuse the Internet, in addition to sending viruses and spam are different forms of economic abuse, aimed at seizing the material used fraudulently in the form of cyber crime.

As stated in the work, due to cyber crime, which took a mah in Serbia, we must do more to protect internet consumers and requires a serious approach. Essential is the continuous growth of knowledge, different training, monitoring and procurement of modern security equipment necessary to combat this crime.

Key words: High-tech crime, internet consumers, consumer protection, internet scams

Prethodno saopštenje - UDK 343.533: : 004.738.5

ANALIZA FENOMENA KRAĐE IDENTITETA

Doc. dr Zvonimir Ivanović,
KPA, Beograd
Mr Sergej Uljanov,
MUP RS Uprava za međunarodnu operativnu policijsku saradnju,
NCB INTERPOL Beograd, Institut za uporedno pravo Beograd
Dr Vladimir Urošević,
MUP RS SBPOK, Institut za uporedno pravo Beograd

Apstrakt: Sve postojeće aplikacije na socijalnim mrežama zamišljene su kao oblik sredstava za olakšavanje komunikacije i kao socijalne proteze, čime se otvaraju mnoga pitanja. Pitanje privatnosti i zaštite distribucije ličnih podataka je u ovom trenutku u Srbiji (ali i u svetu) takvo da ne postoji adekvatna zaštita koja se može pružiti bilo kome ko svoje lične podatke i prateće informacije objavi na Internetu. Za tako nešto nije neophodna socijalna mreža; posmatrajmo samo sajtove srpskih privrednih subjekata, kod kojih postoji pregršt puteva da se pribave mnoge, veoma privatne i vredne, informacije samo sa stranica o zaposlenima u njima. Ukoliko ovome dodamo i mogućnosti alternativnih oblika pribavljanja informacija, možemo samo zamisliti dimenzije mogućih zloupotreba. Nije teško pretpostaviti, s obzirom na bezbednosne mere koje administratori fejsbuka (ili drugih mreža ili veb 2.0 aplikacija) primenjuju, da se one mogu lako zloupotrebiti na različite načine. Ovo je naročito značajno razmotriti u okvirima aktuelnog stanja u Srbiji u pogledu pravne regulative u zaštiti korisnika Interneta, uopšte, a posebno u okvirima socijalnih mreža, ali i drugih virtuelnih prostora koji mogu otkriti najrazličitije lične i druge podatke i informacije. Svaka informacija ostavljena na internetu nepovratno se arhivira na nekom od krolera, te je u svakom trenutku dostupna, a što je dodatna opasnost za ostavioca (ili možda nekog njemu bliskog). Autori sprovode uporednopravnu analizu u pogledu zaštite od krađe identiteta i ukazuju na moguće implikacije rezultata analize u našem pravnom sistemu.

Ključne reči: Socijalne mreže, veb 2.0 aplikacija, pravna zaštita korisnika interneta, krađa identiteta, mobilne socijalne mreže

UVOD

U savremenim okvirima informacionog društva pojedinac je neznatna jedinka koja čini globalno selo, naročito posmatrano kroz prizmu savremenih socijalnih mreža, kao na primer facebook, flicker ili digg, ili druge mreže ili veb 2.0[1] aplikacije. U pogledu razmera problematike možemo samo ukazati na postojeće

[1] Prvi put ovaj termin je 1999. god. iskoristila Darsi Dinući (Darcy DiNucci) u svom članku „Fragmentarna budućnost“ (Fragmented Future), a kasnije ju je O`Rajli grupa (O'Reilly Media) popularisala. Više o ovome na www.wikipedia.org\veb2.0 dostupnoj 23.01.2010.god.

podatke o jednoj od pomenutih mreža. Istorijat razvoja Facebooka prema brojnosti korisnika[2]:

Mesec i godina	Broj aktivnih korisnika
Decembar 2004.	1.000.000
Decembar 2005.	5.500.000
Decembar 2006.	12.000.000
Oktobar 2007.	50.000.000
Avgust 2008.	100.000.000
Januar 2009.	150.000.000
April 2009.	200.000.000
Jul 2009.	250.000.000
Septembar 2009.	300.000.000
Avgust 2010.	Preko 500.000.000
Decembar 2011.	845 miliona mesečno aktivnih korisnika, 245 miliona dnevno aktivnih korisnika, više od 425 miliona dnevno korisnika mobilnih fejsbuk aplikacija[3]

[3]

Sve postojeće aplikacije na socijalnim mrežama zamišljene su kao oblik sredstava za olakšavanje komunikacije i kao socijalne proteze, čime se otvaraju mnoga pitanja. Pitanje privatnosti i zaštite distribucije ličnih podataka je u ovom trenutku u Srbiji (ali i u svetu) veoma problematično, ne postoji adekvatna zaštita koja se može pružiti bilo kome u ovom momentu ko je spreman, ali možda možemo reći i lakoveran, da svoje lične podatke i prateće informacije objavi na Internetu[4]. Za tako nešto nije neophodna socijalna mreža, posmatrajmo samo firme u Srbiji i njihove sajtove, kod kojih postoji pregršt puteva da se pribave mnoge, veoma privatne i vredne, informacije samo sa stranica kojima se opisuju zaposleni u njima[5]. Ukoliko ovome dodamo još i mogućnosti drugih oblika pribavljanja informacija, kao na primer, jedan od oblika koji se veoma dugo koristi na Zapadu – preturanje po tuđem đubretu, ili na primer, socijalni inženjering[6], možemo samo zamisliti dimenzije mogućih zloupotreba.

---

[2] Izvor: http://www.facebook.com/press/info.php?timeline dostupno 02.02. 2011. Jedan od značajnih pokazatelja aktivnosti na internetu je i da se više od 50% korisnika loguje svakodnevno na FB, kao i da je dostupan na preko 70 svetskih jezika.

[3] http://newsroom.fb.com/content/default.aspx?NewsAreaId=22 poslednji put pristupljeno 20.02.2012. god.

[4] Sa ovim se može porediti i glupost jednog od preduzetnika iz SAD koji je na svom autobusu nosio svoj SSN (Social security number, broj socijalnog osiguranja, koji je osnovno sredstvo identifikacije u SAD). Naravno, on je bio žrtva krađe identiteta.

[5] Dovoljno je videti stranice koje u ime svoje firme a u vezi sa svojim zaposlenim na internetu postavljaju najrazličitiji poslodavci bez adekvatnih uputstava za zaposlene i bez obaveštavanja o mogućim rizicima.

[6] Kojim se na najperfidnije načine izvlače informacije najrazličitijih nivoa tajnosti i značaja od ljudi.

PROBLEMATIZACIJA PREDMETA RADA

Svako od nas dobija najrazličitije oblike privatnih podataka upakovane u različite oblike oblandi – račune koji sadrže naše podatke, čak i one kojih nismo sami svesni (tipa: brojevi ugovora u preptlatničkom odnosu sa mobilnim telefonijama, kao i socijalni kontakti koji predstavljaju naše socijalne krugove[7] – kroz listinge u tim računima i mnogi drugi). Uz prikazano se može nadovezati istraživanje Sophosa[8] u kojem je grupa istraživača, u nameri da prikaže nedostatke socijalnih mreža, njihove mogućnosti zloupotrebe, ali i ljudskih slabosti, kreirala fiktivni lik gumene patkice u jednom ili gumene žabice, u drugom istraživanju, i prijavila se kao prijatelj na socijalnoj mreži određenoj grupi ljudi. Socijalne mreže prepune su najrazličitijih ličnih podataka postovanih na profilima. Ovaj podatak uopšte nije zanemariv. Upravo u ovom trenutku jedan kolega iz Turske sprovodi anketu[9] na Internetu o informacijama koje imaju ličnu konotaciju, i koje predstavljaju osnove prava na privatnost, kao i njihovoj raspoloživosti na socijalnim mrežama (on se opredelio za fejsbuk). Naravno, ova aktivnost je povezana sa „deljenjem“ adekvatne količine informacija sa prihvaćenim kontaktima – prijateljima u socijalnim mrežama, što daje posebnu dimenziju ovom proboju informacija. Opisano se vrši kroz podešavanje opcija privatnosti. Nije teško pretpostaviti, s obzirom na bezbednosne mere koje primjenjuju administratori fejsbuka[10] (ili drugih mreža ili veb 2.0 aplikacija), da se one mogu jako lako zloupotrebiti korišćenjem neznanja i neupućenosti fizičkih i pravnih lica, na različite načine. Dovoljno je proveriti nivo zaštite privatnosti neke

---

[7] Gugl koristi ovaj termin u obliku nadogradnje sopstvene socijalne platforme i bukvalno ih naziva socijalnim gugl krugovima.

[8] http://www.sophos.com/blogs/duck/g/2009/12/14/facebook-privacy-video/ Ovaj istraživački poduhvat dvojice entuzijasta Sofosa predstavlja nastavak prethodnog projekta započetog i preduzetog u Velikoj Britaniji (u pitanju je samo ogranak iste firme Sofosa u VB) kada je glavnu ulogu, u smislu mamca za lakoverne, odigrala gumena žabica. Projekat Fejsbuk sonde (ovako nazvan od strane tvoraca) obuhvata kreiranje fiktivnog lika neke bezazlene dečije igračke, koja je potpuno bezopasna i umiljata (u tom slučaju gumene zelene žabice Freddie Staur 1980), kako ne bi izazvala sumnju korisnika i nuđenje postajanja prijateljem na socijalnoj mreži sa njom, što na prvi pogled biva bezazleno ali otkriva značajne nedostatke ovakve aktivnosti. Ovaj produžetak je obuhvatio stvaranje fiktivnih ženskih likova (dva: Dinette Stonily pedesetak godina starosti kojoj je dodeljen lik mačke koja se igra, i Daisy Feletin rođenu 1988. god. sa likom gumene patkice) i ograničio se teritorijalno na Australiju. Opisani su se pojavili na Internetu i tražili prijateljstvo od po sto ljudi iz njihove starosne grupe. Nakon prvih reakcija postigao se isti rezultat kao u slučaju žabice – 87 lica je prihvatilo prijateljstvo, ali ovog puta se otišlo i dalje petoro dodatnih ljudi se prijavilo niotkuda (bili su prijatelji prijatelja) želeći prijateljstvo sa jednom od pomenutih. Veoma su interesantni rezultati razmene podataka „prijatelja“ nakon postajanja prijateljem, pa tako u grupi od dvadesetak godina starosti svi (njih 100%) su razmenili ili učinili dostupnim personalne adrese elektronske pošte, dok su u starijoj grupi, njih 87%, učinili isto. Sa druge strane, telefonski broj je odalo 23% starijih i 7% mlađih, mlađi su podatke o svojim članovima porodice i prijateljima odali u 46% a stariji u 31% i 89% mlađih pun datum rođenja a 57% starijih. Ovo značajno govori o ljudskoj prirodi ali i mogućnostima zloupotrebe ovakvih medija.

[9] Za onoga koga više interesuje o ovome, anketu i pojednostavljenja uz kontakt može pronaći na sajtu http://facebook-uses.questionpro.com/ dostupnom 18.01.2011.god.

[10] http://www.facebook.com/terms.php?ref=pf dostupan 20.01.2012.god. a poslednji put pravila su revidirana u aprilu 2011.god., a takođe i u vezi sa ovim je politika privatnosti dostupna istog datuma na http://www.facebook.com/policy.php

od ovih socijalnih mreža u tzv. izjavama o privatnosti[11]. U okvirima razmatranja kroz prizmu internet tehnologija, neki autori definišu poverenje kao „volju i želju određene strane da postane ranjiva na aktivnosti druge strane zasnovano na očekivanju da će ta druga strana preduzeti određenu aktivnost značajnu za lice koje je nosilac poverenja, bez obzira na mogućnost nadzora ili kontrole te druge strane"[12]. Poverenje je kritična determinanta za transfer ili protok informacija licem u lice. Poverenje je, takođe, neophodna komponenta za ostvarivanje onlajn socijalnih interakcija[13]. Neka istraživanja ukazuju na to da je poverenje veoma značajna komponenta za razmenu informacija u okvirima elektronske trgovine[14]. Studije slučajeva interpersonalne razmene potvrđuju da je poverenje preduslov samootvaranja, jer ono smanjuje rizik koji sadrži otkrivanje ličnih informacija[15]. Upravo tu i leži problem, poverenje ne dajemo neprijatelju, a svako ko ide sa time da zloupotrebi poverenje ne može biti prijatelj. Treba pomenuti da je privatnost u socijalnim mrežama često neočekivana ili nije definisana, socijalne mreže snimaju sve interakcije zadržavajući ih u cilju potencijalne upotrebe pri socijalnom prikupljanju podataka „data miningu"[16]. Realne socijalne veze ne ostavljaju neki fizički trag u spoljašnjoj sredini, dok se kod digitalnog okruženja one javljaju na svakom koraku. Doskora je san svake obaveštajne službe bio utvrđivanje socijalnih kontakata objekta interesovanja, sada nam socijalne mreže daju ovaj san kao realnost.

SRPSKI ASPEKTI AKTUELIZACIJE PROBLEMA

Sve opisano je naročito značajno razmotriti u okvirima aktuelnog stanja u Srbiji u pogledu pravne regulative u zaštiti korisnika Interneta uopšte, a posebno u okvirima socijalnih mreža, ali i drugih virtuelnih prostora koji mogu otkriti najrazličitije lične i druge podatke i informacije. Neverovatna je količina neopreznosti koja se ovom prilikom manifestuje, od strane najrazličitijih profila korisnika. Poseban aspekt ove problematike vezuje se za dečiju psihologiju i dečje

[11] Dovoljno je samo pokušati da citiramo jedan segment ove izjave (neki je nazivaju politika privatnosti), a fejsbuk administratori smatraju da se njome formiraju principi fejsbuka: „predmet zaštite prava na privatnost neće obuhvatati u socijalnoj mreži (dakle predstavlja javnu informaciju dostupnu svima) podatke koji su postavljeni od strane korisnika (definišući je sopstvenom odgovornošću postavioca informacije) i ne može i neće se pružiti zaštita podacima i oni mogu biti predmet pretrage na pretraživačima, analize drugih i trećih lica i sl." To znači da se pretraživačima ipak u poslednjim izmenama bezbednosnih kriterijuma ograničava mogućnost uključivanja pretraga privatno zaštićenih podataka, ali ostaje gorući problem lica koja nemaju posebno adekvatno znanje engleskog jezika i ne mogu da u potpunosti isprate uslove o kojima se ovde govori.

[12] Mayer, R. C., J. H. Davis, and F. D. Schoorman (1995) "An Integrative Model of Organizational Trust," The Academy of Management Review (20) 3, pp. 709-734 (p. 712)

[13] Coppola, N., S. R. Hiltz, and N. Rotter (2004) "Building Trust in Virtual Teams," IEEE Transactions on Professional Communication (47) 2, pp. 95-104.

[14] Metzger, M. J. (2004) "Privacy, Trust, and Disclosure: Exploring Barriers to Electronic Commerce 9 (4)," Journal
of Computer-Mediated Communication (9) 4.

[15] Ibid.

[16] Dwyer, C. (2007) "Digital Relationships in the 'MySpace' Generation: Results From a Qualitative Study.

delovanje u virtuelnom svetu, naročito kroz nesposobnost dece[17] da shvate značaj prosleđivanja različitih informacija, različitim putevima na internetu (gde tata ili mama radi, kako se njegovi roditelji zovu, koliko godina imaju, kada su rođeni... i sl.). Svaka informacija ostavljena na internetu nepovratno se arhivira na nekom od kraulera, te je u svakom trenutku dostupna, a što je dodatna opasnost za onoga ko ju je tamo ostavio (ili možda nekog njemu bliskog).

Veoma je interesantno opisano razmotriti naročito u svetlu Esee agende i Esee agende plus i strateškom konceptu razvoja elektronske uprave u Srbiji postojanje nedostataka u planiranju mnogih zaštitnih mehanizama u ovom prostoru. Naime, sve opisano može imati značajne implikacije na zaštitu podataka o ličnosti[18], i ne samo kao u primeru kolega iz Australije da će biti relativno lako moguće da se izvadi elektronskim putem vozačka dozvola[19] na lice rođeno 1788. godine, već se mogu veoma brzo i lako stvoriti novi upotrebljivi identiteti, koji se mogu prodavati i koristiti u različitim slučajevima i na najrazličitije načine. Nije od malog značaja činjenica da su mnogi pripadnici srpskog ili drugih bliskih „podzemlja“[20] imali pasoše istih serija, što govori o saradnji organizovanog kriminala na našim prostorima ne poznajući nacionalne granice i, do skora, čak zaraćene strane. No, veoma je problematično na koji način se u Srbiji vezuje identitet lica prema javnim službama, naime, recimo pretrage se u veb baziranom Jedinstvenom informacionom sistemu MUP-a rade najčešće i najtemeljnije preko JMBG (Jedinstvenog matičnog broja građana)[21]. Zloupotrebe ovog podatka su nezamislivih razmera, posebno ukoliko razmotrimo način ophođenja osoblja u mnogim državnim organima sa

---

[17] Ovaj termin je dobro odmeren, jer treba imati u vidu da administratori socijalnih mreža, na primer fejsbuka, dozvoljavaju korišćenje ove socijalne mreže samo licima starijim od 13 godina, a što prema kategorizacijama u svetu i dalje obuhvata populaciju dece (kod nas je do 14 godina), a takođe i druge kategorije maloletnih lica (mlađi 14–16 i stariji 16–18g). Naravno, o njihovim sposobnostima shvatanja značaja sopstvenih akata govori i Krivični zakonik i Zakon o maloletnim učiniocima krivičnih dela i krivičnopravnoj zaštiti maloletnih lica, ali i mnoge teorijske rasprave.

[18] Personalno identifikujuća informacija (engl. Personally Identifiable Information, u daljem tekstu PII), prema OMB Memorandumu 07-16,12 (OMB), jeste “informacija koja se može koristiti da bi se razlikovao ili pratio identitet pojedinca, kao što je njegovo ime, SSN (engl. Social Security Number), biometrijski podaci i druge činjenice, pojedinačno ili kombinovano sa drugim ličnim ili identifikujućim informacijama koje su povezane sa određenim pojedincem, kao što su datum i mesto rođenja, devojačko prezime majke i drugi podaci.” Neki primeri PII koji identifikuju pojedinca jesu (NIST, 2009): ime (ime i prezime, nadimak, devojačko prezime), lični identifikacioni broj (npr. SSN, broj pasoša, broj tekućeg računa i drugo), adresa (ulica ili *imejl* adresa), broj telefona, lične karakteristike (kao što su fotografija lica ili druge karakteristike, otisci prstiju ili druge biometrijske slike). Takođe u PII se ubrajaju i informacije koje su povezane sa nekom od sledećih: datumom rođenja, mestom rođenja, rasom, religijom, zaposlenjem, medicinske, edukativne ili finansijske informacije i druge.

[19] http://www.youtube.com/watch?v=wrnYRPRF36E&feature=player_embedded# dostupan 19.01.2011. god.

[20] http://www.revija92.rs/code/navigate.php?Id=599&editionId=50&articleId=217 dostupan 19.01.2010. god.

[21] On se generiše prema unapred utvrđenim pravilima: prvih sedam cifara označavaju datum rođenja, (dan, mesec, godinu bez prve cifre), sledeće je lokacija rođenja u Srbiji (dva broja), a nakon toga redni broj rođenja u tom danu koji se razlikuje prema polu od nule do petsto – muški i od petsto do hiljadu – ženski, poslednji broj je računarski generisan. Interesantno je ovde napraviti paralelu – većina Amerikanaca (87%) može se jedinstveno identifikovati na osnovu datuma rođenja, petocifrenog poštanskog broja i pola (Malin, B. (2005) Betrayed by my shadow: Learning data identify via trail matching, *Journal of Privacy Technology*, June 2005).

ovim oblikom privatne informacije. Na primer, različiti zdravstveni kartoni dece u obdaništima, u domu zdravlja, socijalnom, Nacionalnoj agenciji za zapošljavanje, poreskoj upravi itd. U ovome može da posluži i analiza skorije donetog Zakona o tajnosti podataka[22] u čijoj glavi VII je u kaznenim odredbama predviđeno krivično delo članom 98. koji glasi:

„Ko neovlašćeno nepozvanom licu saopšti, preda ili učini dostupnim podatke ili dokumenta koji su mu povereni ili do kojih je na drugi način došao ili pribavlja podatke ili dokumenta, a koji predstavljaju tajne podatke sa oznakom tajnosti „INTERNO" ili „POVERLJIVO", određene prema ovom zakonu, kazniće se zatvorom od tri meseca do tri godine. Ako je delo iz stava 1. ovog člana učinjeno u odnosu na podatke označene, u skladu sa ovim zakonom, stepenom tajnosti „STROGO POVERLJIVO", kazniće se zatvorom od šest meseci do pet godina. Ako je delo iz stava 1. ovog člana učinjeno u odnosu na podatke označene, u skladu sa ovim zakonom, stepenom tajnosti „DRŽAVNA TAJNA", učinilac će se kazniti zatvorom od jedne do deset godina. Ako je delo iz st. 1. do 3. ovog člana učinjeno iz koristoljublja ili radi objavljivanja ili korišćenja tajnih podataka u inostranstvu ili je izvršeno za vreme ratnog ili vanrednog stanja, učinilac će se kazniti za delo iz stava 1. ovog člana zatvorom od šest meseci do pet godina, za delo iz stava 2. zatvorom od jedne do osam godina, a za delo iz stava 3. zatvorom od pet do petnaest godina. Ako je delo iz st. 1. do 3. ovog člana učinjeno iz nehata, učinilac će se kazniti za delo iz stava 1. ovog člana zatvorom do dve godine, za delo iz stava 2. zatvorom od tri meseca do tri godine, a za delo iz stava 3. zatvorom od šest meseci do pet godina."

REALNOST

Postoji veliki problem što se u Srbiji ovako opisana informacija ne tretira ni kao podatak sa oznakom interne ni kao podatak sa oznakom službene ili bilo kakve druge tajne. Sa druge strane možemo imati situaciju (ova je slučajno iz života jednog od autora teksta) u kojoj se prema internim pravilima određene institucije neki podaci veoma restriktivno koriste, da to ide čak do sledećih granica: prilikom apliciranja za produžetak dozvoljene pozajmice tekućeg računa (koja se tretira kao kredit) neophodno je da banka primalac zahteva za produženje dobije pozitivan izveštaj kreditnog biroa za zahtevaoca – fizičko lice. Najstrašnije je što je za takav upit kod kreditnog biroa neophodan pristanak klijenta, a onda sledi jedno veliko iznenađenje, nakon što ste dali pristanak da jedan (bilo koji činovnik određene banke – jer nije neophodno da sa tim činjenicama i informacijama barataju posebno obučena lica) radnik date institucije ostvari uvid u skoro celokupan život određenog lica (u pitanju su ukupni prihodi i rashodi, kreditna zaduženost i opterećenje određenog lica kao i određenje njegovih kreditnih jemaca – žiranata ili postojećih hipoteka i ko zna sve čega još), Vi nemate pravo da dobijete primerak ovakvog izveštaja. Ovaj momenat je krucijalan – i pored Vašeg pismenog pristanka da se ovakav izveštaj pribavi iz kreditnog biroa, Vi niste kvalifikovani da ga pregledate ili u bilo kom obliku posedujete! Naravno, gore pomenuti radnik ima i mogućnost da

[22] „Sl. glasnik br.104/09" iz decembra 2009. god.

višestruko zloupotrebi ovakve podatke – od tipovanja za neko imovinsko krivično delo do ucene zbog mogućeg postojanja prikrivenih fondova.

KRAĐA IDENTITETA

Neki ovaj fenomen određuju kao krivično delo. Ono obuhvata[23] takvo krivično delo kod kojeg se neko lice lažno predstavlja kao drugo lice u nameri pribavljanja protivpravne imovinske koristi ili druge lične koristi. Žrtva ili pasivni subjekt ovog dela može biti fizičko ali i pravno lice, kao što i izvršilac može biti pojedinac ili više lica koja su delovi organizovane grupe. Neretko se krađa identiteta koristi kao sekundarno krivično delo kako bi se izvršilo primarno, pojavljuje se kao sredstvo kojim se vrši glavno delo, kako bi izvršilac sakrio svoj trag ili ga zametnuo. Primeri za ovo su prevare sa kreditnim karticama ili u podnošenju lažnih dokumenata za dobijanje kredita na ime lica čiji je identitet ukraden.

Šjolberg[24] navodi da se u osnovi krađom identiteta smatra zloupotreba ličnih podataka drugog lica sa namerom vršenja prevare. U istom dokumentu on navodi da se u novom zakonodavstvu Kraljevine Norveške (u Kaznenom zakoniku iz 2009. god.) izbegava termin krađa i koristi supstitucioni termin „zloupotreba identiteta“. Ovaj Zakonik u čl. 202. navodi da delo čini ono lice koje neovlašćeno drži sredstva identifikacije drugog lica ili deteta drugog lica ili koristi identitet koji se lako može zameniti sa drugom osobom u cilju:

-pribavljanja protivpravne imovinske koristi sebi ili drugome ili

-nanošenja štete ili nelagodnosti drugom licu.

Prema zakonu o krađi identiteta (Identity Theft Assumption and Deterrence Act (the Identity Theft Act; U.S. Public Law 105-318) ovim delom se smatra: „svaki akt lica koje svesno transferuje ili neovlašćeno koristi bilo koje ime ili broj, koji se može koristiti samostalno ili u sprezi sa nekom drugom informacijom, kako bi identifikovao određenu osobu, u nameri da izvrši, pomogne u izvršenju ili navede na neku nezakonitu aktivnost koja predstavlja kršenje federalnog zakona, ili predstavlja krivično delo prema nekom zakonu države članice“.

Čl. 18. U.S.C. § 1028 (a) (7) definiše krađu identiteta kao: „svesno transferisanje, posedovanje ili korišćenje identifikacionih sredstava druge osobe (drugog lica) u nameri vršenja ili pomaganja ili podstrekavanja na vršenje ili drugu vezu sa nezakonitim aktivnostima kojima se stiču okolnosti za izvršenje nekog krivičnog dela propisanog federalnim zakonom ili zakonima država SAD“[25].

Ovime se opisanim normama pokriva širi spektar aktivnosti vezanih sa sredstvima identifikovanja.

---

[23] Teri Bidwell: *Hack Proofing Your Identity in the Information Age* Syngress Publishing, Inc, 2002. str.3.

[24] Materijal za 12. kongres UN u vezi s prevencijom kriminala i krivičnog pravosuđa održan u Brazilu 12–19. 4. 2010, na str. 6.

[25] Navedeno prema: Internet related Identity theft, a discussion paper, prepared by Gercke, M. kao deo Project Cybercrime, Council of Europe, ECD, Directorate General of Human Rights and Legal Affairs. Dostupno na Internetu: http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/default_en.asp dana 20.03.2010.god.

Druga definicija koju daje Federalna trgovinska komisija SAD 15. U.S.C. § 1681a (q) (3) označava krađom identiteta: „korišćenje identifikacione informacije drugog lica". Osnovna razlika jeste u tome da li se misli na prevaru i da li se delo vezuje, u osnovi, za prevaru. Upravo ovo ograničava inkriminaciju i domet u realnom životu kada izvršilac koristi informacije u druge svrhe a ne prevarne. Potonja inkriminacija obuhvata korišćenje informacija a ne i njihovo pribavljanje, čime, recimo, fišing i farming otpadaju iz primene ove norme.

Kod nas se Prlja i Reljanović bave pitanjem određivanja pojma krađe identiteta. Oni u svom radu govore o krađi lika i identiteta i drugi vidovima (ne) zakonitog ponašanja[26]. Oni određuju krađu identiteta (pogrešno je identifikujući kao engl. phishing) kao: "preuzimanje"uloge" nekog lica na internetu, redovno u cilju sticanja neke materijalne ili druge koristi"[27]. Kategorizuju ga i kao: najdrastičniji atak na privatnost ličnosti, jer se učinilac, nakon što je prevarom ili na drugi način došao do vitalnih podataka za preuzimanje nečijeg identiteta (internet i druge šifre, brojevi platnih kartica, i sl.) predstavlja u njegovo ime, zaključuje poslove ili ostvaruje društvene kontakte, ispravno primećujući i da tako može vršiti krivična dela na ovaj način, prikriven iza tuđeg identiteta. Daju i sopstvenu definiciju, po kojoj: krađa identiteta pretpostavlja prethodno izvršenje nekog drugog krivičnog dela (prevare, upada u tuđi računar ili računarski sistem, postavljanje virusa ili drugog štetnog softvera). Ovi autori veoma korektno primećuju da postoje i drugi načini upada u privatan život ljudi, koje oni karakterišu kao "manje ili više kažnjive"[28]:

• Korišćenje tuđih (javnih) podataka. Ovde nije reč o preuzimanju identiteta neke osobe radi ostvarivanja koristi, već o jednostavnom korišćenju javno dostupnih podataka radi stvaranja fiktivnog lica koje se pojavljuje na internetu. Ova aktivnost se svodi na razmenu tuđih slika, rezimea, stavova, koje je osoba pronašla na internetu, kako bi se lakše upoznala sa nekom trećom osobom ili ostvarila cilj socijalizacije na neki drugi način. Ova vrsta aktivnosti (za sada) nije kažnjiva niti u jednoj državi – osim, ukoliko se ne radi o silovatelju ili pedofilu, koji na taj način pokušava da pronađe svoju žrtvu, ali je i tada reč o drugim krivičnim delima, a korišćenje tuđih podataka se javlja samo kao jedno od prethodnih sredstava pripreme za izvršenje.

• Korišćenje elektronskih podataka o aktivnosti lica. Zakoni o zaštiti podataka o ličnosti, koji su standard u pravnim sistemima razvijenih zemalja, jasno određuju kako podaci do kojih dođu različite institucije, organi i drugi subjekti, mogu biti upotrebljeni. Međutim, kao i kod sledećeg primera ustupanja podataka o elektronskim adresama, moguća je zloupotreba prikupljenih podataka o jednom licu. Korišćenjem platne kartice kao sredstva plaćanja, može se, npr., jasno videti šta je jedna osoba kupila, u koje vreme i na kom mestu. Ako neko redovno kupuje određenu vrstu proizvoda, ili koristi neke usluge, može se (neprijatno) iznenaditi – na njegovu kućnu adresu će stići reklamni materijal odgovarajuće sadržine. Ako npr.

---

[26] Prlja, D. Reljanović, M. *Visokotehnološki kriminal – uporedna iskustva, u* Strani pravni život, br. 3/09, str. 161–184, Beograd, na str. 169.

[27] Ibid.

[28] Neki od njih su zaista inkriminisani; o nekima zakoni ćute i oni kao takvi predstavljaju samo moralno neprihvatljivo ponašanje.

redovno kupuje hranu za mačke, dobiće ponude za kupovinu hrane za mačke, uz prateći asortiman drugih proizvoda za životinje. Iako deluje bezazleno, možda čak i kao bezopasan marketinški trik, to zapravo znači da su informacije o transakcijama te osobe dostupne nekome ko ih dalje "ustupa" različitim kompanijama.

• "Prodaja" imejl adresa i spamovanje. Postoji nebrojeno programa čija je jedina svrha slanje što većeg broja elektronskih poruka, kako na računare (putem imejl servisa) tako i na mobilne telefone (putem sms servisa). Ove poruke najčešće imaju reklamni karakter, ali ponekad mogu sadržati i elemente prevarnih imejlova (tzv. "Nigerijsko pismo", i sl.) odnosno poruka kojima se otpočinje komunikacija sa licem radi konačnog cilja izvršenja prevare. Zajednički naziv za sve ove poruke je "neželjena pošta" (engl. spam). Druga strana spama jeste dobijanje neželjene pošte zato što neki od sajtova ili drugih servisa kome osoba ostavi svoju važeću imejl adresu (prilikom registracije, ili u nekom sličnom slučaju) ustupa – besplatno ili za određenu naknadu – spiskove tih adresa različitim kompanijama, koje zatim šalju ogroman broj (pravih ili lažnih) reklama za najrazličitije proizvode. Tu se zapravo vrši (nezakonito) filtriranje – za razliku od automatskog slanja na adrese koje možda nisu aktivne ili čak ni ne postoje, ovde se koriste samo postojeće, aktivne adrese i "obezbeđuje" se pažnja njihovih korisnika. Iako je ovakvo "ustupanje" podataka sasvim sigurno kažnjivo u većini zemalja prema propisima o zaštiti podataka o ličnosti, praktično je nemoguće utvrditi da li je i na koji način neki od sajtova ustupio nečiju imejl adresu. Australija je prva država koja je inkriminisala spamovanje. Irska joj se nedavno pridružila, a s obzirom na trendove narastanja neželjene pošte i na prognoze da će ona u najskorijoj budućnosti imati udeo u ukupnom imejl saobraćaju preko 90%, što čini preko milijardu poruka dnevno[29], moguće je da će i druge države slediti ovaj novozapočeti trend inkriminacije.

• Korišćenje opreme za nadzor i obezbeđenje. Oprema koja je do pre nekoliko godina bila suviše sofisticirana i skupa za opštu upotrebu, masovnom proizvodnjom je postala dostupna velikom krugu korisnika. Televizijske kuće svakodnevno koriste kamere koje su instalirane na lokacijama koje su nepoznate prolaznicima na ulici. Za razliku od saobraćajnih kamera, kao i kamera obezbeđenja, koje se fokusiraju na jedan segment okoline u kojoj se nalaze, i koje imaju društveno koristan cilj i samim tim opravdanje postojanja, kamere do kojih se može doći i preko mnogobrojnih internet sajtova, kao i one koje se koriste u televizijskim programima, omogućavaju veće zadiranje u privatnost ljudi nego što imaju korisnu svrhu. Jedan od problematičnih aspekata ovakve situacije jasno se pokazuje i kroz kontroverzni program koji je lansirala kompanija Google – Google Street View, koji može pokazati slike iz različitih ulica većih gradova širom sveta. Ovaj program se zasniva na realnim slikama ulica „uživo", na kojima se nalaze ljudi, automobili i sl. Koliko se duboko na ovaj način zadire u pravo na privatnost? Možda ne najprecizniji, ali u svakom slučaju zanimljiv odgovor može ponuditi gospođa iz Velike Britanije, koja je pokrenula brakorazvodnu parnicu nakon što je slučajno na snimku jedne od ulica videla parkiran automobil svog muža ispred nepoznate kuće, u vreme kada je on navodno bio na službenom putu[30].

---

[29] Izvor: http://www.junk-o-meter.com/stats/index.php, 20.10.2009.

[30] Izvor: Blic online, Preko Gugla otkrila preljubu, http://www.blic.rs/zanimljivosti.php?id=86407, 20.10.2009. uporediti i sa Prlja, D. Reljanović, M. *Visokotehnološki kriminal – uporedna iskustva, u* Strani pravni život, br. 3/09, str. 161–184. Beograd, na str. 170–172.

Moguće je govoriti o krađi identifikacionih podataka – informacija pravnih i fizičkih lica, ali je moguće prepoznati i krađu virtuelnih likova – identiteta.

Krađe identiteta na osnovu pribavljenih informacija o ličnosti mogu se ostvariti na različite načine. Najčešći u 2007. god.[31] bili su u okviru tri glavne kategorije: kreiranje novih računa (kreditnih kartica, tekućih bankovnih računa, podizanje kredita), zloupotreba postojećih računa (na kojima nisu izdate kreditne i platne kartice) i zloupotreba postojećih uz korišćenje debitnih i kreditnih kartica. Moguće je vršiti i klasična krivična dela pribavljanjem ovakvih podataka, pa se tako mogu kreirati falsifikovane kartice a mogu se i zloupotrebiti podaci iz postojećih[32][33].

Značajan momenat jeste da KZ RS nema posebno predviđeno krivično delo krađe identiteta.

ZAKLJUČAK

Sve navedeno sada može biti iskorišćeno u jednoj fikciji – zamislimo u jednoj značajnoj teoriji zavere[34] da se mnogi koriste sofisticiranim sredstvima za pribavljanje informacija o određenim licima, kako bi zloupotrebili ove podatke. O Vama delove informacija jedna osoba (izvršilac krađe identiteta) može pribaviti sa neke od pomenutih onlajn socijalnih mreža (ukoliko progutamo fikciju o ograničavanju distribucije privatnih podataka, a što je teško zbog mogućeg korišćenja kraulera i takozvane vremenske mašine)[35]. Nakon ovako prikupljenih podataka u našoj fikciji dolazimo do momenta koji je značajan za izvršioca; dalji prodor i povezivanje informacija može biti korišćeno za dalju prodaju na internetu kroz baze podataka, koji su ovako prikupljeni, uz dodatne informacije o obavljenim elektronskim trgovinama, kao i najrazličitije identifikacione informacije za obavljanje transakcija – dakle uz kombinovanje prevara sa kreditnim i platnim karticama. Moguće je i da se ovi podaci koriste na neki od sledećih načina – kroz lične interakcije i pokušaje zloupotrebe pribavljenih informacija putem ucene ili moguće zloupotrebe ovih informacija u cilju klasične krađe identiteta i uz vremenski odloženo zloupotrebljavanje takvih informacija (dakle, ne kroz kreiranje fiktivnih identiteta, već zloupotrebom postojećih).

---

[31] www.ftc.gov/opa/2006/12/fyi0688.htm dostupan 06.05.2010.

[32] Videćemo da se naš zakonodavac u čl. 225. KZ definitivno novim izmenama opredelio za inkriminaciju i podataka koji se mogu zloupotrebiti.

[33] Najčešće prijavljivani su: prevare sa kreditnim karticama (61%), krađe i prevare sa tekućih ili štednih računa (33%); prevare u vezi s računima za telefonske usluge (11%); prevare u vezi s plaćanjem preko interneta (5%) i mejl i drugih elektronskih računa (4%), medicinskog osiguranja (3%) i ostalo (1%). U poslednje vreme došlo je do porasta neklasičnih krivičnih dela koja se vrše pomoću izvršenja krađe identiteta – teroristički akti, akti kojima se omogućavaju ili prikrivaju trgovina ljudima i ilegalne migracije. Podaci preuzeti sa: http://www.ag.gov.au/www/agd/rwpattach.nsf/VAP/%284CA0215 1F94FFB778ADAEC2E6EA865329~ID+Theft+Booklet +-+Protecting+your+Identity.PDF/$file/ ID+Theft+Booklet+-+Protecting+your+ Identity.PDF dostupan 06.05.2010.god. Ali najveći porast beleže dela za koja krađa identiteta predstavlja prethodno delo u svrhu pranja novca, finansiranja terorizma i druga dela organizovanog kriminala.

[34] Koju bismo mogli odrediti kao jedan kriminalistički model.

[35] Moguće je preko ovog sredstva vratiti se u prošlost prema veb stranicama i sa različitih trenutaka u vremenu preuzeti kombinacije podataka koje do određenog trenutka nismo prikrili, osim u pretpostavci da smo takve podatke od prvog momenta na socijalnoj mreži sakrili za širu javnost.

Koliko su ova sredstva poluge osamljivanja čoveka u ovakvom svetu hiperkomunikacije, a koliko ona predstavljaju sredstva koja ogoljavaju čoveka i njegov socijalni krug za neke nepozvane goste u ovu vrstu intime? Naime, prvo čovek u ovakvim okolnostima sve oblike komunikacije ostvaruje u okvirima ovih socijalnih relacija pa, naposletku, nije mu potrebno da se izlaže drugim tipovima komunikacije. Ovako zamišljeno matriks okruženje može voditi potpunom zatvaranju čoveka i gubljenjem potrebe da se ostvari fizički kontakt. Sa druge strane, moguće je i da se na ovaj način olakšava posao određenim strukturama obaveštajnih službi o prepoznavanju socijalnih kontakata i veza određene osobe. Ovde se priča ne završava, veoma značajno je razmotriti i mogućnosti korišćenja vaših personalnih dokumenata i foto i video zapisa istaknutih na internetu upravo uz pomoć ovih veb 2.0 aplikacija. U praksi je veoma učestao oblik korišćenja privatnih i ličnih sadržaja sa interneta na zabranjen način, a neretko, od strane seksualnih predatora, i što je naročito opasno, pedofilskih seksualnih predatora. Ovo posebnu dimenziju dobija kada posmatramo fenomen socijalnih mreža i isticanje najrazličitijih fotografija (dece, obnažene dece na kupanju na moru, i tome slično). Srbija još nema krivično delo krađe identiteta, a zašto?

Sve opisano daje samo jednu široku dispoziciju u kojoj su na udaru skoro svi akteri na vebu: od maloletne dece do starijih lica. Izvršioci su takođe veoma različiti i veoma im je dostupna anonimnost, mogućnost prikrivanja i iskorišćavanja pogodnosti udaljenih lokacija, internacionalne dimenzije i mnoga druga sredstva koja nisu na raspolaganju običnom kriminalcu u realnom svetu. Prema INTERPOL-ovim saznanjima, najrazličitiji su oblici prevara putem interneta, od kojih se i na našim prostorima javljaju neke (koje su već značajno prisutne u drugim delovima sveta):

1. Prevare putem interneta u raznim vidovima, npr. «dobici» na internet lutriji – obično ponude stignu sa adrese iz Velike Britanije ili iz Holandije. Potrebno je samo uložiti hiljadu-dve britanskih funti, pa da se, šatro, aktivira devizni račun na koji će da bude uplaćen dobitak od milion funti. U poslednje vreme jako je aktuelna lutrija svetskog kupa u Južnoj Africi.

2. Molba za ulaganje u rad političke partije u Nigeriji ili za pomoć povratku VIP osobe koja je prognana ili je u bekstvu iz svoje države i krije se u nekoj trećoj državi, a baš bi sa tvojim novcem vratila pravdu, red i poredak u nekoj afričkoj državi (obično se radi o državama u kojima je stanje neposredno posle državnog udara ili vojnog puča i sl.). U tipologijama IC3 ova prevara se naziva investicionim prevarama i kao užu grupu ima prevare sa plaćanjem unapred.

3. Međunarodno pružanje advokatske pomoći i ponuda za paušalno plaćanje takve pomoći. Naravno, advokat je npr. neko iz Kenije ili Nigerije, a baš slučajno živi i radi u Holandiji ili Velikoj Britaniji. Kao što se može zaključiti, i ovo je vid prevare sa isplatom unapred.

Kada se ovakvi slučajevi proveravaju sa nadležnim službama Velike Britanije i Holandije posredstvom INTERPOL-a, odgovor je uvek isti: adrese ne postoje, adrese postoje, ali se na njima nalaze fabričke hale ili stovarišta, vlasnici/korisnici fiksnih odnosno mobilnih telefonskih brojeva ne mogu biti utvrđeni ili su dati telefonski brojevi nekih javnih službi ili muzeja i sl. Navedena imena kontakt-osoba ne prolaze evidencije građana i najverovatnije su izmišljena.

Način suprostavljanja ovoj grupaciji zavisi od sistemske pozicije, naime, nemoguće je svakoj od navedenih ugroženih grupa drugačije prići, a nemoguće

je i dejstvovati linijski po svakom od izvršilaca u svakom trenutku. Kao jedno od mogućih rešenja izdvaja se mogućnost da se na strateškom nivou postave određene bezbednosno bazirane politike i da se uz saradnju sa privatnim sektorom i javnošću predupređuju ovakve rizične dispozicije. Prevencija se može ogledati u edukaciji privatnih korisnika kao ugroženih grupa, ali i edukaciji i uspostavljanju novih poslovnih politika u državnim organima i drugim mogućim metama izvršilaca krađe identiteta. Jedan od mogućih slučajeva pokušaja davanja adekvatnog odgovora na ovaj oblik kriminaliteta jeste adekvatno inkriminisanje krađe identiteta kao krivičnog dela, a sa druge strane i dejstvovanje u oblasti zaštite ličnih podataka na primer uvođenjem novog drugačije formulisanog identifikacionog broja građana.

LITERATURA

1. Dwyer, C. (2007) "Digital Relationships in the 'MySpace' Generation: Results From a Qualitative Study.
2. Coppola, N., S. R. Hiltz, and N. Rotter (2004) "Building Trust in Virtual Teams," IEEE Transactions on Professional Communication (47) 2, pp. 95–104.
3. Uljanov, S. Ivanović, Z. Krađa identiteta u Srbiji – rastući problem, (2011) Evropsko zakonodavstvo, br. 37/38. Vol. 10. str. 271–281.
4. Malin, B. (2005) Betrayed by my shadow: Learning data identify via trail matching, *Journal of Privacy Technology*, June 2005.
5. Mayer, R. C., J. H. Davis, and F. D. Schoorman (1995) "An Integrative Model of Organizational Trust," The Academy of Management Review (20) 3, pp. 709–734 (p. 712)
6. Metzger, M. J. (2004) "Privacy, Trust, and Disclosure: Exploring Barriers to Electronic Commerce 9 (4)," Journal of Computer-Mediated Communication (9) 4.
7. Prlja, D., Reljanović, M., Ivanović, Z. Krivična dela visokotehnološkog kriminala, Institut za uporedno pravo, Beograd (2011).

Internet izvori

1. www.wikipedia.org\veb2.0
2. http://www.sophos.com/blogs/duck/g/2009/12/14/facebook-privacy-video/
3. http://facebook-uses.questionpro.com/
4. http://www.facebook.com/terms.php?ref=pf
5. http://www.facebook.com/policy.php
6. http://www.youtube.com/watch?v=wrnYRPRF36E&feature=player_embedded# http://www.revija92.rs/code/navigate.php?Id=599&editionId=50&articleId=217

SUMMARY

ANALYSIS OF THE IDENTITY THEFT PHENOMENON

All existing applications within social networking sites are intended to be some form of facilitating means of communication, and as like of some form of social prosthetics, this raises a lot of questions. The issue of privacy protection and personal data and their distribution is in this moment crucial for Serbia (and the world) in such way that there isn't adequate protection for it, with the meaning for everyone who publishes this kind of information online. For that sort of problem we do not need social networking sites, let's just consider sites of Serbian business firms, they lack with protecting of personal information and by that means they easily facilitate perpetrators many viable ways in obtaining so much personal and other valuable data, just from the Internet pages (or unsecured databases on them) offering, or often freely displaying, personal data of employees. If we add to previous the possibilities of alternative ways of obtaining information (such as social engineering methods and techniques), we just can imagine magnitude of possible exploiting and abuse types. It is not hard to hypothesize, given the security measures that administrators of facebook (or other networks or veb 2.0 applications) enforce, that it can be easily exploited in various ways. This is very important to explore in actual state of Serbia`s legislation, and that is what the authors are trying to stress out here, law system`s dealing with the issue of protecting the Internet user, especially within social networking online, but also within other virtual spaces which could give various personal and other data. Every kind of data and information bit published on the Internet is irreversible permanently archived in the database of Internet Crawlers and, in that way, it is accessible by anyone, anytime, which makes additional risk for information owner (or someone close to him). The authors are trying to do comparative law analysis of the protection norms of law concerning ID theft with their possible implications in incorporation into legal system.

Keywords: Social networks, Veb 2.0 applications, legal protection of Internet users, identity theft, mobile social networks.

Stručni rad - UDK 004.738.5: [343.326: 006

IMPLEMENTACIJA STANDARDA SERIJE ISO/IEC 27000 KAO MJERA SUZBIJANJA VISOKOTEHNOLOŠKOG KRIMINALA

Dragan Popović
Dragan Vučanović
Risto Lazarević

Apstrakt: Današnje organizacije su nezamislive bez savremenih informacionih sistema. Oni omogućavaju da organizacija efikasno i brzo odgovori na sve zahtjeve korisnika na taj način što svoje informacione resurse povezuje sa svojim klijentima. Da bi se informacije zaštitile, potrebno je prije svega poznavati koncepte i mjere zaštite. Zaštita informacija, očuvanje njihove povjerljivosti, integriteta, raspoloživosti, pouzdanosti, neporecivosti informacija i provjerenost postaju od primarne važnosti za organizaciju. Da bi se ispoštovali koncepti i mjere zaštite informacionih sistema, na globalnom nivou razvijeni su odgovarajući standardi koji pokrivaju ovu oblast. U ovom radu je dat pregled serije standarda ISO/IEC 27000, koji se odnose na menadžment sistema za bezbjednost informacija i dobiti koje ostvaruje organizacija njegovim uvođenjem.

Ključne riječi: informaciona bezbjednost, kompjuterski kriminal, ISO/IEC 27000

UVOD

Stalni razvoj i sve šira primjena informacionih tehnologija neminovno dovodi do toga da je rad današnjih poslovnih organizacija postao zavisan od stanja njihovih informacionih sistema. Sve veća pažnja se posvećuje bezbjednosti infomacija koje se koriste, obrađuju i čuvaju.

Tri osnovna cilja koje informacioni sistem treba da zadovolji sa stanovišta bezbjednosti jesu povjerljivost (confidentiality), integritet (integrity) i raspoloživost (availability). Pod povjerljivošću se podrazumijeva čuvanje informacija od neovlašćenog pristupa. Organizacije trebaju zaštitu protiv malicioznih aktivnosti koje ugrožavaju povjerljivost informacija. Pošto su podaci koji se obrađuju i čuvaju u informacionom sistemu podložni promjenama, pod očuvanjem integriteta podataka podrazumijeva se osiguranje sistema od neovlašćenog ili nepredviđenog mijenjana informacija i procesa na kojima počiva informacioni sistem. Raspoloživost kao treći element informacione bezbjednosti odnosi se na potrebu da su informacije dostupne kad god su potrebne ovlašćenom subjektu. Nedostupnost informacija se negativno odnosi kako na samu bezbjednost tako i na reputaciju vlasnika informacionog sistema.

Razvojem računarske tehnike i tehnologije počeo se razvijati i novi poseban i specifičan oblik kriminaliteta, i to onaj kompjuterski. Koliko je visokotehnološki kriminal u usponu, govori i činjenica da većina nacionalnih policijskih organizacija u svoj sastav uvodi posebne jedinice koje imaju zadatak da sprečavaju i istražuju djela povezana sa sajber kriminalom (cyber crime).

Kako se širi upotreba informacionih tehnologija, raste i broj zloupotreba. Da bi organizacije ili pojedinci mogli da se sistemski štite od kriminalnih aktivnosti koje su usmjerene protiv bezbjednosti informacionih sistema u cjelini ili pojedinih komponenti tog sistema, razvijeni su odgovarajući bezbjednosni standardi. ISO je međunarodna organizacija za standarde i aktuelni ISO standard koji se bavi tematikom informacione bezbjednosti ima oznaku ISO 27000. Dakle, svrha međunarodnih standarda serije ISO/IEC 27000 jeste da pruže pomoć organizacijama svih vrsta i veličina da razviju i primjene sistem za upravljanje bezbjednošću sopstvenih informacija. Ovi standardi se odnose na informacione tehnologije, tehnike zaštite i sistem upravljana bezbjednošću informacija.

Organizacija može svoje poslovanje da uskladi prema normama standarda, ali potpuno puvjerenje u sistem upravljanja bezbjednošću informacionih sistema postiže se sertifikacijom organizacije od strane ovlašćenog sertifikacionog tijela.

Prihvatanjem normi koje standard propisuje i primjenom odgovarajućih alata postiže se osiguranje kritičnih resurna na najbolji način i uz najmanje troškove.

KOMPJUTERSKI KRIMINAL

Razvojem računarske tehnike i tehnologije počeo se razvijati i novi poseban oblik kriminaliteta, i to onaj kompjuterski. Kompjuterski kriminal je usmjeren protiv bezbjednosti informacionih sistema, u namjeri da se sebi ili drugom pribavi korist ili nanese kakva šteta. Ova se krivična djela vrše prikriveno, često bez posebne povezanosti počinioca djela i žrtve. Takođe, ova se djela teško otkrivaju i još teže dokazuju, a često dugo vremena ostaju prikrivena sve dok oštećeni ne pretrpi štetu koja je vidljiva u informacionom sistemu. Kompjuterski kriminal je zapravo visokotehnološki kriminal čiji su počinioci u pravilu veoma obrazovane osobe. Visokotehnološki kriminal obuhvata skup krivičnih djela gde se kao objekat izvršenja i kao sredstvo za izvršenje krivičnog djela javljaju računari, računarske mreže, računarski podaci, kao i njihovi produkti u materijalnom i elektronskom obliku. Broj i vrste krivičnih dela iz oblasti visokotehnološkog kriminala, kao i ekonomsku štetu koja nastaje izvršenjem ovih krivičnih djela, veoma je teško procijeniti. Međutim, broj izvršenja krivičnih djela i ekonomska šteta u stalnom su porastu. Načini izvršenja krivičnih djela, zbog same prirode savremenih informacionih tehnologija, veoma su raznoliki i sve sofisticiraniji. Neki od pojavnih oblika visokotehnološkog kriminala su i kompjuterske sabotaže i kompjuterski terorizam, provaljivanje u kompjuterski sistem te kriminal vezan za kompjuterske mreže.

1. Kompjuterski terorizam i sabotaže

Ovo je vrsta terorizma koji je u stalnom razvoju i sve više će se javljati u budućnosti. Teroristi se služe sabotažama kojima uništavaju ili oštećuju kompjuter i druge uređaje za obradu i čuvanje podataka. Razvoj tehnologije i interneta je omogućio terorističkim organizacijama da djeluju globalno, te da stalno postavljaju nove web stranice na kojima propagiraju svoje ideje i vrbuju nove članove. Generalno, u vremenu koje dolazi teroristi će sve više koristiti visoku tehnologiju kako za spijunažu i sabotažu tako i za propagiranje svojih ideja, a njihovi ciljevi mogli bi biti banke podataka, vladini komunikacioni resursi, rafinerije nafte, aerodromska postrojenja i dr.

2. Upadi u kompjuterski sistem

Ovu vrstu djela uglavnom vrše hakeri, koji se preko svojih računara uključuju u druge informativne sisteme, pri čemu najčešće koriste internet. U početku su hakeri nastojali da javno demonstriraju svoju informatičku vještinu ili da ukažu na trenutne slabosti u zaštiti kompjuterskih sistema. Zato su na meti ovih počinilaca najčešće one mreže za koje se očekuje da budu maksimalno zaštićene od elektronskih upada kao što su informatički sistemi obavještajnih službi, državnih institucija, vojnih komunikacija i dr. U današnje vrijeme hakere uglavnom motiviše profit pa je konačan ishod upada u kompjuterske sisteme ostvarivanje finansijske dobiti. Ovakva krivična djela danas se brzo otkrivanju a trag pošiljaoca obično vodi do običnog korisnika koji nije ni svjestan da je njegov računar upotrijebljen za izvršenje krivično djela. Najveća greška je pretjerana žurba da se prati svaki novi trend u ovoj oblasti, bez analize realnih potreba i obraćanja dovoljno pažnje na bezbjednost sistema.

3. Kriminal vezan za kompjuterske mreže

Ovo je oblik kriminalnog ponašanja kod koga je cyberspace okruženje u kome se kompjuterske mreže pojavljuju u trostrukoj ulozi, i to :

- Kompjuterske mreže kao cilj napada
  Vrši se napad na servise i sadržaje koji su na mreži u cilju krađe podataka i uništavanja dijela ili cijele mreže. Počinitelj u mrežu vrši ubacivanje malware-a, izvršava DOS napade i dr.
- Kompjuterske mreže kao alat ili sredstvo
  Počinitelji koriste mrežu, najčešće internet, kao oruđe u izvršenju krivičnog djela kao npr. dječije pornografije, onlajn prodaje ilegalne robe (droga, trgovina ljudima i dr.) te zloupotrebe intelektualne svojine (nelegalni download sa tzv. torrent sajtova).
- Kompjuterske mreže kao okruženje za realizaciju napada
  Kompjuterske mreže mogu da služe i za prikrivanje ilegalnih aktivnosti, npr. pedofilije ili trgovine ljudima, gdje se kriminalci ili kriminalna organizacija kriju iza pseudonima neke legalne ličnosti ili kompanije. Kompjuterske mreže takođe mogu služiti i kao sredstvo zastrašivanja, što uveliko koriste terorističke organizacije.

PREGLED ISO/IEC 27000 SERIJE STANDARDA I SVRHA NJIHOVE IMPLEMENTACIJE U INFORMACIONI SISTEM

Svrha međunarodnih standarda serije ISO/IEC 27000 jeste da pruže pomoć organizacijama svih vrsta i veličina da razviju i primijene sistem za upravljanje bezbjednošću sopstvenih informacija i da se pripreme za nezavisno i nepristrasno ocjenjivanje (sertifikaciju) tog sistema primijenjenog na zaštitu informacija.

Ova serija obuhvata sljedeće standarde :

- *ISO/IEC 27000:2009,* Information security management system – Overview and vocabulary *Daje opšti prikaz sistema menadžmenta bezbjednošću informacija i definiše odgovarajuće termine. Svrha ovog standarda je da specifikuje fundemantalne principe, koncepte*

i termine za seriju dokumenata ISO/IEC 27000. Standard daje pregled standarda ISO/IEC 27000, pokazujući kako se oni koriste za planiranje, implementaciju, certifikaciju i rad sa ISMS, sa osnovnim informacijama o bezbijednosti informacija, upravljanju rizikom i upravljanju sistemom.

- *ISO/IEC 27001:2005,* Information security management system – Requirements *Definiše model za uspostavljanje, primjenu, funkcionisanje, održavanje i poboljšanje sistema menadžmenta bezbjednošću informacija. Da bi se izvršila sertifikacija sa ovim standardom, potrebno je zadovoljiti nekoliko uslova. Neki od tih uslova su i angažovanje dovoljnog broja ljudi na projektu, jasno definisani ciljevi i opseg djelovanja, detaljno napisana ISMS politika i izvještaj o izvršenoj procjeni rizika, implementacija kontrola i procedura, obuka korisnika, uvođenje i nadgledanje ISMS-a, te korektivne i preventivne akcije na informatičkom sistemu.*
- *ISO/IEC 27002: 2005 (prethodno BS 7799 -1 i ISO/IEC 17799),* Code of practice for information security management. *Definiše pravila dobre prakse upravljanja bezbjednošću informacija, odnosno obezbjeđuje specifične savjete i uputstva za kontrolisanje ISMS kao podršku ISO/IEC 27001. ISO/IEC 27002 : 2005 definiše jedanaest glavnih sigurnosnih kategorija, i to:*
  1. Sigurnosna politika (eng. Security Policy),
  2. Organizacija informacione sigurnosti (eng. Organizing Information Security),
  3. Upravljanje resursima (eng. Asset Management),
  4. Sigurnost ljudskih resursa (eng. Human Resources Security),
  5. Fizička sigurnost (eng. Physical and Environmental Security),
  6. Upravljanje komunikacijama i operacijama (eng. Communications and Operations Management),
  7. Kontrola pristupa (eng. Access Control),
  8. Nabavka, razvoj i održavanje informacionih sistema (eng. Information Systems Acquisition, Development and Maintenance),
  9. Upravljanje sigurnosnim incidentima (eng. Information Security Incident Management),
  10. Upravljanje kontinuitetom poslovnih procesa (eng. Business Continuity Management)
  11. Usklađenost sa zakonskim i drugim propisima (eng. Compliance).

  Svaka od navedenih 11 sigurnosnih kategorija definiše sigurnosne ciljeve koje treba ispuniti (eng.control objectives), te kontrole (eng. controls) koje se mogu primijeniti za ispunjenje tih ciljeva. Standard ukupno definiše 36, odnosno 37 ciljeva i 127 mogućih kontrola za njihovo ispunjavanje.
- *ISO/IEC 27003,* Information security management system implementation guidance *Obezbjeđuje uputstvo za procesno orijentisani pristup i uspešnu primjenu ISMS skladu sa ISO/IEC 27001. On opisuje procese specifikacije i dizajna ISMS od početka do implementacije plana projekta. Obuhvata primarne aktivnosti pripreme i planiranja*

aktivnosti sve do stvarne implementacije te daje ključne elemente u upravljanu i finalnoj autorizaciji za nastavak projekta. Vrši procjenu rizika informacione sigurnosti i plan rješavanja opasnosti od rizika, projektovanje ISMS-a i planiranje i implementaciju projekta.

- *ISO/IEC 27004,* Information security management system – Measurement. *Daje uputstva i savjete kako sprovesti mjerenja u cilju ocjene efektivnosti ISMS. To uključuje politike, upravljanje rizikom informacione sigurnosti, kontrole, procese i procedure te podržavanja procesa njihove revizije, pomažući da se utvrdi da li bilo koji od ISMS procesa ili kontrola treba promijeniti ili poboljšati. Standard je prilično detaljan u smislu vršenja mjernih procesa. Opisuje kako prikupiti "osnovne mjere", koristi agregaciju i matematički proračun za generisanje "izvedenih mjera", a zatim primjenjuje analitičke tehnike i kriterije odlučivanja da se kreiraju "smjernice" za upravljanje ISMS procesom.*
- *ISO/IEC 27005:2008,* Information security risk management. *Daje uputstva za ISMS metode i tehnike upravljanja rizikom kao podrška ISO/IEC 27001. Ovaj standard ne preporučuje nijednu konkretnu metodu za analizu rizika, ali objašnjava strukturan i simetričan proces od analize rizika do kreiranja plana za kontrolu rizika. On opisuje procjenu rizika informacionog sistema, tretiranje rizika, prihvatanje rizika, monitoring i izvještavanje o riziku.*
- *ISO/IEC 27006:2007,* Requirement for bodies providing audit and certification of information security system. *Daje zahtjeve, za akreditaciju za sertifikaciona tijela koja sertifikuju ISMS prema ISO/IEC 27001 zahtjevima. On je prvenstveno namijenjen za podršku sertifikacionim tijelima koja provode ISMS sertifikaciju.*
- *ISO/IEC 27007,* Guidelines for information security management systems auditing. *Daje uputstva za interne i eksterne provjere ISMS i program provjera u skladu sa standardom ISO/IEC 27001. Standard obuhvaća ISMS specifične aspekte za reviziju kao što su uspotavljanje ISMS programa revizije (određivanje šta treba revidirati, kada i kako, dodjeljivanje odgovarajućih revizora, upravljanje rizicima revizije, izrada evidencije revizije, kontinualni procesi poboljšanja), obavljanje ISMS revizije (revizija procesa – planiranje, vođenje, ključne revizorske aktivnosti, uključujući i terenski rad, analize, izvještavanje), upravljanje ISMS revizorima.*

Implementacija ISO 27000 serije standarda podrazumijeva dokaz o tome da se u određenom sistemu bezbjedno upravlja informacijama. Sistematskim pristupom i uspostavljanjem sistema menadžmenta bezbjednošću informacija u skladu sa standardom ISO/IEC 27001:2005 ostvaruje se povjerenje u sigurnost i pouzdanost potrebnih informacija. Pouzdanost i poverenje, u sam sistem menadžmenta bezbjednošću informacija, s druge strane, postiže se njegovom sertifikacijom.

Svaka organizacija koja radi sa informacijama, a gotovo da ne postoje one koje ne koriste informacije i informacione sisteme u svom radu, mora da dokaže svojim klijentima da ne postoji curenje informacija, da je sa stanovišta bezbjednosti informacija obezbedila kako informatičku tako i fizičku zaštitu podataka.

Međunarodno priznati standardi, po kojima se može izvršiti sertifikacija od strane tijela koja su priznata po međunarodnoj šemi sertifikacije, predstavlja prije svega zahteve koji se moraju ispuniti kako bi organizacija bezbjedno funkcionisala sa stanovišta, zaštite informacija i dr.

Definisanje novih postupaka rada sa informacijama, dokumentovanje tih istih postupaka, odnosno obezbjeđenje svih zahtjeva koje standard traži jeste projekt koji iziskuje određeno vrijeme i angažovanje svih resursa organizacije.

PRIMJER PRIMJENE STANDARDA ISO/IEC 27000

U ovom radu daćemo konkretan primjer primjene standarda ISO/IEC 27005 na informatičku mrežu jedne organizacije, s posebnim osvrtom na otkrivanje rizika pomoću *penetration* testova. Standrad ISO/IEC 27005 sadrži proces upravljana rizikom informacione sigurnosti i aktivnosti tog procesa. Upravljanje rizikom informacione sigurnosti treba pridonijeti identifikaciji rizika, procijeni rizika, određivanju prioriteta za obradu rizika, određivanju akcija za smanjenje rizika, redovnom nadgledanju i pribavljanju informacija za unapređenje pristupa upravljanju rizikom. U standardu ISO/IEC 27001:2005 opisani su pojedini elementi sistema upravljanja sigurnošću informacija i procesi uspostave takvog procesa u praksi, i to u obliku Demingovog kruga PDCA (Plan-Do-Check-Act). U sledećoj tabeli su date bitne aktivnosti standarda ISO/IEC 27005 u svakoj od četiri faze ISMS procesa.

Tabela 1.-Svrstavanje procesa upravljanja rizikom informacione sigurnosti u ISMS

ISMS proces	Proces upravljanja rizikom sigurnosti informacija
Plan (plan)	Utvrđivanje konteksta Procjena rizika Razvoj plana za obradu rizika Prihvaćanje rizika
Uradi (do)	Implementacija plana za obradu rizika
Provjeri (check)	Kontinualno nadgledanje i osvrt na rizike
Djeluj (act)	Održavanje i poboljšanje upravljanja rizikom informacione sigurnosti

Prije svega, potrebno je prikupiti sve informacije potrebne za utvrđivanje konteksta upravljanja rizikom sigurnosti informacija. Utvrđivanjem konteksta postavljaju se osnovni kriteriji potrebni za upravljanje rizikom sigurnosti informacija, granice djelovanja, te uspostavljanje odgovarajuće organizacije za upravljanje rizikom informacijske sigurnosti.

Procjena rizika određuje vrijednost informacione imovine, identifikuje moguće prijetnje i ranjivosti koje postoje ili bi mogle postojati, identifikuje postojeće kontrole i njihov efekat na identifikovani rizik, određuje moguće posljedice i daje prioritete izvedenim rizicima i rangira ih prema kriterijumu za ocjenu rizika koji je definisan u kontekstu. Metodologija procjene može biti kvalitativna ili kvantitivna,

zavisno od okolnosti, ili njihova kombinacija. Kvalitativna procjena koristi ljestvicu kvalifikovanih atributa za opisivanje veličine potencijalnih posljedica i vjerovatnost da će se te posljedice pojaviti. Postoji veliki broj kvalitativnih metoda procjene a mi ćemo u ovom radu koristi metodu matrice predefinisanih vrijednosti.

Matrica predefinisanih vrijednosti za procjenu rizika koristi tri parametra: vrijednost resursa, prijetnje i ranjivost. Svaki od tih parametara posmatra se u odnosu na moguće posljedice, dok se prijetnje posmatraju u odnosu na odgovarajuće ranjivosti. Svi parametri se kvantuju proizvoljno. Mi ćemo uzeti da se za vrijednosti resursa koriste numeričke vrijednosti u rasponu od 1 (mala) do 5 (vrlo velika), a za kvantifikaciju ranjivosti i prijetnji raspon od 1 (nizak nivo) do 3 (velik nivo). Vrijednost rizika se određuje prema formuli:

$$R=AV+V+T$$

gdje je AV (Asset Value) vrijednost resura, T (Threat) prijetnja i R(Vulnerability) ranjivost. Rizik se može računati prema sljedećoj tabeli.

Tabela 2. - Tabela za računanje rizika

	Prijetnja	1			2			3		
	Ranjivost	1	2	3	1	2	3	1	2	3
Vrijednost resursa	1	3	4	5	4	5	6	5	6	7
	2	4	5	6	5	6	7	6	7	8
	3	5	6	7	6	7	8	7	8	9
	4	6	7	8	7	8	9	8	9	10
	5	7	8	9	8	9	10	9	10	11

Uzećemo da je nivo rizika za vrijednosti 3,4 i 5 nizak, za vrijednosti 6,7 i 8 srednji i za vrijednosti 9,10 i 11 visok.

Da bi se utvrdila vrijednost resursa, neophodno je prvo utvrditi kojom imovinom raspolaže organizacija. Imovina je sve što posjeduje vrijednost za organizaciju. Nakon identifikovanja imovine, potrebno je odrediti prijetnje koje mogu naštetiti imovini, kao što su informacije, procesi i sistemi, a samim tim i organizaciji. Prijetnje mogu biti prirodne ili ljudske i mogu biti slučajne ili namjerne. Za svaku prijetnju treba biti identifikovan izvor. Sledeći korak je identifikacija ranjivosti. Ranjivosti mogu biti identifkovane u sledećim područjima: organizaciji, procesima i procedurama, rutinama upravljanja, osoblju i fizičkoj okolini (konfiguraciji informacionog sistema, hardveru, softveru, komunikacijskoj opremi). Pristutnost ranjivosti ne izaziva štetu sama od sebe, budući da je potrebna prijetnja da bi je iskoristila. Ranjivost koja nema prijetnju ne zahtijeva implementaciju kontrole, ali bi trebala biti prepoznata i praćena zbog promjena. Treba biti zabilježeno da nekorektno implementirana ili neispravna kontrola ili kontrola koja se koristi nekorektno može postati ranjivost. Takođe, prijetnja koja nema odgovarajuću ranjivost ne može biti rizična. Svaki rizik može da izazove posljedice prema organizaciji kao što su gubitak efikasnosti, nepovoljnih uslova poslovanja, gubitak poslovanja, ugleda, štete i sl.

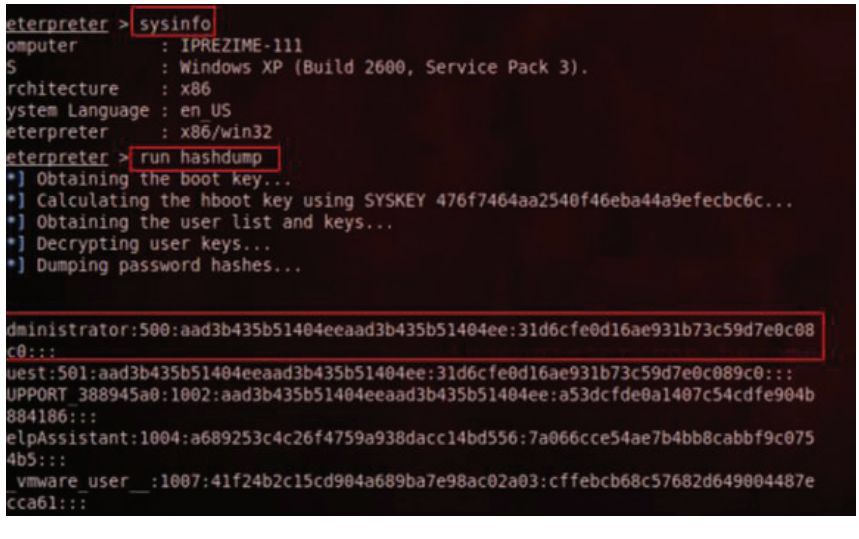
U našem slučaju organizacija posjeduje svoju informatičku mrežu sa velikim brojem hostova (računara), određenim brojem aplikativnih servera i e-mail serverom.

Posmatraćemo samo softversku imovinu. Sada je potrebno utvrditi ranjivost ovih sistema. Primijenićemo *penetration* test na informatičku mrežu kako bismo došli do potrebne ocjene za ranjivost sistema. *Penetration* testovi služe da bi se ispitali postojeći informacioni sistemi, tj. da bi se uočile njegove ranjivosti. Ranjivosti računarskog informacionog sistema i mreža su za kompjuterske kriminalce skriven, ali vrlo vrijedan podatak i imovina. Nove ranjivosti pojavljuju se svakodnevno zbog grešaka u softveru, hardveru, u konfiguraciji aplikacija i informacionih tehnologija, te zbog grešaka ljudi.

Za *penetration* testove koristili smo alate iz *linux* distribucije BackTrack 5. BackTrack 5 je *linux* platforma za *penetration* testove i provjeru sigurnosti naprednim alatima za otkrivanje, detekciju i iskorišćavanje svake ranjivosti otkrivene u ispitivanom mrežnom okruženju. BackTrack 5 se može koristiti na tri načina, kao live DVD, instalacijom na hard disk ili instalacijom na USB. Alati su podijeljeni u nekoliko grupa i sa njima se mogu dobiti informacije o *hostovima*, njihovoj aktivnosti, operativnom sistemu, DNS-u, rutiranju, e-mail adresama, web sajtovima, mail serveru, mreži, *web* aplikacijama, *wireless* mreži, *bluetoothu* i radio frekvencijama kao i informacije o VOIP-u.

Primjenom alata *autoscan* i *zenmap* iz *linux* distribucije BackTrack 5 dobili smo informacije o *hostovima* u mreži kao što su operativni sitem koji posjeduju, MAC adresama, otvorenim portovima i *firewallu*. Nakon ovog skeniranja utvrdili smo moguće mete napada. Sljedeći korak je utvrđivanje da li se može pristupiti određenim *hostovima* koje smo identifikovali kao potencijalna meta napada.

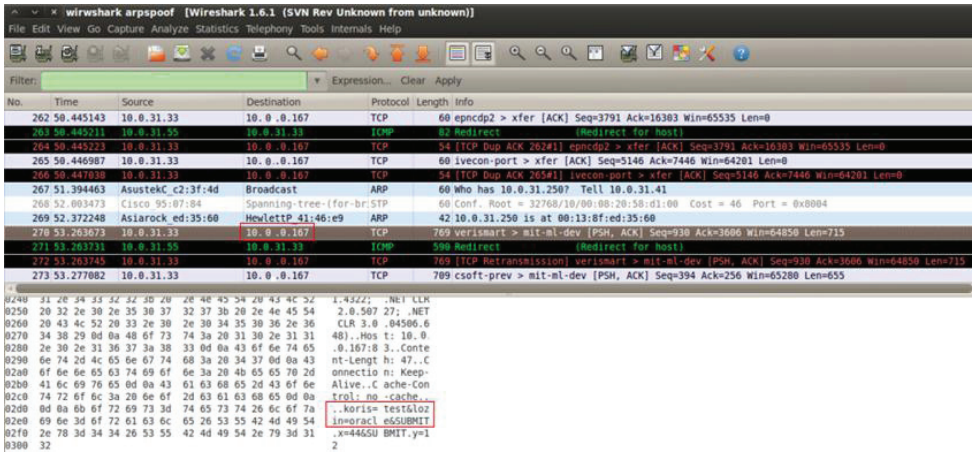
Alat *meterpreter* je napredni, "nečujni", multifunkcionalni i dinamički *payload* koji radi postavljanjem DLL fajla u memoriju odredišnog računara. Ovim alatom se može izvršiti uzimanje lozinke logovanja sa odredišnog *hosta*, omogućavanje *remote desktopa*, praćenje servisa i mnogo drugih mogućnosti. Ovim alatom smo utvrdili da se može pristupiti većini *hostova* i da se mogu izvršiti sve gore pomenute mogućnosti ovog alata. Na sljedećoj slici je prikazan izgled upada u jedan *host* i dobijanje *hash* vrijednosti lozinke za korisničke naloge na računaru koji se lako mogu dekriptovati na internet stranicama predviđenim za to.



Slika 1.-Provjera administratorskog naloga na odredišnom hostu

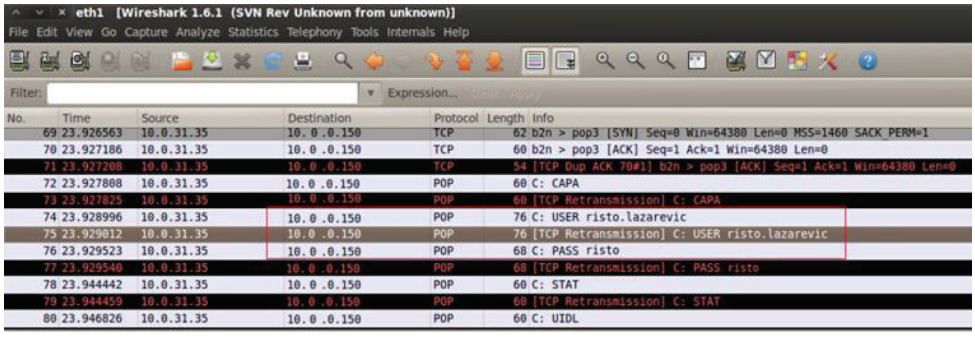
Sljedeći korak je provjera sigurnosti pristupa aplikacijama i sigurnost upotrebe e-maila. Za analizu ovih informacionih sistema koristili smo dva alata *wireshark* i *arpspoof*. *Wireshark* je mrežni analizator protokola. On podržava više od 100.000 protokola, ima mogućnost *offline* analize, ima najbolji filter, mogućnost prezentovanja rezultata preko GUI-a ili komandne linije, može čitati podatke sa IEEE802.11, *bluetooth*-a i *ethernet*-a. *Arpspoof* je alat koji se koristi za snifovanje mreže u *switch* okruženju. On mijenja MAC adresu računara koji se napada. Primjenom ovih alata otkriveno je da se lako mogu otkriti korisnički nalozi i lozinke za pristup aplikacijama zato što se koristi *http* protokol.

Rezultat otkrivanja korisničkog imena i lozinke je dat na sljedećoj slici.



Slika 2. Otkrivanje korisničkog imena i lozinke za pristup aplikaciji

Primjenom istih alata za otkrivanje e-mail naloga i lozinke takođe se pokazao kao vrlo uspješan, s tim da su se ovim alatima mogle dobiti i informacije o sadržini e-maila. E-mail server koristi POP3 i SMTP protokol. Sljedeća slika ilustruje dobijene rezultate.



Slika 3.-Otkrivanje e-mail naloga i lozinke

Na osnovu *penetration* testa možemo zaključiti da nam je ranjivost *hostova*, aplikativnih servera a i e-mail servera velika, ocjena 3. Prijetnju ovom

informacionom sistemu možemo ocijeniti kao srednju, ocjena 2. Vrijednost resursa možemo definisati na sljedeći način: hostovi i podaci na njima ocjenom 3, aplikativni serveri ocjenom 5 i e-mail server ocjenom 4. Sada ćemo odrediti vrijednost rizika i predstavićemo ga u sljedećoj tabeli.

Tabela 3. – Tabela nivoa rizika za pojedine resurse

Resursi	Vrijednost	Prijetnja	Ranjivost	Nivo rizika
Računari	3	2	3	8
Aplikativni serveri	5	2	3	10
E-mail server	4	2	3	9

Vidimo da je nivo rizika za aplikativne servere i e-mail server visok, a za računare srednji. Nakon izvršenog *penetration* testa i utvrđenog rizika potrebno je izabrati kontrole za smanjenje, zadržavanje, izbjegavanje ili prenošenje rizika. Kada postoji mogućnost smanjenja rizika uz relativno niske izdatke, potrebno je implementirati takvu opciju. Svakako bi trebalo štetne posljedice rizika svesti na najmanju mogući nivo. Plan obrade rizika treba definisati tako da se jasno istakne prioritetni rizik za obradu te se moraju definisati vremenski okviri obrade. Prilikom smanjenja rizika treba izabrati odgovarajuće i opravdane kontrole za ispunjavanje koje su identifikovane kod procjene rizika i obrade rizika. Kontrole mogu osigurati jedan ili više tipova zaštita: ispravak, eliminaciju, prevenciju, smanjenje uticaja, odvraćanje, otkrivanje, oporavak, praćenje, opreznost. U standardu ISO/IEC 27002 pružene su detaljne informacije o kontrolama. Takođe, potrebno je donijeti i formalno zabilježiti odluku o prihvaćanju rizika i odgovornosti za tu odluku. Planovi obrade rizika trebaju opisivati kako se procijenjeni rizici trebaju obrađivati, kako bi udovoljavali kriterijumu prihvatljivosti rizika. Kriterijumi prihvaćanja rizika mogu biti mnogo složeniji od samog određivanja hoće li preostali rizik pasti iznad ili ispod određenog niova. Informacije o riziku trebaju se razmjenjivati ili dijeliti između svih interesnih grupa. Informacije uključuju prirodu, oblik, vjerovatnost, težinu, obradu i prihvatljivost rizika. Interesne grupe će donositi odluke o prihvatljivosti rizika na temelju njihove percepcije.

Nakon uočenih nivoa rizika u ispitivanoj organizaciji, pristupili smo izradi plana za poboljšanje informacione bezbjednosti. Nakon svih prikupljenih podatka iz *penetration* testa utvrdili smo da bi se uvođenjem *Active Directoryja* i priključenjem računara na domen, uključivanjem grupnih polisa, kao i uključivanjem *firewalla* na računarima smanjila ranjivost računara. Sljedeći korak je bio uvođenje PKI (*Public Key Infrastructure*) sa upotrebom *smart* kartica. Za zaštitiu aplikacija implementiran je pristup preko *https* protokola sa upotrebom digitalnih sertifikata. I na kraju, e-mail je takođe zaštićen upotrebom digitalnih sertifikata i smart kartica.

Ponovnom primjenom *penetration* testova nismo mogli doći do informacija o informacionom sistemu organizacije, što znači da smo ranjivost sveli na nizak nivo. Nivo rizika se takođe smanjio za 2, pa je sada rizik za računare 6, e-mail server 7 i aplikativne servere 8. Više nemamo visok nivo rizika u organizaciji, sveden je za sve resurse na srednji nivo.

Rizike i činioce treba pratiti i pregledavati kako bi se identifikovale bilo kakve promjene u kontekstu organizacije u ranoj fazi i održao pregled cijele slike

rizika. Prijetnje, ranjivosti, vjerovatnosti ili posljedice mogu se promijeniti vrlo naglo bez ikakvih oznaka. Nove prijetnje, propusti, promjene u vjerovatnosti ili posljedice mogu povećati rizike koji su ranije nisko ocijenjeni. Praćenje upravljanja rizicima može dovesti do mijenjanja ili dodavanja pristupa, metodologije ili alata koji se koristi zavisno od uočenih promjena, iteracije procjene rizika, cilja procesa upravljanja rizicima informacione sigurnosti i objekta procesa upravljanja rizicima informacione sigurnosti.

ZAKLJUČAK

Informacione tehnologije predstavljaju oblast koja se veoma brzo širi i nalaze primjenu u svim oblastima ljudskog stvaralaštva i života uopšte. Sve više se događaju ugrožavanja informacionih sistema i njihovih korisnika. Unapređivanje bezbjednosti informacionog sistema postaje svakodnevni cilj svake organizacije. Proces Plan – Do – Check – Act predstavlja točak koji se stalno okreće i ne smije se zaustaviti . U slučaju da se ovaj proces zaustavi, informacioni sistem je prepušten sam sebi, jer kriminalci ne miruju. Kompjuterski kriminal je – kriminal. I ovaj kriminal je u porastu i štete koje trpe organizacije i pojedinci su sve veće.

ISO/IEC 27000 je procedura koja nam pomaže da osposobimo svoj informacioni sistem kako bi odvratio potencijalne napadače, a u slučaju da se napadi ipak dogode, da ne mogu ugroziti bezbjednost sistema. Organizacije koje ne obraćaju pažnju na bezbjednost svog informacionog sistema jesu mnogo više ugrožene od onih koje vode brigu o svojim informacijama. U modernom dobu reputacija organizacija koje ne pridaju značaj bezbjednosti informacija je na veoma niskom nivou i takve organizacije ne mogu imati svijetlu poslovnu budućnost. Informacioni sistem se definiše kao kombinacija ljudi, hardvera, softvera, komunikacionih uređaja, mreža i podataka koji procesiraju (čuvaju, pretražuju i transformišu) podatke i informacije za specifične namjene. Ljudski faktor je važna komponenta informacionog sistema i upravo su ljudi odgovorni da se proces Plan – Do – Check – Act ne zaustavi.

Pokazali smo kako se može jednostavnim i ne skupim aktivnostima unaprijediti bezbjednost informacionog sistema. Za testiranje bezbjednosnih parametara smo koristili Open source paket Back Track 5. PKI kao mjera povećanja stepena bezbjednosti informacionog sistem, takođe može da bude realizovan pomoću Open source alata. Povećanje bezbjednosti informacionog sistema ne mora uvijek da znači i skupa ulaganja. Međutim, svako ulaganje je opravdano ako sprečava štete koje su mnogostruko puta veće od ulaganja.

LITERATURA:

[1] Dario Šantalab, Ivan Vitez, Kristina Zjakić, ISO 27005 – Upravljanje rizicima, dostupno na *http://security.foi.hr/wiki/index.php/ISO_27005_-_Upravljanje_rizicima*, posjećeno u februaru 2012. godine

[2] Hrvoje Šegudović, Prednosti i nedostaci metoda za kvalitativnu analizu rizika, dostupno na *http://www.infigo.hr/files/INFIGO-MD-2006-06-01-RiskAsses.pdf*, posjećeno u februaru 2012. godine

[3] 16. Information Security Policy, Seminar on Police Info-Communications, Tokyo, Japan, februar . 2010. godine
[4] Jože Knez mr. sc., Goran Budiselić dipl. ing., Sigurnost inforamacija po normi ISO/IEC 27001 u postojećim sustavima upravljanja, dostupno na *http://www.kvaliteta.net/informacije/radovi/Knez_J_rad.pdf*, posjećeno u februaru 2012. godine
[5] Milan Marković prof.dr, Information Security Risk Analysis - ISO/IEC 27005:2008 International Standard, dostupno na *http://www.telegroup.ba/media/pdf/5.MMarkovic_InfoSecurity_Day.pdf,* posjećeno u oktobru 2011. godine
[6] Milan Nikolić, Praktični aspekti zaštite privatnosti korisnika i bezbednosti elektronskih komunikacionih mreža i usluga u Srbiji, dostupno na *http://www.telekomunikacije.rs/arhiva_brojeva/peti_broj/milan_nikolic:_prakticni_aspekti_zastite_privatnosti_korisnika_i_bezbednosti_elektronskih_komunikacionih_mredja_i_usluga_u_srbiji_.305.html*, posjećeno u februaru 2012. godine
[7] Milica Tepšić, Rade Tanjga, Zaštita inofrmacionih sistema, Banja Luka, 2011. godine
[8] Shakeel Ali, Tedi Heriyanto, BackTrack 4: Assuring Security by Penetration Testing, Birmingham UK, april 2011.godine
[9] http://en.wikipedia.org/wiki/Computer_security, posjećeno u januaru 2012. godine
[10] http://www.backtrack-linux.org, posjećeno u februaru 2012. godine
[11] http://www.iso27001security.com, posjećeno u februaru 2012. godine
[12] http://www.27000.org, posjećeno u februaru 2012. godine

SUMMARY

Modern organizations are inconceivable without modern information systems. They enable organizations to efficiently and quickly respond to all user requirements by associateing their information resources with their customers. As such, information systems are becoming targets of attacks that aim to distort safety, damage to system or taking of property. The concept of security of information systems is based on maintaining the confidentiality, integrity and availability of information. One form of threat to these elements is high-tech crime. ISO / IEC 27000 is a procedure used to assess risk and prescribes the mode of action that will reduce risk to acceptable limits. Plan - Do - Check - Act activity must not be stopped. Back Track 5 is an open source product that can be used to assess the risks to the security of information systems. It contains a set of tools for the identification and analysis of information system vulnerabilities and a number of tools for digital forensics and investigations. Risks and factors should be monitored and reviewed to identify any changes in the context of the organization at an early stage and gave an overview of the whole picture of risk.

Stručni rad - UDK 004.738.5: 351.74/.76

ZAŠTITA WEB APLIKACIJA I PROTOKA PODATAKA UPOTREBOM PKI SISTEMA I SMART KARTICE ZA AUTENTIFIKACIJU KORISNIKA

Dragan Popović,
Predrag Nagraisalović,
Aleksandar Krsmanović,
Milanko Topić,
Aleksandar Popović

Apstrakt: U ovom radu su opisane prednosti PKI sistema u zaštiti WEB aplikacija kao i sigurnom protoku poslovnih transakcija od WEB servera do klijenta. Razmotreni su nedostaci klasiče (nezaštićene) konekcije klijenta na WEB aplikaciju, način korišćenja tih nedostataka i presretanje podataka od strane trećeg lica radi pribavljanja informacija.

U cilju jačanja zaštite na relaciji klijent-server predstavljen je SSL (secure sockets layer) protokol za kriptovanu komunikaciju između korisnika i WEB servera te autentifikaciju putem digitalnog sertifikata i smart kartice.

SSL certifakati su svjetski standardi kojeg koriste svi koji rade sa osjetljivim podacima.

SSL omogućava proveru identiteta pomoću sertifikata koji izdaje sertifikaciono telo CA. Ovaj vid SSL transakcije nudi zadovoljavajući nivo sigurnosti, te je relativno brzo postao standard za sigurnu komunikaciju. Upravo zbog ove činjenice, SSL protokol se najčešće koristi u aplikacijama za plaćanje kreditnim karticama i dugim aplikacijama sa osjetljivim sadržajem.

Ključne riječi: web aplikacija, PKI, Pametna kartica, https, http, TSL/SSL

UVOD

Prateći trendove i smjerove razvoja informacionih sistema, svjedoci smo da je u zadnjih nekoliko godina razvoj aplikacija usmjeren na web orijentisane aplikacije. Ove aplikacije su u početku bile namijenjene uglavnom poslovima koji su se odvijali preko interneta, ali sve više se ova tehnologija primjenjuje i u intranet mrežama srednjih i velikih preduzeća, akademskih ustanova, javnom sektoru i sl., istiskujući stariju tehnologiju desktop aplikacija.

Glavni razlog širenja web aplikacija jeste i ekspanzija programskih jezika kao i usavršavanje integrisanih razvojnih alata namijenjenih razvoju ovih aplikacija (Microsoft Visual Studio, NetBeans, Zend studio i sl.). Pored navedenog, administriranje web aplikacija je pojednostavljeno samim tim što je aplikacija postavljena na jednom mjestu i ne zahtijeva se dodatna instalacija na radnoj stanici klijenta. Za rad sa web orijentisanim aplikacijama neophodan je pretraživač web-a (Mozila Firefox, Internet Explorer, Opera, Chrome i sl.)

U savremenom poslovnom svijetu bezbjednost podataka se svrstava u sam vrh poslovne politike većine preduzeća, a pogotovo ako je riječ o podacima osjetljivog

sadržaja koji bi mogli biti iskorišćeni ili zloupotrebljeni. WEB aplikacije u intranet mreži preduzeća nisu samo ograničene na pojedine radne stanice, već pristup istim imaju, u većini slučajeva, sve radne stanice koje se nalaze u pomenutoj mreži. Autentifikacija korisnika se uglavnom svodi na korisničko ime i lozinku, što nije dovoljno.

U vremenu rasta nivoa informatičkog znanja kod većine stanovništva, kada većina ljudi posjeduje računar i pristup Internetu, nije teško pretpostaviti da neko ko se profesionalno ne bavi informacionim tehnologijama dođe do informacije na koji način i kojim alatom mogu da se iskoriste bezbjednosni propusti u aplikaciama. Ovo ima za posljedice „curenje" bitnih informacija koje može da naškodi poslodavcu.

Podizanje nivoa bezbjednosti na način ograničavanja pristupu aplikacijama samo zaposlenima, koji te aplikacije koriste u svom radu, jedan je od načina zaštite podataka. Nije dovoljno da se server na kojem se nalazi aplikacije i radne stanice za pristup aplikacijama izdvoje u zasebnu mrežu. Pristup aplikacijama treba da se svede na konkretno lice, a ne na radnu stanicu. Cilj je da se uspostavi sistem autentifikacije koji jednoznačno identifikuje da li korisnik ima pravo pristupa aplikaciji (npr. stranici za prijavu korisnika u aplikaciju).

Jedna od metoda na kojoj može biti zasnovan sistem zaštite pristupa podacima jeste korišćenje digitalnih sertifikata za jaku autentifikaciju i zaštitu podataka. Preduslov za korišćenje sertifikata kao sredstva zaštite jeste podizanje CA (Certificate Authority) u intranet mreži preduzeća kao i konfigurisanje HTTP servera da koristi TLS/SSL protokol u radu aplikacije.

TLS/SSL PROTOKOL

TLS/SSL je protokol koji treba da obezbijedi sigurnu komunikaciju između dva učesnika preko računarske mreže.

SSL (Secure Socket Layer) protokol je razvijen od strane firme Netscape Communications Corporation. Verzija 1.0 SSL protokola nije javno objavljena, a verzija 2.0 je objavljena u februaru 1995. godine. Već 1996. objavljena je i verzija 3.0. Verzija 3.0 SSL protokola je bila osnova za razvoj TLS (Transport Layer Security) protokola od strane IETF (Internet Engineering Task Force)**.** TLS 1.0 definisan je u januaru 1999. godine u RFC 2246. TLS 1.1 objavljen 2006. godine, a aktuelna je verzija TLS 1.2 iz 2008. godine.

Većina današnje trgovine i bankarskog poslovanja preko interneta zasnovana je na korišćenju TLS/SSL protokola. Ovo se ostvaruje kroz uspješnu autentifikaciju servera i klijenta, te uspostavljanje sigurne komunikacije između njih. Pod serverom se podrazumijeva HTTP server, a klijenta u ovoj komunikaciji predstavlja čitač weba na radnoj stanici korisnika.

TLS omogućava aplikacijama sigurnu komunikaciju putem mreže, jer sprečava prisluškivanje (eavesdropping) i neovlašćeno mijenjanje originalnih poruka (tampering), te omogućava autentifikaciju učesnika u komunikaciji. Autentifikacija, pouzdanost i vjerodostojnost učesnika u komunikaciji zasnovana je na primjeni infrastrukture javnog ključa (PKI).

Ciljevi koje TLS protokol treba da ispuni, poredani po prioritetu, jesu: 1. Kriptovanje – Cryptographic security – TLS će biti korišćen za uspostavljanje sigurne konekcije između dva učesnika

2. Interoperabilnost – Interoperability – omogućiti programerima da stvaraju aplikacije koje koriste TLS tako da mogu razmjenjivati kriptografske parametre bez međusobnog poznavanja kôda.

3. Proširivost – Extensibility – TLS treba da predstavlja okvir u koji se mogu uklopiti nove medote kriptovanja javnim i simetričnim ključem kada se ukaže potreba za tim.

4. Relativna efikasnost – Relative efficiency – potrebno je zadovoljiti sve sigurnosne zahtjeve uz što manje zauzeće procesorskih i mrežnih kapaciteta

Dakle, za učesnike u komunikaciji je važno obezbijediti integritet podataka i međusobnu autentifikaciju.

Pod integritetom podataka podrazumijeva se da niko treći nije mogao da pristupi podacima ili ih promijeni bez znanja učesnika u komunikaciji. TLS/SSL koriste više kriptografskih tehnika kako bi osigurali integritet podataka. Asimetrično i simetrično kriptovanje koristi se da omogući privatnost komunikacije, sprečavajući nepozvane učesnike da imaju pristup sadržaju komunikacije, i u slučajevima presretanja komunikacija. Ovo takođe omogućava zaštitu od brisanja poruka ili ubacivanja nepostojećih poruka u komunikaciju.

Asimetrično kriptovanje ili kriptovanje javnim ključem omogućava kriptovanu komunikaciju između dva učesnika bez potrebe da oni prethodno razmjenjuju tajne ključeve. Asimetrično u nazivu potiče od činjenice da se za kriptovanje i dekriptovanje koriste različiti ključevi. Najpoznatiji algoritam jeste RSA. RSA ključevi imaju dva dijela: privatni ključ i javni ključ. Javni ključ je dostupan svim zainteresovanim za komunikaciju, dok svaki učesnik u komunikaciji odgovara za svoj privatni, odnosno tajni ključ. Privatni ključ se koristi za potpisivanje poruka. Poruka se može verifikovati samo javnim ključem. Obrnuto, javni ključ može biti upotrijebljen za kriptovanje poruke, koju je moguće dekriptovati samo odgovarajućim privatnim ključem. Da bi nečelo relativne efikasnosti bilo zadovoljeno, TLS/SSL koriste asimetrično kriptovanje za verifikaciju i razmjenu tajnog ključa koji će biti upotrijebljen za kriptovanje same poruke.

Simetrično kriptovanje – ovaj princip omogućava kriptovanje komunikacije između dvije krajnje tačke korišćenjem jednog dijeljenog ključa. Simetrično u nazivu potiče od činjenice da se i za kriptovanje i za dekriptovanje koristi isti ključ. Najpoznatiji algoritmi su DES, 3DES i AES.

Pošto se isti ključ koristi i za kriptovanje i za dekriptovanje, od presudne važnosti je da se očuva tajnost ovog ključa između dvije krajnje tačke. Napadač koji posjeduje ovaj ključ, može da kreira lažne poruke ili da pročita presretene poruke. Ova činjenica se veoma često zloupotrebljava na internetu gdje je moguće da napadači presretnu željenu komunikaciju. Zato se asimetrična enkripcija koristi samo za razmjenu ključa za simetrično kriptovanje. Ključ za simetrično kriptovanje može da ima manju dužinu od asimetričnih ključeva, čime se omogućava brže procesiranje kriptovanih poruka.

TLS koristi Message Authentication Codes (MAC) da bi učesnik koji primi puruku bio siguran da je primio originalnu poruku, tj. da originalna poruka nije promijenjena tokom prenosa.

Verifikacija učesnika

Veoma je važno da je učesnik u komunikaciji siguran s kim komunicira, tj. da je drugi učesnik sigurno taj sa kim on želi da kominicira, a ne neko ko se lažno

predstavlja. TLS/SSL ovo obezbjeđuje korišćenjem digitalnih sertifikata. TLS/SSL je klijent-server protokol i ovo određuje da ga koriste drugi klijent server protokoli, kao što su HTTPS ili POP3S.

INFRASTRUKTURA JAVNOG KLJUČA (PKI)

PKI uspostavlja sigurno okruženje za elektronsku trgovinu, bankarstvo i elektronsko poslovanje uopšte.

Ovakav sistem se realizuje da bi se zadovoljili:

- tajnost – obezbjeđuje se simetričnim kriptovanjem
- autentifikacija – obezbjeđuje se asimetričnim kriptovanjem
- integritet podataka – obezbjeđuje se asimetričnim kriptovanjem
- neporecivost (kada učesnik u komunikaciji pošalje poruku, ne može poreći da je to učinio) – obezbjeđuje se asimetričnim kriptovanjem

Da bi se bolje razumjela infrastruktura javnog ključa, potrebno je upoznati se i sa pojmovima digitalni potpis i digitalni sertifikat.

Digitalni potpis je elektronska forma koja se koristi za provjeru autentičnosti pošiljaoca poruke, kao i za provjeru itegriteta same poruke. Digitalni potpis predstavlja podatak kriptovan tajnim ključem pošiljaoca poruke, koji se može dekriptovati samo njegovim javnim ključem. Realizuje se korišćenjem asimetričnog kriptovanja.

Digitalno potpisivanje obavlja se pomoću privatnog ključa pošiljaoca, a provjera integriteta poruke se vrši pomuću javnog ključa pošiljaoca. U slučaju da je poruka mijenjana nakon što je digitalno potpisana, digitalni potpis neće biti ispravan. Hash funkcija – matematička funkcija koja se koristi za izručivanje otiska poruke (message digest) fiksne dužine.

Kako se primjenjuje digitalno potpisivanje?

Svaka strana u komunikaciji ima svoj par ključeva. Jedan privatni i jedan javni ključ. Podatak kriptovan javnim ključem može se dekriptovati samo odgovarajućim privatnim ključem i obrnuto.

Javni ključevi su dostupni objema stranama, a svaki učesnik poznaje samo svoj privatni ključ. Postoje dva učesnika u komunikaciji, koje ćemo označiti kao učesnik A i učesnik B. Poruku šalje učesnik A. Na svoju originalnu poruku učesnik A primjenjuje Hash funkciju i dobija se otisak poruke (message digest), koji je fiksne dužine. Ovako dobijeni otisak poruke učesnik A kriptuje svojim privatnim ključem (za ovo se koristi odgovarajući algoritam za asimetrično kriptovanje npr. RSA). Ovo kriptovanje otiska poruke privatnim ključem se naziva digitalno potpisivanje. Ovaj digitalni potpis se dodaje originalnoj poruci i šalje učesniku B.

Učesnik B odvaja digitalni potpis i dekriptuje ga javnim ključem učesnika A. Dobija se otisak poruke. U drugom koraku učesnik B primjenjuje istu Hash funkciju na poruku koju je poslao korisnik A i dobijeni otisak poredi sa otiskom koji je dobio nakon dekriptovanja digitalnog potpisa učesnika A. Ako su dobijene vrijednosti iste, potvrđeno je da je poruku poslao korisnik A i da poruka nije mijenjana tokom transporta.

Sada možemo zaključiti da su ispunjena tri kriptografska uslova: autentifikacija, integritet i neporecivost, ali nije zadovoljena tajnost komunikacije, jer je javni ključ pošiljaoca poznat širem krugu mogućih učesnika, a ne samo učesniku B.

Tajnost komunikacije se ostvaruje primjenom digitalnih sertifikata. Digitalni sertifikat je digitalno potpisani dokument koji povezuje javni ključ sa subjektom kome pripada. Drugačije rečeno, digitalni sertifikat je skup podataka u elektronskom obliku koji predstavlja elektronski identitet vlasnika u svrhu sigurne i povjerljive komunikacije preko inteneta. Digitalni sertifakat sadrži:

- informacije o samom sertifikatu (format, verzija, primijenjeni algoritam, serijski broj)
- javni kriptografski ključ subjekta (vlasnika sertifikata koji ima odgovarajuću tajni ključ)
- period važenja
- informacije koje se odnose na vlasnika sertifikata
- informacije koje se odnose na tijelo koje je izdalo sertifikat
- digitalni potpis izdavaoca

Kako se postiže tajnost komunikacije na prethodnom primjeru? Kad učesnik A digitalno potpiše svoju poruku, originalna poruka sa digitalnim potpisom se kriptuje simetričnim ključem. Zatim se javnim ključem učesnika B kriptuje taj simetrični ključ. Kako učesnik A poznaje javni ključ učesnika B? Poznaje ga tako što pribavi digitalni sertifikat učesnika B u kome je sadržan javni ključ učesnika B. Sada učesnik A šalje kriptovanju poruku i digitalni potpis i zajedno sa njim ključ za simetrično kriptovanje, koji je kriptovan javnim ključem učesnika B. Dekriptovanje ide obrnutim redoslijedom, korisnik B prvo svojim javnim ključem dekriptuje ključ koji je upotrijebljen za simetrično kriptovanje. Primjenom ovog ključa dobiće originalnu poruku zajedno sa digitalnim potpisom korisnika A. Javnim ključem korisnika A dekriptuje njegov digitalni potpis i dobije otisak originalne poruke. Na ranije dobijenu originalnu poruku primijeni Hash funkciju i uporedi ova dva otiska. Ako su otisci jednaki, ova komunikacija je zadovoljila uslove autentičnosti, integriteta, tajnosti i neporecivosti.

PKI predstavlja kombinaciju hardverskih i softverskih elemenata, ljudi, politika i procedura neophodnih za generisanje, skladištenje, upravljanje, distribuciju i opoziv digitalnih sertifikata. PKI se bazira na politici zaštite informacionog sistema u kome se primjenjuje. PKI objedinjuje kriptografske algoritme, digitalno potpisivanje i digitalne sertifikate u jedan jedinstven sistem koji ima zadatak da očuva bezbjednost informacija i komunikacija. Dakle, implementacija PKI omogućava autentifikaciju učesnika u komunikaciji, razmjenu dokumenata sa mogućnošću kriptovanja, digitalnog potpisivanja, jedinstvenu registraciju javnih ključeva koji su sadržani u digitalnim sertifikatima, a uz sve to su obezbijeđeni tajnost komunikacije i integritet podataka. Korisnici PKI su kako ljudi, tako i softverski klijenti, web serveri i ostale aplikacije. Osnovni dijelovi PKI su Certificate Authority (CA), Registration Authority (RA) te Certificate Repository (CR). Osnovni zadaci CA su izdavanje, administracija i povlačenje sertifikata. CA je najbitnija komponenta u cijeloj PKI hijerarhiji. Kompromitovanje CA kompromituje čitavu hijerarhiju. RA prihvata zahtjeve za izdavanje sertifikata, registruje korisnike i zahtjeve prosljeđuje CA. CR čuva javne ključeve, sertifikate korisnika i liste povučenih sertifikata.

Organizacija može izgraditi sopstvenu infrastrukturu javnog ključa ili može iznajmljivati digitalne sertifikate od komercijalnih sertifikacionih tijela.

Za uspostavljanje privatne PKI postoje kako rješenja zasnovana na komercijalnom softveru, tako i Open Source rješenja (OpenSSL, EJBCA).

HTTP

HTTP (Hypertext Transfer Protocol) je mrežni protokol koji pripada aplikativnom sloju OSI referentnog modela mreže. HTTP predstavlja glavni i najkorišćeniji metod prenosa informacija preko interneta/intraneta.

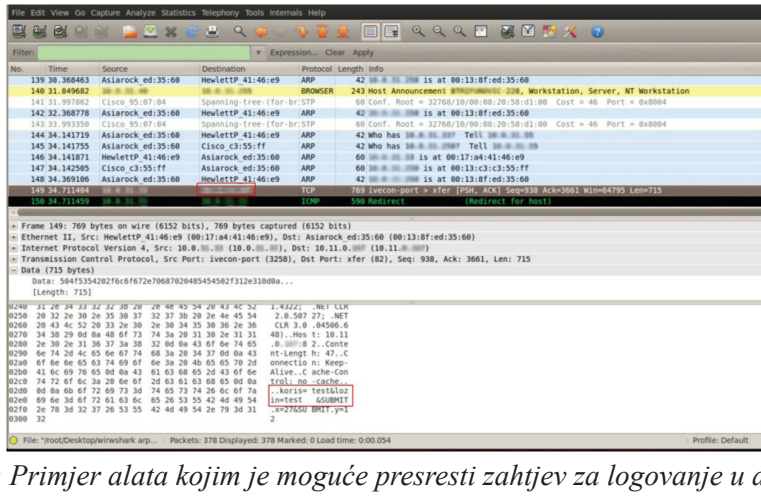
Za komunikaciju i razmjenu podataka između servera i klijenta koristi se HTTP protokol, koji funkcioniše po principu zahtjev/odgovor. HTTP klijent, najčešće čitač weba, nakon što uspostavi TCP/IP vezu sa udaljenim HTTP serverom, zahtijeva prenos podataka na određenom komunikacionom portu (port 80, a rjeđe može biti i 8080 ili drugi).

Komunikacija zasnovana na HTTP protokolu ima nekoliko bitnih slabosti:

- HTTP ne nudi sistem kojim je saobraćaj između klijenta i servera kriptovan. Shodno tome ostavlja se mogućnost trećim licima da presretnu taj saobraćaj, i da iskoriste podatke u svoju ličnu korist ili nanesu veliku štetu preduzeću.
- HTTP je protokol bez stanja (stateless protocol) – ne čuva informacije o korisnicima, nema mogućnost da identifikuje korisnika. To znači da će korisnik prilikom svake posjete Web aplikaciji biti registrovan od strane servera kao da je prvi put pristupio aplikaciji.
- HTTP ne obezbjeđuje autentifikaciju trenutne sesije, što znači da ne može da utvrdi (prepozna) da li je neka druga strana uzela trenutnu sesiju.

Slabosti HTTP protokola

Primjer slabosti HTTP protokola je vrsta napada koja se zasniva na prikupljanju i analiziranju podataka mrežnog prometa kako bi se došlo do osjetljivih podataka kao što su korisnička imena, lozinke, sadržaj ili bilo koje druge povjerljive informacije.



Slika. 1: Primjer alata kojim je moguće presresti zahtjev za logovanje u aplikaciju i saznati upućeno korisničko ime i lozinku

Napadač može presresti komunikaciju između dvije strane, promijeniti poruku i poslati je dalje do odredišta. U tom slučaju ni jedna ni druga strana ne zna da su ti podaci promijenjeni i da im druga strana uopšte nije poslala ovakve podatke kakvi su stigli na odredište. To je primjer tzv. MIT (Man in the Middle) napada, što u prevodu znači „čovjek u sredini«.

Ova metoda predstavlja pasivni napad koji je nemoguće otkriti. Kako je to veliki problem tokom komunikacije klijent/server, zbog presretanja i krađe podatka uvodi se enkripcija TLS/SSL.

ZAŠTITA UPOTREBOM HTTPS PROTOKOLA

Zbog zaštite privatnosti podataka i informacija koje se razmjenjuju na relaciji klijent/server uveden je sigurnosni protokol HTTPS.

Postoji šest vrsta osnovnih sigurnosnih servisa koje je potrebno obezbijediti:

- Autentifikacija (authentication),
- Povjerljivost ili tajnost podataka (data confidentiality),
- Neporecivost poruka (non-repudation),
- Integritet podataka (data integrity),
- Autorizacija i kontrola pristupa (authorization and access control),
- Raspoloživost resursa (resource availability).

HTTPS (Hypertext Transfer Protocol Secure) čini kombinaciju HTTP i TSL/SSL protokola stvarajući enkripciju tokom prenosa podataka i sigurnu identifikaciju servera. Ova vrsta protokola najčešće se koristi na Web aplikacijama (sajtovima) koje razmjenjuju bitne podatke koji su od velike važnosti.

Na osnovu metoda koje SSL koristi, može da se obezbijedi sigurnost klijent-server komunkacije na sljedeće načine:

- Pri uspostavljanju klijent-server komunikacije definišu se tajni ključevi koji se koriste za kriptovanje podataka koji se prenose. To znači ako je saobraćaj presretnut od strane trećeg lica, ne može da bude čitljiv jer je kriptovan.
- SSL podržava kriptografiju javnim ključevima, tako da server može da identifikuje korisnike koristeći metode RSA, DSS.
- Server može da verifikuje integritet tekuće sesije koristeći algoritme izvoda poruka kao što su MD5 i SHA.

Kod zaštite WEB aplikacija u internet/intranet mreži, koje služe za pristup osjetljivim podacima, potrebno je da se obezbijedi jaka autentifikacija korisnika. Svaka WEB aplikacija koja zahtijeva prijavu korisnika mora omogućiti zaštićen pristup prijavi da ne bi došlo do kompromitovanja identifikacionih podataka. Za uspostavljanje i održavanje kriptovane komunikacije mogu da se koriste digitalni sertifikati koji se izdaju korisnicima od strane CA (Certificate authority) tijela. Ukoliko je riječ o aplikacijama koje za pristup koriste internet mrežu, poželjno je da sertifikat bude izdat od strane registrovanog CA, dok za aplikacije koje za komunikaciju sa klijentom koriste intranet mrežu, treba podesiti vlastiti CA za izdavanje digitalnih sertifikata. Izdati korisnički sertifikati se prosljeđuju korisniku na najbezbjedniji način. Digitalni sertifikat je zaštićen sigurnosnim kodom (PIN kod).

Komunikacija uspostavljena na ovakav način omogućava serveru da identifikuje klijenta koji pristupa, kao i kriptovanje saobraćaja na relaciji klijent-server. U opisanom načinu komunikacije server mora da bude podešen tako da klijent koji pristupa mora da posjeduje validan sertifikat u kome su smještene informacije koje omogućavaju serveru da potvrdi identitet klijenta prilikom slanja povjerljivih podataka. Čitač weba šalje klijentski sertifikat serveru, dok istovremeno server prosljeđuje serverski sertifikat klijentskom čitaču weba.

Kao što je ranije navedeno, klijentski sertifikat je zaštićen PIN kodom koji je neophodno unijeti prilikom uspostavljanja komunikacije. Na ovaj način se uspostavlja sigurna komunikacija koja traje sve dok oba sertifikata učestvuju u njoj. Ukoliko jedan od sertifikata (najčešće klijentski) napusti uspostavljenu komunikaciju (izvađena kartica na kojoj se nalazi sertifikat iz čitača kartica), dolazi do prekida komunikacije i pristup WEB aplikaciji više nije moguć. Da bi se obnovio pristup, potrebno je ponovo uspostaviti sigurnu komunikaciju između klijenta i servera.

ČUVANJE SERTIFIKATA I PRIVATNOG KLJUČA

Jedana od glavnih stvari u ovakvom sistemu zaštite pristupu WEB aplikacijama jeste čuvanje digitalnog setrifikata kojim se omogućava pristup. Digitalni sertifikat se može čuvati na:

- radnoj stanici korinika (HDD),
- pametnoj kartici (Smart Card),
- USB smart token-u.

HDD radne stanice

Čuvanje sertifikata na radnoj stanici (hard disku računara, laptop-a i sl.) je način koji pruža najmanji nivo zaštite. Svako ko ima pristup radnoj stanici može da iskoristi digitalni sertifikat, koji se nalazi na njoj, i da pistupi nedozvoljenim sadržajima WEB aplikacija. Kod ovakvog načina čuvanja digitalnog sertifikata omogućeno je lako kopiranje sertifikata i prenošenje na drugo mjesto (druga radna stanica).

Ovaj način čuvanja digitalnog sertifikata treba izbjegavati.

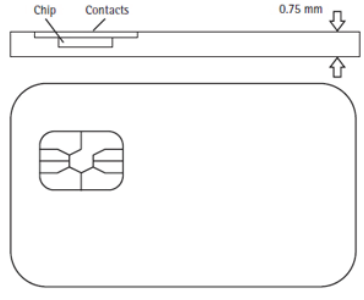
Pametne kartice (SmartCard)

Pametna kartica je obična plastična kartica koja posjeduje procesor (CPU) kao i memoriju – RAM koju koristi CPU kao radnu memoriju, ROM u koju je smješten operativni sistem kartice i EEPROM za smještanje podataka. Pamete kartice nemaju vlastito napajanje, već se napajaju iz čitača kartica. Može se reći da je pametna kartica mali računar.

Osnovne funkcionalnosti pametnih kartica su zaključavanje podataka (pohranjeni podaci se ne mogu preuzeti sa kartice), autentifikacija, validacija i pohranjivanje podataka. Većina kartica posjeduje dijelove memorije koji su nepromjenjivi (tamperproof), dok su ostali dijelovi memorije dostupni su aplikacijama za komunikaciju sa karticom. Ova sposobnost pametnih kartica pruža

mogućnost čuvanja određenih tajnih podataka kao što je privatni ključ, biometrijski podaci i sl. Pametne kartice posjeduju vlastite kriptografske operacije kojima štite podatke.

Izgled kartice, smještaj i raspored kontaktnih mjesta definisan je standardima ISO-7816-1 i ISO-7816-2.



Slika. 2: Izgled pametne kartice

Trenutno, pametne kartice se mogu naći u dva formata

- kontaktne kartice,
- beskontaktne kartice i
- kombinovane kartice.

Kontaktne kartice zahtijevaju čitač kartica. Kartica se mora umetnuti u čitač koji dodiruje kontaktne tačke na kartici i na taj način se omogućava komunikacija sa čipom koji je na kartici. Kontaktna površina pametne kartice posjeduje osam (8) kontaktnih tačaka.

Način komunikacije čitača i kartice zasnovan je na principu da čitač kartice šalje zahtjev prema kartici, gdje ga prihvata operativni sistem kartice, interpretira i prosljeđuje određene upravljačke signale prema drugim uređajima na smart kartici, te nakon njihove obrade prihvata rezultate i prosljeđuje ih čitaču kartica.

Beskonataktne kartice su bazirane na elektromagnetnom prenosu podataka od kartice do uređaja za čitanje. Sama kartica sadrži, pored čipa na kome su smješteni podaci, i antenu koja je omotana oko obima kartice i koja se aktivira kada se kartica približi uređaju za očitavanje. Antena i mikroprocesorski čip su nevidljivi na samoj kartici. Beskontaktne kartice, takođe, nemaju napajanje, već se koristi napajanje sa uređaja za čitanje ovih kartica (induktivna ili kapacitivna veza), kada se kartica dovoljno prbliži samom uređaju. Prenos podataka, u oba smjera, između kartice i uređaja je kodiran i može da se šifruje kombinaciojom algoritma koji je ugrađen na čip od strane proizvođača, PIN broja, sertifikata i tajnog ključa korisnika kartice.

Ranjivost smart kartica

Kao i svi informacioni sistemi, ni pametne kartice nisu potpuno sigurne i otporne na napade. Generalni problem ranjivosti svih informacionih sistema, pa samim tim i pametnih kartica, leži u činjenici da se uspješno izvedeni napadi vrlo brzo šire i kopiraju.

Napade na pametne kartice, s obzirom na način izvođenja, možemo podijeliti u napade na tri nivoa:

- sociološkom
- fizičkom i
- logičkom nivou

Napadi na sociološkom nivou su usmjereni prema vlasnicima pametnih kartica, licima koja izrađuju programe za pametne kartice, zaposlenima u fabrikama koje dizajniraju i proizvode čipove, a sve u cilju pribavljanja podataka koji se mogu iskoristiti. Ne postoji univerzalan način zaštite od ovakve vrste napada. Problem se uglavnom rješava poboljšavanjem organizacionih mjera kojima se sprečava "curenje" informacija.

Napadi na fizičkom nivou su usmjereni na mikroprocesor kartice i zahtevaju određenu vrstu opreme. Ovi napadi se izvode mjenjanjem fizičkih uslova kao što su frekvencija, napon i sl. Napadi na fizičkom nivou se mogu podjelitu u *statičke,* koji se izvode kada napajanje nije prisutno na mikroprocesoru, i *dinamičke,* koji se izvode u toku rada mikroprocesora. Dinamički napad na fizičkom nivou zahtijeva opremu za mjerenje određenih podataka.

Napadi na logičkom nivou jesu napadi koji se najuspješnije izvode. Ovi napadi se sastoje od određenih kriptoanaliza, korišćenja poznatih propusta kod operativnog sistema kartice, korišćenja trojanskih konja na radnim stanicama korisnika i sl.

Treba napomenuti da se sigurnost pametne kartice svakodnevno usavršava i da je ona jedan od najsigurnijih medija za čuvanje osjetljivih podataka.

USB smart token

USB smart token (često se naziva i ''dongl'') je hardverski uređaj koji ima iste karakteristike kao i pametne kartice, a razlikuje se u činjenici da je lako prenosiv i da ne zahtijeva uređaj za čitanje, već se jednostavno prikači na USB port radne stanice i koristi. Kao i pametne kartice tako je i USB token zaštićen PIN brojem ili lozinkom. Digitalni sertifikat, pohranjen na USB token, nikad ne napušta.

ZAKLJUČAK

U današnje vrijeme WEB aplikacije predstavljaju najčešće korišćenu tehnologiju u različitim poslovima kako na internetu tako i u intranet okruženju. Zbog široke primjene, WEB aplikacije su postale predmet interesa raznih subjekata u pogledu korišćenja bezbjednosnih propusta u komunikaciji između klijenta i servera.

Bezbjednost ovako orijentisanih aplikacija je predmet stalnog usavršavanja informacionih tehnologija koje se koriste kao njihova zaštita. Prilikom izrade i implementacije WEB aplikacija neophodno je da se pronađe pravi omjer između nivoa bezbjednosti, funkcionalnosti i cijene.

Jedan od najsigurnijih načina zaštite je korišćenje PKI infrastrukture. Autentifikacija korisnika upotrebom digitalnog sertifikata smanjuje mogućnost neovlašćenog pristupa WEB aplikaciji. Ono što je bitno jeste da se ova infrastruktura

može veoma lako implementirati u intranet okruženju preduzeća bez značajnijih finansijskih ulaganja. Najveći dio finansijskih ulaganja se odnosi na kupovinu hardverskih komponenti (pametne kartice, čitač kartica i sl.), dok se kao softwerska platforma mogu koristiti Open Source riješenja (OpenSSL, EJBCA).

LITERATURA

[1] ANONYMOUS (2003). *Maksimalna sigurnost Apache servera*, „Kompjuter biblioteka“ Čačak,

[2] Best Practices for Implementing a Microsoft Windows Server 2003 Public Key Infrastructure: http://technet.microsoft.com/en-us/library/cc772670(v=ws.10).aspx, posjećivano januara 2012,

[3] Dujella A., & Maretić M. (2007). *Kriptografija,* „Element“ Zagreb,

[4] Đorđević, D. (2007). *Digitalni potpis i digitalni sertifikat*, 15. Telekomunikacioni forum TELFOR 2007 Srbija, Beograd ,

[5] Underdahl, B., & Willett E.(2002): *Internet Biblija*, „Mikro knjiga“ Beograd,

[6] Understanding Digital Certificates: http://technet.microsoft.com/en-us/library/bb123848(v=exchg.65).aspx, posjećivano januara 2012. godine.

[7] Web Application Security Consortium, Web Application Security Consortium: Threat Clasification (pdf). URL: http://www.webappsec.org/projects/threat/v1/WASC-TC-v1_0.pdf ,

SUMMARY

Information protection is implemented through the use of advanced cryptographic methods, which are incorporated within the PKI hierarchy. Since its introduction, SSL / TLS protocol has many modifications in order to best answer the growing security challenges. PKI hierarchy is a logical sequence of events, whose introduction of the organization trying to provide their business. Ensuring confidentiality, authentication, integrity of information is, and will remain, the goal for all organizations, not just those dealing with electronic business.

HTTPS is a protocol that prevents eavesdropping of communication and man-in-the-middle attack in a way that encrypted traffic moving between client and server.

Smart cards and smart USB token are the safest media for storing digital certificates. This security is reflected in the fact that private or secret key never leaves the card, or USB smart token. As the trend for organizations to use WEB applications in their information systems, and PKI, as a condition for increasing the security of information is more important.

Prethodno saopštenje – UDK 341.48: [343.326: 004.738.5

KOMPJUTERSKI KRIMINALITET

Mr Gojko Vasić[1]
Ministarstvo unutrašnjih poslova Republike Srpske
Mr Borislav Šarić[2]
Ministarstvo unutrašnjih poslova Republike Srpske
Vlado Jovanić[3]
Ministarstvo unutrašnjih poslova Republike Srpske

Apstrakt: Početkom devedesetih godina prošlog vijeka, u sektoru djelatnosti globalne tehnologije informacija i komunikacija započeta je značajna transformacija usvajanjem tehnologija baziranih na kompjuterskim sistemima. Ove tehnologije postavile su pred organe reda širom svijeta, nove, složene izazove. Pojava i nagli porast kompjuterskog kriminala ima značajne implikacije za vlade i građane širom svijeta.[4] Danas je primjena računara veoma rasprostranjena i skoro da nema oblasti društvenog života gdje ovo moćno sredstvo nije našlo primjenu.

Pod kompjuterskim kriminalitetom podrazumijevaju se konkretna krivična djela koja se izvršavaju pomoću kompjutera kao sredstva izvršenja ili objekta napada, i kao takva su predviđena krivičnim ili nekim posebnim zakonima i sadrže sva specifična obilježja koja su vezana za sredstva i način njihovog izvršenja. Kompjuterski kriminal predstavlja jednu od najvećih prijetnji za široko rasprostiranje i korišćenje informaciono-komunikacionih tehnologija. Kompjuterski kriminalitet je sve zastupljeniji, dobija nove forme i predstavlja sve veću opasnost, naročito kroz oblike kriminalnog djelovanja transnacionalnog organizovanog kriminaliteta, jer mu upravo informacione tehnologije u potpunosti odgovaraju za ostvarenje novih ciljeva. Elektronska elita, zbog njenog monopola nad tokovima informacija, biće u stanju da manipuliše socijalnim, političkim i ekonomskim ambijentom. Takve elite su već demonstrirale uticaj na ishod političkih procesa.

Ključne riječi: kriminal, kompjuterski kriminalitet, računarski sistemi, kompjuter, policija, oblici kompjuterskog kriminaliteta, suzbijanje kriminaliteta**.**

POJAM, OSNOVNE KARAKTERISTIKE I POJAVNI OBLICI KOMPJUTERSKOG KRIMINALITETA

Prvi evidentiran slučaj kompjuterskog kriminaliteta pojavio se 1958. godine, a prvi slučaj koji je procesuiran na federalnom nivou u SAD bio je izmjena

[1] Gojko Vasić, direktor policije, predavač za grupu kriminalističkih predmeta, VŠUP Banja Luka, e-mail: *Direktor@mup.vladars.com*
[2] Borislav Šarić, načelnik Jedinice za strateško planiranje i analitiku i stručni saradnik za grupu policijskih predmeta, VŠUP Banja Luka, e-mail*: borislav.saric@yahoo.com*
[3] Vlado Jovanić, načelnik Jedinice za profesionalne standarde i stručni saradnik za grupu kriminalističkih predmeta, VŠUP Banja Luka, e-mail: *vlado.jovanic@hotmail.com*
[4] Vebsti, R. DŽ.: Međunarodni vodič za borbu protiv kompjuterskog kriminaliteta.

bankarskih slogova (zapisa) iz 1966. godine. Na prostorima bivše SFRJ, prvi slučaj kompjuterskog kriminala zabilježen je 1983. godine.

Kod pojmovnog određenja kompjuterskog kriminala, prisutna su dva osnovna pristupa. Prvi pristup jasno opredjeljuje i daju njegovu egzaktnu definiciju, dok drugi, usvajajući deskriptivan pristup, navodi ponašanja koja pripadaju ovom vidu delinkvencije. Statistički biro Ministarstva pravde SAD kompjuterski kriminalitet definiše kao: „...svaki kriminal za koji izvršilac mora imati tehnička znanja o kompjuterima da bi u njemu učestvovao."

INTERPOOL je organizovao prvu seminarsku obuku posvećenu suzbijanju kompjuterskog kriminaliteta 1981. godine, i tom prilikom definicija je proširena na sljedeći način: „...svaki ilegalni akt za čije je uspješno izvršenje, istragu, gonjenje ili kažnjavanje esencijalno poznavanje kompjuterske tehnologije." Kada je riječ o pokušajima definisanja ovog pojma u domaćoj literaturi, jasno je da su oni nedovoljni, a razlog tome svakako leži u činjenici da su naša iskustva u fazi dostizanja. Od domaćih autora, definicija vrijedna pažnje jeste svakako ona koju je dao prof. dr Đorđe Ignjatović, koji se prema ovom pitanju precizno određuje:[5] „kompjuterski kriminal predstavlja poseban vid inkrimisanih ponašanja kod kojih se računarski sistem pojavljuje kao sredstvo izvršenja ili kao objekat krivičnog djela, ukoliko se to djelo na drugačiji način, ili prema drugom objektu, uopšte ne bi moglo izvršiti ili bi ono imalo bitno drugačije karakteristike."

Priznati svjetski stručnjak u oblasti kompjuterskog kriminaliteta Parcer, pod pojmom kompjuterski kriminalitet podrazumijeva zloupotrebu kompjutera, a to je svaki događaj u vezi sa upotrebom kompjuterske tehnologije u kome žrtva trpi ili bi mogla da trpi gubitak, a učinilac djeluje u namjeri da sebi pribavi ili bi mogao da pribavi korist. U oblasti kompjuterskog kriminaliteta „tamna brojka" vidno je prisutna, što ukazuje na činjenicu da je priličan broj izvršenih krivičnih djela ostao neotkriven. Mjesto i vrijeme izvršenja krivičnih djela iz domena kompjuterskog kriminaliteta, koji predstavljaju odgovore na dva zlatna pitanja kriminalistike „gdje i kada", u izvjesnoj mjeri odstupaju od tradicionalnih kriminalističkih učenja u odnosu na krivična djela opštega i privrednog kriminaliteta. Kompjuterski kriminalitet ima sopstveni način izvršenja, koji njegovi učinioci stalno usavršavaju i dopunjuju novim elementima kompjuterske tehnike i korišćenjem kriminalističke informatike. Posebna karakteristika kompjuterskog kriminaliteta jeste nastala štetna posljedica, kako u odnosu na privredne, finansijske i druge institucije, tako i u odnosu na građane. Štetna posljedica se ispoljava u vidu nastale imovinske štete, ali isto tako može da se ispolji i u vidu gubljenja povjerenja u bezbjednost i tačnost dobijenih informacija iz kompjuterskog sistema. U stranoj i domaćaj naučnoj literaturi, koja obrađuje problematiku kompjuterskog kriminaliteta, nema bitnih razlika oko prezentovanja oblika kompjuterskog kriminaliteta i određivanja njegovog sadržaja.

Prof. dr V. Vodinelić[6] oblike kompjuterskog kriminaliteta dijeli u četiri grupe:

- neovlašćeno korišćenje računara,
- manipulisanje računarima,
- računarska špijunaža,
- sabotaža računara.

[5] Ignjatović, Đ.: Pojmovno određenje kompjuterskog kriminala, Beograd, 1991, str. 142–143.
[6] Jovičić, D., Bošković, M.: Kriminalistika metodika, Banja Luka, 2002, str. 446–449.

S druge strane, autor Stevan Petrović,[7] razmatrajući problematiku ispoljavanja kompjuterskog kriminaliteta, navodi njegove sljedeće oblike:

- finansijska prevara,
- zloupotreba računara,
- vandalizam,
- sabotaža,
- špijunaža.

U Krivičnom zakonu Republike Srpske, u glavi HHIVa (Krivična djela protiv bezbjednosti računarskih podataka) implementirana je Međunarodna konvencija o suzbijanju kompjuterskog kriminaliteta, koja je razrađena kroz sedam članova:

- oštećenje računarskih podataka i programa,
- računarska sabotaža,
- izrada i unošenje računarskih virusa,
- računarska prevara,
- neovlašćeni pristup zaštićenom računaru, računarskoj mreži, telekomunikacionoj mreži i elektronskoj obradi podataka,
- sprečavanje i ograničavanje pristupa javnoj računarskoj mreži,
- neovlašćeno korišćenje računara ili računarske mreže.

POTENCIJALNI CILJEVI KOMPJUTERSKOG KRIMINALITETA I PROFIL KOMPJUTERSKOG DELINKVENTA

Kompjuterski sistem označava svaki uređaj ili grupu međusobno povezanih ili uslovljenih uređaja, od kojih jedan ili više njih, u zavisnosti od programa, vrši automatsku obradu podataka, dok kompjuterski podaci označavaju svako izlaganje činjenica, podataka ili koncepata u obliku koji je pogodan za njihovu obradu u kompjuterskom sistemu, uključujući tu i odgovarajući program na osnovu kojeg kompjuterski sistem vrši svoju funkciju.

U tom kontekstu, potencijalni ciljevi kompjuterskog kriminaliteta mogu biti:[8] hardver, softver, programi, podaci, zaštita, usluge, dok bi se brojne aktivnosti koje mogu imati karakter kriminalnih radnji mogle grupisati na slijedeći način:

- **atak na hardver** (uništenje, oštećenje ili otuđenje računarskog sistema ili njegovih komponenti),
- **atak na softver** (uništenje, oštećenje, otuđenje i neovlašćena izmjena, objavljivanje ili korišćenje softverskih proizvoda),
- **atak na program** (uništenje, oštećenje, otuđenje i neovlašćena izmjena, objavljivanje ili korišćenje programskih proizvoda),
- **atak na podatke** (uništenje, oštećenje, otuđenje i neovlašćena izmjena, objavljivanje ili korišćenje podataka),
- **atak na zaštitu** (narušavanje ili probijanje sistema zaštite), i
- **atak na usluge** (neovlašćeno korišćenje informacionih resursa).

Većina ljudi ima stereotipnu sliku kriminalca, koju su formirali filmovi i televizija, a ona je najčešće nastala na osnovu tipa gangstera iz doba prohibicije

[7] Banović, B., Bošković, M.: Kriminalistika metodika, Beograd, 2001, str. 400.
[8] Petrović, S.: Kompjuterski kriminalitet, MUP Republike Srbije, Beograd, 2001, str. 45–46.

u SAD, dvadesetih godina prošlog vijeka. Danas, mnogi pišu o tome kakav je kompjuterski kriminalac. Svako profilisanje može da bude varljivo i da odvede na stranputicu. Struktura izvršilaca kompjuterskog kriminala razmatrana je sa različitih aspekata. Prema Wongovoj analizi, kada je riječ o učešću muškaraca i žena u izvršavanju kompjuterskog kriminala, odnos učešća je četiri na prema jedan u korist muškaraca. Međutim, prema studiji koja je rađena u Švedskoj, zastupljenost ženskog pola u registrovanim djelima kompjuterskog kriminala iznosila je 44%.

Današnjeg kompjuterskog eksperta moguće je profilisati kao uglavnom mladog, inteligentnog, visokomotivisanog, uzornog i povjerljivog radnika, spremnog da radi prekovremeno, da istražuje i da se bori s iznenadnim radnim situacijama kada je potreban dodatni napor kako bi se prevazišao problem. Ima čvrsto izgrađenu logiku i odlično poznavanje kompjuterskog sistema, njegove mogućnosti i način korišćenja. Potencijalno, on je savršeni kompjuterski kriminalac. Iz ovako širokog skupa potencijalnih izvršilaca kompjuterskih krivičnih djela moguće je izdvojiti tipične grupe sa određenim karakteristikama, a to su amateri i profesionalci.[9] Ove grupe su identične u oblasti klasičnog kriminala. Međutim, u oblasti kompjuterskog kriminala u okviru ove dvije grupe, izdvojila se posebna grupacija koju čine širom svijeta poznati hakeri.[10]

METODIKA OTKRIVANJA I DOKAZIVANJA KOMPJUTERSKOG KRIMINALITETA

Kompjuterski kriminalitet je relativno novi vid kriminalnog ponašanja koji se još nije u potpunosti izdiferencirao u odnosu na druge vidove kriminaliteta. Njegova osnovna karakteristika jeste da ispoljava veliku fenomenološku raznovrsnost, što otežava njegovo definisanje i precizno uređivanje i sistematizovanje. To je osnovni razlog što se u većini zakonodavstava još i sada oblici djela koji obuhvataju ovu vrstu kažnjivih ponašanja postavljaju dosta široko i razvrstani su u različita zakonska poglavlja (standardizacija se vrši kroz implementaciju Međunarodne konvencije o sprečavanju kompjuterskog kriminala), koja uglavnom uređuju djela protiv imovine, ljudskih prava, privrede i dr. Kompjuterska krivična djela su po svojim osobinama slična krivičnim djelima protiv imovine, posebno djela prevare i otuđenja tuđe stvari, sa kojima ih povezuje kako sličnost u radnji izvršenja tako i identičnost motiva vršenja djela (potrebno je preciznije razmišljati o kategoriji „virtuelne svojine“ kao oblika svojine i o problemu njenog zakonskog određenja).

Ovo djelo čini onaj ko neovlašćeno uđe u tuđu zaštićenu bazu podataka i unese izmjene, uništi, kopira, upotrijebi, sakrije, objavi ili unese kakav svoj

[9] Aleksić, Ž., Milovanović, Z.: Kriminalistika, Beograd,1994, str. 260.

[10] Pojam „haker“ ima više značenja: novajlija, početnik u igri golfa koji raskopava teren; kopač rovova ili taksista; kreativni programer ili onaj koji neovlašćeno ulazi u tuđi kompjuterski sistem. Dodatne karakteristike hakera jesu: dominiraju pripadnici muškog pola; ekstremno su bistri, skloni istraživačkom i logičkom razmišljanju i uvijek takmičarski raspoloženi; sa svakom uspješnom realizacijom na tastaturi oni vide sebe kao afirmisane autoritete nad računarom i nad bilo kim ko je povezan sa njim, što im daje osjećaj snage i kontrole; teže da se informatičkim proizvodima bave površno; imaju malo respekta prema onima koji ne znaju ništa o njihovoj omiljenoj temi – kompjuteru. U: Krstić, O.: Maloljetnička delinkvencija, Banja Luka, 2009, str. 197–199.

podatak ili kompjuterski virus, ili na neki drugi način učini neupotrebljivim tuđe kompjuterske podatke ili programe.[11] Radnja izvršenja je postavljena alternativno i obuhvata, kao što se vidi, raznovrsne djelatnosti kojima se provaljuje u kompjuterski sistem. Izvršioci ovih djela su u najvećem broju slučajeva tzv. hakeri, koji se putem svojih personalnih računara, koristeći globalnu mrežu internet, uključuju u druge informacione sisteme. Za postojanje djela potrebno je da se u kompjutersku bazu podataka ulazi neovlašćeno.

U subjektivnu stranu djela nije unesena namjera pribavljanja imovinske koristi (postavlja se ponovo pitanje „virtelne svojine"), ali ukoliko je ta korist pribavljena, sud je može cijeniti pri odmjeravanju kazne. Ovo je učinjeno zbog teškoća u profilisanju učinilaca ovakvih krivičnih djela, jer je nekad teško dokazati da li se radi o tzv. zlonamjernim učiniocima, tj. onim učiniocima koji su to učinili radi sticanja protivpravne imovinske koristi ili nanošenja drugom štete, ili jednostavno radi zadovoljstva u neovlašćenom prodiranju u neki dobro čuvani informacioni sistem.

Takođe, inkriminacijom krivičnog djela upad u kompjuterski sistem obezbjeđuje se krivičnopravna zaštita kompjuterskih podataka u privrednom poslovanju od njihovog neovlašćenog mijenjanja. Djelo vrši onaj ko u privrednom poslovanju, u namjeri da sebi ili drugom pribavi protivpravnu imovinsku korist ili drugog ošteti, neovlašćeno unese izmjene, sakrije, izbriše ili uništi tuđe kompjuterske podatke ili programe, dakle, pod uslovom da to radi neovlašteno.[12]

Kod kompjuterskih krivičnih djela suština radnje izvršenja sastoji se u neovlašćenom ulaženju, odnosno upadu u tuđu kompjutersku bazu podataka, gdje radnjama navedenim u opisu krivičnih djela učinilac i izvršava neko od ovih krivičnih djela. S obzirom na to da je objekt napada, odnosno da je kompjuter i sredstvo izvršenja, da se radi o neovlašćenom ulaženju i upadu u kompjuterski sistem, odnosno zaštićenu kompjutersku bazu podataka, a ako se uzme u obzir identičnost i sličnost radnje izvršenja, jasan je zaključak da je i metodika otkrivanja, razjašnjavanja i dokazivanja ovih krivičnih djela dosta slična, a u nekim fazama i ista.

Krivična djela u kojim sa računar javlja u određenoj vezi sa izvršenim djelom, uglavnom spadaju u oblast opšteg i privrednog kriminaliteta, ali s obzirom na to da se izvršavaju uz pomoć kompjutera, to im daje specifičnosti koje se odražavaju i na tragove koji mogu nastati od strane kompjutera kao sredstva izvršenja tih krivičnih djela. Sa stanovišta kriminalističkooperativnog korišćanja tragova kompjutera, veoma je bitno poznavati i sljedeće specifičnosti u izvršavanju kompjuterskih krivičnih djela:[13]

- mjesto izvršenja kompjuterskih krivičnih djela vezano je za lokaciju kompjutera, ali ne kao kod klasičnih oblika kriminaliteta gdje učinilac uglavnom mora da bude na mjestu izvršenja krivičnog djela,
- za izvršenje pojedinih kompjuterskih krivičnih djela potrebno je sasvim malo vremena, jer se ono mjeri sekundama i minutama,
- lica koja vrše krivična djela kompjuterskog kriminaliteta moraju da

[11] Babić, M., Marković, I.: Krivično pravo – posebni dio, Banja Luka, 2005, str. 247–249.
[12] Isto, str. 284.
[13] Matijević, M., Bošković, M.: Kriminalistika operativa, Banja Luka, 2007, str. 399–403.

posjeduju odgovarajući fond znanja i vještina iz oblasti kompjuterske tehnike,

- kompjuterski kriminalitet ima sopstveni modus operandi, koji njegovi učinioci stalno usavršavaju,
- posljedice kompjuterskog kriminaliteta mogu se ispoljiti u pribavljanju protivpravne imovinske koristi, nanošenju materijalne štete, zatim u prisvajanju tajnih podataka i drugih povjerljivih informacija, te u stvaranju nepovjerenja prema kompjuterskoj tehnici.

Indicije u vezi sa kompjuterskim krivičnim djelima mogu se ispoljiti prije, za vrijeme i nakon izvršenja krivičnog djela i imaju isključivo operativni značaj, jer čak i ne moraju da znače da se u svakoj takvoj situaciji odvija određena kriminalna djelatnost. Stoga je nužno da se sve informacije koje pružaju ove indicije provjere odgovarajućom operativnom djelatnošću, te na osnovu prikupljenih nivoa informacija sagleda cjelokupno činjenično stanje, pa da se zaključi da li postoje osnovi sumnje da je izvršeno kompjutersko krivično djelo, što i opredjeljuje dalji tok operativne djelatnosti.

Tragovi kompjutera koji nastaju izvršenjem određenih krivičnih djela imaju odgovarajući kriminalističkooperativni značaj, jer pružaju informacije o izvršenom kompjuterskom krivičnom djelu i omogućavaju planiranje operativne djelatnosti u pravcu osumnjičenih lica. Pored toga, pojedini tragovi kompjutera, a naročito nosioci podataka, mogu da dobiju i procesni značaj putem vještačenja, čime se dobija dokazna informacija u odnosu na određeno krivično djelo i učinioca.

Specifičnosti kompjuterskog kriminaliteta i operativnog rada po kompjuterskim krivičnim djelima, zahtijevaju određeni vid specijalizacije operativnih radnika koji rade na suzbijanju ovog vida kriminaliteta. U nedostatku operativnih radnika koji raspolažu takvim znanjima, potrebno je od samog početka u operativni rad uključiti i odgovarajućeg stručnjaka za kompjutere, kako bi se zajedničkim radom doprinijelo efikasnijem pronalaženju tragova i obezbjeđenju materijalnih dokaza.

Problematika otkrivanja kompjuterskih krivičnih djela svakim danom je sve složenija, s obzirom na to da je u početnoj fazi primjene kompjuterske tehnike i tehnologije manji broj ljudi posjedovao odgovarajuća stručna znanja i vještine koje su im omogućavale da kompjuter koriste u kriminalne svrhe. Danas, naročito pojavom mikro računara i personalnih računara stvoreni su uslovi za mnogo širi krug korisnika kompjutera, a samim tim i za veći broj lica koja su u situaciji da kompjuter koriste kao sredstvo izvršenja krivičnog djela ili kao objekat napada u realizaciji svoje kriminalne djelatnosti.

Dosadašnja praksa ukazuje na to da se mnogi oblici kompjuterskog kriminaliteta ne otkrivaju sve dok neko od učinilaca ne napravi grešku u manipulaciji kompjuterom. Takođe, moguće je da se tragajući za nekom drugom uočenom greškom otkrije određena kriminalna djelatnost bilo pojedinca ili grupe koji su neovlašćeno upali u kompjuterski sistem, pa je moguće da se primjenom specijalnog programa napravi odgovarajuća zamka koja će poslužiti da se učinioci otkriju. Do saznanja o kompjuterskom krivičnom djelu može se doći na više načina, među kojima su najčešći:[14] prijava radnika, anonimne i pseudonimne prijave i nadzor i kontrola.

[14] Aleksić, Ž., Milovanović, Z.: Kriminalistika, Beograd, 1994, str. 297.

Radnici su često najbolji izvor informacija o zloupotrebi računara, iz prostog razloga što se nalaze na mjestu događanja i imaju detaljan uvid u sve što se oko njih dešava, a jedan od osnovnih preduslova za takav njihov odnos prema zloupotrebi jesu lojalnost i moral. Kao izvor informacija o izvršenoj zloupotrebi mogu da posluže i anonimne ili pseudonomne prijave, koje nikako ne bi trebalo bezrezervno prihvatiti, ali ni olako odbaciti, dok se ne izvrši provjera njihove istinitosti. Prijava oštećenog pojavljuje se kao češći način saznanja o izvršenom kompjuterskom krivičnom djelu, bez obzira na to da li je krivično djelo otkriveno slučajno, u postupku kontrole, ili zahvaljujući grešci učinioca.

Kao izvor saznanja koji ukazuje na sumnju da je izvršeno određeno krivično djelo korišćenjem kompjutera ili uopšte u vezi sa kompjuterom, mogu se pojaviti i sredstva javnog informisanja. Policija u sklopu svojih operativnih djelatnosti može doći do relevantnih informacija koje sadrže sumnju da je izvršeno neko od kompjuterskih krivičnih djela. U određenim slučajevima, s ciljem otkrivanja pojedinih oblika kompjuterskog kriminaliteta, policija može primjenjivati odgovarajuća kriminalističkotehnička sredstva, zatim posebne istražne mjere i radnje u dokazivanju (npr. prikriveni istražitelj, odnosno online undercover), a u posljednje vrijeme sve je češća primjena digitalne forenzičke analize računarskog sistema.[15]

MJERE ZAŠTITE

Novi izazovi koje ekspanzija visokotehnološkog kriminala postavlja pred policijske službe sastoje se u činjenici da je prikupljanje tačnih statističkih podataka o ovim aktivnostima na internetu veoma otežano. Statistika vezana za broj krivičnih prijava, odnosno izvještaja o počinjenim krivičnim djelima i krivičnih djela iz oblasti visokotehnološkog kriminala nije dovoljno precizan pokazatelj kojim se mogu iskazati pojavni oblici, niti njihova konačna struktura i obim. Ona može predstavljati samo trenutni pokazatelj i orijentir, a nikako relevantan prikaz trendova. Takođe, treba naglasiti i da je tamna brojka vezana za broj krivičnih djela najizraženija upravo kada je u pitanju ovaj tip kriminalnih aktivnosti. Savremene informacione tehnologije, memorijski kapaciteti računarskih mreža i globalna distribucija podataka i informacija dodatno otežavaju mogućnost otkrivanja ovih krivičnih djela.

Neki od problema koji se pojavljuju, kada je u pitanju otkrivanje ovih krivičnih djela, jesu:

1. tehnička opremljenost i osposobljenost policijskih službenika vezana za otkrivanje izvršilaca u *online* okruženju,
2. pravna regulativa koja nije u skladu sa savremenim oblicima izvršenja krivičnih djela iz oblasti visokotehnološkog kriminala, pri čemu se vrlo

[15] Digitalna forenzička nauka ili digitalna forenzika jeste relativno nova naučna disciplina (uspostavljena 1999. godine) koja obezbjeđuje pouzdani alat za istragu kompjuterskog kriminala, akviziciju i analizu digitalnih podataka i pripremu i prezentaciju digitalnih podataka pred sudom. U: Milosavljević, M., Grubor, G.: Digitalna forenzika računarskog sistema, Univerzitet Singidunum, Beograd, 2009, str. 10.

često javlja potreba za usklađivanjem postojećih zakonodavnih riješenja pravnim propisima koji bi pratili promjene u tehničkoj strukturi i savremene tokove u razvoju informacionog društva,

3. nedostatak operacionalnih obuka koje bi omogućile da policijski službenici koji se bave sprečavanjem visokotehnološkog kriminala budu dovoljno obučeni i tehnički opremljeni za vršenje ovih zadataka,
4. veoma velike poteškoće u otkrivanju izvršilaca krivičnih djela koji koriste lažne identitete u *online* okruženju, posebno kada se u obzir uzme činjenica da je u velikom broju slučajeva međunarodna policijska saradnja slaba, i da treba da bude mnogo efikasnija,
5. poteškoće u otkrivanju tačne lokacije izvršenja krivičnog djela, pošto se ova krivična djela vrše sa mnogih mjesta širom svijeta, a u velikom broju slučajeva izvršioci krivičnih djela koriste mreže sa javnim pristupom.

Odgovor na pitanje čime se štititi podrazumijeva identifikaciju svih mjera koje stoje na raspolaganju u izgradnji cjelovitog i pouzdanog sistema zaštite. Sve te mjere, po svojim prirodnim svojstvima, mogu se razvrstati na sljedeći način:[16] normativne, fizičko-tehničke i logičke.

Ovakva klasifikacija raspoloživih mjera omogućava navođenje njihovih, sa stanovišta efikasnosti i troškova, najbitnijih karakteristika, koje mogu poslužiti kao vrlo pouzdani kriterujumi prilikom njihovog izbora. Mjere normativnog karaktera, u koje spadaju pravne, organizacione i kadrovske mjere, pripadaju kategoriji netehničkih mjera. Osnovna karakteristika ovih mjera jeste da ne degradiraju rad sistema, već naprotiv, znatno doprinose povećanju njegove raspoloživosti i produktivnosti, a istovremeno značajno utiču na efikasnost sistema zaštite. Njihovom realizacijom stvara se osnov na koji će se, primjenom fiziko-tehničkih i logičkih mjera, nadograđivati sistem zaštite do konačne realizacije.

Ove mjere predstavljaju kohezivne spone koje sva ostala sredstva, mjere i procedure povezuju u jedinstven zaštitni mehanizam, pretvarajući klasičnu lančanu zaštitu u mrežnu zaštitu, sa svim prednostima koje ovakav oblik zaštitnog mehanizma nosi sa sobom. Kod lančane zaštite, kidanje jedne karike dovodi do raspada cijelog sistema. Nasuprot tome, kidanjem jedne spone ne mreži nastaje šupljina, ali sistem opstaje, njegova funkcionalna sposobnost jeste umanjena, ali nije neutralisana.

Fizičko-tehničke mjere mogu biti vrlo efikasne za određivanje problema zaštite, ali isto tako povlače za sobom i znatne troškove. Njihova zajednička karakteristika jeste da uslovljavaju finansijske investicije prije nego što počnu da dejstvuju, znači unaprijed, plus troškove njihovog tekućeg održavanja. Pozitivna strana se ogleda u činjenici da se ovakvi troškovi mogu tačno procijeniti i izbor planski podesiti raspoloživim finansijskim mogućnostima. Ono što svakako treba imati u vidu je činjenica da efikasnost ovih mjera značajno opada u ambijentu u kojem normativne mjere nisu primijenjene ne adekvatan način.

Logičke mjere za nemali broj problema zaštite automatizovanih informacionih sistema predstavljaju jedino, ali i vrlo složeno sredstvo. Visok stepen efikasnosti se prvenstveno postiže korišćenjem logičkih mjera u paketu. S druge strane, ove mjere povlače za sobom tzv. nevidljive troškove, jer direktno utiču na smanjenje

[16] Petrović, S.: Kompjuterski kriminalitet, MUP Republike Srbije, Beograd, 2001, str. 16–18.

raspoloživosti i efikasnosti računarskog sistema, a to je dovoljan razlog da se njihovoj primjeni pristupi krajnje odgovorno, osmišljeno i racionalno. Takođe, efikasnost ovih mjera je uslovljena adekvatnom primjenom mjera normativnog karaktera.

PODRUČJE PRIMJENE MEĐUNARODNOG PROJEKTA ZA BORBU PROTIV KOMPJUTERSKOG KRIMINALITETA

Međunarodni projekat za borbu protiv kompjuterskog kriminala nastoji da:

a) unaprijedi međunarodnu saradnju i koordinaciju u borbi protiv kompjuterskog kriminala, i
b) proširi rad Grupe 8, Savjeta Evrope i drugih multinacionalnih organizacija i industrijskih zemalja u vezi sa kompjuterskim kriminalom na zemlje u razvoju, sa ciljem da se ubrza:[17]

1. usvajanja zakona o kompjuterskom kriminalu i razvoj usaglašenih pravnih okvira,
2. poštovanje ljudskih prava, privatnosti i bezbjednosti,
3. saradnja po pitanjima nadležnosti i rješavanje tih pitanja,
4. saradnja između organa reda, davalaca usluga komunikacija i kompanija koje se bave elektronskom trgovinom,
5. prihvatljivi načini rada pretresa i zapljene kompjutera i elektronskog dokaznog materijala,
6. saradnja između organa državnog i privatnog sektora u borbi protiv kompjuterskog kriminaliteta.

Objašnjavajući značaj ovih pitanja za budući napredak zemalja u razvoju, Komitet za zaštitu privatnosti i borbe protiv kompjuterskog kriminala Američke advokatske komore smatra da će ovaj projekat pomoći zemljama u razvoju da privuku direktna strana ulaganja i operacije informaciono-komunikacionih tehnologija i njihovim građanima donijeti ekonomske i društvene prednosti koje pruža tehnologija.

Zakoni rezimirani u projektu nude smjernice zemljama koje namjeravaju da uvedu ili razviju djelotvorne zakone o kompjuterskom kriminalu. U nedostatku saglasnosti ili pristupa javnim komunikacijama, presretanje komunikacija od strane državnih organa, kao i zapljena ili prinudno otkrivanje podataka koji se nalaze u posjedu preduzeća ili pojedinca, smatraju se narušavanjem privatnosti. Memorisani digitalni dokazni materijal može se dobiti neposrednim pristupom memorisanim podacima ulaskom u kuću ili kancelariju. U većini pravnih sistema to se smatra ozbiljnim narušavanjem privatnosti i zahtijeva prethodno pravno odobrenje, često od strane sudskog službenika nakon što mu istražioci pokažu da postoji potreba i opravdanost. Otkrivanje memorisanih podataka može se postići i prinudnim putem, pozivom na svjedočenje. To će zahtijevati obraćanje pažnje kako na praktična, tako i na pravna pitanja koja se tiču pristupa komunikacijama i memorisanim podacima.

Takođe, priroda kompjuterskog kriminala zahtijeva blisku saradnju između državnog i privatnog sektora. Elektronska krivična djela mogu da počine nezadovoljni ili bivši radnici, hakeri i lica koja se bave organizovanim kriminalom, domaći i

[17] Džodi R. Vebsti: Međunarodni vodič za borbu protiv kompjuterskog kriminaliteta, str. 42–43.

strani konkurenti, teroristi, kao i druge države. Mreže i sisteme koji su napadnuti, ili upotrijebljeni za kompjuterski kriminal, često koriste privatne kompanije. Saradnja između državnog i privatnog sektora oko kompjuterskih napada i kompjuterskih kriminalnih aktivnosti važna je i pomaže da obje strane bolje shvate kako da reaguju na kompjuterski kriminal i ublaže njegov uticaj. To obavezno podrazumijeva razmjenu informacija, što za različite ljude može da ima različito značenje.

ZAKLJUČNA RAZMATRANJA

Kontinuiran razvoj nauke i tehnike izvršio je značajan uticaj na oblike i metode suzbijanja kriminaliteta, dok je ekspanzija razvoja informacionih tehnologija i telekomunikacija omogućila korišćenje dokaza u elektronskoj formi. Ubrzani razvoj kompjuterskih tehnologija zahtijeva budnost zakonodavca i neprestano praćenje promjena koje se dešavaju, te neophodnost podešavanja pozitivnog zakonodavstva kako bi se moglo odgovoriti novim izazovima. Naime, nesporno je da će proširivanje nadležnosti specijalizovanih organizacionih jedinica MUP-a Republike Srpske za borbu protiv visokotehnološkog kriminala i na takva krivična djela, omogućiti brže i efikasnije njihovo otkrivanje i procesuiranje.

Istovremeno, evidentno je da radnje u krivičnom postupku i istrazi za ovaj tip krivičnih djela po prirodi stvari moraju zadirati u privatnost lica, zbog čega je bitno da to bude samo u mjeri koja je nužna i saglasna međunarodnim standardima u ovoj oblasti. U tom smislu s pravom se insistira na poštovanju osnovnih standarda ustavom garantovane zaštite od nezakonitog pretresanja (presretanja i analize poruka) i zapljene (sakupljanja poruka, programa i računara), tako da u u postupanju postoji ravnoteža između interesa zaštite privatnosti i društvenog interesa za krivični progon. S tim u vezi treba podsjetiti i na činjenicu da podatke kojima se narušava pravo na privatnost, a do kojih dođu organi otkrivanja i krivičnog gonjenja u toku kriminalističke istrage, oni moraju čuvati kao službenu tajnu i ne smiju ih koristiti ni u kakve svrhe osim za potrebe krivičnog postupka.

Nijedna računarska instalacija nije apsolutno otporna na kriminalne aktivnosti iz prostog razloga što ne postoji ni apsolutna zaštita, pa broj i vrsta registrovanih objavljenih slučajeva predstavljaju pravu riznicu za kriminalnu hroniku, mada se otkriva dio od ukupnog broja učinjenih djela. Današnji stepen tehničkog i tehnološkog razvoja omogućio je korišćenje novih metoda u kriminalistici, ali je i ostvario uticaj na formiranje novih oblika kriminaliteta i na usavršavanje učinilaca u izvršavanju raznih krivičnih djela.

Kompjuter, kao moćno tehničko sredstvo, našao je primjenu u svim sferama ljudskog života, ali najveći problem jeste to što se pojavio i kao sredstvo pomoću kojeg se vrše krivična djela. Veliki problem i ono što ga naročito otežava jeste činjenica da je u pitanju kriminalitet čiji su izvršioci, ne samo naoružani visokim intelektom, već su podržani i snagom informacione tehnologije koja njihove mogućnosti multiplicira.

Činjenica je da nedostaje dovoljno efikasan sistem nadgledanja interneta u cilju otkrivanja krivičnih djela visokotehnološkog kriminala, kao i efikasna platforma za prijavljivanje ovih krivičnih djela u *online* okruženju. Kao poseban problem se javlja i potreba za boljom saradnjom sa fakultetima, nevladininim

organizacijama, privatnim sektorom itd. Porebno je da se ustanovi efikasan *CERT* tim (*Computer Emergency Responce Team*) za sprečavanje ovih krivičnih djela, i odrede institucije čiji bi predstavnici trebali da se angažuju u ovom pravcu. Uspostavljanje ovakvog tima u velikoj mjeri bi doprinijelo efikasnijem sprečavanju ovih krivičnih djela, bržem i odgovornijem pristupu u istraživanju ove pojave i objedinjenom odgovoru na izazove i prijetnje koje ova pojava donosi.

LITERATURA

1. Aleksić, Ž.; Milovanović, Zoran: Kriminalistika, Beograd, 1994. godina;
2. Babić, Miloš; Marković, Ivanka: Krivično pravo – posebni dio, Banja Luka, 2005. godina;
3. Banović, Božidar; Bošković, Mićo: Kriminalistika metodika, Beograd, 2001. godina;
4. Bošković, Mićo: Kriminalistika metodika II, Beograd, 1996. godina;
5. Bošković, Mićo: Organizovani kriminalitet i korupcija, Banja Luka, 2004. godina;
6. Vebsti, R. Džodi: Međunarodni vodič za borbu protiv kompjuterskog kriminaliteta, Rukovodilac projekta i urednik edicije;
7. Ignjatović, Đ: Pojmovno određenje kompjuterskog kriminaliteta, Beograd, 1991. godina;
8. Jovičić, Dragomir; Bošković, Mićo: Kriminalistika metodika, Banja Luka, 2002. godina;
9. Krstić, Ostoja: Maloljetnička delinkvencija, Banja Luka, 2009. godina;
10. Matijević, Mile; Bošković, Mićo: Kriminalistika operativa, Banja Luka, 2007. godina;
11. Milosavljević, M., Grubor, G.: Digitalna forenzika računarskog sistema, Univerzitet Singidunum, Beograd, 2009. godina;
12. Petković, Slobodan: Kompjuterski kriminalitet, Beograd, 2001. godina;
13. Simović, N. Miodrag: Krivično-procesno pravo, drugo izmijenjeno i dopunjeno izdanje, Banja Luka, 2007. godina;
14. Krivični zakon Republike Srpske (Službeni glasnik RS br. 49/03);
15. Zakon o izmjenama i dopunama Krivičnog zakona Republike Srpske (Službeni glasnik RS br. 73/10);
16. Konvencija o visokotehnološkom kriminalu, Budimešta, 2001.

Mr Gojko Vasić
Ministry of Internal Affairs
Mr Borislav Šarić
Ministry of Internal Affairs
Vlado Jovanić
Ministry of Internal Affairs

CYBER CRIME

Abstract: At the beginning of the 20th century, on the global level of information exchange, an important transformation based on the computer systems began. These technologies brought the new complex challenges to law enforcement units. The appearence and growth of the cyber crime influences on citizens and governments in the world. The usage of computers is applicable in every segment of human lives.

This way of crime acts means the specific crime acts which are performed with computers, and as such those are described in the penalty code or some other distinguish laws. Cyber crime presents a major threath for using informative techniques in the world. Cyber crime is present everywhere, has new forms, and larger threath, especially through acts of transnational organized crime, since the informative techniques give an opportunity to reach new goals. Electronic elite that has a monopol over the global informations will manipulate with social, political and economic environment. The power of these elites has already been demonstrated by influencing the political processes.

Key words: crime, cyber crime, computer systems, computer, police, shapes of computer crime, crime prevention.

Prethodno saopštenje – UDK 341.48: 004.738.5(094.5)(100)

MEĐUNARODNOPRAVNI DOKUMENTI KOJIMA SE UREĐUJE OBLAST VISOKOTEHNOLOŠKOG KRIMINALA

Dr Miodrag Romić[1]
Fakultet političkih nauka, Banja Luka
romicdrmiodrag@blic.net
Nikolina Grbić-Pavlović[2]***, mr***
Visoka škola unutrašnjih poslova, Banja Luka
nikolinagrbic@blic.net

Apstrakt: U radu se daje prikaz relevantnih međunarodnih propisa koji se odnose na borbu protiv visokotehnološkog kriminala. Tačnije, u radu će se ukazati na brojne rezolucije Ujedinjenih nacija, zatim na konvencije Savjeta Evrope, te direktive Evropske unije kojima se uređuje navedena problematika. Konkretno, u radu će biti govora o rezolucijama UN u borbi protiv zloupotrebe informatičkih tehnologija, te Rezoluciji Ekonomsko-socijalnog savjeta. Centralni dio rada odnosiće se na Konvenciju Savjeta Evrope o sajber kriminalu i njen Dodatni protokol. Takođe, biće govora i o drugim konvencijama koje se tiču ove materije, poput: Konvencije o zaštiti prava pojedinca u vezi sa automatskom obradom ličnih podataka, Konvencije o zaštiti djece od seksualne eksploatacije i seksualnog zlostavljanja, te Konvencije o sprečavanju terorizma. Nadalje, od pravnih instrumenata koji su nastali u okvirima Evropske unije, ukazaćemo na Direktivu o pravnoj zaštiti kompjuterskih programa i Direktivu o čuvanju podataka koji su dobijeni ili obrađeni prilikom pružanja javno dostupnih usluga elektronske komunikacije ili javnih komunikacionih mreža.

Ključne riječi: visokotehnološki kriminal, međunarodnopravni instrumenti.

UVOD

Obavljanjem svakodnevnih (poslovnih i privatnih) aktivnosti putem informatičkih tehnologija identifikovana je potreba za obezbjeđivanjem njihovog rada, kao i za obezbjeđivanjem korisnika tehnologija od zloupotreba i primjena zarad obavljanja protivpravnih radnji. Kada se ustanovilo da računarska oprema i internet komunikacije mogu poslužiti za pripremu i izvršenje čitavog niza kriminalnih radnji, ovom problemu se pristupilo znatno ozbiljnije (Reljanović, 2008: 90).

Danas, veoma značajno područje savremenog transnacionalnog kriminala[3]

[1] Autor je docent na Fakultetu političkih nauka Univerziteta u Banjoj Luci.
[2] Autorka je doktorand na Pravnom fakultetu Univerziteta Union u Beogradu i asistentica na Pravnoj katedri na Visokoj školi unutrašnjih poslova.
[3] Sajber kriminal je po svojoj prirodi transnacionalni iz prostog razloga jer se počinioci i žrtve često nalaze u različitim jurisdikcijama, što predstavlja znatnu poteškoću agencijama za sprovođenje zakona u njihovom istraživanju i procesuiranju počinilaca krivičnih djela "na mreži" (Schreier, Weekes, Winkle, 2010: 20).

jeste računarski, kompjuterski ili visokotehnološki kriminal[4] (Schmallager, 2006: 474). U širem smislu, to je kriminalna djelatnost u kojoj su računar ili mreža izvor, sredstvo, predmet, cilj ili prostor krivičnog djela. Mnogi međusobno različiti oblici krivičnih djela mogu se podvesti pod ovaj pojam. U tom smislu, visokotehnološki kriminal se može definisati kao kriminalna djelatnost koja uključuje informacionu tehnologiju, infrastrukturu, neovlašćen pristup, ilegalno presretanje putem informatičkih uređaja, oštećenje, uništenje, izmjenu ili potiskivanje podataka, uticaj na djelovanje informacionog sistema unošenjem, prenosom, oštećenjem, uništenjem ili izbacivanjem podataka, krađom podataka, prevarom i dr. (Degan, Pavišić, Beširević, 2011: 292–293). Uzroci za pojavu visokotehnološkog kriminala su prije svega u lakom pristupu podacima, slaboj zaštiti (relativnoj), neobučenosti državnih institucija za gonjenje novih formi kriminala i (relativno) lakom skrivanju dokaza o izvršiocu krivičnog djela (ili čak činjenici da je djelo izvršeno) (Reljanović, 2008: 90).

Ubrzan razvoj[5] kompjuterskih tehnologija zahtijeva konstantnu aktivnost zakonodavaca i neprestano praćenje promjena koje se dešavaju na polju razvoja kompjuterskih tehnologija, te usaglašavanje pozitivnog zakonodavstva sa međunarodnim instrumentima kojima bi trebalo odgovoriti novim izazovima. Mnogobrojni su međunarodni propisi koji se direktno ili indirektno odnose na borbu protiv visokotehnološkog kriminala.[6] Posljednjih godina vlade mnogih država, ali i međunarodne organizacije postale su više fokusirane na hitnost djelovanja u oblasti sajber bezbjednosti[7] (Cornish, 2010: viii).

Kroz djelatnost Komisije za prevenciju kriminaliteta i krivično pravosuđe Ujedinjenih nacija[8] doneseni su sljedeći dokumenti:

- Rezolucija br. 55/63 od 22. januara 2001. godine[9],
- Rezolucija br. 56/121 od 23. januara 2002. godine[10],
- Rezolucija Ekonomsko-socijalnog savjeta br. 2007/20 od jula 2007. godine[11].

---

[4] *Computer crime, cybercrime, e-crime, hi-tech crime, electronic crime.* Vidi šire u (Moore, 2005). Prema stanovištvu MUP Republike Srbije, visokotehnološki kriminal obuhvata skup krivičnih djela gdje se kao objekat izvršenja i kao sredstvo za izvršenje krivičnog djela javljaju računari, računarske mreže, računarski podaci, kao i njihovi produkti u materijalnom i elektronskom obliku.

[5] Ubrzani razvoj kompjuterskih tehnologija sa sobom je donio niz problema vezanih za, između ostaloga, primjenu složenih posebnih istražnih radnji, ali i za primjenu osnovnih radnji dokazivanja, kao što je pretresanje pokretnih stvari, tj. pretresanje kompjuterskih sistema, uređaja za pohranjivanje kompjuterskih i elektronskih podataka i mobilnih telefonskih aparata. Vidi šire u: (Barašin, Hukeljić, 2010: 439).

[6] U radu ćemo ukazati na najznačajnije pravne instrumente u borbi protiv sajber kriminala koji su nastali pod okriljem OUN, Savjeta Evrope i Evropske unije. Međutim, imajući u vidu da bi opširno obrazlaganje svakog od njih posebno predstavljalo jedan ogroman napor, a s obzirom na to da je obim rada ograničen, u radu će se opširnije obrazložiti samo najznačajniji međunarodni dokumenti.

[7] O sajber bezbjednosti vidi šire u: Cornish P., Hughes R., Livingstone, D. (2009): *Cyberspace and the National Security of the United Kingdom - Threats and Responses*. A Chatham House Report. London: Royal Institute of International Affairs.

[8] Organizacija kojoj su Ujedinjene nacije povjerile vodeću ulogu u postupku harmonizacije nacionalnih zakonodavstava u oblasti visokotehnološkog kriminala, kao i generalno u materiji bezbjednosti u sajber prostoru, jeste Međunarodna telekomunikaciona unija (ITU), koja predstavlja vodeću agenciju u okviru OUN za pitanja komunikacionih i informatičkih tehnologija. O agenciji vidi šire na internet stranici: *http://www.itu.int*

[9] „Resolution A/res/55/63“ General Assembly of the United Nations, 22. januar 2001.

[10] „Resolution A/res/56/121“, General Assembly of the United Nations, 23. januar 2002.

[11] „Resolution 2007/20“, The Economic and Social Council of the United Nations, 26. jul 2007.

Dokumenti Savjeta Evrope jesu:

- Preporuka o kriminalnim aktivnostima povezanim sa upotrebom računara, iz 1989. godine[12],
- Preporuka koja je za predmet regulisanja imala pitanja koja se tiču procesnih pravila u vezi sa informatičkim tehnologijama, iz 1995. godine[13],
- Konvencija o zaštiti prava pojedinca u vezi sa automatskom obradom ličnih podataka, iz 1981. godine, stupila na snagu 1985. godine[14],
- Konvencija i Dodatni protokol Savjeta Evrope o visokotehnološkom kriminalu, konvencija je iz 2001. godine, a stupila na snagu 1. jula 2004. godine, dodatni protokol iz 2003. godine, stupio na snagu 1. marta 2006. godine[15],
- Konvencija o sprečavanju terorizma, iz 2005. godine[16],
- Konvencija o zaštiti djece od seksualne eksploatacije i seksualnog zlostavljanja, iz 2007. godine[17].

Pravni instrumenati nastali u okvirima Evropske unije jesu:

- Direktiva o pravnoj zaštiti kompjuterskih programa, iz 1991. godine, sa obavezom primjenjivanja od 1. januara 1993. godine[18],
- Direktiva o čuvanju podataka koji su dobijeni ili obrađeni prilikom pružanja javno dostupnih usluga elektronske komunikacije ili javih komunikacionih mreža, iz 2006. godine.[19]

UJEDINJENE NACIJE

Ogranizacija ujedinjenih nacija (OUN) kao međunarodna organizacija osnovana je 1945. godine na Konferenciji u San Francisku. Formiranjem OUN uspostavljeni su efektivni instrumenti za zaštitu međunarodnog mira, ljudskih prava i poboljšanja uslova života širom svijeta (Popović, Turčinović, 2007: 62). Danas navedena organizacija okuplja 192 suverene države. Legislativna aktivnost ove organizacije je veoma obimna, pogotovo ako se zna da su specijalizivane agencije odgovorne za veliki broj legislativnih formi koje opslužuju međunarodnu trgovinu,

---

[12] Savjet Evrope, Preporuka No. R. (89) 9.

[13] Savjet Evrope, Preporuka No. R. (95) 13.

[14] *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (ETS No. 108, the 28 January 1981, Entry into force: 1. 10. 1985).

[15] *Convention on Cybercrime*, Budapest, 23. XI 2001. (ETS No. 185). *Additional protocol to the convention on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems*, Strasbourg, 28. I 2003. (ETS No. 189).

[16] *Convention on the Prevention of Terrorism* (CETS No. 196).

[17] *Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse*, Lanzarote, 25. 10. 2007.

[18] „*Council Directive of 14 may 1991 on the Legal Protection of Computer Programs*“, Directive 91/250/EEC, Official Journal no L 122/42.

[19] „*Directive 2006/24/EC of the European Parliament and of the Council: on the retention of data generated or processed in connection with provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC*“, Official Journal of the European Union, 13. 4. 2006.

transport, komunikacije, obrazovanje, kulturu itd. (Popović, Turčinović, 2007: 80). Kada su pitanju nove tehnologije, naročito informatičke i komunikacione, OUN je još u tzv. milenijumskoj deklaraciji[20] kao jedan od prioritetnih ciljeva utvrdila potrebu da se nove tehnologije učine bezbjednim i dostupnim svima. Isto tako, OUN kroz djelatnost svojih specijalizovanih tijela, a posebno putem Komisije za prevenciju kriminaliteta i krivično pravosuđe, čini napore da se promoviše međunarodna saradnja u oblasti harmonizacije i primjene krivičnih zakona i u oblasti borbe protiv visokotehnološkog kriminala. Upravo kao rezultat ovih napora 2001. i 2002. godine nastale su Rezolucije br. 22/63 i br. 56/121 o borbi protiv zloupotrebe informatičkih tehnologija (Komlen-Nikolić i dr., 2010: 36).

Rezolucija br. 55/63 o borbi protiv zloupotrebe informatičkih tehnologija

Navedenom Rezolucijom, a izražavajući zabrinutost zbog novih mogućnosti za razvoj kriminalnih aktivnosti u svijetu informatičkih tehnologija, države članice OUN usaglasile su se oko deset mjera u borbi protiv visokotehnološkog kriminala. Kao prvo, sve države treba da, kroz svoja nacionalna zakonodavstva i praksu, onemoguće postojanje tzv. „sigurnih utočišta“ za izvršioce krivičnih djela visokotehnološkog kriminala. Drugo, navodi se da mora postojati koordinacija između svih zainteresovanih država u vezi sa saradnjom u istrazi i krivičnom gonjenju međunarodnih slučajeva zloupotrebe informacionih tehnologija. Dalje, potrebno je razmjenjivati informacije između država koje su u vezi sa problemima sa kojima se suočavaju u borbi protiv sajber kriminala. Zatim, svaka država treba da posveti naročitu pažnju edukaciji, odnosno savremenim metodama obuke lica angažovanih na otkrivanju i krivičnom progonu izvršilaca krivičnih djela ovog kriminala. Takođe, potrebno je pravnim mehanizmina zaštititi povjerljivost, integritet i dostupnost računarskih podataka i sistema od neovlašćenog uništenja, izmjene ili brisanja, a u vezi sa navedenim je i obaveza da se pravno reguliše postupak čuvanja i brzog pristupa elektronskim podacima koji su u vezi sa aktuelnim krivičnim istragama. Nadalje se ukazuje na potrebu da se javnost upozna sa opasnostima koje prijete iz sajber prostora, kao i na činjenicu da odgovarajuće mjere prevencije mogu spriječiti izvršenje mnogih krivičnih dela ili barem uticati na njihovo blagovremeno prijavljivanje. U mjeri u kojoj je to izvodljivo, informacione tehnologije treba da budu osmišljene tako da pomognu da se spriječi i otkrije kriminalno ponašanje, da se prate kriminalci i prikupe dokazi. Konačno, Rezolucija upozorava da se u borbi protiv zloupotrebe računarskih tehnologija mora očuvati balans između individualnih prava i sloboda garantovanih svakom pojedincu, sa jedne strane, i prava države da krivično goni počinioce krivičnih djela, sa druge strane (Resolution 55/63, 2001: 2–3).

Rezolucija 56/121 Generalne skupštine UN

Rezolucija 56/121 usvojena 23. januara 2002. godine, takođe za predmet ima borbu protiv zloupotrebe informatičkih tehnologija. Kao dopuna rezoluciji 55/63, još jednom je ukazano na potrebu da se prilikom usvajanja odgovarajućih

[20] Rezolucija br. 55/2 Generalne skupštine UN od 18. septembra 2000. godine.

zakona, kao i prilikom utvrđivanja politike krivičnog progona, uzmu u obzir rezultati rada Komisije za prevenciju kriminala i krivično pravosuđe, kao i drugih relevantnih međunarodnih i regionalnih organizacija. Takođe, još jednom je ukazano na potrebu da se mjerama navedenim prethodnom rezolucijom posveti adekvatna pažnja (Resolution 56/121, 2002: 2).

Rezolucija Ekonomsko-socijalnog savjeta 2007/20

Međunarodna saradnja u oblasti prevencije, istrage, krivičnog progona i kažnjavanja privrednog kriminaliteta i djela povezanih sa zloupotrebom identiteta našla se na dnevnom redu Ekonomsko-socijalnog savjeta OUN, što je rezultiralo usvajanjem Rezolucije 2007/20 u julu 2007. godine. Neposredan povod za akciju bila je zabrinutost zbog uloge koju informatičke i komunikacione tehnologije imaju u evoluciji, odnosno širenju međunarodnog privrednog kriminaliteta, kao i kriminaliteta koji nastaje kao rezultat krađe i zloupotrebe identiteta (Udruženje javnih tužilaca i zamenika javnih tužilaca Srbije, 2010: 39).

Rezolucija poziva države članice da ozbiljno razmotre potrebu za modernizacijom postojećeg nacionalnog zakonodavstva, naročito imajući u vidu dramatičan porast transnacionalnog privrednog kriminaliteta i u vezi s tim upotrebu modernih računarskih tehnologija kao sredstva za izvršenje ovih krivičnih djela. Ukazuje se i na potrebu da nacionalna krivična zakonodavstva, ukoliko to nisu učinila, predvide neovlašćenu upotrebu ili izradu identifikacionih dokumenata kao i podataka o identitetu. S tim u vezi, podstiče se i šira i efikasna upotreba modernih tehnologija u prevenciji i suzbijanju kako privrednog kriminaliteta, tako i kriminaliteta koji je u vezi sa zloupotrebom identiteta (Komlen-Nikolić i dr., 2010: 38–39). Konačno, ukazuje se i na potrebu da države članice razmotre pristupanje Konvenciji Saveta Evrope o visokotehnološkom kriminalu, kao i svim drugim međunarodnim pravnim aktima koji su primjenljivi kada je u pitanju privredni kriminalitet i zloupotreba identiteta i identifikacionih podataka (Ekonomsko-socijalni savjet, 2007: 3). Takođe, postignuta je i saglasnost da se pitanja privrednog kriminaliteta i zloupotrebe identiteta, kao posebna tema, nađu na dnevnom redu Komisije za prevenciju kriminaliteta i krivično pravosuđe OUN.

SAVJET EVROPE

Savjet Evrope je regionalna evropska organizacija, osnovana 1949. godine. Cilj ove organizacije jeste unapređenje integracije evropskog kontinenta putem zaštite i ostvarenja zajedničke baštine država članica, i to prije svega slobode pojedinca, političke slobode i vladavine prava. Radi ostvarenja ovog cilja, Savjet Evrope može da razmatra široku lepezu pitanja, od politike i ekonomije do nauke i kulture, ali nema ovlašćenja da se bavi vojnim pitanjima (Dimitrijević i dr, 2007:120). Savjet Evrope se još od osamdesetih godina prošlog vijeka bavi suzbijanjem visokotehnološkog kriminala, a u okviru ove organizacije je nastala i zasad jedina međunarodna konvencija koja uređuje pojedina pitanja iz ove oblasti na nadnacionalnom nivou. Osnovni pravni

izvor o visokotehnološkom kriminalu na evropskom nivou jeste Konvencija o visokotehnološkom kriminalu[21]. Upravo zbog toga će se pažnja posvetiti ovoj Konvenciji i njenom dodatnom protokolu.

Konvencija o visokotehnološkom kriminalu sadrži odredbe materijalnog i procesnog krivičnog prava, kao i pravila o međunarodnoj pravnoj pomoći, izručenju i odredbe o njenoj primjeni. Unutar pojedinih grupa predviđaju se posebna krivična djela, s tim što treba imati u vidu posebna obilježja koja nacionalna zakonodavstva mogu propisati kao zakonska obilježja ovih djela (Degan, Pavišić, Beširević, 2011: 294). Ciljevi Konvencije su, prije svega, harmonizacija između nacionalnih zakonodavstava kada je riječ o materijalnopravnim odredbama u oblasti visokotehnološkog kriminala, zatim uvođenje adekvatnih instrumenata u nacionalna zakonodavstva kada je riječ o procesnim odredbama, kako bi se stvorila osnova za istraživanje i procesuiranje ovih krivičnih djela, te ustanovljavanje brzih i efikasnih institucija i procedura međunarodne saradnje (Komlen-Nikolić i dr., 2010: 42).

Konvencija se sastoji od preambule i četiri poglavlja. Prvo poglavlje Konvencije ima samo jedan član i daje kratak pregled i definicije osnovnih termina koji su upotrebljeni u daljem tekstu, odnosno definiše se šta je to: računarski sistem[22], računarski podatak[23], davalac usluge[24] i podatak u saobraćaju[25]. Drugo poglavlje Konvencije podijeljeno je najprije na dva odjeljka koja se tiču materijalnih i procesnih mjera, koje se države potpisnice obavezuju da će uvesti u nacionalno zakonodavstvo, a ovi opet na više dijelova. Svrha materijalnopravnih odredaba je da unaprijede sredstva prevencije i kažnjavanja krivičnih djela koja su izvršena upotrebom savremenih tehnologija, odnosno povezana sa upotrebom računara i računarskih mreža. Pri tom, Konvencija treba da uspostavi minimum zajedničkih standarda kada je riječ o inkriminisanju tih djela. Na taj način se stvara osnova za saradnju između nadležnih organa država kao i za razmjenu iskustava. Takođe, ovakav pristup će eliminisati mogućnost da se u slučaju eventualne ekstradicije počinioca stavi prigovor nedostatka dvostruke inkriminacije (Udruženje javnih tužilaca i zamenika javnih tužilaca Srbije, 2010: 41–42).

Prvi dio inkriminisanih krivičnih djela obuhvata krivična djela protiv povjerljivosti, cjelovitosti i dostupnosti računarskih podataka i sistema, i to su:

---

[21] Konvencija je usvojena 2001. godine, a stupila na snagu 1. jula 2004. godine, dok je dodatni protokol usvojen 2003. godine, a stupio je na snagu 1. marta 2006. godine. Do februara 2012. godine Konvenciju su ratifikovale 32 zemlje, među kojima i BiH, a 15 zemalja ju je potpisalo.

[22] Računarski sistem je grupa povezanih uređaja, od kojih najmanje jedan može da izvodi automatsku obradu podataka.

[23] Računarski podatak je svaka činjenica, odnosno informacija koja se nalazi u formi pogodnoj za obradu u računarskom sistemu, uključujući i programe koji se mogu upotrebljavati za vršenje određenih funkcija računara.

[24] Davalac usluge ima dvostruko značenje: pod njime može da se podrazumijeva svako fizičko ili pravno lice koje pruža usluge omogućavanja komunikacije putem računarske mreže, ali i svako lice koje čuva, odnosno procesuira računarske podatke nastale za vrijeme takve komunikacije, odnosno upotrebe uređaja.

[25] Podatak u saobraćaju podrazumijeva svaki računarski podatak koji je vezan za komunikaciju unutar računarskog sistema ili je nastao kao dio takve komunikacije, i nosi informaciju o porijeklu i odredištu komunikacije, njenom putu, datumu, vremenu, veličini i trajanju, ili vrsti usluge.

nezakonit pristup[26], nezakonito presretanje[27], ometanje podataka i ometanje rada sistema[28], te zloupotreba uređaja[29]. Drugi dio inkriminisanih djela označen je pod nazivom kompjuterska krivična djela, a obuhvata samo dva djela, i to: falsifikovanje[30] i prevaru[31]. Treći dio ima samo jedan član, a bavi se djelima koja su vezana za sadržaj komunikacije na računarskoj mreži, odnosno koja su posvećena dječijoj pornografiji[32]. Četvrti dio ovog odjeljka takođe je sadržan u jednom članu Konvencije, a posvećen je djelima kršenja autorskih i srodnih prava. U tri stava, kršenje autorskih prava se ne inkriminiše samostalno, već putem definicija sadržanih u već postojećim međunarodnim ugovorima. Konačno, posljednji članovi drugog poglavlja grupisani su u peti dio pod nazivom sporedna odgovornost i sankcije, a bave se inkriminacijom pokušaja izvršenja, pomaganja i podstrekavanja za navedena djela, odgovornosti pravnih lica[33] i propisivanjem sankcija za počinjena djela iz Konvencije (Savjet Evrope, 2001: 4–8).

Drugi odjeljak drugog poglavlja pod nazivom „Procesno pravo“, takođe se dijeli dalje na pet dijelova, a bavi se procesnim ovlašćenjima državnih organa

---

[26] Nezakonit pristup je pristup informacijama sadržanim na računaru ili računarskom sistemu, u namjeri da se te informacije prisvoje, izmijene ili unište. Za ovo djelo se traži namjera, tako da je državama potpisnicama ostavljena mogućnost da inkriminišu samo posebne radnje koje dovode do ilegalnog pristupa nekom računaru ili mreži. (Član 2. Konvencije).

[27] Nezakonito presretanje je prestretanje privatnih podataka koji se prenose na bilo koji način između dva računara (ili mreže). Konvencija ostavlja mogućnost državama da ovako definisano djelo ograniče postojanjem namjere. (Član 3. Konvencije).

[28] Ometanje podataka i ometanje sistema na računaru podrazumijeva namjerno potpuno ili djelimično oštećenje, brisanje, promjenu sadržine, kompresiju i bilo koji drugi način izmjene originalnih podataka. (Član 4. i 5. Konvencije).

[29] Zloupotreba uređaja je složeno krivično djelo, stoga, generalnom odredbom države potpisnice preuzimaju na sebe obavezu da kazne svaku namjernu ilegalnu proizvodnju, posjedovanje, upotrebu ili nabavku, prodaju, kao i svaki drugi oblik distribucije i činjenja dostupnim nekome, ko na to inače nema pravo, bilo kog „uređaja“, pod kojim se podrazumijevaju i računarski programi, kao i bilo koji drugi oblik podataka. Konvencija, dopušta državama da stave rezervu na ovaj član, osim kada je riječ o prodaji ili drugom obliku distribucije lozinki ili drugih računarskih podataka pomoću kojih se mogu počiniti navedena djela. Na ovaj način se državama ostavlja da same odrede domašaj pomenutog principa da nema kažnjavanja bez (jasno) inkriminisanog krivičnog djela. (Član 6. Konvencije).

[30] Falsifikovanje se odnosi samo na umišljajno, neovlašćeno ubacivanje, brisanje, izmjenu ili sakrivanje računarskih podataka, koje rezultira izmijenjenim sadržajem tih podataka. Državama je ostavljena mogućnost da predvide i posebnu vrstu namjere da se učini prevara da bi postojalo ovo krivično djelo. (Član 7. Konvencije).

[31] Prevara je definisana kao umišljajno, neovlašćeno ubacivanje, brisanje, izmjena ili sakrivanje računarskih podataka, kao i svako drugo miješanje u rad računarskog sistema, u cilju da se pribavi protivpravna imovinska korist za sebe ili treće lice. (Član 8. Konvencije).

[32] Države potpisnice se obavezuju da kao krivično djelo u domaćim zakonodavstvima inkriminišu sljedeće aktivnosti: proizvodnju dječije pornografije u cilju njenog distribuiranja kroz računarski sistem; nuđenje ili činjenje dostupnim dječije pornografije kroz računarski sistem; distribuciju ili slanje dječije pornografije kroz računarski sistem; nabavljanje dječije pornografije za sebe ili drugoga putem računarskog sistema; posjedovanje dječije pornografije na računarskom sistemu ili na medijumu za prenos računarskih podataka. Inkriminisano je, u stvari, svako ponašanje vezano za dječiju pornografiju, uključujući i pribavljanje i posjedovanje. Konvencija sadrži i neke odredbe koje se tiču starosnih granica onih koji se smatraju djecom. (Član 9. Konvencije).

[33] Predviđena je krivična, građanska i administrativna odgovornost pravnog lica, kao i posebna krivična odgovornost samih počinilaca djela. Da bi se pravno lice moglo smatrati odgovornim za krivično djelo iz Konvencije, ono mora biti počinjeno u njegovu korist, a izvršilac (saizvršilac, pomagač, podstrekač) tog djela mora biti jedan od funkcionera pravnog lica. (Član 12. Konvencije).

prilikom istraživanja krivičnih djela vezanih za nove tehnologije[34]. Prvi dio odnosi se na opšte odredbe koje nalažu državama da u svoje krivično pravo uvedu prethodno navedena krivična djela, kao i druga djela koja se ne nalaze u tekstu Konvencije a koja se mogu podvesti pod ovu grupu. Drugi dio nosi naziv hitna zaštita pohranjenih kompjuterskih podataka, dok treći govori o nalogu za dostavu podataka. Četvrti dio nosi naziv pretresanje i oduzimanje pohranjenih kompjuterskih podataka, a prema Konvenciji, nadležni državni organi imaju ovlašćenja da pregledaju i zaplijene svaki računar ili nosač podataka na kome se nalaze, ili sumnjaju da se mogu nalaziti, sporni materijali, kao i da od provajdera elektronskih komunikacija prikupljaju podatke koji se odnose, prije svega, na upotrebu interneta i kreditnih kartica, preko kojih se može doći do imena ili IP adrese potencijalnog počinioca krivičnog djela[35] (Komlen-Nikolić i dr., 2010: 47–48). Peti dio nosi naziv prikupljanje kompjuterskih podataka u realnom vremenu, a sastoji se od dva člana koja govore o prikupljanju podataka o prometu u stvarnom vremenu i presretanju podataka[36].

Treći odjeljak drugog poglavlja sastoji se samo od jednog člana, a odnosi se na sudsku nadležnost. Naime, država će imati nadležnost za procesuiranje ukoliko je krivično djelo počinjeno na njenoj teritoriji, na brodu ili avionu koji nosi njenu zastavu, kao i ako je krivično djelo počinio državljanin te države, pod uslovom da je ono kažnjivo u drugoj državi koja poznaje istu takvu inkriminaciju, ili van državnih teritorija. Međutim, stav 2 istog člana omogućava državama da ne primjenjuju pravila o nadležnosti u određenim slučajevima ili pod određenim okolnostima. [37]

Treće poglavlje Konvencije se bavi međunarodnom saradnjom država na suzbijanju visokotehnološkog kriminala, i to prije svega na način koji bi trebalo da prevaziđe praktične prepreke pri sprovođenju nacionalnog zakonodavstva za krivična djela koja po pravilu prelaze državne granice, a često podrazumijevaju i učešće pojedinaca iz nekoliko zemalja širom svijeta.[38] Otuda su glavne odredbe ovog djela posvećene saradnji država na organizovanoj ili spontanoj razmjeni podataka[39] koji se tiču eventualnog izvršenja nekog od krivičnih djela vezanih za upotrebu elektronskih komunikacija, kao i mogućnosti ekstradicije počinilaca takvih djela iz jedne države potpisnice u drugu. Svaka država potpisnica mora povjeriti određenom tijelu posao saradnje sa drugim državama u oblasti visokotehnološkog kriminala, a u slučaju hitnosti, saradnja može biti uspostavljena i direktno između pravosudnih organa dvije države, kao i preko Interpola i drugih relevantnih kanala saradnje, dakle bez dugih procedura koje bi išle preko centralnih vlasti država a koje su predviđene kao pravilo pri saradnji u ovoj oblasti.[40] Prema članu 31 Konvencije, svaka država potpisnica može tražiti od druge da sprovede određene istražne radnje na svojoj teritoriji, ako je to neophodno za vršenje istrage u vezi sa nekim od djela

[34] Članovi od 14. do 22. Konvencije.
[35] Članovi od 19. do 20. Konvencije.
[36] Član 21. Konvencije.
[37] Ipak, ako država ne izvrši ekstradiciju svog državljanina, mora mu suditi za počinjena djela na teritoriji druge države potpisnice, takođe, odredbe o nadležnosti države sadržane u Konvenciji neće derogirati odredbe domaćeg prava prema kojem država može i na neki drugi način uspostaviti svoju krivičnu nadležnost. (Član 22. Konvencije).
[38] Članovi od 23. do 35. Konvencije.
[39] Član 26. Konvencije.
[40] Član 27. stav 9. Konvencije.

predviđenih Konvencijom. Ukupno gledano, Konvencija predviđa različite vidove saradnje država, prilagođene tehnologiji vršenja istraga i procesuiranja ove vrste krivičnih djela. Takođe, državama je ostavljeno dosta prostora da u praksi, ili u dodatnim bilateralnim sporazumima, dalje preciziraju one vrste saradnje za koje imaju poseban interes (Komlen-Nikolić i dr., 2010: 50).

Kada je riječ o ekstradiciji, treba posvetiti pažnju izuzecima – kada država neće biti u obavezi da izruči neko lice. To je prije svega slučaj kada je u pitanju nedostatak dvostruke inkriminacije, ali Konvencija predviđa i dopunski uslov – djelo mora biti označeno kao ozbiljno u samom zakonu, odnosno za njegovo izvršenje mora biti zaprijećena minimalna kazna od jedne godine zatvora, ako nije drugačije predviđeno nekim drugim međunarodnim ugovorom između država u pitanju, koji se može primijeniti na datu situaciju. Takođe, između država koje nemaju međusobne bilateralne ili multilateralne ugovore o ekstradiciji, Konvencija će služiti kao osnov za ekstradiciju (Udruženje javnih tužilaca i zamenika javnih tužilaca Srbije, 2010: 52). Zanimljiva je i odredba koja se tiče osnivanja „mreže 24/7“ u svakoj od država, a koja bi služila kao podrška policijskim i drugim organima, kao kontakt za sva obavještenja i početna tačka za sve zahtjeve koji se tiču procesuiranja i istraživanja krivičnih djela visokotehnološkog kriminala[41] (Savjet Evrope, 2001: 13–19).

Peto, posljednje poglavlje Konvencije nosi naziv završne odredbe, a odnosi se na potpisivanje i stupanje na snagu, pristupanje, teritorijalnu primjenu i učinke, rješavanje sporova, otkaza Konvencije i drugo.[42]

Dodatni protokol uz Konvenciju o visokotehnološkom kriminalu odnosi se na inkriminaciju djela rasističke i ksenofobične prirode izvršenih preko računarskih sistema. Osnovna svrha njegovog donošenja jeste da se inkriminišu ponašanja koja nisu obuhvaćena Konvencijom, a koja se tiču širenja mržnje, netolerancije i netrpeljivosti prema rasnim, nacionalnim, vjerskim i drugim grupama i zajednicama, korišćenjem računara kao sredstva komunikacije i širenja propagande. Protokol uvodi obavezu za države potpisnice da u nacionalnom zakonodavstvu inkriminišu sljedeća ponašanja: širenje rasističkog i ksenofobičnog materijala preko računarskih sistema[43], prijetnja motivisana rasizmom ili ksenofobijom[44], uvreda motivisana rasizmom ili ksenofobijom, poricanje, značajno umanjenje, odobravanje ili opravdanje genocida ili zločina protiv čovječnosti. Rješenja o implementaciji, procesnim radnjama i međunarodnoj saradnji, koja sadrži Konvencija, shodno se primjenjuju i na djela koja su utvrđena Protokolom (Komlen-Nikolić i dr., 2010: 52–53).

---

[41] Član 35. Konvencije.

[42] Članovi od 35. do 48. Konvencije.

[43] Širenje rasističkog i ksenofobičnog materijala preko računarskih sistema podrazumijeva svaku radnju kojom se ovakav materijal čini dostupnim javnosti korišćenjem računara, odnosno računarskog sistema. Materijal se može učiniti dostupnim na različite načine, kao što je njegovo slanje na veliki broj imejl adresa ili postavljanje na internet prezentacije. Državama je ostavljena sloboda da li će za ovakav postupak povući krivičnu odgovornost ili ne, kao i da stave rezervu na one oblike ponašanja koji su prema njihovom unutrašnjem pravu dozvoljeni kao vid izražavanja slobode govora.

[44] Prijetnja motivisana rasizmom ili ksenofobijom predstavlja stavljanje u izgled pojedincu ili grupi da će prema njima biti izvršeno neko teško krivično djelo, kako je definisano u domaćem zakonodavstvu država, korišćenjem računara ili računarskih sistema. Pojedinac ili grupa treba da se izdvajaju prema svojoj rasi, boji kože, porijeklu, nacionalnoj, etničkoj ili vjerskoj pripadnosti da bi ovo djelo imalo specifičan oblik predviđen Protokolom.

EVROPSKA UNIJA

Od pravnih instrumenata koji su nastali u okvirima Evropske unije, izdvajaju se dvije direktive, i to: Direktiva o pravnoj zaštiti kompjuterskih programa i Direktiva o čuvanju podataka koji su dobijeni ili obrađeni prilikom pružanja javno dostupnih usluga elektronske komunikacije ili javih komunikacionih mreža.

Direktiva Savjeta Evropske zajednice o pravnoj zaštiti kompjuterskih programa

Direktiva Savjeta Evropske zajednice o pravnoj zaštiti kompjuterskih programa usvojena je 17. maja 1991. godine sa obavezom primjenjivanja u državama članicama od 1. januara 1993. godine. Potrebu za uniformnim rješenjima u oblasti pravne zaštite kompjuterskih programa nametnule su razlike u nacionalnim zakonodavstvima država članica koje su imale nepovoljan uticaj na funkcionisanje zajedničkog tržišta, kao i opasnost da bi se ovi problemi mogli pojačati ukoliko bi se nastavilo sa praksom pojedinačnog i neusklađenog regulisanja ove materije. Takođe, uzeto je u obzir i ekskluzivno pravo autora da spriječi neovlašćeno umnožavanje svog djela. U skladu sa odredbama Direktive, države članice zaštićuju autorskim pravom kompjuterske programe kao književna djela, i to u smislu odredaba Bernske konvencije za zaštitu književnih i umjetničkih djela, a pojam „kompjuterski program“ obuhvata i pripremni materijal za koncipiranje programa (Udruženje javnih tužilaca i zamenika javnih tužilaca Srbije, 2010: 68).

Direktiva predviđa i obavezu da se kao nedozvoljena, pravno sankcionišu tačno navedena ponašanja, i to: stavljanje u promet kopije kompjuterskog programa, sa znanjem da je kopija nedozvoljena ili uz poštovanje razloga za osnovanu sumnju u njenu nedozvoljenost; držanje iz komercijalnih razloga kopije kompjuterskog programa, sa znanjem da je kopija nedozvoljena ili imajući razloge za osnovanu sumnju u njenu nedozvoljenost; i stavljanje u promet ili držanje u komercijalne svrhe svakog sredstva čija je jedina svrha da olakša nedozvoljeno uklanjanje ili neutralizaciju svakog tehničkog mehanizma eventualno napravljenog u cilju zaštite kompjuterskog programa. Propisana je i obaveza da se zaplijeni svaka nedozvoljena kopija kompjuterskog programa u skladu sa pocedurom koja je propisana procesnim pravilima nacionalnih zakonodavstava. Što se tiče trajanja, zaštita je obezbijeđena tokom života autora i pedeset godina nakon njegove smrti ili smrti poslednjeg živog autora ukoliko je u pitanju grupa autora (Komlen-Nikolić i dr., 2010: 61–62).

Direktiva 2006/24/EU Evropskog parlamenta i Savjeta o čuvanju podataka koji su dobijeni ili obrađeni prilikom pružanja javno dostupnih usluga elektronske komunikacije ili javnih komunikacionih mreža

Osnovni cilj Direktive o čuvanju podataka jeste da se usklade odredbe država članica koje se tiču obaveze davaoca javno dostupnih usluga elektronske komunikacije i javnih komunikacionih mreža da čuvaju određene podatke koje dobijaju ili obrađuju, kako bi se osiguralo da ti podaci budu dostupni u svrhu istrage, otkrivanja i progona teških krivičnih djela[45]. Da bi se ispravno razumjelo područje

[45] Član 1. Direktive.

primjene ove Direktive, nužno je objasniti da se ona primjenjuje samo na podatke o prometu i lokaciji pravnih i fizičkih lica i na uz to vezane podatke nužne za identifikaciju pretplatnika ili registrovanog korisnika. Dakle, ona se ne primjenjuje na podatke na sadržaj elektronske komunikacije, kao ni na informacije do kojih se dolazi korišćenjem mreža elektronske komunikacije (Komlen-Nikolić i dr., 2010: 64).

Za potrebe Direktive primjenjuju se odgovarajuće definicije najznačajnijih pojmova, kao što su: podatak[46], korisnik[47], telefonska usluga[48], korisničko ime[49], identitet ćelije[50] i neuspješan poziv[51]. Centralni dio Direktive zauzima kategorizacija podataka koji se čuvaju, a taksativno su nabrojani i razvrstani u kategorije i potkategorije. Prva kategorija podataka su podaci potrebni za pronalaženje i identifikaciju izvora komunikacije; druga kategorija podataka koji se čuvaju jesu podaci potrebni za otkrivanje odredišta komunikacije; treća kategorija podataka odnosi se na one podatke koji su namijenjeni za utvrđivanje datuma, vremena i trajanja komunikacije; četvrtu kategoriju čine podaci koji su neophodni za otkrivanje vrste komunikacije; peta kategorija podataka koji se čuvaju jesu podaci neophodni za identifikaciju komunikacijske opreme korisnika ili njihove navodne opreme; i šesta grupa podataka koji se moraju čuvati jesu podaci potrebni za otkrivanje lokacije opreme za mobilne komunikacije (Udruženje javnih tužilaca i zamenika javnih tužilaca Srbije, 2010: 73–75).

Prema odredbama Direktive, države članice preuzimaju obavezu da sve navedene kategorije podataka čuvaju u razdoblju koje nije kraće od šest mjeseci niti duže od dvije godine od datuma komunikacije.[52] Međutim, države članice mogu preduzeti potrebne mjere koje u posebnim okolnostima opravdavaju produženje najdužeg vremena čuvanja koje propisuje Direktiva, uz obavezu da o navedenom produženju roka obavijeste Komisiju i druge države članice o preduzetim mjerama i razlozima zbog kojih su ove mjere primijenjene. Po pitanju pravne zaštite lica o kojima se podaci prikupljaju i čuvaju za određeni period, popisana je obaveza preduzimanja potrebnih mjera kako bi za svaki protivpravan pristup podacima koji se čuvaju bile predviđene zakonske posljedice i odgovornost koja se utvrđuje bilo u upravnom, bilo u krivičnom postupku. Navodi se da sankcije po svojoj prirodi i težini moraju biti srazmjerne i takve da odvraćaju od daljeg kršenja zakona (Komlen-Nikolić i dr., 2010: 66).

---

[46] Pod podatkom se smatraju podaci o prometu i lokaciji i uz njih vezani podaci nužni za identifikaciju pretplatnika ili korisnika.

[47] Korisnici su pravna ili fizička lica koja koriste javno dostupne elektronske komunikacije za poslovne ili privatne potrebe, a koja nisu nužno i pretplaćena na tu uslugu.

[48] Telefonska usluga se odnosi na pozive (glasovne, glasovnu poštu i konferencijske pozive), dopunske usluge (preusmjeravanje i prenos poziva) i usluge slanja poruka i multimedijalne poruke (SMS, EMS i MMS).

[49] Korisničko ime je jedinstvena identifikacija koja se dodjeljuje osobi koja stupa u pretplatnički odnos ili se registruje za pristup internetu ili uslugu komunikacije putem interneta.

[50] Identitet ćelije je identitet ćelije u mobilnoj telefoniji iz koje poziv otpočinje ili u kojoj se taj poziv završava.

[51] Neuspješan poziv je komunikacija u kojoj je telefonski poziv uspješno spojen, ali na njega nije odgovoreno ili je došlo do intervencije uprave operatera telefonije.

[52] Član 6. Direktive.

LITERATURA:

27. Barašin, M., Hukeljić, M. (2010). *Pretresanje pokretnih stvari prema Zakonu o krivičnom postupku Bosne i Hercegovine: Problem forenzičke analize kompjuterskih sistema, uređaja za pohranjivanje kompjuterskih i elektronskih podataka i mobilnih telefonskih aparata*, Pravna riječ, časopis za pravnu teoriju i praksu, broj 23. Banja Luka.
28. Cornish P., Hughes R., Livingstone, D. (2009). *Cyberspace and the National Security of the United Kingdom - Threats and Responses*. A Chatham House Report. London: Royal Institute of International Affairs.
29. Cornish, P., Livingstone, D., Clemente, D.,Yorke, C. (2010). *On Cyber Warfare*. A Chatham House Report. London: Royal Institute of International Affairs.
30. Dimitrijević, V. i dr. (2007). *Osnovi međunarodnog javnog prava*. Drugo izdanje. Beograd: Beogradski centar za ljudska prava.
31. Đuro-Degan, V., Pavišić, B., Beširević, V. (2011). *Međunarodno i transnacionalno krivično pravo*. Beograd: Pravni fakultet Univerziteta Union i Službeni glasnik.
32. Komlen-Nikolić, L., i dr. (2010). *Suzbijanje visokotehnološkog kriminala*. Beograd: Udruženje javnih tužilaca i zamenika javnih tužilaca Srbije.
33. Moore, R. (2005). *Cybercrime – investigating high-technology computer crime*. Cincinnati: Anderson Publishing.
34. Popović, V., Turčinović, F. (2007). *Međunarodno javno pravo*. Banja Luka: Pravni fakultet.
35. Udruženje javnih tužilaca i zamenika javnih tužilaca Srbije. (2010). *Priručnik za trening tužilaca i sudija u oblasti visokotehnološkog kriminala*. Beograd: Udruženje javnih tužilaca i zamenika javnih tužilaca Srbije.
36. Reljanović, M., i dr. (2008). *Borba protiv organizovanog kriminala u Srbiji, od postojećeg zakonodavstva do sveobuhvatnog predloga reforme*. Beograd: UNICRI.
37. Schmallager, F. (2006). *Criminology Today*, *An Integrative Introduction*. Fourth Edition. New Jersey: Pearson Education.
38. Schreier, F., Weekes, B., Winkle, H. T. (2010). *Cyber Security:The Road Ahead*. Geneva: The Geneva Centre for the Democratic Control of Armed Forces.
39. Council of Europe (2001). *Convention on Cybercrime*. Budapest: Council of Europe.
40. Council of Europe (2003). *Additional protocol to the convention on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems*, Strasbourg: Council of Europe.
41. *Council Directive of 14 may 1991 on the Legal Protection of Computer Programs*. Directive 91/250/EEC, Official Journal no L 122/42.
42. *Directive 2006/24/EC of the European Parliament and of the Council: on the retention of data generated or processed in connection with provision of publicly available electronic communications services or of public communications networks and amending.* Directive 2002/58/EC, Official Journal of the European Union, 13. 4. 2006.

43. Ekonomsko-socijalni savjet UN (2007). *Rezolucija 2007/20 o Međunarodnoj saradnji u oblasti prevencije, istrage, krivičnog progona i kažnjavanja privrednog kriminaliteta i djela povezanih sa zloupotrebom identiteta.* Njujork: UN.
44. Generalna skupština UN (2001). *Rezolucija br. 55/63 o borbi protiv zloupotrebe informatičkih tehnologija*. Njujork: UN.
45. Generalna skupština UN (2002). *Rezolucija br. 56/121 o borbi protiv zloupotrebe informatičkih tehnologija*. Njujork: UN.

RESUME

INTERNATIONAL DOCUMENTS REGULATING THE AREA OF TECH CRIME

Cyberspace – the global digital communication and information transfer infrastructure – presents a wide range of security challenges for private individuals, commercial enterprises, governments and international organizations. In recent years, governments and international organizations have become more focused on cyber security and increasingly aware of the urgency connected with it. This paper provides an overview of the relevant international regulations relating to the fight against cyber crime. Specifically, in this paper we have pointed out the numerous United Nations resolutions, the Council of Europe conventions and the Europea Union directives regulating this issue. The central part of the work refered to the Council of Europe Convention on Cyber Crime and its Additional Protocol. Also we have pointed to the Directive on the legal protection of computer programs and Directive on the retention data obtained or processed in the provision of publicity available electronic communications services or of public communications networks.

Prethodno saopštenje – UDK 004.738.5: 343.326(497.6 RS

VISOKOTEHNOLOŠKI KRIMINAL U REPUBLICI SRPSKOJ

spec. Gojko Šetka,
Visoka škola unutrašnjih poslova Banja Luka
gojkosetka@yahoo.com
spec. Željko Ratković,
Uprava kriminalističke policije MUP-a Republike Srpske
zeljoratkovic@yahoo.com

Apstrakt: Visokotehnološki kriminal koji u svijetu uzima sve više maha nije zaobišao ni prostor Republike Srpske. Aktuelnost i važnost ovog problema najbolje se spoznaje na osnovu uvida u pokazatelje koji govore o gubitcima svjetske privrede zbog ovog oblika kriminala. Na osnovu izvještaja kompanije Norton, **sajber kriminal** godišnje košta svjetsku ekonomiju 338 milijardi dolara, što znači da je ova vrsta kriminala isplativija od trgovine drogom, jer se pretpostavlja da je **profit** koji se ostvaruje visokotehnološkim kriminalom za 100 milijardi dolara veći od onog koji se ostvari trgovinom droge. Policija Republike Srpske uhvatila se u koštac sa ovim oblikom kriminala i veoma uspješno radi na njegovom suzbijanju. Ova činjenica će biti potvrđena kroz rad, jer će u njemu biti prikazani slučajevi koji su otkriveni u proteklom periodu, a koji su u vezi sa visokotehnološkim kriminalom. U radu su navedeni i pravni okviri, domaći i međunarodni, koji su omogućili policiji Republike Srpske da se bavi sprečavanjem krivičnih djela iz oblasti visokotehnološkog kriminala. U radu će biti prezentovana i nadležnost najznačajnije organizacione jedinice Ministarstva unutrašnjih poslova Republike Srpske koja se bavi sprečavanjem visokotehnološkog kriminala – Odjeljenja za sprečavanje visokotehnološkog kriminaliteta.

Ključne riječi: visokotehnološki kriminal, odjeljenje za visokotehnološki kriminal, sprečavanje, policija Republike Srpske.

UVOD

Profit koji donosi izvršiocima krivičnih djela, mnogobrojni načini izvršenja, veliki broj potencijalnih žrtava, kao i širok manipulativni prostor predstavljaju samo neke od razloga na osnovu kojih se može reći da je visokotehnološki kriminal jedan od najzastupljenijih oblika kriminaliteta u današnjem društvu. ‘’Izvještaj kompanije Norton za 2011. godinu zasnovan je na podacima i procjenama o šteti koju je pretrpjelo 12.000 žrtava visokotehnološkog kriminala u 24 zemlje, pri čemu od ukupno procijenjene štete od 388 milijardi dolara, 114 milijardi iznosi direktni finansijski gubitak, a 274 milijardi dolara je šteta koju su žrtve pretrpjele kao posljedicu toga što su se našle na meti kriminalaca’’[1]. Ovaj podatak ukazuje na

[1] Preuzeto sa: http://www.symantec.com/content/en/au/home_homeoffice/html/cybercrimereport/, pretraženo: 14.1.2012. godine.

ogromnu imovinsku korist koju na protivpravan način pribavljaju lica koja se bave ovim vidom kriminaliteta.

''Svake sekunde 19 internet korisnika postanu žrtve nekog oblika sajber kriminala, a najčešće je riječ o hakovanju na društvenim mrežama i prevarama sa kreditnim karticama. To znači da se dnevno dogodi milion incidenata u kojima neki ljudi postanu žrtve prevaranata na internetu. Najčešći oblik ovog kriminala podrazumijeva učešće kompjuterskih virusa, koji su sastavni dio 54% svih napada, a najčešće žrtve su muškarci uzrasta između 18 i 31 godine, što u Symantec-u objašnjavaju time da internet korisnici iz te kategorije provode više vremena na internetu i gledaju češće pornografski sadržaj. U izveštaju se poseban akcenat stavlja na porast kriminala čije su žrtve korisnici mobilnih telefona. Oko 10% internet korisnika postanu žrtve kriminalaca preko mobilnih telefona jer kriminalci sve češće zloupotrebljavaju ranjivost mobilnih operativnih sistema.''[2]

Na ovako rasprostranjen i aktuelan oblik kriminala nije ostalo imuno ni društvo Republike Srpske, nego je, naprotiv, postalo svakodnevno izloženo prijetnjama i finansijskim štetama koje mu prouzrokuju lica koja se bave visokotehnološkim kriminalom. Ratna dešavanja na ovim prostorima dovela su do toga da se društvo Republike Srpske ne može baš pohvaliti ukupnom informatičkom obrazovanošću, što direktno omogućava izvršiocima krivičnih djela visokotehnološkog kriminala lakše izvršenje krivičnih djela i sticanje protivpravne imovinske koristi na ovaj način. Prije svega, problem je u tome što mali broj građana koji aktivno koristi računare ne vodi dovoljno računa o zaštiti svojih podataka sa računara, kao i o uobičajenim prevarama kojima se služe izvršioci krivičnih djela visokotehnološkog kriminala. Veliki broj korisnika računara samo je površno upoznat sa njihovim mogućnostima i u svom radu ih koristi veoma naivno i bez razmišljanja o eventualnim poslijedicama. Ovakvim načinom korištenja računara stvara se jedan ogroman prostor za razne malverzacije, prevare, utaje, krađe, oštećenje ili uništenje privatne svojine, narušavanje ugleda i klevetu. Taj prostor u kome se sve ovo dešava naziva se sajber (''cyber'') prostor, koji čovječanstvu donosi mnogo toga dobrog, ali isto tako i određene negativne stvari. Policija Republike Srpske uhvatila se u koštac sa ovim pojavnim oblikom kriminala i aktivno radi na sprečavanju vršenja krivičnih djela iz oblasti visokotehnološkog kriminala u Republici Srpskoj. O aktuelnosti ovog problema govori i podatak ''da Bosna i Hercegovina godišnje gubi između 11 i 14 miliona dolara direktnih poreza zbog softverske piraterije, koja se procjenjuje na 66% od ukupnog softverskog tržišta''[3].

PRAVNI OSNOV ZA SPREČAVANJE VISOKOTEHNOLOŠKOG KRIMINALA U REPUBLICI SRPSKOJ

Sprečavanje visokotehnološkog kriminala na ovim prostorima omogućeno je na osnovu potpisivanja međunarodnih konvencija i direktiva međunarodne zajednice. Najznačajniji međunarodni dokumenti koje je potpisala Bosna i

[2] Preuzeto sa: http://www.symantec.com/content/en/us/home_homeoffice/html/ncr/, pretraženo: 10.1.2012. godine.

[3] Preuzeto sa: http://www.lokoportal.com/index.php?option=com_content&view=article&id=5069:sajber-kriminal-u-bih&catid=57:tehnologija&Itemid=96, pretraženo 12.1.2012. godine

Hercegovina, a samim tim i Republika Srpska, jesu Direktiva Savjeta Evropske zajednice o pravnoj zaštiti kompjuterskih programa i Konvencija o suzbijanju visokotehnološkog kriminala. Na osnovu ovih temeljnih propisa izgrađena je pravna regulativa u pravnom sistemu Republike Srpske, koja je omogućila policiji Republike Srpske da radi na otkrivanju i sprečavanju visokotehnološkog kriminala.

Direktiva Savjeta Evropske zajednice o pravnoj zaštiti kompjuterskih programa naložila je zemljama da ‘’u skladu sa odredbama ove direktive zaštićuju kompjuterske programe autorskim pravom kao književna djela u smislu Bernske konvencije za zaštitu književnih i umjetničkih djela. Pojam «kompjuterski program», za potrebe ove direktive, obuhvata i pripremni materijal za koncipiranje programa. Zaštita predviđena ovom direktivom primjenjuje se na svaki oblik formulisanja nekog kompjuterskog programa. Ideje i principi koji se nalaze u osnovi bilo kog elementa kompjuterskog programa, uključujući i ideje i principe koji se nalaze u osnovi njegovih interfejsa, nisu zaštićeni autorskim pravom u skladu sa ovom direktivom. Kompjuterski program je zaštićen kada je originalan, u tom smislu da je lična intelektualna tvorevina svog autora. Nikakav drugi kriterijum se ne primjenjuje za utvrđivanje da li on može potpadati pod ovu zaštitu.’’[4]

Konvencija o suzbijanju visokotehnološkog kriminala koja je usvojena 23. novembra 2001. godine u Budimpešti govori o tome da su se države članice Savjeta Evrope i druge države potpisnice ove konvencije dogovorile da od mjera koje će se primjenjivati na nacionalnom nivou u okviru materijalnog krivičnog prava uvedu: krivična djela protiv povjerljivosti, integriteta i dostupnosti kompjuterskih podataka i sistema; krivična djela u vezi sa kompjuterima; krivična djela u odnosu na sadržaj; krivična djela koji se odnose na kršenje autorskih i njima sličnih prava; a pored ovoga dogovoreno je da se donesu i odredbe o odgovornosti za pomaganje i podstrkavanje u vršenju ovih krivičnih djela, kao i uspostavljanje efikasnog sistema sankcija za navedene grupe krivičnih djela.

Kao posljedica navedenih međunarodnih dokumenata, u Krivični zakon Republike Srpske (objavljen u „Službenom glasniku Republike Srpske“ broj 49/03) inkorporirana su sljedeća krivična djela: neovlašćeno ulaženje u zaštićenu kompjutersku bazu podataka (član 238), proizvodnja i prikazivanje dečije pornografije (član 200), neovlašćeno fotografisanje (član 175), neovlašćeno korištenje ličnih podataka (član 176), iskorišćavanje dece i maloljetnih lica za pornografiju (član 199), upad u kompjuterski sistem (član 271). Pored ovog zakona, donesen je i Zakon o izmjenama i dopunama Krivičnog zakona Republike Srpske (objavljen u „Službenom glasniku Republike Srpske“ broj 73/10), gdje je u članu 56. predviđeno da se u Krivični zakon Republike Srpske doda nova glava (glava 44a.) koja nosi naziv: ‘’Krivična djela protiv bezbjednosti računarskih podataka’’ u kojoj se propisuju sljedeća krivična djela: oštećenje računarskih podataka i programa (član 292a.); računarska sabotaža (član 292b.); izrada i unošenje računarskih virusa (član 292v.); računarska prevara (član 292g.); neovlašćen pristup zaštićenom računaru, računarskoj mreži, telekomunikacionoj mreži i elektronskoj obradi podataka (član 292d.); sprečavanje i ograničavanje pristupa javnoj računarskoj mreži (član 292đ.); neovlašćeno korišćenje računara ili računarske mreže (član 292e.).

[4] Član 1. Direktive Savjeta Evropske zajednice o pravnoj zaštiti kompjuterskih programa, Preuzeto sa: http://www.mup.vladars.net/vtk/regulativa/zakoni/medjunarodni_cir.html, pretraženo: 17.1.2012. godine.

Smatramo da bi kao pozitivne primjere dobre pravne osnove za sprečavanje visokotehnološkog kriminala trebalo navesti zakonodavstava: SAD, Velike Britanije, Njemačke i Francuske.

Američko zakonodavstvo posjeduje najviše zakonskih propisa koji uspostavljaju dobru pravnu bazu za sprečavanje visokotehnološkog kriminala, a najznačajniji propisi su: Zakon o elektronskoj špijunaži (Electronic Espionage Act iz 1996. godine), Zakon o sprečavanju kompjuterskih prevara i zloupotreba (Computer Fraud and Abuse Act iz 1986. godine), Zakon o privatnosti elektronskih komunikacija (Electronic Communications Privacy Act iz 1986. godine), Zakon o iskorjenjivanju računarskih virusa (Computer Virus Eradication Act iz 1988. godine), Zakon o prevenciji dječije pornografije (Child Pornography Prevention Act iz 1990. godine). Svi navedeni zakoni doprinose kvalitetu američkog zakonodavstva u pogledu suzbijanja svih oblika visokotehnološkog kriminala, a ujedno predviđaju i izuzetno stroge sankcije za učinioce krivičnih djela.

Velika Britanija je ovu oblast regulisala pravnim aktima: Zakon o krađi (Theft Act iz 1968. godine), Zakon o falsifikovanju i krivotvorenju (Forgery and Counterfeiting Act iz 1981. godine), Zakon o zaštiti podataka (Data Protection Act iz 1998. godine), Zakon o zaštiti autorskih i srodnih prava (Copyright, Design and Patents Act iz 1988. godine), dok je 1990. godine donesen poseban Zakon o zloupotrebi kompjutera, koji predviđa niz krivičnih djela vezanih za zloupotrebu kompjutera i drugih informacionih sistema za koje su propisane veoma stroge kazne.

U Njemačkoj je već 1970. godine u pokrajini Esen donesen Zakon o zaštiti podataka. Međutim, tek u saveznom Zakonu o zaštiti podataka iz 1977. godine unesene su krivičnopravne sankcije na području zaštite automatske obrade podataka. Iako njemački krivični zakon iz 1978. godine ne poznaje kompjuterska krivična djela, to ne znači da ta protivpravna, nedopuštena ponašanja nisu inkriminisana. Naime, u Njemačkoj je 1988. godine donet poseban Krivični zakon za suzbijanje privrednog kriminaliteta, koji predviđa niz kompjuterskih krivičnih dela, i to: krađu podataka, kompjutersku špijunažu, kompjutersku prevaru, falsifikovanje podataka, obmanu u pravnom prometu pri obradi podataka, promjenu podataka, kao i kompjutersku sabotažu. Pored pomenutih pravnih izvora, svakako treba pomenuti i Zakon o autorskim djelima.

Francusko zakonodavstvo je karakteristično po tome što je prednjačilo u sankcionisanju krivičnih djela koja se vrše upotrebom novih tehnologija. To je bio slučaj i sa visokotehnološkim kriminalom. Krivična djela kompjuterskog kriminala sadržana su u francuskom krivičnom zakonu (neovlašćeno pribavljanje podataka, neovlašćeno pristupanje, mijenjanje sadržaja, brisanje ili oštećenje podataka, ometanje normalnog rada kompjutera, prevara i falsifikovanje), dok je prikupljanje, informatička obrada i korišćenje podataka za potrebe stvaranja različitih baza podataka, regulisano posebnim Zakonom o zaštiti podataka iz 1978. godine. Odredbama ovog zakona uređena je obaveza svih korisnika banaka podataka, bili oni državni organi ili privatna lica, da se za svako otvaranje nove banke podataka moraju obratiti pismenim zahtjevom za odobrenje državnoj Komisiji za informatiku i slobode građana, koja je ovlašćena da se brine o informacijskom samoodređivanju građana (Polić, 2010: 10–13).[5]

[5] Više u: Polić, V., (2010): Komparativna analiza kompjuterskog kriminala u zakonodavstvima Republike Srbije i nekih stranih zemalja, dostupno na: http://www.singipedia.com/content/1066-Komparativna-analiza-kompjuterskog-kriminala-u-zakonodavstvima-Republike-Srbije-i-nekih-stranih-zemalja, pretraženo: 21.1.2012. godine.

SPREČAVANJE VISOKOTEHNOLOŠKOG KRIMINALA U REPUBLICI SRPSKOJ OD STRANE POLICIJE REPUBLIKE SRPSKE

Stvaranjem pravnog okvira za suprotstavljanje visokotehnološkom kriminalu stvorena je pravna osnova za uspostavljanje posebne organizacione jedinice u okviru Ministarstva unutrašnjih poslova Republike Srpske koja će se baviti sprečavanjem vršenja krivičnih djela iz oblasti visokotehnološkog kriminala. Koliko je neophodno bilo formiranje jedne ovakve uskospecijalizovane organizacione jedinice u okviru Ministarstva unutrašnjih poslova Republike Srpske govori i podatak de je ‘’prema rezulatima ankete koju je provela Agencija o informisanosti građana Republike Srpske o visokotehnološkom kriminalu, manje od 20 odsto stanovništva zna da postoji bilo kakva legislativa u vezi sa visokotehnološkim kriminalitetom’’[6]. Sama pomisao na to kako se građani ponašaju u nekom prostoru i okruženju za koje misle da nije uopšte pravno regulisano i uređeno opravdava osnivanje Odjeljenja za sprečavanje visokotehnološkog kriminala MUP-a Republike Srpske.

Odjeljenje za sprečavanje visokotehnološkog kriminaliteta oformljeno je 1. 1. 2010. godine i nalazi se u sklopu Jedinice za operativnu i tehničku podršku unutar Uprave kriminalističke policije Ministarstva unutrašnjih poslova Republike Srpske. Po Pravilniku o unutrašnjoj organizaciji i sistematizaciji radnih mjesta Ministarstva unutrašnjih poslova Republike Srpske predviđeno je da odjeljenje za sprečavanje VTK ima nadležnost da u sprečavanju visokotehnološkog kriminaliteta koristi specijalne metode za izvođenje istražnih radnji kada ne postoje drugi načini za prikupljanje dokaza, čime se stvaraju uslovi za njihovu primjenu u skladu sa Zakonom o krivičnom postupku Republike Srpske, a protiv lica za koja postoje osnovi sumnje da učestvuju u izvršenju krivičnih djela predviđenih Krivičnim zakonom Republike Srpske. Može se reći da Odjeljenje za VTK obavlja četiti grupe poslova:

1. istrage krivičnih djela visokotehnološkog kriminala,
2. operativna forenzička podrška,
3. forenzička analiza i
4. visokotehnološka asistencija.

Istrage krivičnih djela visokotehnološkog kriminala podrazumijevaju istrage gdje visokotehnološka sredstva predstavljaju: sredstva pružanja novih (nezakonitih) usluga korisnicima, sredstva napada, sabotaže, prevare, sredstva krađe, izmjene i zloupotrebe elektronskih podataka fizičkih i pravnih lica, sredstva nelegalnih oblika komunikacije, sredstva upada u zaštićeni sistem i kompjutersku bazu podataka, kao i istrage najtežih oblika transnacionalnog sajber kriminala.

Operativno-forenzička podrška usmjerena je na krivična djela gdje je došlo do upotrebe visoke tehnologije u pripremi i izvršenju klasičnih krivičnih djela. Radi se o krivičnim djelima gdje su visoke tehnologije upotrebljene kao: sredstva komunikacije, sredstvo skladištenja podataka koji služe izvršenju krivičnih djela ili su proizvod krivičnih djela, sredstva izvršenja krivičnih djela, sredstvo za izradu digitalnih i štampanih sadržaja koji služe izvršenju krivičnih djela ili su proizvod

[6] Preuzeto sa: http://www.lokoportal.com/index.php?option=com_content&view=article&id=5069:sajber-kriminal-u-bih&catid=57:tehnologija&Itemid=96, pretraženo 12.1.2012.

krivičnih djela. Operativna forenzička podrška pomaže tužiocu u vođenju istrage krivičnih djela i na taj način predstavlja važan dio istrage.

Forenzička analiza predstavlja najveći izazov za pripadnike Odjeljenje za VTK, jer se u njoj dolazi do konkretnih saznanja o izvršiocima krivičnih djela, uzročno-posljedičnim vezama, načinima izvršenja pojedinih krivičnih djela, te svakom konretnom koraku i radnji koja je preduzeta u toku izvršenja konkretnog krivičnog djela visokotehnološkog kriminala. Ovo ukazuje da se forenzičkom analizom dolazi do potpunog rasvjetljavanja krivičnog događaja, tj. prikupljaju se dokazi i činjenice o konkretnom krivičnom djelu koje omogućavaju davanje odgovara na svih devet zlatnih pitanja kriminalistike.

Visokotehnološka asistencija podrazumijeva pružanje pomoći drugim operativnim linijama rada koje se bave rasvjetljavanjem krivičnih djela: opšteg, organizovanog, privrednog i ostalih oblika kriminaliteta od strane pripadnika Odjeljenja za VTK.

UMJESTO ZAKLJUČKA

Umjesto zaključka, navešćemo sve aktivnosti (pregled svih akcija) koje je sprovela policija Republike Srpske u 2011. godini u cilju sprečavanja krivičnih djela visokotehnološkog kriminala.

26.1.2011. godine. Ministarstvo unutrašnjih poslova Republike Srpske upozorava građane na pojavu prevara posredstvom interneta u Republici Srpskoj, u svijetu poznatijih kao „Nigerijske igre na sreću“ ili „Scamming“. Prevare se odvijaju tako što građani posredstvom interneta dobijaju elektronske poruke u kojima stoje primamljive ponude od stranih državljana koji im nude da dostave svoje podatke, kao što su ime i prezime, broj računa u banci, kako bi mogli da uplate na njihov račun velike sume novca, koje oni navodno ne mogu da iznesu iz svoje zemlje. Naravno, umjesto velike količine novca na svom računu, građani dožive da im se račun u banci isprazni, tako što je sav novac preko interneta potrošen od strane nekog drugog lica. Poseban oblik prevara jeste i da preko društvenih internet mreža poput ‘’Facebooka’’ lica pod lažnim profilom pristupaju drugim licima kroz prepisku, nudeći im zajedničku budućnost i ostvarivanje ljubavne veze. Kada uspiju da čvrsto vežu žrtvu za sebe, traže od žrtve novac da im pomogne, odnosno da im nakratko pozajmi novac. Vrlo čest je slučaj da u više navrata uspiju izvući novac od žrtve, nakon čega im se gubi svaki trag. Način slanja novca u ogromnom broju slučajeva je preko komercijalnih banaka, odnosno „Western Union“-a.[7]

20.3.2011. godine. Ministarstvo unutrašnjih poslova Republike Srpske podnijelo je Okružnom tužilaštvu Doboj dvije dopune Izvještaja o postojanju osnova sumnje o počinjenom krivičnom djelu „Proizvodnja i prikazivanje dječije pornografije“ iz člana 200 KZ RS, a u vezi s članom 44 Zakona o izmjenama i dopunama KZ Republike Srpske protiv jednog lica iz Dervente. Dvije dopune Izvještaja protiv lica kod kojeg je pronađeno 2 miliona fotografija dječije pornografije. Protiv ovog lica, Policijska stanica Derventa ranije je podnijela je

[7] Preuzeto sa: http://www.mup.vladars.net/index2.php?st=vijesti/opsirnije_novosti&id=5737, pretraženo: 13.1.2012. godine

Izvještaj zbog postojanja osnova da je počinilo krivično djelo „Proizvodnja i prikazivanje dječije pornografije“ i njemu je izrečena mjera pritvora do 9. maja 2011. godine. Prilikom pretresa, policija je kod ovog lica pronašla do sada najveću količinu dječije pornografije u BiH. Policija je u računaru koji je koristio počinilac i na diskovima pronašla oko dva miliona fotografija i 7.000 video snimaka dječije pornografije, a pored toga i torbu punu dječije gardarobe.[8]

24.3.2011. godine. Pripadnici Ministarstva unutrašnjih poslova Republike Srpske uspješno okončali aktivnosti u okviru međunarodnih akcija ‘’EG STOP’’, ‘’HIDDEN’’ i ‘’OLIVER’’ čiji je cilj suzbijanje svjetske mreže iskorištavanja djece i maloljetnika za dječiju pornografiju putem interneta. Policija Republike Srpske je nakon razmjene informacija sa kancelarijama Interpola u Luksemburgu, Londonu i Njemačkoj pretresla tri lokacije na području Republike Srpske – u Banjaluci, Prijedoru i Šamcu zbog postojanja osnova sumnje da su lica koja žive na ovim lokacijama pristupala sadržajima dječije pornografije. U ovim aktivnostima policija je saslušala pet lica zbog postojanja osnova sumnje da su počinila krivično djelo iz člana 199. ‘’Iskorištavanje djece i maloljetnih lica za pornografiju’’ i krivično djelo iz člana 200. ‘’Proizvodnja i prikazivanje dječije pornografije ‘’ Krivičnog zakona Republike Srpske.[9]

12.4.2011. godine. U organizaciji Ministarstva unutrašnjih poslova Republike Srpske, a uz podršku TAIEX-a - Tehničkog istrumenta Evropske komisije i Akademije evropskog prava ERA u Banjaluci je održan dvodnevni seminar na temu: ‘’Borba protiv dječije pornografije na internetu».[10]

31.5.2011. godine. Pripadnici Uprave kriminalističke policije Ministarstva unutrašnjih poslova Republike Srpske proveli su na području Republike Srpske akciju kodnog naziva ‘’Košnica’’. U okviru nje su izvršeni pretresi na području grada Banjaluke, a saslušano je nekoliko lica. Prilikom pretresa oduzeta je veća količina računarske opreme i ilegalnog naoružanja. Ove aktivnosti su dio velike međunarodne akcije usmjerene na razbijanje organizovane kriminalne grupe koja se bavila zloupotrebom platnih kartica i zloupotrebom računarskih podataka.[11]

7.6.2011. godine. Ministarstvo unutrašnjih poslova Republike Srpske u saradnji sa Tehničkim instrumentom za edukaciju Evropske komisije organizovalo je seminar na temu «Zloupotrebe platnih kartica», koji je održan u Banjaluci, a čiji su učesnici bili predstavnici policijskih agencija i tužilaštava i predstavnici agencija za bankarstvo Republike Srpske i Federacije Bosne i Hercegovine.[12]

20.9.2011. godine. Provedena akcija Ministarstva unutrašnjih poslova Republike srpske i Federalne uprave policije usmjerena na sprečavanje ‘’piramidalnih prevara’’. Inspektori Odjeljenja za sprečavanje visokotehnološkog

---

[8] Preuzeto sa: http://www.mup.vladars.net/index2.php?st=vijesti/opsirnije_novosti&id=5950, pretraženo: 13.1.2012. godine

[9] Preuzeto sa: http://www.mup.vladars.net/index2.php?st=vijesti/opsirnije_novosti&id=5965, pretraženo: 13.1.2012. godine

[10] Preuzeto sa: http://www.mup.vladars.net/index2.php?st=vijesti/opsirnije_novosti&id=6051, pretraženo: 14.1.2012. godine

[11] Preuzeto sa: http://www.mup.vladars.net/index2.php?st=vijesti/opsirnije_novosti&id=6234, pretraženo: 14.1.2012. godine

12 Preuzeto sa: http://www.mup.vladars.net/index2.php?st=vijesti/opsirnije_novosti&id=6258, pretraženo: 14.1.2012. godine

kriminaliteta Uprave kriminalističke policije MUP Republike Srpske izvršili su pretres jedne lokacije na području opštine Prnjavor u cilju prikupljanja materijalnih dokaza koje se odnose na krivično djelo ‘’Prevara” po Krivičnom zakonu Federacije Bosne i Hercegovine.[13]

4.10.2011. godine. Počela kampanja «Neko vreba preko veba» koju provodi Ministarstvo unutrašnjih poslova Republike Srpske. Cilj kampanje jeste da se građani upoznaju sa ovom vrstom kriminala o kome se relativno malo zna, a koji predstavlja opasnost za djecu, omladinu, pa i odrasle koji koriste usluge računara i visoke tehnologije.[14]

7.12.2011. godine. Ministarstvo unutrašnjih poslova Republike Srpske pod nadzorom Specijalnog tužilaštva RS, a po naredbi Okružnog suda u Banjaluci, Odjeljenja za organizovani i najteže oblike privrednog kriminala, provelo je akciju kodnog naziva ‘’KUBIKUS”. Akcija se provodila zbog počinjenog krivičnog djela: Organizovani kriminal iz člana 383a. Krivičnog zakona Republike Srpske, a u vezi s krivičnim djelom Organizovanje nedozvoljenih igara na sreću iz člana 241. Krivičnog zakona Republike Srpske, odnosno zbog postojanja osnova sumnje da je organizovana kriminalna grupa putem interneta, bez licence i odobrenja Republičke uprave za igre na sreću Republike Srpske, priređivala igre na sreću, te na taj način ostvarivala protivpravnu imovinsku korist u višemilionskim iznosima, a za milionski iznos oštećen je budžet Republike Srpske. Pretreseno je 39 lokacija na području Republike Srpske i to u opštinama Banjaluka, Laktaši, Gradiška, Prnjavor, Srbac, Pale, Istočno Novo Sarajevo, Foča, Čelinac, Bijeljina, Srebrenica, Bratunac, Zvornik, Vlasenica, Bileća i Gacko.[15]

LITERATURA:

1. Babić, M. (2008). *Krivično pravo (opšti i posebni dio).* Banja Luka: Pravni fakultet.
2. Babić, M., Marković, I. (2005). *Krivično pravo (posebni dio).* Banja Luka: Pravni fakultet.
3. Chawki, M. (2006). Anonymity in Cyberspace. Funding the Balance between Privacy and Security. *Revista da Faculdade de Direito Milton Campos*, vol. 11. Brazil: Nova Lima.
4. Mocas, S. (2009). *Topics in Computer Science Introduction to Digital Forensics.* Washington: Washington State Univrsity.
5. Petrović, R. S. (2001). *Kompjuterski kriminal*. Beograd: Ministarstvo unutrašnjih poslova.
6. Polić, V. (2010): *Komparativna analiza kompjuterskog kriminala u zakonodavstvima Republike Srbije i nekih stranih zemalja*. dostupno na: http://

[13] Preuzeto sa: http://www.mup.vladars.net/index2.php?st=vijesti/opsirnije_novosti&id=6636, pretraženo: 15.1.2012. godine

[14] Preuzeto sa: http://www.mup.vladars.net/index2.php?st=vijesti/opsirnije_novosti&id=6685, pretraženo: 15.1.2012. godine

[15] Preuzeto sa: http://www.mup.vladars.net/index2.php?st=vijesti/opsirnije_novosti&id=6693, pretraženo: 15.1.2012. godine

www.singipedia.com/content/1066-Komparativna-analiza-kompjuterskog-kriminala-u-zakonodavstvima-Republike-Srbije-i-nekih-stranih-zemalja, pretraženo: 21. 1. 2012. godine.
7. Stojanović, Z. (2009). *Komentar krivičnog zakonika*. Beograd: Službeni glasnik.
8. Stojanović, Z., Perić, O. (2009). *Krivično pravo (posebni dio)*. Beograd: Pravni fakultet.
9. Škulić, M. (1997). *Kompjuterski kriminalitet*. Beograd: Pravni fakultet.
10. *Krivični zakon Republike Srpske*, (Službeni glasnik Republike Srpske, broj 49/03).
11. *Zakon o izmjenama i dopunama Krivičnog zakona Republike Srpske*, (Službeni glasnik Republike Srpske, broj 73/10).
12. Direktiva Savjeta Evropske zajednice o pravnoj zaštiti kompjuterskih programa, Preuzeto sa: http://www.mup.vladars.net/vtk/regulativa/zakoni/medjunarodni_cir.html, pretraženo: 17.1.2012. godine,
13. http://www.symantec.com/content/en/au/home_homeoffice/html/cybercrimereport/, pretraženo: 14.1.2012. godine.
14. http://www.lokoportal.com/index.php?option=com_content&view=article&id=5069:sajber-kriminal-u-bih&catid=57:tehnologija&Itemid=96, pretraženo 12.1.2012. godine,
15. http://www.mup.vladars.net/index2.php?st=vijesti/opsirnije_novosti&id=5737

SUMMARY

Cyber crime that the world takes shape, no exception in this area of the Republic of Srpska. Relevance and importance of this problem is best insights on the basis of the indicators that speak of the losses of the world economy because of this crime.

Based on reports the company Norton, cybercrime annually costs the world economy 338 billion dollars, which means that this type of crime more cost effective than drug trafficking, because it is assumed that the profit that is realized by cyber crime by 100 billion dollars higher than that achieved in trade drug.

The police Republic of Srpska has began the fight against this crime and is very successful in its combat. This fact will be confirmed through the work, because it will be displayed in cases that were discovered in the past, and which are related to cyber crime. This article describes the legal framework, national and international, who made the Republic of Srpska police, to deal with the prevention of crime in the area of cyber crime. The article will be presented to the jurisdiction of the most important organizational units of the Ministry of Internal Affairs Republic of Srpska dealing with the prevention of cyber crime - Cyber crime depatment.

Stručni rad – UDK 343.326: 004.738.5

MERE I STRATEGIJE ZAŠTITE INFORMACIONIH SISTEMA OD VISOKOTEHNOLOŠKOG KRIMINALA

Mr Nenad Putnik
nputnik@fb.bg.ac.rs
Fakultet bezbednosti Univerziteta u Beogradu
Nevena Gavrić
Fakultet bezbednosti Univerziteta u Beogradu
ngavric@pregovarac.rs

Apstrakt: U informacionim sistemima skoncentrisana je ogromna količina podataka i informacija koje, po svojoj prirodi, mogu da izražavaju materijalnu vrednost, ali isto tako mogu da predstavljaju ličnu, poslovnu, profesionalnu, vojnu ili državnu tajnu. Upravo iz tog razloga, bilo kakvo ugrožavanje informacionih sistema može naneti znatnu štetu individualnim korisnicima, društvenim subjektima i informacionom društvu u celini. Neprestano povećanje učestalosti napada, kao i metoda i sredstava visokotehnološkog kriminala, njihov specifični karakter i prepoznata društvena opasnost u sve većoj meri postaju vrlo ozbiljan društveni problem, i to ne samo u nacionalnim već i u međunarodnim razmerama. Poslednjih godina su, u tom smislu, izražene intenzivne aktivnosti na formiranju širokog odbrambenog fronta, sačinjenog od svih zainteresovanih subjekata, u cilju suprotstavljanja bezbednosnim pretnjama i smanjenja rizika od njihovog manifestovanja. Dosadašnja iskustva u suprotstavljanju bezbednosnim pretnjama u kiber prostoru ukazuju na potrebu stvaranja koherentnog delatnog okvira koji podrazumeva primenu kako preventivnih, tako i represivnih mera u stvaranju bezbednog kiber ambijenta. U radu će biti precizno izložene mere i strategije zaštite informacionih sistema od visokotehnološkog kriminala.

Ključne reči: informacioni sistemi, kiber prostor, zaštita, visokotehnološki kriminal

UVOD

Globalna računarska mreža otvorila je nove mogućnosti za izvršavanje kriminalnih dela. Internet, koji je po svojoj prirodi ranjiv i nesiguran, usled ogromnog broja korisnika, otvorenosti i pravne neregulisanosti, postao je poligon, ali i idealno skrovište za kriminalce različitog tipa. Visokotehnološki kriminal je kompleksan fenomen pod kojim se podrazumevaju raznovrsne kriminalne aktivnosti. One najčešće podrazumevaju napade na računarske sisteme i mreže, sadržaje ili intelektualnu svojinu. Za ovaj vid kriminala često se upotrebljavaju i drugi termini: *Internet-kriminal*, *elektronski kriminal*, *kiber kriminal*, *mrežni kriminal* itsl.

Usled rasprostranjenosti i decentralizovanosti globalne računarske mreže, aktivnosti zlonamernih aktera u kiber prostoru postale su međunarodni

problem i otvorile pitanja zaštite ne samo vlastitih već i tuđih informacionih sistema, sprovođenja međunarodnih istraga, ekstradicije i kažnjavanja izvršilaca. Poslednjih godina su, u tom smislu, izražene intenzivne aktivnosti na formiranju širokog odbrambenog fronta, sačinjenog od svih zainteresovanih subjekata, u cilju suprotstavljanja visokotehnološkom kriminalu. U suprotstavljanju bezbednosnim pretnjama u kiber prostoru na raspolaganju su različite mere koje mogu pomoći da se uspešno odgovori na ove izazove, kao što su: alati za zaštitu, zakonska regulativa, bezbednosni standardi, promovisanje bezbednosne kulture i kompjuterske etike itd.

Dosadašnja iskustva u suprotstavljanju bezbednosnim pretnjama u kiber prostoru ukazuju na potrebu stvaranja koherentnog delatnog okvira koji podrazumeva primenu kako preventivnih, tako i represivnih mera u stvaranju bezbednog kiber ambijenta. Preventivne aktivnosti, na prvome mestu, podrazumevaju osmišljavanje različitih mera i strategija zaštite informacionih sistema i njihovu implementaciju, unapređivanje zakonske regulative, kako na nacionalnom tako i na međunarodnom nivou, kao i njihovo usklađivanje sa obaveštajnim aktivnostima u pokušaju suprotstavljanja kiber pretnjama.

ASPEKTI ZAŠTITE

Globalno gledajući, neophodni preduslovi za uspešnu realizaciju mera za suprotstavljanje pretnjama u kiber prostoru morali bi se obezbediti na tri nivoa: lokalnom (nivou korisnikâ informacionih sistema), nacionalnom i međunarodnom. Adekvatan sistem zaštite, primeren svakom od navedenih nivoa, morao bi da ima dvojaku funkciju: da odvrati od zloupotrebe računara, odnosno spreči njegovu zloupotrebu, i da, u slučaju da je zloupotreba izvršena, omogući brzo otkrivanje i dokazivanje učinjenog dela.[1]

Pod zaštitom informacionih sistema podrazumeva se primarni, bazični nivo zaštite. Ovaj nivo odnosi se na zaštitu informacionih sistema, informacija i informacionih mreža u privatnom vlasništvu građana i u svim bitnim državnim i privatnim organizacijama.[2] Informacije, informacioni sistemi i mreže predstavljaju važnu imovinu, koja ima materijalnu i upotrebnu vrednost za svakog pojedinca i svaku organizaciju. Informacija i informaciona infrastruktura mogu biti od presudne važnosti za očuvanje: nacionalne bezbednosti, privatnosti pojedinaca ali i konkurentnosti preduzeća i drugih aspekata poslovanja (gotovinskih tokova, isplativosti, pravne usaglašenosti i poslovnog ugleda). Zaštitom informacija od širokog opsega pretnji se, sa aspekta korporativne bezbednosti, osigurava kontinuitet poslovanja, sa ciljem da se gubici u poslovanju svedu na minimum.

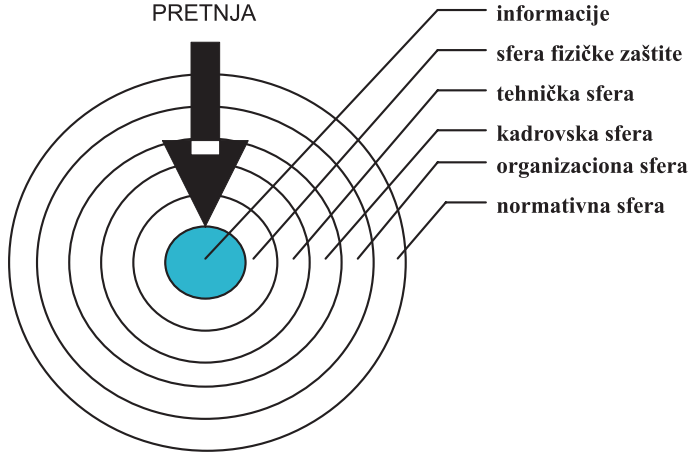
Sa aspekta nacionalne bezbednosti, u cilju suprotstavljanja visokotehnološkom kriminalu, neophodno je sprovoditi zaštitne mere na sledeća tri nivoa:

- Operativni nivo – podrazumeva primenu najsavremenijih sredstava za zaštitu podataka i informatičkih resursa, kod svih korisnika IK tehnologija. Osim toga, potrebno je sprovoditi česta testiranja informacionih sistema i odmah uklanjati uočene bezbednosne probleme.

[1] Petrović, S.: *Policijska informatika*, Kriminalističko-policijska akademija, Beograd, 2007, str. 171.
[2] Putnik, N.: *Sajber prostor i bezbednosni izazovi*, Fakultet bezbednosti, Beograd, 2009, str. 334.

- Proizvodni nivo – razviti sredstva za monitoring i automatsku proveru bezbednosti kod proizvođača informatičkih sredstava. Sprovoditi rigorozna testiranja hardvera i softvera informacionih sistema na bezbednosne propuste.
- Državni nivo – realizovati kritične državne informacione sisteme kao visokobezbedne modele. Uvesti politiku zaštite informacija i informacionih sistema i mreža, koja bi se sprovodila na sva tri navedena nivoa.[3] Individualni korisnici, kao i privatni i državni sektor, suočavaju se sa širokim opsegom bezbednosnih pretnji u kiber prostoru – prevarama, špijunažom, sabotažama, vandalizmima itd. Tehnike napada se usavršavaju, a sami napadi postaju sve učestaliji, ambiciozniji i sofisticiraniji. Da bi se pomenute pretnje predupredile, na primarnom nivou zaštite moraju se u obzir uzeti različiti aspekti zaštite. Na osnovu dosadašnjih iskustava, tzv. dobre prakse, može se reći da je poželjno primenjivati model višeslojne zaštite. On predstavlja vid proaktivnog delovanja i obuhvata nekoliko aspekata:
- Fizički (onemogućava fizički pristup – fizičko obezbeđenje);
- Tehnički (tehničko obezbeđenje – elektronsko obezbeđenje; zaštita od elektromagnetnog zračenja; identifikacija, verifikacija i autorizacija pristupa; sistemi za detekciju i sprečavanje napada; kriptografija);
- Organizacioni (organizaciona struktura, definisanje radnog procesa, razvoj softverskih sistema, praćenje smernica i standardâ, planiranje itd.);
- Kadrovski (planiranje i izbor kadrova, rukovođenje, stručno usavršavanje i bezbednosno obrazovanje itd.) i
- Normativni (zakoni, uputstva, planovi i druga regulativa koja obavezuje i propisuje izvršenje neke radnje i način izršenja te radnje).

Shema br. 1: Model višeslojne zaštite



[3] Džigurski, O.: *Informacione tehnologije u borbi protiv terorizma*, Zbornik Fakulteta civilne odbrane, Beograd, 2005, str. 179.

Sfere fizičke i tehničke zaštite se, uobičajeno, nazivaju tehničkim aspektom zaštite, dok se organizaciona, kadrovska i normativna sfera podvode pod društveni aspekt zaštite. Oba aspekta su podjednako značajna i samo se njihovom kombinacijom, i sinergijskim efektom, može postići zadovoljavajući nivo zaštite informacionih sistema.

TEHNIČKI ASPEKT ZAŠTITE

Fizička i tehnička sfera zaštite predstavljaju prvu liniju odbrane informacionih sistema. Ovaj aspekt zaštite podrazumeva korišćenje mera koje imaju za cilj regulisanje načina i tehničkih postupaka kojima se može umanjiti rizik od zlonamernog narušavanja funkcionalnosti informacionih sistema. U cilju sprečavanja pristupa (fizičkog i putem mreže) štićenom sistemu, u upotrebi su različiti tehnički uređaji i sredstva ali i raznovrsni informatički alati.

Prilikom planiranja fizičkog obezbeđenja koristi se nekoliko metoda. Kontrola pristupa je termin koji se koristi kada se govori o mehanizmu koji reguliše pristup računarima, softveru i drugim resursima. Serveri koji čuvaju važne podatke, ruteri i druge bitne mrežne komponente trebalo bi da se nalaze u zaključanim ormanima, ili obezbeđenim računarskim centrima. Dobro obezbeđen centar ili orman predstavlja fizičku prepreku za svaku osobu koja nije ovlašćena da pristupi serveru.

Instalacija sa dobrom fizičkom bezbednošću trebalo bi da koristi koncentrične prstenove progresivnih fizičkih prepreka, pri čemu se najosetljiviji resursi postavljaju u centralni prsten. Brava sa šifrom na vratima računarskog centra je i dalje nezamenljiva, ali je preporučljivo i postavljanje video-interfona. Lokacija servera i drugih ključnih komponenata unutar računskog centra bi trebalo da bude zaštićena još jednim zaključanim vratima pod nadzorom. Ukoliko je potrebno jače obezbeđenje, mogu se uvesti magnetne kartice, video kamere i stražari. Niko ne bi trebalo da ulazi u računarski centar, a da to ne bude dokumentovano. Unutrašnji prstenovi obezbeđenog područja bi trebalo da pružaju zaštitu sa svih šest strana prostorije, što znači sva četiri zida, plafona i poda. U nekim slučajevima se ove mere mogu pojačati alarmnim sistemima i kamerama. Standardni mehanizmi za otvaranje vrata poput metalnih ključeva, magnetnih kartica i lozinki mogu da budu nedovoljni za prostorije koje zahtevaju posebno obezbeđenje. U tom slučaju treba primeniti kombinaciju biometrijskih provera: proveru otiska prsta, geometriju ruke, skeniranje dužice, skeniranje mrežnjače ili facijalni termogram. Na primer, sistem može da koristi skeniranje ruke za brzu proveru identiteta a otisak prsta za detaljnu proveru.[4]

Bežično umrežavanje je, pored eksplozije umreženih sistema, donelo i nove bezbednosne izazove. Lokacija je jedan od glavnih faktora koji utiču na bezbednost bežičnih komunikacija. Kada se biraju i instaliraju komponente za bežično umrežavanje, a pogotovo tačke pristupa, treba pažljivo izvršiti testove kako bi se utvrdio operativni opseg uređaja. Antena bi trebalo da bude postavljena u centar zgrade, što dalje od spoljašnjih zidova. U slučajevima kada se prenose

[4] Kovačević, Ž.: *Kompjuterska špijunaža i zaštita*, master rad, Fakultet bezbednosti, Beograd, 2010, str. 80.

poverljivi podaci, potrebno je da se snaga prenosa svih bežičnih uređaja obavlja na minimumu koji dozvoljava efikasno obavljanje operacija, tako da je potencijalnim špijunima van zgrade otežano povezivanje na mrežu i prisluškivanje. Drugi faktor koji može uticati na podizanje bezbednosti bežičnih mreža je zaklanjanje operativnog područja. Time se mreža štiti od DoS napada, kojima je izuzetno podložna. Tehnologija mobilnih komunikacija ima praktično neograničen domet, i sada postoji mnogo proizvoda koji prenosivim računarima omogućavaju da se povežu sa mrežom koja se nalazi bilo gde u svetu. Pored toga, Bluetooth uređaji kratkog dometa mogu se iskoristiti za povezivanje laptopa sa mrežom mobilnog provajdera internet usluga. Zbog toga, uvek treba imati u vidu da je opasnost od ove tehnologije daleko veća, jer nije potrebno da špijun bude u blizini mrežnih instalacija da bi dobio pristup resursima. U tesnoj vezi sa fizičkom bezbednošću jeste pitanje čuvanja rezervnih kopija podataka. U svetu se otvaraju specijalizovane ustanove za takve namene.

U cilju podizanja nivoa zaštite mrežnih uređaja i matičnih računara, preporučljivo je poštovanje sledećih pravila:

- Onemogućiti nepotrebne programe i procese – što više instaliranih programa i što više pokrenutih procesa, veća je verovatnoća da će maliciozni kod iskoristiti slabost sistema;
- Onemogućiti nepotrebne servise – postoji mnogo servisa koji se ne koriste ili se koriste alternativno, a koji predstavljaju bezebednosnu pretnju, ili u najbanalnijem slučaju usporavaju sistem;
- Onemogućiti nepotrebne protokole;
- Proveriti, testirati i instalirati sve bezbednosne ispravke koje distributer objavi (upgrade, service pack, patch, hot fix);
- Koristiti skenere slabih tačaka, da bi se takva mesta otkrila i zaštitila;
- Onemogućiti neselektivni režim mrežnih adaptera (osim u slučaju pregleda slabih tačaka i nadzora mreže, kada ovaj režim mora biti omogućen).

Pored uklanjanja svih nepotrebnih komponenti i primene nadogradnji, u zaštiti operativnih sistema, pored već navedenih mera, treba uključiti i sledeće:

- Postaviti složene lozinke za sve korisničke naloge i često ih menjati;
- Odrediti pravila za blokiranje naloga;
- Ukloniti i onemogućiti nepotrebne modeme;
- Omogućiti nadgledanje, zapisivanje, proveravanje i detekciju;
- Održavati rezervne kopije i duplikate diska.

Treba se odlučiti za bezbedan sistem datoteka koji omogućava podešavanje dozvola na nivou datoteka i foldera. Dozvole treba konfigurisati po principu najmanje privilegije.

Prilikom razmatranja bezbednosti informacija i uređaja koji ih prenose, u obzir se moraju uzeti i zamenljivi medijumi, kao što su magnetne trake, CD-ROM, DVD, fleš memorije I sl. Ovi medijumi se mogu upotrebiti za kopiranje podataka sa servera ili za čuvanje rezervnih kopija ili arhiviranje. U tom smislu, potrebno je osmisliti mere kako bi se sprečilo iznošenje poverljivih podataka iz preduzeća na ovim medijumima. Ako se na njima čuvaju poverljivi podaci, treba znati kako ih zaštititi, koji je najbolji način za čuvanje medijuma da bi informacije ostale netaknute i kako efikasno izbrisati sadržaj sa medijuma kada je to neophodno.

Upotreba gotovih softverskih alata za zaštitu, dostupnih na tržištu (poput antivirusnih programa, firewall-filtera I sl.), svakako je od velikog značaja na osnovnom nivou zaštite. Informatički usko specijalizovani metodi i tehnike za otkrivanje i suprotstavljanje kiber napadima uključuju korišćenje specijalnih softverskih aplikacija za zaštitu personalnih računara i računarskih mreža, upotrebu kriptografskih i enkriptičkih metoda, tehnika i sistema, kao i sistema za otkrivanje i sprečavanje upada.[5]

DRUŠTVENI ASPEKTI ZAŠTITE

Budući da mnogi informacioni sistemi nisu projektovani tako da se mogu štititi tehničkim sredstvima (čiji je domet, takođe, ograničen), efikasna zaštita se mora bazirati na odgovarajućim upravljačkim politikama i procedurama u pogledu: definisanja radnog procesa, razvoja softverskih sistema, praćenja smernica i standardâ, planiranja i izbora kadrova, rukovođenja, stručnog usavršavanja i bezbednosnog obrazovanja, kao i donošenja normativnih akata, i druge regulative koja obavezuje i propisuje izvršenje neke radnje i način izršenja te radnje.

Sa organizacionog aspekta, posebno je značajna implementacija međunarodnih i nacionalnih bezbednosnih standarda u ovoj oblasti. U poslednjoj deceniji XX veka i prvoj deceniji ovog veka publikovani su, ili prerađeni, brojni nacionalni i međunarodni standardi koji se odnose na upravljanje bezbednošću podataka u računarskim sistemima. Ovi standardi se, prema nameni, mogu podeliti na: standarde za bezbednost proizvoda, standarde za bezbednost procesa i standarde bezbednosti sistema.[6]

Čuvanje informacija, kao mere znanja i suštinskog resursa dobilo je svoj okvir u seriji standarda ISO 27000, gde su specificirani zahtevi koje treba da poštuje organizacija da bi ostvarila sistem za zaštitu informacija. U oktobru 2005. godine objavljen je standard ISO 27001 pod nazivom Sistemi upravljanja bezbednošću informacija – Zahtevi (engl. Information Security Management System /ISMS/ requirements).[7] On definiše zahteve koje mora da ispuni sistem za upravljanje

---

[5] Sistemi za otkrivanje i sprečavanje upada se dele na sisteme za detekciju napada (*engl.* Intrusion Detection System – IDS) i sisteme za prevenciju napada (*engl.* Intrusion Prevention System – IPS). Detektovanje napada je proces nadgledanja i procene događaja u računaru i mrežnog saobraćaja, sa ciljem da se otkriju znaci napada. Sistem za detekciju napada je hardverski uređaj sa softverom, ili softver koji se koristi za otkrivanje neovlašćenih aktivnosti na mreži. Uređaj se može implementirati na pojedinačne računare, servere, na mrežnoj periferiji ili celoj mreži. Sistemi za prevenciju napada su znatno napredniji od sistema za detekciju napada. Oni su fokusirani na to šta napad radi, što je u osnovi nepromenljivo. Osnovne funkcije sistema su: identifikacija neovlašćenih aktivnosti na osnovu potpisa i detektovanih anomalija, vođenje evidencije i slanje alarma administratorima u realnom vremenu, prikupljanje forenzičkih podataka i sprečavanje napada. I ovi sistemi mogu biti smešteni na računaru ili mreži. O sistemima za otkrivanje i sprečavanje upada videti više u: The Honeynet Alliance, Know Your Enemy Whitepapers, http://www.honeynet.org/papers/kye.html; Rehman R.: *Intrusion Detection Systems with Snort*, Prentice Hall PTR, 2003; Spitzner L.: *Honeypots: Tracking hackers*, Addison Wesley, 2002; Endorf C., Schultz E., Mellander J.: *Intrusion Detection & Prevention*, McGraw-Hill, 2004; Chirillo J.: *Hack Attacks Revealed – A Complete Reference with Custom Security Hacking Toolkit*, John Wiley & Sons, New York, 2001.

[6] Kukrika, M.: *Upravljanje sigurnošću informacija*, INFOhome Press, Beograd, 2002, str. 102–103.

[7] Srpska verzija ovog standarda pod oznakom SRPS ISO/IEC 27001 Informacione tehnologije – Tehnike bezbednosti – Sistemi menadžmenta bezbednošću informacija – Zahtevi, objavljena je 3.

bezbednošću podataka, da bi ga akreditovana organizacija mogla sertifikovati.[8] Razvoj ovog standarda tesno je povezan sa standardom ISO 9001.

Grupa standarda ISO 27000 značajana je za sve organizacije koje se bave uslugama u oblastima koje su na bilo koji način povezane sa informacionim tehnologijama i koje imaju potrebu za očuvanjem poverljivosti informacija. Njegova implementacija i primena omogućavaju bolju saradnju sa sličnim organizacijama širom sveta koje posluju po ovom modelu. Ovim standardom organizacije demonstriraju svojim korisnicima da je poslovna politika usmerena na stalna poboljšavanja u sistemu menadžmenta za bezbednost informacija. Značajne su koristi koje model za uređenje sistema za bezbednost informacija ISO 27001 ostvaruje kod svih koji ga usvoje, pre svega u smislu poboljšavanja organizacionih performansi. Ovaj model predstavlja najbolju praksu u oblasti zaštite i bezbednosti informacija, koja je pretočena u zahteve standarda.

Sa aspekta preventivnog delovanja i zaštite informacionih sistema, posebnu pažnju zauzima izgradnja i razvoj etičkih normi i principa u domenu informatike. Uspostavljanje i razvoj ovih normi i principa je od izuzetnog značaja, jer oni mogu pronaći primenu u svim onim slučajevima narušavanja bezbednosti koji nisu u suprotnosti sa pravom ali se percipiraju kao neprihvatljivo ponašanje.

Razvoj i sve veća upotreba Interneta doveli su do, naizgled, beskrajnog niza etičkih pitanja, pošto je Internet vremenom poprimao sve značajniju primenu u različitim domenima života. Internet je pokrenuo i spektar važnih etičkih pitanja, poput: pitanja privatnosti, demokratičnosti, svojinskih prava itd.[9] Globalni opseg komunikacije mnogih sa mnogima, anonimnost i mogućnost reprodukcije su crte komunikacije na Internetu koje stvaraju niz mogućih prednosti i poteškoća. Pred organizacijama koje sprovode urađivačku politiku na Internetu stoji izazov da, do maksimuma, ostvare pozitivne potencijale ove tehnologije i da, istovremeno, ograniče mogućnosti za njenu zloupotrebu. Izazov se, između ostalog, sastoji u tome da se pristupi rešavanju problema kriminala i zloupotrebe na Internetu, a da se za to primene strategije koje ne bi umanjile moć koju on pruža pojedincima.

Razmatrajući vezu između tehnologije i etike, može se doći do zaključka da je, kroz istoriju, polje kompjuterske etike naprosto sledilo razvoj kompjuterske tehnologije.[10] U istorijskom smislu, dakle, polje kompjuterske etike je bilo reaktivno u odnosu na tehnologiju – kompjuterski etičari su pratili tehnološki razvoj i tek naknadno reagovali na njega. Svakako da bi bilo bolje kada bi tehnologija sledila etiku. Tada bi se, sigurno, posvećivalo više pažnje onim tehnologijama koje povećavaju stepen zaštite privatnosti korisnika računarskih sistema.

STRATEGIJE ZAŠTITE

S obzirom na brojnost i raznovrsnost sredstava i tehnika koje koriste kriminalci u oblasti visokih tehnologija, u praksi nije moguće realizovati odbranu i zaštitu

novembra 2011. Prema: Institut za standardizaciju Srbije, http://www.iss.rs/news/news_33.html

[8] ISO 27001, ISMS requirements, http://www.iso27001/security.com/html/iso27002.html

[9] Džonson D.: *Kompjuterska etika*, Službeni glasnik, Beograd, 2006, str. 18–19.

[10] *Ibid*., str. 16.

napadnutih sistema na univerzalno primenljiv način. Iz tog razloga, potrebno je strateški razvijati programe koji bi povećali mogućnosti za detekciju, reakciju i oporavak od kiber napada. Ovakvi programi bi bili od posebnog značaja za bezbednost države i podrazumevali bi istraživanje u tri ključne oblasti: zaštita informacija i informaciono-komunikacionih mreža, sistemi C3I za brze odgovore i fuzija informacija.[11]

Postizanje zadovoljavajućeg stepena zaštite informacija i informaciono-komunikacionih mreža zahteva osmišljeno sprovođenje aktivnosti na poboljšanju autentifikacije (sprečavanju neautorizovanih korisnika da pristupe sistemu i nanesu štetu), detekcije napadača (otkrivanju upada spolja i iznutra), održavanja funkcionalnosti sistema koji je oštećen u napadu (unapređenje projektnih rešenja koja ispunjavaju ovaj zahtev) i oporavku sistema (dekontaminacija sistema i vraćanje sistema u prvobitno stanje). Osim toga, poželjno je razvijati i implementirati softverske alate koji neprekidno testiraju ispravnost rada informatičkih sredstava. Svaka kompjuterska i mrežna komponenta mora imati ugrađenu funkcionalnu komponentu koja je neprekidno testira i osigurava bezbedno funkcionisanje, kao i zaštitu od zloupotreba.[12] U ovu svrhu mogu se koristiti tzv. embedded sistemi, tj. sistemi posebne namene koji su pravljeni mimo uobičajenih standarda i poznatih, komercijalnih, projektnih rešenja prisutnih na tržištu.[13]

Sistemi C3I (*engl*. command, control, communication, intelligence) za brze odgovore su osmišljeni sa ciljem povećanja koordinisanosti bezbednosnih službi u vanrednim situacijama. Ovi sistemi treba da povećaju međusobnu povezanost i time poboljšaju komunikaciju, saradnju i koordinaciju različitih državnih i privatnih bezbednosnih institucija. Ovi sistemi su bazirani na upotrebi informatičke tehnologije i koriste se za sortiranje, vrednovanje, filtriranje i integraciju informacija koje potiču iz različitih izvora.

Fuzija različitih vidova informacija je veoma bitna u prevenciji, detekciji i odgovoru na različite vrste subverzivnih aktivnosti, uključujući i kiber ratovanje. Unapređene mogućnosti za prikupljanje, integrisanje i interpretaciju velike količine podataka mogu pomoći donosiocima odluka i obaveštajnim službama na polju suprotstavljanja bezbednosnim pretnjama. Ekstrakcija podataka (*engl*. data mining) predstavlja tehnologiju za analiziranje i selekciju odgovarajućih formi podataka iz velike količine prikupljenih ili tekućih podataka. Ovi, ekstrahovani podaci (iz mnoštva različitih i nestrukturiranih formata podataka kao što su: tekst, slika, govor, video, i to na različitim jezicima), po unapred zadatoj formi, koriste se kao podrška u donošenju odluka i preduzimanju preventivnih aktivnosti na zaštiti informacionih sistema i, uopšte, kritičnih infrastruktura.

ZAKLJUČAK

Sa aspekta individualne, korporativne, nacionalne, ali i regionalne i globalne bezbednosti, razumljiva je teza po kojoj se bezbedan kiber prostor smatra imperativom informacionog doba. Ne treba, međutim, smetnuti s uma da se priroda

[11] Džigurski O., *op. cit.*, str. 180.
[12] *Ibid*., str. 181.
[13] Ravi S., Raghunathan A., Kocher P., Hattangady S.: "Security in embedded systems: Design challenges", *ACM Transactions on Embedded Computing Systems*, Volume 3 Issue 3, August 2004.

kiber prostora protivi stanju apsolutne bezbednosti. Brzina kojom se pretnje uvećavaju, zahteva usvajanje pouzdanih, brzih i efikasnih bezbednosnih mera koje treba da budu diskriminišuće prema tvorcima pretnje.

Efikasan odgovor visokotehnološkom kriminalu nije moguće pružiti samo pravnim merama. Zadovoljavajući stepen zaštite kiber prostora nije moguće postići ni usvajanjem i sprovođenjem tehničkih mera, već, iznad svega, formulisanjem strategija zaštite i sinergijskim sprovođenjem serije protivmera od strane međunarodnih organizacija, državnih institucija, ekspertskih udruženja i individualnih korisnika informacionih sistema.

Zaštitne aktivnosti, prema tome, moraju podrazumevati konstantan napor svih onih koji su odgovorni za funkcionisanje informacione infrastrukture. Na individualnom nivou, odnos korisnika prema informacionim sistemima može da obezvredi i najsavremenije i najskuplje limitirajuće bezbednosne sisteme. Svaki korisnik, dakle, ima važnu ulogu u unapređivanju bezbednosti kiber prostora. Bilo koji računar, ukoliko nije adekvatno zaštićen, može postati objekt i/ili sredstvo napada protiv drugih sistema. Prema tome, promovisanje bezbednosne kulture i razvijanje kompjuterske etike spadaju u red prioritetnih aktivnosti na polju prevencije visokotehnološkog kriminala.

LITERATURA

1. Chirillo J.: *Hack Attacks Revealed – A Complete Reference with Custom Security Hacking Toolkit*, John Wiley & Sons, New York, 2001.
2. Endorf C., Schultz E., Mellander J.: *Intrusion Detection & Prevention*, McGraw-Hill, 2004.
3. Institut za standardizaciju Srbije, http://www.iss.rs/news/news_33.html
4. Kovačević, Ž.: *Kompjuterska špijunaža i zaštita*, master rad, Fakultet bezbednosti, Beograd, 2010.
5. Kukrika, M.: *Upravljanje sigurnošću informacija*, INFOhome Press, Beograd, 2002.
6. Petrović, S.: *Policijska informatika*, Kriminalističko-policijska akademija, Beograd, 2007.
7. Putnik, N.: *Sajber prostor i bezbednosni izazovi*, Fakultet bezbednosti, Beograd, 2009.
8. Rehman R.: *Intrusion Detection Systems with Snort*, Prentice Hall PTR, 2003.
9. Ravi S., Raghunathan A., Kocher P., Hattangady S.: "Security in embedded systems: Design challenges", *ACM Transactions on Embedded Computing Systems*, Volume 3 Issue 3, August 2004.
10. Spitzner L.: *Honeypots: Tracking hackers*, Addison Wesley, 2002.
11. The Honeynet Alliance, *Know Your Enemy Whitepapers*, http://www.honeynet.org/papers/kye.html
12. Džigurski, O.: *Informacione tehnologije u borbi protiv terorizma*, Zbornik Fakulteta civilne odbrane, Beograd, 2005.
13. Džonson, D.: *Kompjuterska etika*, Službeni glasnik, Beograd, 2006.

RESUME

Due to a tremendous number of users, its openness and lack of legal norms the Internet, which is in its nature vulnerable and insecure, has become a playground, as well as the perfect shelter, for all sorts of criminals. An enormous amount of data and information, which, in their nature, can represent material values, but at the same time they can personal, trade, professional, military or state secret, has been collected and saved in information systems. That is why any compromising of information systems can cause an immense damage to individual users, social subjects, and to the information society as a whole. Due to the fact that the global computer network is widespread and decentralized, activities of malicious actors in cyberspace have become an international problem, and they have opened questions about protection not only personal, but also somebody else's information systems, conducting international investigations, extradition and punishment of malicious actors. Cyber crime is a complex phenomenon and it stands for various criminal activities. The most frequent of them are attacks on computer systems and networks, contents or intellectual property. The other terms used for this form of criminal activity are: *the Internet crime, electronic crime (e-crime), cyber crime, network-based crime, etc.* Previous experience in confronting security threats in cyberspace points out at the necessity of creating a coherent framework of actions which embraces both preventive and repressive measures in order to create and maintain a safe cyber environment. Preventive activities, in the first place, entail creating various measures and strategies of protecting information systems and their implementation, improving legal regulations both on national and international levels, as well as their coordination with intelligence activities in their efforts to confront cyber threats. Protective activities, thus, have to entail constant efforts of all those who are responsible for maintaining the information infrastructure. On the individual level, users' attitude towards information systems can disable even the most expensive and state-of-the art limiting security systems. Thus, each user has an important role in improving the security of the cyberspace. Any computer, if it is not properly protected, can become a subject and/or means of attack against other systems. Accordingly, promoting a security culture and developing computer ethics are among the priority activities in the field of preventive measures against cyber crime.

Stručni rad - UDK 341.48: [343.326+004.738.5

HOW A CYBERCRIMINAL DOES LOOK LIKE? BUILDING A PROFILE OF MODERN CRIMINALS

***Stanojoska Angelina, MA*[1]**
***Petrevski Blagojce, Master candidate*[2]**
***Nikolova Kristina, Postgraduate student*[3]**
Faculty of Security – Skopje, Republic of Macedonia

Abstract: Cybercrime, by definition, is strongly connected with computers and networks. But machines, how much important they can be for this crime, are totally amoral and do whatever we tell them to do. Cybercrime has always been in step with new technology, better said it was born with it. Without any regrets we can call it the newest type of crime, the crime that showed us how dark human soul can be, because people started using its tools for better life to destroy some parts of it. As a mirror on moral character, the phrase "Jekyll and Hyde" has become accepted in popular culture to describe a person's hidden dark side. It pierced the veil between the fundamental dichotomy of the 19th century's notion of outward respectability versus a hidden and fulminating inward lust, depicting moral and social hypocrisy, while providing yet another instance of a fulminating criminal mind. On the surface, Dr. Jekyll is portrayed as an honorable physician with many friends and acquaintances; he nurtures his patients and his reputation by virtue of an engaging personality. Transitioning to Mr. Hyde, Jekyll disappears and is replaced by a person who is small in stature, mysterious, criminal, secretive, sexual, and violent.[4] Criminal profiling is the art and science of developing a description of a criminal's characteristics based on information collected at the scene of the crime. The profile is a psychological assessment made without knowing the identity of the criminal. The profile consists of a set of defined characteristics that are likely to be shared by criminals who commit a particular type of crime. The profile is used to narrow the field of suspects or evaluate the likelihood that a particular suspect committed the crime. The paper will try through its words to show how a criminal profile is built and how a typical cybercriminal looks like. Also it will pay attention to some stereotypes that totally change the profile and photo of a cybercriminal among ordinary people.

Key words: analysis, characteristics, cybercriminal, information, profiling, and profile.

INTRODUCTION: WHAT CYBER CRIME IS?

In less than two decades, the Internet has grown from a curiosity to an essential element of modern life for millions. As with other aspects of globalization,

[1] angelinastanojoska@yahoo.com
[2] blagojcedugal@yahoo.com
[3] tincenikolova@yahoo.com
[4] Don Jacobs. *Analyzing Criminal Minds: Forensic Investigative Science for the 21st Century.* (Santa Barbara-Denver-Oxford: Praeger, 2011), p.15-16

its rapid expansion has far exceeded regulatory capacity, and this absence of authority has left space for many abuses. The problem is compounded by the fact that the Internet was fashioned on a military system designed to circumvent interference and external controls. But even those who most loudly champion its creative anarchy have come to realize that the Internet can only reach its full potential if some basic ground rules are established and if antisocial behavior is vigorously discouraged. The challenge remains how, exactly, to do this. (United Nations, 2010)

"Cybercrime" has been used to describe a wide range of offences, including offences against computer data and systems (such as "hacking"), computer-related forgery and fraud (such as "phishing"), content offences (such as disseminating child pornography), and copyright offences (such as the dissemination of pirated content). It has evolved from the mischievous one-upmanship of cyber-vandals to a range of profit-making criminal enterprises in a remarkably short time. Of course, criminals, like everyone else with access, make use of the Internet for communication and information gathering, and this has facilitated a number of traditional organized crime activities. But the growing importance of the Internet and our collective dependence on it has also created a number of new criminal opportunities. (United Nations, 2010)

Going step by step together with technology development, cyber crime can surely be called the new age crime. The "machines" today are used very smartly from criminals for fulfilling their criminal ideas and necessities. Although most of these crimes are carried from the other side – the criminals in the most cases are on the other side of the wire and we do not have a classical crime scene.

''Cybercrime'' also consists of engaging in conduct that is outlawed because it threatens order. Cybercrime differs from crime primarily in the way it is committed: Criminals use guns, whereas cybercriminals use computer technology. Most of the cybercrime we see today simply represents the migration of real-world crime into cyberspace. Cyberspace becomes the tool criminals use to commit old crimes in new ways. (Brenner, 2010)

Symantec Corporation defines cybercrime broadly as "any crime that is committed using a computer or network, or hardware device". This is a very broad definition that not only includes crimes that use or target computer systems and networks, but it also includes crimes that happen within a standalone hardware device or computer. Kshetri analyses cybercrime and its motivation in terms of cost-benefit to the cyber-criminal and defines cybercrime as a crime that utilizes a computer network during the committing of crimes such as online fraud, online money laundering, identity theft, and criminal uses of Internet communication. Wall describes cyberspace and the new types of crime as "new wine, no bottles", however, in contrast, Grabosky suggests that it is a matter of "old wine in new bottles", since the cybercrime is "basically the same as the terrestrial crime with which we are familiar". However, generally and as indicated previously, the term 'cybercrime' involves not only new crimes against computer data and systems, but it also involves traditional crimes such as fraud. (Baggili, 2011)

The Council of Europe Convention classifies cybercrime into four main categories: offences against confidentiality, integrity and availability of computer systems and data; computer related offences (forgery, fraud); content related

offences; and offences related to infringements of copyright and related rights. We note that the Council of Europe cybercrime categorization does not include some types of crimes that have been committed or facilitated using the computer such as money laundering, identity theft and storing illegal content. (Baggili, 2011)

The United Nations manual on the prevention and control of computer-related crime, published in 1999, lists five common types of computer crime: fraud by computer manipulation; computer forgery; damage to or modification of computer data or programs; unauthorized access to computer systems and services; and unauthorized reproduction of legally protected computer programs. Though the UN manual includes crimes against computer data and systems, it also covers some crimes that utilize computer systems such as fraud and forgery. However, the manual does not refer to other types of offences that are committed or facilitated by a computer or computer system such as identity theft, money laundering and storing illegal content. (Baggili, 2011)

The U.S. Department of Justice defines *computer crimes* as "crimes that use or target computer networks, which we interchangeably refer to as 'computer crime,' 'cybercrime,' and 'network crime'", and refers to viruses, worms and Denial of Service attacks. The UK Association of Chief Police Officers (ACPO) has defined e-crime as the "use of networked computers, telephony or Internet technology to commit or facilitate the commission of crime", which is consistent with the original, network-specific, origins of the term cybercrime. (Baggili, 2011)

Today, it is obvious that, cybercrime just like many other types of crimes, especially the modern ones, still causes differences between countries in the process of making one, only and for everyone acceptable definition. The lack of a unique definition results with problems between countries in processes of investigation, in processes of prosecution and sanctioning of perpetrators.

In the next few pages, readers will have the opportunity to read how profiling, as one of the most used methods in investigations, can help in the cases of cybercrimes and how with it usage law enforcement officials build a profile of a cybercriminal.

CRIMINAL PROFILING: A METHOD OF "DRAWING" A CRIMINAL

One of the first documented uses of criminal profiling involves the demonization of Jews with a fairly crude form of profiling. Its origins are found in a report made by the anti-Semite scholar Apion to the Roman Emperor Caligula in 38 ce. Apion felt the Jews of Alexandria, where he had studied, had too many rights and privileges. Apion, documented in the writings of Flavius Josephus (*Contra Apionem*, circa 90s ce), falsely reported to Caligula that the Jews were often responsible for the ritual killing and eating of Greeks as part of Passover. (Turvey, 2008)

The *blood libel*, or false accusation of ritual killing, is an early and persistent form of criminal profiling because it involves a predetermined set of crime-related characteristics used to infer and consequently accuse a particular suspect pool—namely the Jews. From the available literature cited in this work, the general profile used included one or more or the following elements:

- A young Christian male goes missing.
- A Jewish community is nearby.
- The child goes missing on or just prior to Passover.
- The body may have injuries that appear to be the result of a ritual.
- The body may have lost a great deal of blood or may simply appear so.

One of the first published texts that offered explicit instruction on the subject and practice of profiling criminal behavior is the *Malleus Maleficarum* (*The Witches' Hammer*). Two Dominican monks, Henry Kramer and James Sprenger, professors of theology of the Order of Friars Preachers, originally published this work around 1486. Written in Latin, it was intended as a rationale and guide for those involved with the Inquisition (namely the authors), to assist in the identification, prosecution, and punishment of witches. Upon publication, *Malleus Maleficarum* was fully sanctioned by the Catholic Church in fear of being made impotent by the existence of heretics, nonbelievers, and the failed Crusades against the Muslims, which had been waged in vain to occupy and control the Holy Land. Included in the *Malleus Maleficarum* was the bull of Pope Innocent VIII, written two years previously on December 9, 1484. (Turvey, 2008)

According to the *Malleus Maleficarum,* witches and other criminals may be identified by specific circumstances, abilities, and characteristics. For example, the witches were described as women who have a spot, scar, or birthmark, sometimes on the genitals and sometimes invisible to the Inquisitor's eye, live alone, keep pets (a demon in animal form known as a *familiar*), suffer the symptoms of mental illness (auditory or visual hallucinations, etc.), cultivate medicinal herbs, have no children. (Turvey, 2008)

Profiling is an approach to solving a crime by asking, "What does this crime say about the person who committed it?" At the beginning of its life it was used as a tool for building a typical criminal offender. Today profiling is used to understand why crimes are being committed, how the criminal behavior can be classified and to solve the already committed crimes.

The term *criminal profiling,* today has many different meanings and sometimes scientists use different nomenclature for its explanation.

More detailed descriptions of criminal profiling, however, include the following:

A forensic technique which seeks to provide investigative agencies with specific information which will help focus attention on individuals with personality traits that parallel traits of other perpetrators who have committed similar other offenses; or *The process of identifying personality traits, behavioral tendencies, and demographic variables of an offender based on characteristics of the crime.* More recent descriptions of profiling have suggested the following: *Criminal profiling refers to the process of identifying personality traits, behavioral tendencies, geographic locations and demographic or biological descriptors of an offender based on characteristics of the crime. It is an attempt to provide investigators with more information on a serial murderer who is yet to be identified.* (Kocsis, 2006)

The earliest usage of criminal profiling for making a bridge and symbiosis between behavior and personality comes from England at the time of Queen Victoria. Although the origins can be found into the novels of Sir Arthur Conan Doyle and the infamous character Sherlock Holmes, however the most notable

example of profiling is the one of the earliest serial killer known as Jack the Ripper. Dr. Bond was asked using his skills and the traces found on the crime scenes to build a profile of the possible perpetrators. Written 120 years ago, Dr. Bond's profiling notes included facts that can be found in today's profiling cases, especially the modus operandi. In his reports he describes the main characteristics of the possible perpetrator, as the age, gender, profession, demeanor, the way he dresses, and the possible mental problems.

Also, one the best historical example of criminal profiling is the one from 1943 when Dr. Walter Langer built the profile of Adolf Hitler. In his report Dr. Langer named a number of potential reactions in a situation of defeat, but marked the suicide as the most likely to be used from Hitler to avoid possible capture and humiliation.

Criminal profiles typically contain information about the probable offender concerning the following:

- Likely demographics, such as age and gender.
- Legal history, including any antecedence (i.e., history of prior criminal offenses/ convictions).
- Vocational background (i.e., the work the offender is likely to be engaged in, if any).
- Family characteristics (i.e., the likely background of the offender's family).
- Habits and social interests (sports, hobbies, or other interests that the offender may have).
- Mode of transport (type of vehicle, if any, the offender has).
- Various personality characteristics (the offender's demeanor, appearance, etc). (Kocsis, 2006)

There two types of criminal profiling. They are inductive and deductive criminal profiling. The inductive profiling uses statistics and comparative analysis during the creation of criminal profile. The information comes from studies of already convicted criminals, their observation, the usage of clinical methods, interviews, and data from official databases. All this information is being analyzed and the profiler builds a possible profile of a perpetrator of a kind of crimes which is based on the characteristics of other criminals that have already committed such type of crime. But it is a method that results with nonspecific and generalized examples.

The deductive profiling is a method of building the profile on the information, the evidences that can be found on the crime scene. Using this type of profiling, professionals try to get inside the criminal mind and to think as the perpetrator did during the crime. This type is not used on statistical data; it is based on human intelligence.

In addition to such biographical information, it should be noted that criminal profiles frequently also include information pertaining to the approximate location of an offender's residence. This type of information is often the product of what is now commonly referred to as *geographic profiling.* Although some arguments exist for the formulation of a discrete discipline known as geographic profiling, the basis for these arguments appears to be largely sourced in vocational interests. Although some research developments have indeed emerged in the evaluation of geographic

features relevant to criminal profiling, information such as an offender's likely area of residence have long been components of the information typically contained in criminal profiles. Consequently, although a separate set of methods exist for the evaluation of such geographic information, it is preferable to view these methods as simply a subcomponent of information that comprises a criminal profile. (Turvey, 2008)

At the end we must conclude that criminal profiling and criminal profiles never solve crimes by itself. For best results criminal profiling should be seen as tool and source of information for better usage of the other methods during the criminal investigation.

PROFILING CYBERCRIMINALS: STEPS, METHODS, MODUS OPERANDI, STEREOTYPES

The role of the Internet as the tool for committing most of these crimes, results with dividing criminals into two groups. Criminals who use the Internet as a tool to commit the criminal act and criminals whose usage of the Internet for the committing of the crime was incidental.

The first ones are may be white-collar criminals, computer con artists, hackers, crackers, network attackers. The second type are those who use the network to find victims, who use computers for keeping records, who use e-mail or other services for communicating with accomplices.

Wherever computer centers' have become established…bright young men of disheveled appearance, often with sunken glowing eyes, can be seen sitting at computer consoles, their arms tensed, and waiting to fire, their fingers, already poised to strike at the buttons and keys on which their attention seems to be as riveted as a gambler's on the rolling dice. When not so transfixed they often sit at tables strewn with computer print-outs over which they pore like possessed students of a cabalistic text…. They exist, at least when so engaged, only through and for the computers. These are computer bums, compulsive programmers. They are an international phenomenon. (Taylor, 1999)

The motivations offered by hackers for their activity frequently seemed influenced by their sensitivity to the agendas of the various groups that oppose hacking. The computer security industry, for example, is accused of over - emphasizing the vandal- orientated motivations and pathological aspects of hacking. The motivations lying behind hacking, according to the internal account, are categorized into six main areas:

1. Feelings of addiction;
2. The urge of curiosity;
3. Boredom with educational system;
4. Enjoyment of feelings of power;
5. Peer recognition;
6. Political acts.

The cybercriminal is usually not the only person on the scene of the cybercrime, however. Some cybercrimes appear to be victimless, such as a network intrusion that occurs without anyone knowing about it, in which no files are harmed

and no information is "stolen" or misused. In most cases, though, some person(s) are ultimately harmed by the cybercriminal's actions. These victims might be workers who lose productive time due to a DoS attack or have to redo their work because of cyber vandalism. They might be company shareholders who lose money due to extra charges for the bandwidth that a hacker uses. They might be managers who lose "brownie points" in their bosses' eyes because of the impact on their budgets. They might be IT administrators who lose their jobs for "allowing" the attack to happen. In most cases of cybercrime, if you look hard enough, you'll find a victim. (Schinder, 2002)

Because of the untypical type of crime that cybercrime is, today, also with a huge thanks to Hollywood, we are witnesses of many stereotypes about how cybercriminals look like. So, some of those stereotypes are:

- All cybercriminals are "nerds"—bright but socially inept.
- All cybercriminals have very high IQs and a great deal of technical knowledge.
- All cybercriminals are male, usually teenage boys.
- All teenage boys with computers are dangerous cybercriminals.
- Cybercriminals aren't "real" criminals because they don't operate in the "real world."
- Cybercriminals are never violent.
- All cybercriminals neatly fit one profile. (Schinder, 2002)

When a law enforcement official starts with building a profile of a cybercriminal, he should always start with some generalities that are typical for most cybercriminals from most categories.

Well, a person to commit a crime into the cyber space must be capable to do basic tasks that Internet requires. Also, some crimes require even greater computer knowledge. This type of criminals is just the same as the other ones. They don't believe they should respect the law just because it is the law. They think sometimes laws are unreasonable and that's why they should be broken. Many of the cybercriminals use the Internet as a possibility for fulfilling their fantasies. Using the Internet they build completely new identities and start to play the role of someone different.

Criminals committing crimes often expend more energy than what they practically get for return. So it is normal to ask ourselves than why do they do those things? Why to act as such a high risk manner? For some of them it is the risk of getting caught – the thrill of doing a forbidden act. For others it is the possibility of controlling and manipulating the others.

Most cybercriminals are strongly motivated, but the motivations range from just wanting to have fun to the need or desire for money, emotional or sexual impulses, political motives, or dark compulsions caused by mental illness or psychiatric conditions. Discerning the motivation for a particular crime is an important aspect of building a useful profile of the criminal who committed it. (Schinder, 2002)

Why do criminals commit crimes? Because they are criminals. If it was that simple. People break the law for many different reasons. Some of those reasons might even seem reasonable, such as the out-of-work mother with no money left who steals baby food to feed her child. On the other hand, many people in

dire straits find solutions to their problems that don't involve breaking the law. Some cybercriminals - for example, the longtime loyal employee who suddenly embezzles company funds to pay unexpected medical bills or get a relative out of trouble - might do so out of desperation, too. Most, though, are driven by far less noble motives: greed, anger, lust, or just plain boredom. (Schinder, 2002)

Why does motive matter? In many jurisdictions, an important element of proving guilt is showing that the accused possesses each component of the so called *crime triangle:* means (a way to commit the crime), motive (a reason for committing the crime), and opportunity (being in the right place at the right time to commit the crime).Thus understanding the criminal's motive is useful at two points in the investigation: when we are creating a profile to help us identify the correct suspect(s) and later when we present the case against our suspect. (Schinder, 2002)

Common motives for committing cybercrimes include: (Schinder, 2002)

- ✓ Just for fun;
- ✓ Monetary profit;
- ✓ Anger, revenge, and other emotional needs;
- ✓ Political motives;
- ✓ Sexual impulses;
- ✓ Serious psychiatric illness.

All the above mentioned characteristics can and should be used during the profiling of cybercriminals. Every trace, every message, every word is important, especially because of the absence of criminals from crime scene that is common for this kind of crime.

CONCLUSION

From the already analyzed in the words you could read, we can surely conclude how much criminal profiling means to the investigation. Being a method which makes a clear connection between motive, behavior, character and acts of the perpetrator, it surely deserves a high spot in the classification of important criminal investigation's methods.

When a profiler uses profiling as a one of the methods in a solving a case, it is always better to have the opportunity to see the crime scene, to find the evidences, the traces that sometimes the criminal leaves there. Using all those things allows the profilers to make a good and potential profile of the criminal.

But when cybercrime is in the middle of an investigation, then in the most of the cases the crime scene and the presence of the perpetrator on the place in the time of the committing of the crime is never a case. That's why it is so difficult to build a profile of a cybercriminal in a case. In these cases, profilers use statistical data and build their results on other cases' information.

BIBLIOGRAPHY

1. Brent, E.T. (2008). *Criminal Profiling: An introduction to behavioral evidence analysis.* Oxford: Academic Press;
2. Debra, L.S. (2002). *Scene of the cybercrime: Computer Forensics Handbook.* Rockland: Syngress Publishing;
3. Ibrahim, B. (2011). *Digital Forensics and Cyber Crime.* London-New York: Springer;
4. Jaishankar, K. (2011). *Cyber criminology: Exploring Internet Crimes and Criminal Behavior.* Boca Raton-New York-London: CRC Press;
5. Jonathan, C. (2010). *Principles of cybercrime.* Cambridge: Cambridge University Press;
6. Paul, A.T. (1999). *Hackers: Crime in the digital sublime.* London-New York: Routledge;
7. Rebecca, S. (2011). *Criminal Profiling.* New York: Marshall Canvendish;
8. Richard, N.K. (2006). *Criminal Profiling: Principles and practice.* New Jersey: Humana Press;
9. Sumit G. & Elliot T. (2010). *Cybercrimes: A multidisciplinary analysis.* London-New York: Springer;
10. Suzan, W.B. (2010). *Cybercrime: Criminal Threats from cyberspace.* Santa Barbara-Denver-Oxford: Praeger Publications.

Stručni rad - UDK 341.48: [343.326: 004.738.5

DESIGNING CLASSROOM ACTIVITIES FOR TEACHING CYBER CRIME TO STUDENTS OF ENGLISH FOR LAW ENFORCEMENT

Vesna Trajkovska, MA
Faculty of Security- Skopje
trajkovska_vesna@yahoo.com
Radomir Trajkovic, BA
radomir.trajkovic@gmail.com

Apstract: The paper elaborates on the importance of the inclusion of topics related to various types of cyber crime in course materials for teaching English to law enforcement students. It specifically focuses on offering alternatives for successfully designing exercises and activities centered around cyber crime-related content. The aim of those activities is to present the issue of cyber crime through exercises which are modified and adapted to students' level of knowledge. They are specifically designed so as to address the issue from different aspect, and to involve students in interactive and group work. By participating in activities of this kind, students will be able to acquire knowledge about various types of cyber crime which would simultaneously enable them to improve their reading, listening, writing and speaking skills in English.

Key words: English language, cyber crime, language skills, law enforcement

INTRODUCTION

In recent years the possession of relevant foreign language skills has become mandatory for specialists in various areas. Being the world lingua franca, i.e. the globally accepted language of international communication, English has managed to impose itself as the most widely spoken language in the world, which necessarily led to its inclusion in the curricula at all levels of education.

As far as police profession is concerned, English language skills form an integral and very important segment in the education of prospective law enforcement professionals. Apart from the need to communicate in English in various situational settings, knowledge of English is also necessary in dealing with crime-related issues on a daily basis in the performance of police duties. The latter is particularly true for those departments which deal with new, sophisticated types of crimes for whose detection it is necessary to have sufficient knowledge of the specific terminology. This is also the case with the various types of cyber crime whose commission is directly linked with the knowledge of internet and computer technology and English as its "operative" language.

Another aspect that needs to be considered is the lexical influence of English on other languages which is particularly felt in the area of IT technology and the development of new and sophisticated forms of crimes assisted by computers. This actually means that lexical solutions for newly-developed concepts are directly transferred from English and it is necessary for students of English for law enforcement

to be able to make a clear distinction between the different types of computer crimes like spam, phishing, cyber stalking etc. which are also used in their language in their identical form. This knowledge will surely help them later in tackling these problems in practice in a more efficient way.

The topic of cyber crime is also specific because of the complex nature of this phenomenon in terms of the use of IT technology for its commission. For this reason, it is recommended that law enforcement students get some insights into the basic concepts related to IT technology and computer networks. Since most of these concepts are originally derived from English, it is necessary that they are also included in the English syllabus.

Having considered these aspects, it becomes clear why the issue of cyber crime is an important topic in the English language curriculum for law enforcement students. Among various approaches which can be used for achieving this goal, in this paper we will present a model for developing a lesson plan on this topic based on the communicative approach, which has particularly been applied to ESP courses. For this purpose, in the following sections we will present several different exercises, each one addressing the issue of cyber crime from a different aspect. We will present a model for integrating this issue in English teaching materials, which has successfully been implemented at the Faculty of Security in Skopje, with the aim that it may help other English language teachers in their efforts to enrich their classroom activities with this specific group of target students.

ESP: DEVELOPMENT AND CHARACTERISTICS

English for specific purposes (ESP) is one of the branches of teaching English as a foreign language (EFL). The need for developing ESP emerged not long after the end of the Second World War, when, as a result of the growth of the economic and political power of the United States of America the English language was promoted as the commonly accepted language for international communication. This period was characterized by a great change as far as the motivation for learning foreign languages was concerned. The new "generation" of learners became completely aware of the reasons for learning English which were derived from the demands of their specific professions. For the first time in the history of foreign language learning, they knew why they needed the language, and in what contexts and situations they were going to use it.

Bearing this in mind, it was logical that the needs of the new target learners could only be addressed and satisfied by developing a separate branch of English for specific purposes which would focus only on learners specializing in specific areas. As a result, the development of ESP was directed towards its numerous sub-branches, each one dealing with a specific subject area: economics, law, medicine, engineering etc. Each of these ESP branches had its own specificities, due the different target students to which they appealed.

Along with the economic and political reasons behind the new role of English on the world linguistic map, the growth of ESP was also fostered by the major shift in foreign language teaching methodology and the introduction of the communicative teaching approach, which happened in the beginning of the 1970s.This approach was primarily based on the developments in linguistics and the new role of the learners as

active participants in the language acquisition process. They had specific needs, which differed according to the subject area in question, and the teaching resources had to be adapted so as to address them to greater effect. According to CLT tenets, their needs could best be addressed by engaging students in activities which would demand their active involvement in communicative, interactive activities aimed at solving a specific problem or fulfilling certain tasks. The teachers' role was mainly instrumental and they primarily served as facilitators in the language acquisition process. The syllabus became dominated by fluency-based exercises, and accent was put on functional use of language in simulated real-life situations and contexts.

THE PROCESS OF DESIGNING ESP TEACHING MATERIALS

The specificity of ESP teaching led to the adoption of specific methodology for successfully designing appropriate course materials that would satisfy the specific needs of the target learners. Unlike general English course books which covered general topics, ESP instruction was centered around topics relevant to the target area of study. This is the reason why ESP methodology was mainly developed on the grounds of content-based instruction, which was a segment of the previously mentioned wider concept of communicative language teaching.

In content-based instruction teaching is "organized around the content or information that students will acquire, rather than around a linguistic or other type of syllabus" (Richards, 2001:204). This practically means that the lessons are designed in a manner that would enable students to acquire knowledge about certain topic relevant to their profession or area of interest. In other words, English language is used as a sort of an instrument for acquisition of professional knowledge. Viewed from this perspective, one might get a wrong impression that this type of learning is directed solely towards the target contents. This is, actually, a two-way process where language is used as a medium for acquiring knowledge about the specific content taught, while at the same time by learning about the specific topic students acquire and practically use different language skills. The benefit is, therefore, two-fold, because through ESP teaching materials learners are exposed to the language of a particular discipline as it is actually used (Dudley-Evans and St John, 1998: 171). They simulate real-life events and are given an abundance of input based by adequately adapted authentic resources, thus adding a feeling of usefulness of the course materials for the students' professional development in future.

Designing ESP course materials is a time-consuming and tedious process. It requires great efforts by ESP course designers, due to the fact that their role is quite different from the role of designers of general English courses. Apart from the adequate knowledge of English language teaching methodology, they should also possess satisfactory knowledge about the specific contents that should be incorporated into the teaching materials. This process actually consists of the following steps:

1.*Needs analysis.* This is the initial stage in the process of developing course materials. It refers to the collection of information about the specific needs of the learners related to foreign language learning. They are often described in terms of linguistic deficiency, which refers to the difference between what the learner can do at the moment and what s/he should be able to do. This is a very important instrument for

collecting relevant information about the elements that should constitute the specific course, in terms of the specific topics, vocabulary, functions etc.

2. *Selection and adaptation of contents*. Having collected the necessary information about the needs and the expectations of the learners, course designers move to the process of collection of appropriate teaching resources which are directly related to the specific area of study of the target learners. However, this content cannot always be used in its original form. The course designer has the complex task of extracting only those resources that are most useful and relevant to the subject. Sometimes it is feasible to use authentic materials integrally, but much often they should undergo certain modifications. This means that they should be adapted to the learners' level of knowledge of English, in order to provide greater effectiveness among them, thus reducing learners' affective filter.

3.*Course materials piloting.* After the collection and modification stage has finished, the newly designed teaching materials should be piloted, i.e. tested among a selected group of learners. This stage is important in that it provides an opportunity for language instructors to see how learners react to the teaching contents and to identify any possible aspects that need to be worked on and improved in future.

4.*Evaluation.* The final stage refers to the evaluation of the piloted teaching materials. The evaluation is done by the learners, and it is useful since it serves for eliciting learners' feedback and washback which was possibly achieved with the specific course materials.

DESIGNING COURSE MATERIALS FOR ENGLISH FOR LAW-ENFORCEMENT BASED ON CONTENT-BASED INSTRUCTION: THE ISSUE OF CYBER CRIME IN THE ENGLISH LANGUAGE CLASSROOM

The procedure described in the previous section is also applied when creating materials for teaching English to law-enforcement students. In this specific case, the teaching materials should consist of topics related to police job, which would help the learners as prospective professionals in this area to perform their duties in a successful and efficient manner. Bearing in mind the specific nature of this profession which requires a high level of interaction, it would be logical to organize the syllabus in such a manner that would allow the development of students' communicative competence through exposing them to situations in contexts that would foster functional use of English language. This can be achieved through a combination of various methods within communicative language teaching, and should be focused on the integration of all four language skills: reading and listening as receptive skills, and speaking and writing as productive skills. On the bases of what we have previously elaborated on, it is logical to put greatest emphasis on content-based instruction as part of CLT, which would require adaptation of authentic law enforcement materials and their transformation into didactic units. In order to achieve the aim of students' enhanced communicative competence, the units will comprise activities and tasks fostering students' interaction and participation in pair, group and whole-class work.

For the purpose of this paper, we chose to present a model for successfully designing an English lesson plan for law enforcement students on the topic of cyber crime. Being a relatively new phenomenon, we found it challenging to try to explore

the topic and transform some of the contents we selected into interesting and appealing classroom activities and exercises which would raise students' interest in the subject and motivate them to use the English language for acquiring knowledge about this issue. On the following pages, we will present the sample lesson plan about cyber crime, describing the various steps and illustrate them with appropriate and relevant exercises.

Activity 1 - Introduction of the topic (Goal: developing students' speaking and listening skills)

Based on the experience gained from our teaching practice, both at the Faculty of Security and other educational institutions in Macedonia, we decided to offer a lesson plan which begins with a speaking activity. It could be a good idea to start the lesson by engaging students in whole-class discussion which would contribute to the creation of a pleasant learning atmosphere- a prerequisite for successful acquisition of the subject being taught. As for our topic of interest, one of the possible alternatives would be to play a short documentary which would provide the students with basic input related to cyber crime phenomenon. The video would serve as a medium for introducing the topic and raising certain questions that would later be addressed in the class discussion. After watching it, students could be asked to discuss some basic concepts regarding cyber crime and answer some of the following questions: *How would you define the concept of cyber crime? In what ways is it different from "ordinary" types of crime? What type of people are most likely to engage in virtual criminal activities? What are the different types of cyber crime? How can cyber criminals be tracked? Have you heard or read about cases of cyber crime in your country?* etc.

The aim of the discussion is to provide students with certain amount of cyber crime- related input, that would help them get a general idea about this issue and will prepare them for successful fulfillment of their subsequent classroom tasks. Spoken interaction in this initial stage is also very important for lowering students' affective filter and for creating an atmosphere that would stimulate and encourage all students (irrespective of their level of knowledge of the language) to participate in class discussion.

Activity 2- The history of cyber crime (Goal: developing students' reading skills)

Now that students have some general idea about the notion of cyber crime, it would be useful to continue with a more detailed elaboration on this issue. We thought that it would be good to provide a sort of a historical overview of the development of this phenomenon. However, we wanted to avoid falling into the trap of providing students with exhaustive list of events that would surely be boring for them, so we decided to approach this activity from a different, student-centered aspect. In order to achieve greater interaction, we propose that students are given the different pieces of information about specific "stages" in the historical development of cyber crime, and their task is to work in groups of several students and try to put them in appropriate chronological order. The advantage of this type of activity lies in the possibility for the inclusion of all students, both stronger and weaker ones, and the interaction between them which is necessary in order to negotiate meaning and reach a logical "solution".

The following are excerpts from this exercise:

- *The first criminals who dared abuse the electronic communication network were born. These were called* ***phreakers****, whose specialty was to break into phone networks to make free calls.* **(1970s)**
- *As computer network becomes a more attractive way of electronic communication, cybercriminals specialize in breaking into computers, and now become known as* ***hackers****.* **(1980s)**
- *The first virus in the wild came into being. Founded on the Apple II operating system, it was spread on Apple II floppy disks containing the operating system.* **(1981)**
- ***AIDS Trojan*** *was created. the Trojan encrypts the user's hard drive, preventing him access to it and demands payment for the decryption key or password.* **(1989)**
- *Launched by Symantec,* ***Norton AntiVirus*** *was one of the first anti-virus programs developed by a large company.* **(1990)**
- *After a highly eventful and publicized chase, serial computer criminal, Kevin Mitnick is captured by federal agents and charged with stealing 20,000 credit card numbers. He was kept in the prison for four years without any bail.* (1995)
- *Cybercriminals undertook the first phishing activities: stealing of account usernames, passwords, and other personal information. At its onset, this was mainly done by simply sending fake emails to various users and tricking them into mailing back their personal information.* **(1996)**
- ***Denial of Service*** *(DoS) emerged as a new form of attack, mainly targeting the domain name servers of well-known websites such as Yahoo!, eBay and Microsoft.* **(2000)**
- *Cyber crooks devise a new method to phish for users' personal information: they start to fake legitimate web sites. One way was to register domain names that tend to mimic the well-known websites thus tricking the victims into believing that they are accessing a safe and trustworthy site that they are familiar with. Another technique involves the legitimate website opening in the background, but a fake log-in page appearing in the front as pop-up window.* **(2003)**

Activity 3- Testimonies of victims of cyber crime (developing students' listening skills)

The lesson may continue with an activity that would help students enhance their listening skills. Bearing in mind the fact that we are concentrated on the specific topic of cyber crime, the listening activity should also address certain aspect related to it. In this case, we propose an activity which focuses on different types of cyber crimes. As a pre-listening activity, students are given sufficient lexical input about the meanings of various cyber crimes, like: cyber stalking, phishing, credit card fraud etc. After they acquire the knowledge necessary for the listening task, they are given clear instruction about the content of the listening part and what they are supposed to pay attention to, as they are listening. They will actually hear parts from testimonies of several people who have been victims of different types of cyber crime or who have witnessed or heard about cases of cyber crime. While the people are speaking, students have the task to identify the type of crime which was committed in each case and match it with the corresponding answer. The possible answers are given as options in the book. In order to make it more challenging, we decided to put 2 extra options. By doing so, the teacher will get a clearer picture about whether students are truly able to distinguish between various cyber crimes. This activity is usually carried out as pair work. After they finish they compare their ideas and have a short discussion about their matches.

To illustrate this task, we are presenting excerpts from the testimonies below[1]:

Person A:
"This is the second day we've been staying at home, and some believe we're not going back to the office until next week. Officially, our computer system has crashed; but off the record, some cyber crooks have broken into our system, got hold of company's confidential files, and now demand ransom to retrieve the data! No one is allowed to use the company's computer system until it is fully backed up and secured." **(net extortion)**
Person B:
"This morning I opened my inbox, and it was full with mails advertising breast enlargement! I don't remember to have received such mails for 3-4 years now. Wasn't there a law in place against such junk mails? How come they started flooding my inbox again?" **(spamming)**
Person C:
"You are never going to believe this! The police confiscated our next-door's computer because they thought they were going to find evidence of his company's tax evasion. But what they actually found were loads of photos and videos of Suzie, the girl from the beauty-parlor two blocks down. Apparently, he's also been stealing her email, and chats she's been having with her Facebook friends! And Bertha told me some sexually explicit videos were there, too!" **(cyber stalking)**
Person D:
"I was so lucky he was beginner in this shady business and made this stupid, rooky mistake! He used my credit card number, but forgot to clear my address. So, all the stuff he bought online was actually delivered to me! Just imagine my surprise when I saw all this car parts at my doorstep!" **(credit card fraud)**
Person E:
"How many times do you want me to repeat this? I just own the internet café. I really don't care what my clients' use the computers for, nor am I allowed to pry into their online chats! Most of the people use the computers to download pornography, arrange dates, or make long-distance calls to friends and relatives. How could I imagine that those kids were actually organizing their drug dealings from my internet café? I really have nothing to do with this!" **(furtherance of criminal conspiracies)**
Person F:
"I was having hard time saving money for my next vacation, so I decided to go over all my transactions this year and see what I spend my money most on and where I can make certain cuts. As I was going through bank statements, I saw that for three consecutive months the salary amount I was receiving was not 430 euros, but 428.50 euros. I immediately called Becky to see what was the problem, and she said that according to my company's record they've been paying me exactly 430 euros each month. So, I approached the bank… And there you go, soon the bank discovered that an equal amount of 1.50 euros was being deducted from all their clients' accounts on the same day in the month. And all this money was immediately being transferred to another account in the same bank! A clever customer they had, indeed!" **(salami attack)**
Person G:
"The captain told us we had to make an emergency landing due to engine's malfunctioning. Only few days later did we learn that the whole airport was shut down because their electronic security system was broken into by secessionist supporters." **(cyber terrorism)**

[1] The excerpts are taken and adapted from "Cybercrimes: types of cybercrime ", http://cybercrimes09.blogspot.com/2009/10/types-of-cybercrime.html , retrieved on 20.02.2012

Activity 4- Psychological profile of cyber criminals (Goal: developing functional language use)

A very important aspect in the process of foreign language acquisition is the functional use of language. This aspect is particularly important for law enforcement students, since their future profession will necessarily require use of language for achieving specific functional goal. They should be able to prepare presentations in English, participate in negotiations, conduct interviews, hold press conferences etc.

Taking into consideration all these issues, as a logical follow-up in the sample exercise we propose the integration of English functions. In this case we decided to include functional language use incarnated through fostering students' competence for preparing and making presentations for a wider audience. Therefore, as a model we chose a presentation provided by a psychologist- an expert in criminal psychology who talks about the psychological profile of people who indulge in criminal activities using the Internet. The students are given the transcript of the presentation with some parts which are missing. As a pre-listening activity they should work in pairs and try to fill in the gaps with the missing words or phrases. After they finish, they listen to the presentation and check their answers. The goal of this exercise is to expose students to authentic use of English for functional purposes (in this case for oral presentation) and to enhance their skills for guessing meaning from a given context with the gap-filling exercise.

The excerpts from the presentation are given below[2]:

technical knowledge
fun
embezzlement
manipulative and risk-taking nature an ***active imagination***
Revenge

serial rapists and serial killers
profit
a psychiatric illness
contempt for the law and order
sexual satisfaction

[2] The text for the sample presentation is adapted from "Cybercrime: Piercing the darkness" http://library.thinkquest.org/04oct/00460/prologue.html, retrieved on 20.02.2012

Dear law enforcement students, my name is Dr. Annabel Stewart, and I'm psychologist with the Computer Crime and Intellectual Property Section of the United States Department of Justice. I'm an expert in psychological profiling of criminals, and for 7 years now I've been specializing in creating psychological profiles of cybercriminals.

Let me take few second first to thank the Computer Crime Department of your Academy for inviting me to give this lecture; in particular, I would like to thank Prof. Hubert for providing me an insight into your curriculum, so that I can make sure I cover all the necessary points here.

So, who are cybercriminals? What are their general characteristics? What are their motives? What types of cybercriminals do we know?

Remember, cybercriminals are criminals, and they do share certain generic traits with other criminals of any sort.

First and foremost, they feel **.....** (Key 1: ***contempt for the law and order***) Why so? Either because they believe something wrong has been done to them and they are victims of the legal system; or, because they believe particular laws are unnecessary or unfair or illogical; or, because they simply believe they are above the law and can outsmart the system.

Second*,** they are of the **.....**(Key 2: ***manipulative and risk-taking nature). This is what makes the fine line between criminals and non-criminals. We have all been through this awful pain when something wrong has been done to us, and we have wished to simply retaliate. But we were prevented from revenging because we were afraid of the legal consequences. Well, criminals are willing to take this risk and manipulate the people, the circumstances and the resources in all possible ways, just to see their plan through.

Third*,** criminals have..... (Key 3: ***an active imagination). It takes brains to design the perfect plot, commit the crime and get away with it; but it really takes a vivid imagination to develop a kind of double personality, pretending to be an ordinary, even boring next-door guy during the day, and a cunning criminal during the night.

Last*,** but not least, the criminal needs to have a substantial amount of **.....** **.....** (Key 4: ***technical knowledge) in a given area. If you rob a bank in the old-fashioned way, you need to know everything about guns – to scare the people and force them into surrendering their money, and cars – to be able to escape as soon as possible. But if you steal money from someone's bank account, then you need to know every single detail about how electronic monetary transactions work.

Why do people commit cybercrime?

Believe it or not, many do this just for the **.....** ***(***Key 5: ***fun*** **)**of it! This is very typical of teenagers who simply want to earn additional respect by their peers. When I was young, boys would prove their bravery by crashing the school windows; nowadays, they prefer crashing the school computers.

Besides entertainment, **.....** ***(***Key 6: ***profit*** **)**is the major reason why cybercriminals hack into computers. This includes the people who break into computer systems for personal material gain or access to free services, but also people who are hired and paid by large corporations to perform ..... (embezzlement), or corporate espionage, and the like.

..... ***(***Key 7:***Revenge*** **)**is an epic reason to commit a crime, and this you find a lot among cybercriminals, too! Here you find dumped lovers, cheated on spouses, fired workers, or even businessmen who are convinced they've been ripped off by other corporations, by the banks or even by the national financial system.

The motive for cybercrime that receives the widest and greatest social condemnation is ..... *(Key 8:* ***sexual satisfaction).*** When one mentions the Internet and sex in the same sentence, you immediately think of paedophiles. Some paedophiles are passive, they just want to indulge in the pornographic stories, photos and videos, which – in spite of all the globally organized efforts – are still largely available on the Internet. The more dangerous group of paedophiles are the active ones – they use the various chat rooms to befriend children, and either choose to rape them at the first meeting, or seduce them into maintaining a fairly long sexual relationship. However, besides paedophiles, ... ***(***Key 9: ***serial rapists and serial killers)*** are also known to use computers and the Internet to intricately approach and abuse their victims, or to cover up their criminal actions afterwards.

The rarest but potentially most harmful cybercriminals are those suffering from ..... (Key 10 : ***a psychiatric illness)*****:** schizophrenia, depression, mania, personality disorders etc. What makes them particularly dangerous is that they are partially to completely detached from the society, and, as such, they are prepared to do just about anything! Besides, their motivations are illogical to the normal mind; their next course of action is highly unpredictable; and this makes it especially hard for law enforcers to track them down.

Activity 5- Cyber crime in the newspapers (project assignment)

We have learned from our experience that one of the most efficient ways for finishing a lesson is to engage students in an activity which sublimes most of the new contents they were exposed to. In this particular case, we propose a project which can either be given as a homework assignment or carried out in a classroom where internet access is provided. Students are divided into several groups. Using all the acquired knowledge from the lesson, they are given the task to browse the Internet and find information related to the issue of cyber crime in their country. More specifically, each group chooses a different daily newspaper and searches for articles dealing with cases of cyber crime. After they finish, a representative from each group presents orally the results of their search and the presentations are followed by a group discussion about the most common types of cyber crime they came across, the methods which were used for their commission, the characteristics of the target victims, the motivation of the perpetrators etc.

CONCLUSION

The aim of this paper was to offer a model for successful integration of cyber crime as a topic in English language instruction for students of English for law enforcement. With the sample lesson presented in the previous sections we could see how web-based content can successfully be modified and adapted so as to suit students' level of knowledge of English. The sample lesson plan is a good example of how students' interest can be raised and how motivation can be enhanced by their constant engagement in interactive activities which require pair, group and whole-class work, on the basis of the key tenets of content-based communicative language teaching. By participating in tasks of various types, students will have the

opportunity to get acquainted with the key features and specifities of cyber crime, its perpetrators and various forms of occurrence, while simultaneously acquiring English linguistic knowledge. Only in this manner shall we educate students- future professionals in the area of law enforcement, who will possess adequate skills for efficiently performing their professional duties and tasks.

BIBLIOGRAPHY

1. Dudley-Evans, Tony and Maggie-Jo St. John. 1998. "Developments in ESP: a multi-disciplinary approach". Cambridge: Cambridge University Press
2. Hutchinson, Tom and Alan Waters. 1987. "English for Specific Purposes: a learning- centered approach". Cambridge: Cambridge University Press
3. Richards, Jack C. and Theodore S. Rodgers. 2001. Approaches and Methods in Language Teaching. Cambridge: Cambridge University Press
4. "Cybercrime: Piercing the darkness" http://library.thinkquest.org/04oct/00460/prologue.html
5. "Cybercrimes: Types of cybercrime" http://cybercrimes09.blogspot.com/2009/10/types-of-cybercrime.html

Prethodno saopštenje – UDK 341.48: [343.326: 004.738.5

MJESTO I ULOGA PRIKRIVENOG ISTRAŽITELJA U SPREČAVANJU I SUZBIJANJU KRIVIČNIH DJELA IZ OBLASTI VISOKOTEHNOLOŠKOG KRIMINALITETA

Svjetlana Dragović
Dragana Milijević
Dražen Višnjić

Apstrakt: Kompjuter kao savremeno sredstvo komunikacije može biti predmet zloupotreba koje se odnose na ugrožavanje integriteta, dostupnost ili povjerljivost računarskih mreža i telekomunikacionih sistema, a može poslužiti i kao sredstvo za vršenje tradicionalnih krivičnih djela. Visokotehnološki kriminalitet je specifičan u odnosu na druge vrste kriminaliteta i, kao takav, zahtijeva primjenu specifičnih mjera, između ostalog, i primjenu posebnih istražnih radnji. Jedna od posebnih istražnih radnji koja se vrlo često primjenjuje u suprotstavljanju visokotehnološkom kriminalitetu, jeste prikriveni istražitelj. U radu će se govoriti o mjestu i ulozi prikirivenog istražitelja u suprotstavljanju ovoj vrsti kriminaliteta.

Ključne riječi: visokotehnološki kriminalitet, prikriveni istražitelj, *online*prikriveni istražitelj.

O VISOKOTEHNOLOŠKOM KRIMINALITETU (*CYBER CRIME)*

Kompjuter predstavlja jednu od najznačajnijih tekovina ljudske civilizacije i njegova upotreba, odnosno doprinos razvoju čovječanstva je nesporan. No, korištenje računara ima i drugu stranu. Tačnije, računari se sve više upotrebljavaju u svrhu činjenja krivičnih djela. Tako se razvio jedan, uveliko specifičan, savremeni oblik kriminaliteta – visokotehnološki kriminalitet *(Cyber Crime)*. Visokotehnološki kriminalitet, uopšte, predstavlja takav oblik kriminaliteta koji je danas gotovo nemoguće precizno pojmovno odrediti. Štaviše, treba istaći da visokotehnološki kriminalitet predstavlja svojevrstan vid forme kroz koji se ispoljavaju različiti oblici kriminalne djelatnosti.[1] Ove djelatnosti se mogu ispoljavati u vidu klasičnog visokotehnološkog kriminaliteta kod koga je računar ili računarski sistem sredstvo izvršenja krivičnog djela *(Computer Related Crime)* ili objekat napada krivičnog djela *(Computer Crime)*, u vidu internet kriminaliteta kod koga je zloupotreba mreže određujući faktor (posjedovanje i distribucija dječije pornografije, raspirivanje nacionalne i rasne mržnje, neovlašćena distribucija autorskih djela i predmeta

[1] Detaljnije dostupno na www.techterms.com, pristupljeno 17.02.2012. godine; U literaturi se izdvajaju pokušaji definisanja kompjuterskog kriminaliteta. Prema definiciji jedne ekspertne grupe *OECD-a* iz 1983. godine kompjuterski kriminalitet predstavljaju *„sva protivpravna, nemoralna i nedopuštena ponašanja u vezi sa automatskom obradom podataka i/ili njihovim prenosom“,* o ovome više Krapac, D.; Kompjuterski kriminalitet; Pravni fakultet; Zagreb; 1992. god.; str. 226; navedeno prema *Pavlović, Š., „Kompjuterska kaznena djela iz Kaznenog zakonika“,* u Hrvatski ljetopis za kazneno pravo i praksu (Zagreb), vol. 10, broj 2/2003, str. 627;

intelektualne svojine), a može se pojaviti i u vidu e-kriminaliteta koji se vezuje za zloupotrebu komunikacionih uređaja za skladištenje elektronskih podataka.[2]

Visokotehnološki kriminalitet ujedno predstavlja važan segment organizovanog kriminaliteta, gdje nastaju nove kriminalne kategorije, i razvijaju se „atipične" generacije kriminalaca. Tako je jedna od karakteristika virtuelnog svijeta da osobe koje vrše različita krivična djela mogu brzo, jednostavno i anonimno da komuniciraju. Komunikacija između izvršilaca ovih krivičnih djela je transnacionalna, za razliku od krivičnog pravosuđa koje funkcioniše u okviru državnih granica, što predstavlja problem u suzbijanju kompjuterskog kriminaliteta.[3] Što se tiče fenomenologije visokotehnološkog kriminaliteta, nju je najbolje oslikao *Pavlović,* koji ističe da se *„elektronske komunikacije koriste za širenje i korištenje pornografije, stvara se novi oblik piratstva (Software Piracy), moderni pirati plagiraju kompjuterske programe, nedopušteno prisvajaju tuđa autorska prava (Copyrights) i na njima ostvaruju ogromnu zaradu; u kompjuterske programe i sustave ubacuju se virusi; vrše se prevare; dekodiraju se tajne i zaštićene elektroničke poruke; neovlašćeno se pristupa u elektroničke sustave (Computer Hacking); organiziraju se zabranjene lančane igre i kockanje (Gambling)."*[4]

Svi navedeni oblici ispoljavanja visokotehnološkog kriminaliteta vrše se u posebnom ambijentu koji karakterišu mnoštvo provjerenih podataka na malom prostoru koji su dostupni i ovlaštenim i neovlaštenim korisnicima, proširen prostor kriminalnog djelovanja koji ne zahtijeva prisustvo izvršioca krivičnog djela na licu mjesta, skraćeno vrijeme kriminalnog djelovanja (nekoliko sekundi), smanjena mogućnost nadzora i upravljanja ovim podacima, suptilne metode i tehnike izvršenja ovih krivičnih djela, korištenje istog modusa vršenja krivičnog djela sa niskim rizikom otkrivanja, sve jednostavnije mogućnosti korištenja kompjutera od strane sve većeg broja lica i sl.[5] *Cyber Crime* u formi kako je prikazan prouzrokuje štetu kako pojedincima, tako i široj društvenoj zajednici. U najkraćem, posljedice se pojavljuju kao imovinska šteta, gubljenje povjerenja, gubljenje sigurnosti u tačnost dobijenih informacija, narušava se poslovni ugled i sl.

Ekspanzija krivičnih djela iz oblasti visokotehnološkog kriminaliteta, sa ovako predočenim karakteristikama, nužno je nametnula potrebu njegovog tematiziranja na međunarodnom planu,[6] gdje je od značaja izdvojiti Konvenciju Savjeta Evrope o kibernetičkom kriminalitetu[7] iz 2001. godine, kao i Međunarodni kolokvij o kibernetičkom kriminalitetu koji je održan u organizaciji Međunarodnog udruženja za krivično pravo u Atini 2003. godine.[8]

---

[2] Vidjeti: *Jerković, R., Borba protiv visokotehnološkog kriminala u Srbiji,* dostupno na www.telekomunikacjers.com, pristupljeno 16.02.2012. godine;

[3] Derenčinović, D., „Prikaz kolokvija AIDP-a o kibernetičkom kriminalu (*Colloquy on Cyber-Crime*)", u Hrvatski ljetopis za kazneno pravo i praksu (Zagreb), vol. 10, broj 1/2003, str. 223;

[4] *Pavlović, Š.,* op.cit., str. 628;

[5] O ovome detaljnije Petrović, S., navedeno prema Matijašević, J.; Ignjatijević, S., „Kompjuterski kriminalitet u pravnoj teoriji, pojam, karakteristike, posledice", u Infoteh-Jahorina, vol 9, god. 2010, str 853;

[6] Riječ je o dokumentima Ujedninjenih nacija, Savjeta Evrope, odnosno Evropske unije.

[7] Konvencija Savjeta Evrope o kibernetičkom kriminalu, usvojena 23. 11. 2001. godine; dostupno na www.poslovniforumhr.info, pristupljeno 16.02.2012. godine;

[8] *Derenčinović, D.,* op. cit., str. 225;

Iako je problemu *Cyber Crime* i ranije posvećivana pažnja, ipak su pomenuta Konvencija, a posebno Međunarodni kolokvij, eksplicitno ukazali na opasnost i štetnost ove vrste kriminaliteta.

S obzirom na navedeno, društvo, u okviru kaznene politike, treba da pronađe adekvatne mehanizme za zaštitu od ovoga oblika kriminaliteta. Aktivnosti društva se kreću u dva pravca. Kao prvo, neophodno je postaviti racionalan zakonski okvir u materijalnom krivičnom zakonodavstvu (inkriminisati određena ponašanja kao krivična djela), i drugo, neophodno je, prevashodno u krivičnoprocesno zakonodavstvo inkorporirati procesne radnje koje će djelotvorno uticati na *Cyber Crime.*

Naš zakonodavac je, svjestan dubokih promjena nastalih digitalizacijom, konvergencijom i neprekidnom globalizacijom računarskih mreža, a uvažavajući Konvenciju Savjeta Evrope o kibernetičkom kriminalu[9] proširio zonu kažnjivosti u pogledu visokotehnološkog kriminaliteta, na način da je dodatno okvalifikovao određena ponašanja kao krivična djela. Tako je, Zakonom o izmjenama i dopunama Krivičnog zakona Republike Srpske,[10] *Cyber Crime* uveliko tematiziran: u pomenutim izmjenama i dopunama Krivičnog zakona nalazi se potpuno nova glava krivičnih djela (glava 24a) pod nazivom *Krivična djela protiv bezbjednosti računarskih podataka.* U okviru ove glave nalaze se sljedeća krivična djela: *Oštećenje računarskih podataka i programa (član 292a), Računarska sabotaža (član 292b), Izrada i unošenje računarskih virusa (292v), Računarska prevara (292g), Neovlašćeni pristup zaštićenom računaru, računarskoj mreži, telekomunikacionij mreži i elektronskoj obradi podataka (član 292d), Sprečavanje i ograničavanje pristupa javnoj računarskoj mreži (član 292đ),* kao i *Neovlašćeno korišćenje računara ili računarske mreže (član 292e).*

Krivična djela protiv bezbjednosti računarskih podataka, barem prema predviđenim kaznama, spadaju u oblast srednje teškog kriminaliteta. Tako je naš zakonodavac samo u pogledu težih oblika ovih inkriminacija predvidio kaznu zatvora od tri godine (*Oštećenje računarskih podataka i programa* iz člana 292a stav 3, odnosno *Računarska prevara* iz člana 292g stav 2 i stav 3). Treba istaći da u ovome slučaju računar predstavlja „samo“ objekt napada. Međutim, konstatovano je da se pored ovakve uloge, računar može pojaviti kao sredstvo izvršenja gotovo svih krivičnih djela, u pogledu kojih se na drugi način ne mogu pribaviti dokazi ili bi njihovo pribavljanje bilo povezano sa nesrazmjernim teškoćama (*npr. Proizvodnja i prikazivanje dječije pornografije* iz člana 200. Krivičnog zakona Republike Srpske). Navedeno predstavlja dva osnova za korištenje posebnih istražnih radnji, između ostalog i posebne istražne radnje prikriveni istražitelj.

---

9 U Konvenciji Savjeta Evrope o kibernetičkom kriminalu predviđene su četiri grupe krivičnih djela: a) Krivična djela protiv tajnosti, cjelovitosti i dostupnosti računarskih podataka i sistema, b) Računarska krivična djela, c) Krivična djela u vezi sa sadržajem, d) Krivična djela povrede autorskih i srodnih prava. Pored navedenog, u članu 11 je inkriminisan Pokušaj, pomaganje ili podstrekavanje na izvršenje ovih krivičnih djela. Detaljnije o Konvenciji Savjeta Evrope o kibernetičkom kriminalitetu pogledati Herzog, F.: „Straftaten im Internet, Computerkriminalität und die Cybercrime Convention“ in Política Criminal, vol 8, year 2009, pg. 1–11;

10 Zakon o izmjenama i dopunama Krivičnog zakona Republike Srpske („Službeni glasnik RS“ broj 73/10);

PRIKRIVENI ISTRAŽITELJ

Upotreba prikrivenog istražitelja, prema Zakonu o krivičnom postupku Republike Srpske, predstavlja najsloženiju posebnu istražnu radnju.[11] Primjena ove istražne radnje zahtijeva, prije svega, ispunjenje uslova koji su predviđeni za primjenu posebnih istražnih radnji.[12] Međutim, pored uslova koji važe za sve posebne istražne radnje, primjena prikrivenog istražitelja zahtijeva ispunjenje i drugih uslova, nužnih za ostvarenje svrhe njenog određivanja (osiguranje dokaza, predmeta i tragova koji upućuju na izvršenje krivičnog djela određenih lica, odnosno pripadnika kriminalne grupe i ispunjenje isto toliko važnih uslova koji garantuju tajnost). Takođe, primjena ove radnje zahtijeva „*zaštitu tjelesnog integriteta lica koje se pojavljuje u ulozi prikrivenog istražitelja*“.[13] Pored toga, pri izvršenju posebne istražne radnje prikrivenog istražitelja (isto važi i za informatora i radnje simulovanog i kontrolisanog otkupa predmeta i simulovanog davanja potkupnine), zahtijeva se ispunjenje i posebnog uslova, a to je da lice koje ima ulogu prikrivenog istražitelja ne smije preduzimati aktivnosti koje predstavljaju podstrekavanje na izvršenje krivičnog djela. Upotreba tzv. agenata provokatora (*agent provocateur)* nije dozvoljena.

Prikriveni istražitelj je posebno obučeno ovlašćeno službeno lice koje istražuje i nastupa pod izmijenjenim identitetom (tzv. *legendom)*. S obzirom na to

---

[11] ZKP RS predviđa sedam posebnih istražnih radnji: 1.nadzor i tehničko snimanje telekomunikacija, 2. pristup kompjuterskim sistemima i kompjutersko sravnjenje podataka 3. nadzor i tehničko snimanje prostorija, 4. tajno praćenje i tehničko snimanje lica, transportnih sredstava i predmeta koji stoje u vezi sa njima, 5. korišćenje prikrivenih istražitelja i korišćenje informatora**,** 6. simulovani i kontrolisani otkup predmeta i simulovano davanje potkupnine i 7. nadzirani prevoz i isporuka predmeta krivičnog djela. Šire o posebnim istražnim radnjama pogledati takođe *Sijerčić-Čolić, H., „Prikrivene istražne radnje u borbi protiv organizovanog kriminaliteta – primjer BiH“* u Zbornik pravnog fakulteta u Splitu, vol 4, god. 2009, str. 687–700;

[12] Prvo, važno je reći da se posebne istražne radnje određuju u slučajevima krivičnih djela protiv RS, krivičnih djela protiv čovječnosti i međunarodnog prava, krivičnih djela terorizma i krivičnih djela za koja se prema KZ RS može izreći kazna zatvora od tri godine ili teža kazna. *Materijalni uslov* za njihovu primjenu jeste nemogućnost pribavljanja dokaza na drugi način ili nesrazmjerne teškoće pri njihovom pribavljanju. *Formalni uslov* jeste naredba suda, kojoj prethodi inicijativa nadležnog organa. Nakon što to ocijeni potrebnim, tužilac daje obrazloženi prijedlog sudiji za prethodni postupak radi primjene neke od posebnih istražnih radnji, a koji „u slučaju prihvatanja prijedloga, donosi naredbu o primjeni posebne istražne radnje nad tačno određenim licima za koja postoje osnovi sumnje da su učinioci ili učesnici prethodno navedenih krivičnih djela. *Procesnopravni razlozi* za preduzimanje posebnih istražnih radnji jesu: da postoje “osnovi sumnje“ protiv lica da je samo ili s drugim licima učestvovalo u krivičnom djelu; ako nadležni sudski organ (sudija za prethodni postupak) obrazloženom pisanom naredbom (izuzetno usmenom) odredi njihovu primjenu; trajanje primjene posebnih radnji ograničeno je na šest, odnosno tri mjeseca, s tim što njihovu svrsishodnost nadzire sudija za prethodni postupak, tako da će se u slučajevima da se postigne svrha, odnosno slučajevima uočavanja da ne postižu očekivanu svrhu ili se uopšte njihovom primjenom ne dobijaju podaci zbog kojih su određeni - prekinuti njihova primjena. Izuzetno, ako postoje dva kumulativno određena uslova: ako se pisana naredba ne može dobiti na vrijeme i ako postoji opasnost od odlaganja, može se započeti sa primjenom posebnih istražnih radnji i na osnovu usmene naredbe sudije za prethodni postupak. U ovom slučaju pisana naredba sudije za prethodni postupak mora biti pribavljena u roku od 24 sata od izdavanja usmene naredbe.

[13] Simović, N. M.: Krivično procesno pravo – treće izmijenjeno i dopunjeno izdanje; Fakultet za bezbjednost i zaštitu; Banja Luka; 2009; str. 266.

da pod svojim izmijenjenim identitetom može učestvovati u pravnom prometu, ukoliko je za formiranje i održavanje tog identiteta to neophodno, mogu mu se izraditi ili izmijeniti odgovarajuća dokumenta, koja prikriveni istražitelj ima pravo da koristi (član 234. stav 6).

Prikriveni istražitelj pripada grupi posebnih istražnih radnji koje se zovu *mjere prodora u kriminalne grupe*[14] i funkcioniše na principu „ubacivanja" u kriminalnu grupu ili nekog drugog oblika povezivanja sa članovima grupe, kako bi, na krajnje diskretan način, prikupio što više podataka o određenoj kriminalnoj grupi ili kriminalnim grupama, odnosno uopšte o organizovanom kriminalitetu. Uspjeh rada prikrivenog istražitelja zavisi od niza faktora. Od posebnog je značaja njegova priprema i način infiltriranja u kriminalnu organizaciju. Ništa manje nije važan metod rada u kriminalnoj organizaciji.

Nakon što stekne povjerenje članova kriminalne organizacije i, na neki način, postane dio te organizacije, on će biti u prilici da prikuplja informacije o konkretnim oblicima i načinima izvršenja krivičnih djela. Saznanja do kojih dolazi mora na konspirativan i, uglavnom ranije dogovoren način, blagovremeno dostavljati svojim pretpostavljenim, kako bi se mogao organizovati efikasan procesno-kriminalistički rad lišenja slobode članova kriminalne organizacije, te istraživanja i dokazivanja njihove kriminalne djelatnosti.

U našem procesnom zakonodavstvu nije određeno vrijeme trajanja ove posebne istražne radnje. S obzirom na to da nijedna druga istražna radnja ne može trajati duže od šest mjeseci, logičkim tumačenjem se može zaključiti da bi i ova radnja mogla trajati najduže do šest mjeseci.

Po završetku primjene ove posebne istražne radnje, prikriveni istražitelj može da se pojavi u postupku kao svjedok, i njegov iskaz ima snagu dokaza. Zbog njegove lične bezbjednosti, a i zaštite operativnih aktivnosti, pravila kriminalistike nalažu da prikrivenog istražitelja ne bi trebalo izlagati davanju javnog svjedočkog iskaza.[15]

Sve navedeno predstavlja prikrivenog istražitelja uopšte, odnosno predstavlja prikrivenog istražitelja kao posebnu istražnu radnju, onako kako je predviđena Zakonom o krivičnom postupku Republike Srpske. Međutim, prikriveni istražitelj je novina u našem procesnom zakodavstvu i za sobom povlači niz pitanja. Ono što je centralna problematika ovog rada, jeste angažovanje prikrivenog istražitelja u sprečavanju i suzbijanju krivičnih djela iz oblasti visokotehnološkog kriminaliteta, tzv. *online* prikrivenog istražitelja.

ONLINE PRIKRIVENI ISTRAŽITELJ

U zapadnoj literaturi, prikriveni istražitelj se naziva OCE (*online undercover employee*) – online prikriveni istražitelj. Upotreba online prikrivenog istražitelja nije isključivo vezana za borbu protiv visokotehnološkog kriminaliteta

[14] U ovu grupu se ubrajaju još i angažovanje informatora i simulovani i kontrolisani otkup predmeta i simulovano davanje potkupnine.

[15] O saslušanju prikrivenog istražitelja detaljnije u: Simović, N. M.: Krivično procesno pravo – uvod i opšti dio; Pravni fakultet univerziteta u Bihaću; Bihać; 2005; str. 371–372.

(definisanog kod nas u vidu odredbi Krivičnog zakona Republike Srpske: Krivična djela protiv bezbjednosti računarskih podataka), već i za krivična djela gdje se *cyber* tehnologije koriste kao sredstvo komunikacije i razmjene informacija i podataka. (krivična djela dječije pornografije, terorizam – regrutovanje, *cyber* terorizam,..).

Na ovom mjestu, mi ćemo se fokusirati na ulogu *online* prikrivenog istražitelja u borbi protiv najtežih oblika visokotehnološkog kriminaliteta. Sa tog aspekta, neophodno je napraviti razliku između pojmova „sajber patrola" i *online* prikriveni istražitelj. "Sajber patroliranje" predstavlja operativni rad u *cyber* prostoru i treba ga razlikovati od tradicionalnog operativnog rada koji se takođe sprovodi u borbi protiv visokotehnološkog kriminaliteta. Realizuje se kroz prisustvo i aktivnostima na specifičnim internet forumima i grupama zatvorenog tipa, u cilju detektovanja novih *cyber* prijetnji, detektovanja i identifikovanja potencijalnih izvršilaca krivičnih djela iz oblasti visokotehnološkog kriminaliteta koji se nalaze u našoj zemlji, imaju veze sa licima u našoj zemlji ili im je mjesto izvršenja krivičnih djela u našoj zemlji. Ova vrsta operativnog rada, u konjunkciji sa međunarodnom razmjenom informacija i učešćem u međunarodnim *cyber* operacijama, predstavlja glavnu polugu za borbu protiv visokotehnološkog kriminaliteta u smislu prevencije, kao i detektovanja i identifikovanja najvećih *cyber* prijetnji.[16]

Angažovanje *online*prikrivenog istražitelja proizilazi iz informacija do kojih se dođe radom „sajber patroliranja", kada je neophodno konkretizovati aktivnosti za određeno lice ili grupu lica. Problemi u radu na „sajber patroliranju" i u radu *online* prikrivenog istražitelja jesu: teškoće pristupa internet lokacijama, teškoće uspostavljanja komunikacije, stručnost kadra koji ga provodi. Teškoće leže i u prirodi lica povezanih sa ovom vrstom kriminala: zavidan nivo poznavanja *social engineering-a* (metoda prikupljanja informacija, metoda obmane), visok nivo poznavanja tehničke i personalne zaštite, zaštite informacija, brze provjere informacija, kao i velika zatvorenost i sumnjičavost prema sagovorniku.

Što se tiče zaštite identiteta *online* prikrivenog istražitelja, pred istražne strukture se stavlja čitav niz specifičnosti postupanja: postupanje vezano za prikrivanje identiteta (lažni identitet stvarne IP adrese, lažni pretplatnički broj mobilnog telefona, bankarskog računa, lažne identifikacione isprave), postupanje vezano za vlastite mogućnosti (mogućnost kupovine preko interneta, mogućnost pokretanja firmi), postupanje vezano za stručnost (velika tehnička stručnost, poznavanja *social engineering-a*...).

Informacije do kojih dođe *online* prikriveni istražitelj imaju samo operativan karakter. Iako, u nekim slučajevima, podaci dobijeni radom „sajber patroliranja" u digitalnoj formi imaju neporecivu dokaznu prirodu, u praksi se najčešće koriste kao operativni podaci, ali ne kao dokazi. Čak i u međunarodnoj razmjeni informacija, oni se vrednuju kao operativni podaci, i ne mogu se koristiti kao dokaz. Podaci dobijeni radom *online* prikrivenog istražitelja se ne koriste kao dokazi i ovdje leži

[16] Međunarodna saradnja u pogledu *online* prikrivenog istražitelja ima određene spečifičnosti. Ova saradnja se odvija kroz 4 aspekta: razmjena informacija, učešće u međunarodnim *cyber* operacijama kroz praćenje aktivnosti određenih lica, učešće u međunarodnim *cyber* operacijama zajedničkog djelovanja i učešće *online* prikrivenog istražitelja u međunarodnim *cyber* operacijama. Učestvovanje *online* prikrivenog istražitelja u međunarodnim operacijama je vid asistencije inostranim policijskim partnerima.

jedan od osnovnih razloga neophodnosti uvođenja *online* prikrivenog istražitelja kao posebne istražne radnje.

Kao što smo već istakli, Zakon o krivičnom postupku Republike Srpske predviđa prikrivenog istražitelja kao posebnu istražnu radnju, ali ne u smislu *online* prikrivenog istražitelja o kome je sada bilo riječi. Pojmovno, operativni rad u *cyber* prostoru kod nas se svodi pod tradicionalni operativni rad. S obzirom na to, neophodno je izvršiti reorganizaciju uloge i napraviti jasnu diferencijaciju *cyber* operativnog rada od *online* prikrivenog istražitelja. Operativni rad je po svojoj prirodi širi i nije kao posebne istražne radnje predmetno orijentisan. Neophodnost da se, u nekom momentu, po pribavljanju dovoljnog broja informacija, krene u realizaciju predmeta, nameće neophodnost adekvatne predmetno orijentisane mjere – posebne istražne radnje. Neophodno je *online* prikrivenog istražitelja predvidjeti kao posebnu istražnu radnju, samostalno ili kao varijantu postojećeg prikrivenog istražitelja, koji bi funkcionisao pod sličnim uslovima kao i prikriveni istražitelj. Anomija prema ovom fenomenu stvara problem u realizaciji predmeta i efektnosti borbe protiv visokotehnološkog kriminaliteta.

REZIME

Visokotehnološki kriminalitet predstavlja specifičan vid kriminaliteta kroz koji se ispoljavaju različiti oblici kriminalne djelatnosti. S obzirom na to da tradicionalne metode suprotstavljanja visokotehnološkom kriminalitetu nisu dovoljno efikasne, posebno mjesto i ulogu u sprečavanju i suzbijanju ovih krivičnih djela ima *online* prikriveni istražitelj. *Online* prikriveni istražitelj nije predviđen odredbama Zakona o krivičnom postupku Republike Srpske i, kao što smo već istakli, informacije do kojih dođe ne predstavljaju dokaz u krivičnom postupku. Drugim riječima, *online* prikriveni istražitelj ima status stručnog lica, koje nema karakter dokaznog sredstva, te njegov iskaz predstavlja samo savjet, odnosno mišljenje. Navedeno podrazumijeva da *online* prikriveni istražitelj nije vještak i on ne utvrđuje činjenice. Mišljenje *online* prikrivenog istražitelja ima samo savjetodavan karakter i organu krivičnog postupka i krivičnoprocesnim strankama objašnjava određena tehnička i stručna pitanja. S obzirom na činjenicu da je upotreba *online* prikrivenog istražitelja u suprotstavljanju visokotehnološkom kriminalitetu nužna, a uvažavajući značaj informacija koje se dobijaju upotrebom *online* prikrivenog istražitelja, nepohodno je „ozakoniti" njegovu djelatnost, odnosno predvidjeti ga kao posebnu istražnu radnju. Samo bi na ovaj način, informacije do kojih dođe *online* prikriveni istražitelj, imale najveću upotrebnu vrijednost, tj. predstavljaju dokaz.

LITERATURA

1. Derenčinović, D.: „*Prikaz kolokvija AIDP-a o kibernetičkom kriminalu (Colloquy on Cyber-Crime)",* u Hrvatski ljetopis za kazneno pravo i praksu (Zagreb), vol. 10, broj 1/2003, str. 223–227;
2. Herzog, F.: „Straftaten im Internet, Computerkriminalität und die Cybercrime Convention" in Política Criminal, vol 8, year 2009, pg. 1–11;

3. Matijašević, J.;Ignjatijević, S.: *„Kompjuterski kriminalitet u pravnoj teoriji, pojam, karakteristike, posledice“,* u Infoteh-Jahorina, vol 9, god. 2010, str 852–856;
4. Pavlović, Š.: *„Kompjuterska kaznena djela iz Kaznenog zakonika“,* u Hrvatski ljetopis za kazneno pravo i praksu (Zagreb), vol. 10, broj 2/2003, str. 625–664;
5. Sijerčić-Čolić, H.: „*Prikrivene istražne radnje u borbi protiv organizovanog kriminaliteta – primjer BiH“* u Zbornik pravnog fakulteta u Splitu, vol 4, god. 2009, str 687–700;
6. Simović, N. M.: Krivično procesno pravo – treće izmijenjeno i dopunjeno izdanje; Fakultet za bezbjednost i zaštitu; Banja Luka; 2009; str. 266.
7. Simović, N. M.: Krivično procesno pravo – uvod i opšti dio; Pravni fakultet univerziteta u Bihaću; Bihać; 2005; str. 371–372.
8. Konvencija Savjeta Evrope o kibernetičkom kriminalu, usvojena 23. 11. 2001.
9. Zakon o izmenama i dopunama Krivičnog zakona Republike Srpske („Službeni glasnik RS“ broj 73/10);

THE PLACE AND ROLE OF THE UNDERCOVER INVESTIGATOR IN PREVENTING AND COMBATING CRIMINAL OFFENSES RELATED TO CYBERCRIME / COMPUTER CRIME

Svjetlana Dragovic
Dragana Milijevic
Drazen Visnjic

Abstract: The computer, as a modern medium of communication can be an object of abuse, in terms of threat to the integrity, accessibillity or confidentiality of computer networks and telecommunication systems, but it can also be used for commiting the traditional criminal offenses. Comparing to other sorts of criminality, cybercrime is special, and as such, requires implementation of specific measures, among others, the implementation of specific investigative activities. One of the specific investigative activities, that is often used in fighting against cybercrime, is the undercover investigator. This paper will discuss the place and role of undercover investigator in combating this type of crime.

Key words: cybercrime, undercover investigator, onlineundercover investigator

Stručni rad - UDK 004.738.5: 316.624

KRIMINOGENI ASPEKT DRUŠTVENIH MREŽA

Aleksandar Miladinović
MUP RS – Policijska akademija Banja Luka
E-mail: aaleksandarbl@yahoo.com
Vitomir Petričević
MUP RS – Visoka škola unutrašnjih poslova Banja Luka
E-mail: vitomir.petricevic@education.muprs.org

Apstrakt: Kvalitativna i kvantitativna ekspanzija društvenih mreža rezultira i ekspanzijom kriminalnih aktivnosti na društvenim mrežama ili prema korisnicima društvenih mreža. Uzrok navedenom je svakako masovnost korisnika društvenih mreža, (bezbjednosno)informatička nepismenost korisnika, vlastita pasivizacija zaštite, virtuelni aspekt društvenih mreža, mogućnost anonimnog ili pseudonimnog djelovanja... Okruženje društvenih mreža omogućava da se gotovo cjelokupne faze određenih kriminalnih aktivnosti (planiranje, pripremanje, vrbovanje žrtvi, obezbjeđenje sredstava, sama realizacija, pribavljanje koristi) realizuju ‘’iz sobe’’, odnosno korišćenjem usluga interneta preko društvenih mreža, što je uslovilo ekspanziju, kako klasičnih kriminalnih aktivnosti (prevara, krađa, razni oblici nasilja, antiestablišmentsko djelovanje, terorizam), tako i savremenih oblika kriminalnih aktivnosti (krađe identiteta, krađe vremena, internet piraterije, raznih oblika internet nasilja). U tom kontekstu, u radu se kao najučestaliji oblici kriminalnih aktivnosti na društvenim mrežama (primarno na Fejsbuku, Tviteru, Jutjubu...) posmatraju prevare, krađe identiteta, piraterija, pornografija, pedofilija, terorizam, vršnjačko nasilje, govor mržnje i razni oblici antiestablišmentskog djelovanja korišćenjem društvenih mreža.

Ključne riječi: društvene mreže, kriminalitet, krađa identiteta, internet prevare, pedofilija...

UVODNA RAZMATRANJA

Društvene mreže su zadnjih nekoliko godina jedna od najpopularnijih usluga na internetu, sa kvalitativnom i kvantitativnom ekspanzijom. Međutim, navedeno svakako ima i svoju ‘’tamnu stranu’’. Uporedo sa ekspanzijom društvenih mreža, primijetna je i ekspanzija kriminalnih aktivnosti na društvenim mrežama ili prema korisnicima društvenih mreža.

Navedenom je razlog, prije svega, masovnost korisnika društvenih mreža, ali isto tako i needukovanost korisnika o bezbjednosnim rizicima na društvenim mrežama, vlastita pasivizacija mogućnosti zaštite, virtuelni aspekt okruženja u kojem egzistiraju ove mreže...

Usljed navedenog, razni se oblici kriminaliteta i drugih kriminogenih i asocijalnih pojava, kao i sami akteri navedenih aktivnosti, ‘’preseljavaju’’ u okruženje društvenih mreža, s obzirom na to da im navedeno okruženje omogućava

da gotovo cjelokupne faze kriminalne aktivnosti (planiranje, pripremanje, vrbovanje žrtvi, obezbjeđenje sredstava, sama realizacija, pribavljanje koristi) realizuju ‘’iz sobe’’, odnosno korišćenjem usluga interneta preko društvenih mreža, znajući da je mogućnost otkrivanja njihovog identiteta minimalna. To je uslovilo ekspanziju klasičnih kriminalnih aktivnosti (prevare, krađe, razni oblici nasilja, antiestablišmentsko djelovanje, terorizam), ali, isto tako, i savremenih oblika kriminalnih aktivnosti (krađe identiteta, krađe vremena, internet piraterije, internet nasilja). U tom kontekstu, kao najučestaliji, ali naravno ne i jedini oblici kriminalnih aktivnosti na društvenim mrežama se posmatraju prevare, krađe identiteta, piraterija, pornografija, pedofilija, terorizam, vršnjačko nasilje, govor mržnje, te razni oblici antiestablišmentskog djelovanja korištenjem društvenih mreža.

KONCEPT DRUŠTVENIH MREŽA

Ideja društvenih mreža je vrlo jednostavna. Korisnik se registruje i zapisuje interesantne podatke iz svog života (ili o sebi), potkrepljuje to fotografijama, video snimcima i komunicira sa prijateljima koji to isto rade... Iz ideje je proistekao i način funkcionisanja ovih mreža, koji je uglavnom isti. Neophodno je registrovati se na konkretnoj mreži, gdje se najčešće daju osnovni podaci, a nakon valorizacije na elektronskoj pošti, pristupa se odabranoj mreži. Svaki registrovani član dobija, odnosno kreira vlastitu stranicu, koja se (uglavnom) naziva profil. Nakon toga se biraju i pozivaju drugi korisnici, od čega se sačinjava lista prijatelja, koja se vremenom širi, mada se određeni prijatelji mogu i brisati sa liste. Nakon kreiranja profila, što se smatra početnim korakom u pristupu društvenoj mreži, pristupa se komunikaciji sa drugim članovima mreže koji takođe imaju svoje profile. Ta komunikacija može biti i u formi dijaloga, ali i monologa, a može se odvijati i kroz popularno ‘’lajkovanje’’, komentarisanje fotografija, snimaka ili tuđih komentara... Korisnici društvenih mreža kao jednu od glavnih prednosti navode upravo mogućnost da stalno budu u kontaktu sa prijateljima, a naročito onima koje dugo nisu vidjeli.

Društvene mreže su novija pojava na internetu i ne spadaju u jednu posebnu kategoriju, jer sadrže gotovo sve internet usluge (ćaskaonice, forume, elektronsku poštu...), objedinjene za rad na lak i prihvatljiv način, odnosno moglo bi se reći da društvene mreže predstavljaju funkcionalno i za korisnike star(ij)e usluge interesantno povezane u jednu kvalitativno novu uslugu. Vjerovatno usljed navedenog, korisnici interneta su iznenađujuće brzo i masovno prihvatili koncept društvenih mreža uopšte.

Društvene mreže su usluga ili, bolje rečeno, funkcionalno povezan skup usluga na internetu koji objedinjava i tehnologiju (posmatrano kroz mogućnosti) i društvenu interaktivnost u cilju komunikacije između članova konkretne društvene mreže. Pored toga što omogućavaju komunikaciju između korisnika, predstavljaju i jedan oblik onlajn druženja (‘’novu društvenost’’), ali omogućavaju (što je takođe bitno) i jedan vid samopromocije u razne svrhe, zatim mogućnost postavljanja video snimaka, fotografija, pisanje svojevrsnih blogova, igranje raznih igara i druge korisne (ili manje korisne) aktivnosti. Neophodno je reći da su društvene mreže

besplatne za korištenje, odnosno učlanjenje u ove mreže je besplatno (što ne znači da su i sve mogućnosti i aplikacije na njima besplatne), a isto tako, zahvaljujući razvoju mobilnog interneta, na većinu društvenih mreža se može pristupiti sa mobilnog telefona, što je takođe uticalo na njihovu popularnost i masovnost korišćenja.

Formalna i jedna od najpoznatijih akademskih definicija sajtova društvenih mreža, koja doprinosi daljem razmišljanju i istraživanju društvenog onlajn umrežavanja, definiše onlajn društvene mreže kao veb zasnovane servise koji omogućavaju pojedincima da kreiraju javne ili polujavne profile unutar zatvorenog centralizovanog sistema, artikulisanu listu ostalih korisnika, te mreže sa kojima imaju zajedničke konekcije (veze) i selektivnu listu konekcija koju nazivaju – prijateljima (povjerljiv krug prijatelja). To su obično lista prijatelja, kao i pregled komunikacijskih konvencija i praksi koje se dešavaju na ‘’zidovima’’, bilježnicama, ličnim stranicama korisnika (Radovanović, 2011: 20).

ENISA[1] definiše društvene mreže kao onlajn zajednice koje omogućavaju ljudima da preko izgrađenih profila ostvaruju kontakte, komuniciraju, da se susreću, razmjenjuju fotografije i video zapise sa drugim članovima te zajednice, sa kojima je veza u okviru zajednice dozvoljena (prihvaćena) sa njihove strane (dijeljena). Sa funkcionalnog stanovišta, ENISA društvene mreže dijeli u dvije glavne kategorije: društvene mreže opšte namjene i posebne društvene mreže. (Ivanović, Banović, 2010).

Društvene mreže se često poistovjećuju sa Fejsbukom (*Facebook*), što je razumljivo, ali i pogrešno, jer je Fejsbuk samo jedna od mnogobrojnih društvenih mreža koje postoje na internetu, iako svakako najposjećenija (najmasovnija), a samim tim (može se reći) i najpopularnija. Pored Fejsbuka, kao najpopularnije društvene mreže na internetu, na globalnom nivou su (bili) aktuelni i popularni *Twitter, YouTube, MySpace, Google+, Flickr, LinkedIn, Last FM, Netlog, Orkut, Hi5, Badoo, Bebo, Friendster, Medina, TogetherVille, Xanga, Pinterest*...

KRIMINOLOŠKO-ETIOLOŠKI ASPEKT DRUŠTVENIH MREŽA

Uzroci koji dovode do (ekspanzije) kriminalnih aktivnosti na društvenim mrežama ili prema korisnicima društvenih mreža jesu brojni i uglavnom se odnose na faktore koji dovode i do pojave internet kriminaliteta. Međutim, činjenica je da su navedeni faktori ipak u većoj ili manjoj mjeri prilagođeni okruženju u kojem egzistiraju društvene mreže, a takođe su prilagođeni i samim korisnicima društvenih mreža, kao specifičnoj populaciji internauta (koja se, između ostalog, ogleda u specifičnom ‘’mrežnom identitetu’’ koji uslovljava i druge specifičnosti ove populacije). Kao glavni uzroci ispoljavanja kriminalnih aktivnosti na društvenim mrežama se posmatraju masovnost korisnika društvenih mreža, informatička nepismenost i nepostojanje svijesti o bezbjednosnim rizicima korišćenja društvenih mreža, virtuelno okruženje u kojem egzistiraju društvene mreže, vlastita pasivizacija mogućnosti zaštite na društvenim mrežama, mogućnost

[1] ENISA je akronim Evropske agencije za bezbjednost mreža i informacija (*European Network and Information Security Agency*).

anonimnog (pseudonimnog) djelovanja, otežana mogućnost identifikacije izvršilaca kriminalnih aktivnosti na društvenim mrežama...

Kao što je i navedeno, društvene mreže su jedna od najpopularnijih usluga na internetu. U prilog tome svjedoče brojni aktivni, ali i pasivni članovi mnogih društvenih mreža. Korisnici biraju društvene mreže na osnovu afiniteta, popularnosti, jednostavnosti i slično, uz napomenu da su dosta članova jedne mreže istovremeno članovi i druge ili drugih mreža. Naravno, činjenica je da dosta internauta nisu članovi nijedne mreže, već koriste druge usluge interneta. Međutim, brojne analize ukazuju na to da su sve više internauta korisnici i neke od brojnih društvenih mreža, pogotovo globalno najpopularnijih (najmasovnijih). Upravo navedeno i uslovljava ekspanziju kriminalnih aktivnosti na društvenim mrežama, odnosno masovnost korisnika se posmatra kao glavni etiološki faktor kriminalnih aktivnosti na društvenim mrežama. Naime, planeri, organizatori ili neposredni izvršioci kriminalnih aktivnosti na društvenim mrežama koriste racionalan izbor uslovljen statističkim zakonima vjerovatnoće teorije velikih brojeva kako bi korisnici društvenih mreža postali žrtve njihovih kriminalnih aktivnosti. Konkretno, ovaj etiološki faktor kriminalnih aktivnosti na društvenim mrežama polazi od velikog broja potencijalnih žrtvi (svih korisnika društvenih mreža), kojom prilikom izvršioci kriminalnih aktivnosti smatraju da je dovoljno i da samo mali procenat korisnika postane žrtvom, kako bi njihova aktivnost bila ‘’uspješna’’. Drugim riječima, glavni uzrok ispoljavanja kriminalnih aktivnosti na društvenim mrežama se nalazi u shvatanju (racionalnom izboru) izvršilaca kriminalnih aktivnosti da im se ‘’isplati’’ vršiti razne kriminalne aktivnosti na društvenim mrežama, imajući u vidu da, iako vjerovatnoća uspješnosti realizacije aktivnosti, procentualno posmatrano, nije velika, kvantitativno svakako jeste, s obzirom na broj korisnika (potencijalnih žrtvi) društvenih mreža. Pojednostavljeno predstavljajući navedeno, samo da minimalni procenat korisnika određene društvene mreže (npr. 1% ili čak i manje), pa i ne posmatrano na globalnom, već na regionalnom ili lokalnom nivou, od ukupne populacije korisnika, postane žrtvom kriminalne aktivnosti, usljed velikog broja korisnika ovih mreža kriminalcima se isplati realizovanje vlastitih kriminalnih aktivnosti korišćenjem mogućnosti društvenih mreža.

Generalno posmatrajući, velika većina internauta, uključujući i korisnike društvenih mreža, uopšte nije svjesna opasnosti i bezbjednosnih rizika koje internet i mogućnosti na internetu, a pogotovo na društvenim mrežama nose. Navedeno je posljedica niske informatičke pismenosti internauta i korisnika društvenih mreža, ali, isto tako, i virtuelnog ambijenta u kojem internet egzistira, bez obzira na to što se posljedice narušavanja privatnosti, krađe identiteta, raznih prevarnih aktivnosti i drugih kriminalnih aktivnosti konkretizuju prema žrtvi u realnom svijetu. Često se internet, odnosno surfanje (krstarenje) internetom i društvenim mrežama nekritički i bespogovorno prihvata, čime internauti direktno potpomažu, pa čak i podstiču i favorizuju vršenje kriminalnih aktivnosti na internetu. Čak bi se moglo reći da informatička nepismenost i nepostojanje svijesti o bezbjednosnim rizicima na internetu prilikom korištenja društvenih mreža, posmatrano kao etiološki faktor kriminalnih aktivnosti na društvenim mrežama, savremene i informatički obrazovane kriminalce (kojih je sve više) jednostavno ohrabruje da vlastite kriminalne sklonosti ‘’sele’’ na internet, a pogotovo u okruženje društvenih mreža, gdje je informatička pismenost i svijest

o mogućnostima ispoljavanja kriminalnih aktivnosti, te svijest o nužnosti vlastite zaštite izuzetno mala, gotovo zanemarljiva.

Iako su brojni faktori koji doprinose informatičkoj nepismenosti, neophodno je da se ukaže i na virtuelni aspekt interneta i društvenih mreža kao faktor koji onemogućava, odnosno ograničava podizanje svijesti internauta o bezbjednosnim rizicima na društvenim mrežama. Usljed okruženja u kojem egzistiraju društvene mreže, pa i sam internet, a koji karakteriše prostorna i vremenska virtuelnost, internauti na osnovu navedenog zaključuju i o vlastitoj bezbjednosti, odnosno o ugroženosti korišćenja interneta i društvenih mreža, naivno smatrajući da im se u virtuelnom okruženju, bez obzira na to što se koriste realnim, konkretnim mogućnostima interneta i društvenih mreža, ništa loše ne može desiti. Da navedeno nije tačno, odnosno da virtuelnost ne znači virtuelnu, a pogotovo ne stvarnu bezbjednost, pored svakodnevnih kriminalnih aktivnosti u ovakvom okruženju svjedoče i brojne negativne aktivnosti koje se u zadnje vrijeme nazivaju virtuelnim zločinima (Trivić, 2011: 300), a koje svakako imaju uticaj i na same korisnike.

Vjerovatno nepostojanje svijesti o bezbjednosnim rizicima na društvenim mrežama, kao i sama informatička nepismenost, te posmatranje interneta i društvenih mreža kroz koncept *rerum quae intelleguntur* (''svijet koji se zamišlja'') u kojem vlada virtuelna bezbjednost svih korisnika, uslovljava i vlastitu pasivizaciju zaštite privatnosti korisnika društvenih mreža. Naime, činjenica je da veliki procenat korisnika društvenih mreža (ne)podešavanjem alata privatnosti direktno ''privlači'' seksualne grabežljivce i druge izvršioce kriminalnih aktivnosti na društvenim mrežama, s obzirom na to da mogućnost dijeljenja postavljenog sadržaja i materijala, kao i ličnih informacija i podataka uopšte ne zaštićuju, odnosno čine ih dostupnim svima ili većini korisnika društvenih mreža, direktno omogućavajući njihovu zloupotrebu. Usljed neznanja i lijenosti, ali i u cilju samopromocije, veliki broj korisnika društvenih mreža, pogotovo Fejsbuka, pristup ličnim informacijama i podacima, kao i postavljenom sadržaju dijeli sa svim ili sa većinom korisnika, direktno omogućavajući zloupotrebu od strane korisnika koji se nalaze u populaciji kojoj je dozvoljen pristup tim podacima ili materijalu. Ovo direktno dovodi do mnogobrojnih primjera kršenja privatnosti tih korisnika, ali i do raznih oblika kompromitacije ili krađe identiteta korisnika, kao i do niza drugih kriminalnih aktivnosti. U prvom redu, sami korisnici su najdirektnije odgovorni za brojne primjere kršenja privatnosti, kao i za druge oblike ispoljavanja kriminalnih aktivnosti uslovljenih slabom ili nikakvom zaštitom korisničkih podataka, ali ne treba zapostaviti ni ulogu samih društvenih mreža u zaštiti ličnih podataka. Naime, bez umanjivanja uloge korisnika u vlastitoj zaštiti podataka na profilu, činjenica je da su pojedine mogućnosti zaštite podataka na društvenim mrežama izuzetno neprilagođene korisnicima, pogotovo informatički nepismenijim, usljed čega oni i zanemaruju te mogućnosti. Pored korisničkog neznanja i lijenosti, te drugih razloga, sasvim sigurno je da ovaj tehnički propust društvenih mreža uveliko doprinosi ispoljavanju kriminogenih aktivnosti na društvenim mrežama. Usljed navedenog, u zadnje vrijeme je primijetno da većina društvenih mreža, pogotovo globalnog karaktera, veliku pažnju posvećuje i politici privatnosti, u okviru koje je akcenat na činjenju lako dostupnim i jednostavnim za korišćenje određenih mogućnosti (alata) zaštite ličnih korisničkih podataka, što je, naravno, pohvalno, ali, ipak, (još uvijek) nedovoljno.

Sa kriminalne strane posmatrano, ekspanziji kriminalnih aktivnosti na društvenim mrežama sigurno doprinosi i mogućnost njihovog anonimnog, odnosno pseudonimnog djelovanja. Anonimnost (pseudonimnost) korisnika je uslovljena mogućnošću lažnog ili pseudonimnog predstavljanja, kako u ličnoj ili grupnoj komunikaciji preko društvenih mreža, tako i u vlastitom predstavljanju kroz kreirane lažne ili kompromitovane profile. Anonimnost posmatrana na ovaj način, a koju omogućava koncept društvenih mreža, ali i sam internet, direktno favorizuje vršenje kriminalnih aktivnosti na društvenim mrežama, pogotovo određenih oblika ispoljavanja tih aktivnosti, poput vršnjačkog nasilja, vrbovanja žrtvi, prevarnih aktivnosti... Pseudonimno ili lažno predstavljanje omogućava i brojne prevarne aktivnosti u sklopu tzv. prevara autoriteta, koje su uglavnom fokusirane na cijeli niz kriminalnih aktivnosti, od kojih se ovaj vid prevare posmatra samo kao početna faza, najčešće i najblaža po posljedicama.

Direktno povezana sa anonimnim (pseudonimnim) djelovanjem jeste i (ne)mogućnost otkrivanja identiteta pravih izvršilaca kriminalnih aktivnosti na društvenim mrežama. Naime, usljed mnogobrojnih faktora, kriminalističke mjere, radnje i aktivnosti na identifikovanju, pronalaženju i hvatanju izvršilaca konkretnih krivičnih djela ili kriminalnih aktivnosti izvršenih na društvenim mrežama ili korištenjem mogućnosti društvenih mreža ili prema korisnicima društvenih mreža su umnogome otežane, što ne znači i da su nemoguće. Takođe, usljed brojnih tehničkih, ali i normativnih ograničenja, mogućnost prikupljanja operativnih saznanja i dokaznog materijala je umnogome otežana. Naravno, navedenog su svjesni i sami planeri, organizatori i izvršioci kriminalnih aktivnosti na društvenim mrežama.

KRIMINOLOŠKO-FENOMENOLOŠKI ASPEKT DRUŠTVENIH MREŽA

Imajući u vidu prethodno navedene (najznačajnije) etiološke faktore ispoljavanja kriminaliteta na društvenim mrežama, jasno je usljed čega se na njima ispoljava cijeli niz kriminalnih aktivnosti, kako krivičnih djela koja potpadaju pod dijapazon računarskog kriminaliteta, tako i niz krivičnih djela koja i nisu a priori krivična djela iz dijapazona računarskog, već uglavnom krivična djela opšteg kriminaliteta.

Kada su u pitanju specifičnosti konkretnih kriminalnih aktivnosti koje se ispoljavaju na društvenim mrežama, one se ogledaju kroz modifikaciju mogućnosti koje im pružaju društvene mreže kao jedna od (najpopularnijih) usluga na internetu. U tom kontekstu, kriminalne aktivnosti koje se ispoljavaju preko društvenih mreža, u suštini, predstavljaju prilagođene oblike ispoljavanja samog internet kriminaliteta. Sledstveno tome, razumljivo je i da internet kriminalitet, s obzirom na specifičnosti ‘’prostora’’ na kom se ispoljava, (uglavnom) predstavlja prilagođene oblike ispoljavanja klasičnog kriminaliteta. Tako se kao najučestaliji oblici ispoljavanja kriminalnih aktivnosti na društvenim mrežama pojavljuju razni oblici prevara i krađa (zloupotreba) identiteta, ali su prisutni i razni oblici verbalnog (elektronskog) nasilja, piraterija, pornografija i pedofilija, zatim su prisutne razne aktivnosti terorističkog karaktera, antiestablišmentskog djelovanja, propagiranje zabranjenih ideja ili sadržaja...

Krađe (zloupotrebe) identiteta na društvenim mrežama se najčešće konkretizuju kroz kompromitaciju naloga ili profila na društvenim mrežama.[2] Krađa identiteta kompromitacijom profila na društvenim mrežama je, najčešće, samo prva u nizu kriminalnih aktivnosti koje se ispoljavaju u sklopu kriminalne aktivnosti na društvenim mrežama, bez obzira na to da li se kriminalna aktivnost ispoljava ka konkretnom korisniku usluga društvenih mreža ili se kriminalna aktivnost ispoljava ka neodređenom i neindividualizovanom broju ili grupi korisnika društvene mreže. Drugim riječima, krađa identiteta kroz kompromitaciju profila najčešće nije sama sebi cilj, već služi u cilju realizacije drugih kriminalnih aktivnosti (prevare, pedofilije, ispoljavanja nasilja, širenja zabranjenih ideja ili sadržaja...). Isto tako, kompromitacijom profila se rjeđe napada sam konkretni korisnik (bez obzira na to što se njegov profil kompromituje), već se, u sklopu kriminalne aktivnosti, pogotovo koja je zasnovana na sofisticiranijem programskom pristupu, napadaju neindividualizovani korisnici ili grupno filtrirani profili korisnika (po određenim kategorijama koje omogućava sama društvena mreža). Naravno, iako rjeđe, cilj krađe profila može biti i nanošenje direktne nematerijalne štete korisniku profila, a u ovim slučajevima se najčešće radi o raznim oblicima elektronskog nasilja, uglavnom vršnjačkog.

Kao što je već navedeno, krađa (preuzimanje) profila najčešće nije sama sebi cilj, već, uglavnom, predstavlja (pred)fazu raznih kriminalnih aktivnosti, uglavnom prevarnih aktivnosti. Kvalitativni i kvantitativni aspekt raznih prevarnih aktivnosti na internetu je nemjerljiv, a imajući u vidu da su ‘’internet prevare tek nešto malo mlađe od interneta’’, razumljivo je da su one posebno zastupljene na društvenim mrežama, s obzirom na to da internet prevarantima posebno pogoduje broj korisnika, kao i opšte i informatičko (ne)znanje korisnika, te velike mogućnosti anonimnog djelovanja, a, nasuprot tome, male ili gotovo zanemarljive mogućnosti identifikacije prevaranata, pa i prevarantske aktivnosti.[3] Cilj svih prevarnih

[2] Najjednostavnije predstavljeno, pod krađom ili kompromitacijom profila se podrazumijeva preuzimanje tuđeg profila što se, uglavnom, sastoji u neovlašćenom, a najčešće i prevarnom pristupu i kontroli identifikacionih i autentifikacionih podatka korisnika (korisničkog imena i lozinke). Kompromitacija profila najčešće podrazumijeva i krađu, odnosno preuzimanje profila, mada se kompromitacija može izvršiti i bez potpunog preuzimanja kontrole nad profilom. Načini krađe profila su mnogobrojni i upravo se kod krađe profila, kao kriminalne aktivnosti na društvenim mrežama, uviđa sličnost sa ispoljavanjem ovih kriminalnih aktivnosti i na internetu. Naime, fenomenološki aspekti krađe identiteta kompromitacijom profila na društvenim mrežama su mnogobrojni, ali se kao najčešći pojavljuju poznate metode za krađu identiteta na internetu, poput metode fišinga (*phishing*), spufinga (*spoofing*) i kubfejsa (*koobface*), zatim razni oblici ‘’provaljivanja’’ lozinke (i korisničkog imena)... Poseban aspekt krađe, odnosno kompromitacije identiteta predstavlja tzv. skvoting (*squatting)* imena, pogotovo poznatijih, odnosno ‘’zvučnijih’’ imena među populacijom korisnika na određenoj društvenoj mreži, te lažni (i dupli) profili, kao i kompromitacija brenda, odnosno marke (imena firme) kroz nedozvoljeno kreiranje ili krađu identiteta firme na društvenim mrežama. Sve ove, ali i brojne druge metode krađe identiteta su prilagođene okruženju društvenih mreža.

[3] Nabrojati sve oblike prevarnih aktivnosti na društvenim mrežama se čini bespredmetnim, pogotovo imajući u vidu da se aktuelni oblici konstantno usavršavaju, dok se istovremeno pojavljuju i novi. Kao najčešći oblici ispoljavanja prevarnih aktivnosti na društvenim mrežama pojavljuju se razni oblici internet prevara prilagođeni okruženju društvenih mreža, poput nigerijske prevare, prevare autoriteta (prevare sa lažnim profilima, odnosno lažnim ili kompromitovanim profilima), prevare sa uslugama, spem (*spam*) prevare, prevare sa nagradama (*scam* prevare), prevare sa zlonamjernim aplikacijama, prevare iz oblasti elektronskog bankarstva, klik prevare (Banović, Miladinović, 2010: 45)...

aktivnosti na društvenim mrežama je primarno motivisan sticanjem materijalne koristi, kom prilikom prevaranti na društvenim mrežama, kao i prevaranti uopšte, lažno ili prikriveno predstavljaju postojeće činjenice, te na taj način obmanjuju žrtve, najčešće lakovjerne, mada je činjenica da na ove prevare ‘’nasjedaju’’ i žrtve za koje se ne bi moglo reći da su lakovjerne, bar ne u stvarnom životu. Iako se i za korisnike društvenih mreža koji vrše i krađu profila i prevarne aktivnosti može reći da su korisnici sa prosječnim, pa čak i natprosječnim znanjem iz oblasti informaciono-komunikacionih tehnologija, za izvršioce prevarnih aktivnosti se čak može reći da posjeduju određena znanja iz psihologije, te da veoma dobro koriste mogućnosti socijalnog inženjeringa, odnosno imaju empatičke sposobnosti, a pogotovo su vješti u komunikaciji sa drugima, bez obzira na to što je ta komunikacija najčešće virtuelna.

Pored krađa profila i raznih oblika ispoljavanja prevarnih aktivnosti na društvenim mrežama, posebno su učestali razni oblici ispoljavanja nasilja, prije svega elektronskog nasilja, kroz govor mržnje. S obzirom na masovnost korisnika, kao i heterogenost korisnika u smislu pripadnosti određenim neformalnim društvenim grupama (nacionalnoj, vjerskoj, regionalnoj, lokalnoj, polnoj, obrazovnoj, seksualnoj, manjinskoj), a pogotovo imajući u vidu mogućnost anonimnog djelovanja, preko društvenih mreža se sve više ispoljavaju razni oblici elektronskog nasilja koji se najčešće ispoljavaju kroz govor mržnje koji se ogleda u prijetnjama, ponižavanju, maltretiranju, ismijavanju i na druge slične degradirajuće načine. Karakteristika ovog oblika ispoljavanja govora mržnje jeste da se on najčešće realizuje prema određenoj populaciji korisnika društvenih mreža, najčešće manjinskoj (nacionalnoj, vjerskoj, seksualnoj) populaciji u određenom društvu, dok se rjeđe ispoljava prema konkretnom korisniku, iako ni navedeno ne izostaje, pogotovo kada su u pitanju korisnici društvenih mreža koji su u određenoj zajednici poznatiji, odnosno u određenom društvu imaju konkretnu formalnu ili neformalnu ulogu.

Pored govora mržnje, jedan od najučestalijih oblika kriminogenog ponašanja na društvenim mrežama je vršnjačko nasilje. Ovaj oblik elektronskog nasilja usmjeren ka mlađim korisnicima društvenih mreža je posebno poguban, pogotovo u odnosu na klasične oblike ispoljavanja vršnjačkog nasilja, s obzirom na to da su žrtve ovom nasilju izložene konstantno i kontinuirano, pa čak i bez obzira na to da li su korisnici društvene mreže. Drugim riječima, žrtva vršnjačkog nasilja na društvenim mrežama može da se postane čak i ukoliko ona sama nije korisnik društvenih mreža, pa čak ni interneta. Uzrok ovome je što nasilnički sadržaj (bez obzira na to o kakvoj vrsti sadržaja se radi) dolazi do drugih korisnika društvenih mreža koji poznaju žrtvu ili su iz njenog životnog okruženja, a čega je svjesna i sama žrtva, usljed čega dolazi do njene reakcije u vidu pasivizacije i drugih posljedica koje vršnjačko nasilje nanosi samoj žrtvi. S obzirom na to da su mlađi korisnici interneta (iz kojeg ce ‘’crpe’’ žrtve vršnjačkog nasilja, ali najčešće i sami nasilnici) uglavnom korisnici Fejsbuka, dok ostale društvene mreže rjeđe koriste, oblici elektronskog nasilja na društvenim mrežama se najučestalije i ispoljavaju na ovoj društvenoj mreži (Miladinović, Petričević, 2011).

Piraterija je takođe veoma rasprostranjena pojava na društvenim mrežama, u prvom redu usljed određenih aplikacijskih mogućnosti na društvenim mrežama, kao i usljed nepostojanja tehničkih (aplikacijskih) ograničenja u pogledu

distribucije piratskog sadržaja. Štaviše, neke društvene mreže (poput Jutjuba) vlastitim aplikacijskim mogućnostima u potpunosti afirmišu piratsku aktivnost na internetu posmatranu kroz postavljanje određenih video ili muzičkih ili sličnih sadržaja, dok se na drugima (Fejsbuk) aplikacijski omogućava dijeljenje piratizovanih sadržaja na profilu korisnika, čineći ih na taj način dostupnim i drugim korisnicima, a potom i cijeloj populaciji korisnika na konkretnoj društvenoj mreži. Naravno, iz ovog ne treba izvlačiti zaključak da je piraterija dozvoljena na društvenim mrežama. Naprotiv, ona je izričito zabranjena. Međutim, i pored pokušaja ograničenja (širenja) piratizovanog sadržaja preko društvenih mreža, ipak su one same, kao što je već navedeno, usljed mnogobrojnih okolnosti, ‘’idealne’’ za širenje piratizovanog sadržaja, bez obzira na to da li se radi o softverskoj pirateriji (koja se dijeli kroz posebno kreirane grupe korisnicima zainteresovanim za tu vrstu sadržaja), dijeljenju piratizovanog muzičkog, filmskog, video ili sličnog sadržaja ili o drugim načinima piraterije. Piraterija na društvenim mrežama je posebno pogubna po nosioca autorskih prava, s obzirom na to da, s jedne strane, onemogućava brzu, adekvatnu i pravovremenu reakciju u cilju obustavljanja piratske aktivnosti, dok se, s druge strane, na ovaj način piratizovani sadržaj izuzetno brzo dijeli velikom broju korisnika društvenih mreža, a potom i internautima uopšte.

Za razliku od piraterije, društvene mreže pornografiju i pedofiliju izričito brane i mnogo energičnije suzbijaju nego kada je u pitanju piraterija. Međutim, kao i kada je u pitanju piraterija, i pornografija i pedofilija su na društvenim mrežema, iz mnogobrojnih razloga, zastupljene. U prvom redu, usljed masovnosti, društvene mreže su pogodne za brzo i masovno širenje pornografskog materijala, a takođe su i podobne za pronalaženje pornografskih, a pogotovo pedofilskih ‘’istomišljenika’’. Isto tako, s obzirom na mogućnosti filtriranja određenih podataka o korisnicima, pedofili na društvenim mrežama relativno lako mogu da pronalaze, identifikuju i vrbuju žrtve vlastitih nastranih sklonosti. Mogućnost pregleda postavljenog sadržaja na društvenim mrežama, kao i razne softverske mogućnosti preuzetog sadržaja omogućavaju kompromitaciju tog sadržaja pornografskim kontekstom, što je takođe bitno imajući u vidu da korisnici koji postavljaju ili objavljuju ove materijale i sadržaje najčešće nisu ni svjesni tih mogućnosti, a nerijetko i sami dijele sadržaj koji, uz određene softverske ili vizuelne modifikacije ili čak i bez njih, ali u određenom kontekstu, postaje kompromitujući za njih.

Sajber terorizam, odnosno terorizam koji se u potpunosti ili parcijalizovano realizuje na internetu ili korištenjem mogućnosti interneta je sasvim sigurno realnost današnjeg društva globalizovanog, između ostalog, i informaciono-komunikacionim tehnologijama. U cilju realizacije terorističke aktivnosti ili samog akta, teroristi sve više koriste internet usluge i resurse, primarno forume i društvene mreže u okviru kojih pronalaze i vrbuju saradnike i istomišljenike. Društvene mreže se koriste i za samu komunikaciju između terorista, s obzirom na to da im ovaj vid komunikacije omogućava mnogobrojne prednosti (prije svega, zaštićenost komunikacije), pogotovo u kontekstu mnogobrojnih ograničenja koja su rezultat globalnih aktivnosti ‘’rata protiv terorizma’’. Društvene mreže su im posebno pogodne s obzirom na masovnost, usljed čega je primijetno da se u okrivu društvenih mreža sve više vrbuju korisnici za vršenje terorističkih akata ili propagiranje terorističkih stavova i vrijednosnog sistema, ali se takođe preko društvenih mreža pronalaze i istomišljenici, te se na ovaj način povezuju, a potom i

omasovljavaju terorističke organizacije ili simpatizeri ovih organizacija ili njihovih stavova. Takođe, društvene mreže se koriste i u cilju propagiranja terorističkih aktivnosti, pogotovo objavljivanjem terorističkih proglasa ili preuzimanjem odgovornosti za realizovane terorističke akte, kojom prilikom se preko društvenih mreža ''eksploatiše'' efekat koji je izazvao konkretan teroristički akt (ne podrazumijevajući pod navedenim samo povratne informacije, odnosno komentare odobravanja ili neodobravanja samog akta, već upravo strah i užas koji je takav akt izazvao među korisnicima društvenih mreža, a koji se vidi na osnovu sadržaja i broja komentara na društvenim mrežama).

Jedna od prednosti interneta je što omogućava (globalnu) društvenu emancipaciju i (djelimičnu) neformalnu participaciju određenih grupa ili populacije u okviru zajednice, uprkos neformalnim tradicionalističkim (konzervativnim), kulturološkim, konfesionalnim, nacionalnim, političkim ili formalnim normativnim ili drugim vrstama ograničenja. To konkretno implicira da se preko određenih usluga interneta, prevashodno preko društvenih mreža, određeni pojedinci, grupe ili cijela populacija ne pridržava nametnutih ograničenja (ne ulazeći u opravdanost postavljenih ograničenja). Na ovaj način posmatrano nepridržavanje nametnutih ograničenja uz pomoć društvenih mreža, imajući u vidu masovnost korisnika, te mogućnost brzog širenja ideja i sadržaja, uz mogućnost i anonimnog djelovanja, te nepostojanje adekvatne zaštite od propagiranja ove aktivnosti, čini suštinu antiestablišmentskog djelovanja preko društvenih mreža. Naime, usljed mnogobrojnih ograničenja koja se postavljaju u nedemokratskim i institucionalno i društveno nerazvijenim (korumpiranim) društvima, društvene mreže se pojavljuju kao efikasno sredstvo ''premošćavanja'' tih barijera u cilju djelovanja protiv aktuelnog režima u državama.[4] Naravno, kvalitativno i kvantitativno analizirajući domete i značaj društvenih mreža u ovom vidu antiestablišmentskog djelovanja, njih ne treba ni potcjenjivati, ali ni precjenjivati. Međutim, da režimi shvataju opasnost od antiestablišmentskog djelovanja korišćenjem društvenih mreža, vidi se na osnovu toga što je nekoliko država za vrijeme kriznih stanja blokiralo pristup društvenim mrežama (kao i drugim sadržajima interneta).[5] Kao poseban aspekt

[4] Konkretan primjer antiestablišmentskog djelovanja preko društvenih mreža se odnosi na ulogu Fejsbuka i Tvitera u događajima poznatim pod nazivom ''arapsko proljeće'', usljed čega se revolucije izazvane u dijelu arapskih (i drugih) država nazivaju i Fejsbuk, odnosno Tviter revolucijama (demonstracije u Iranu). Iako se često uloga društvenih mreža u ''arapskom proljeću'' precjenjuje, činjenica je da su vinovnici protesta u Egiptu, Tunisu, Siriji i drugim državama u početku koristili društvene mreže u cilju dogovaranja o protestima. Ovaj način komunikacije preko društvenih mreža u cilju svrgavanja režima na vlasti je svakako zadavao velike probleme represivnom aparatu, s obzirom na to da su ovi protesti bili, s jedne strane, pokretljivi i disperzivni, što je onemogućavalo (brzu) pokretljivost represivnih snaga (u prvom redu, policije) na suzbijanju okupljanja ili razbijanju protesta, dok je, s druge strane, otežavalo praćenje komunikacije samih korisnika, a pogotovo predviđanje aktivnosti, ali je, isto tako, onemogućavalo i identifikaciju i pronalaženje organizatora protesta. Štaviše, u toku ovih protesta, ulogu organizatora su preuzimali i sami učesnici komunicirajući preko mobilnih uređaja priključenih na internet, odnosno na društvene mreže, usljed čega se ovaj vid organizacije pokazao demokratičnim, ali je i eliminisao lidera protesta, čime je ograničena mogućnost kompromitacije tih lidera od strane represivnih aparata.

[5] Da ovaj vid cenzure društvenih mreža, pa i samog interneta, nije karakteristika samo država koje su od strane globalnih aktera ''međunarodne zajednice'' proglašene nedemokratskim i diktatorskim režimima (poput Egipta, Libije, Tunisa, Sirije, Irana...), vidi se i u reakciji vladinih funkcionera na građanske nemire u Velikoj Britaniji koji su se desili u toku ljeta 2011. godine. Naime, usljed eskalacije

antiestablišmentskog djelovanja preko društvenih mreža mogu da se posmatraju i razni oblici ispoljavanja informacionog (i informativnog) ratovanja.

Slično antiestablišmentskom djelovanju preko društvenih mreža, može da se posmatra i distribucija određenih zabranjenih sadržaja ili propagiranje određenih ideja ili vrijednosti koje su u određenom društvu ili zajednici ograničene, odnosno zabranjene. Naime, s obzirom na mogućnost dijeljenja postavljenog ili sa interneta preuzetog sadržaja drugim korisnicima na društvenim mrežama, određeni antiestablišmentski nastrojeni korisnici ili korisnici koji nemaju logističke, ni normativne mogućnosti za promovisanje određenih sadržaja, preko društvenih mreža uspijevaju širiti ideje ili dijeliti sadržaj koji je u određenoj zajednici potpuno ili djelimično zabranjen. To se najčešće odnosi na određena politička, naučna ili umjetnička djela, primarno na određene filmske, muzičke i slične materijale kojim je zajedničko da je njihova proizvodnja, distribucija ili sam sadržaj u određenoj zajednici zabranjen ili djelimično ograničen. Usljed navedenog, preko društvenih mreža se uspješno ‘’premošćavaju’’ normativna ili druga ograničenja u pogledu proizvodnje, distribucije ili samog sadržaja ovakvih materijala ili ideja. U kontekstu navedenog, treba posmatrati i jedan oblik insajderskog i disidentskog djelovanja unutar društva ili institucija društva, kojom prilikom se društvene mreže javljaju kao ‘’lokacija’’ za kritikovanje ili iznošenje ‘’prljavog veša’’ široj zajednici oličenoj kroz korisnike samih društvenih mreža. Bez obzira na to što insajdersko i disidentsko djelovanje, kao uostalom i cijeli konglomerat aktivnosti antiestablišmentskog karaktera, mogu da budu afirmativni za ljudska prava i slobode pojedinaca, kao i za određenu zajednicu u cjelini, činjenica je da su ovakvi načini djelovanja uglavnom protivni aktuelnom normativnom sistemu, bez obzira na to koliko je on pravičan ili ne, u čemu se i konkretizuje kriminogeni aspekt društvenih mreža posmatranih kroz antiestablišmentsko djelovanje pojedinaca ili formalnih i neformalnih grupa kroz organizovanje protesta, nelegalno udruživanje, informaciono ratovanje, širenje zabranjenih materijala ili promovisanje određenih zabranjenih ideala i ideja, insajdersko ili disidentsko djelovanje...

Od samih početaka masovnih i globalnih društvenih mreža privatnost korisnika je ‘’rak-rana’’, odnosno negativan nusprodukt ekspanzije ove usluge na internetu. Iako se za sve usluge na internetu, odnosno ni za sam internet ne može reći da mnogo brine o privatnosti korisnika, kod društvenih mreža se ta privatnost najdrastičnije, ali i najkonkretnije i najčešće narušava, i to kroz nekoliko segmenata, od kojih su korisnički i aplikacijski (tehnički) aspekt najkonkretniji. U prvom redu, korisnici sami postavljaju određene lične informacije, podatke i materijal koji spada u domen privatnosti, te ih potom dijele drugim korisnicima, nesvjesno direktno omogućavajući narušavanje vlastite privatnosti na razne načine, odnosno omogućavajući da se njihovi lični podaci zloupotrijebe, kako od strane drugih korisnika, tako i od strane same društvene mreže. S druge strane,

---

nemira koji su se desili u većim gradovima Velike Britanije, a koji su djelimično organizovani i koordinisani uz pomoć društvenih mreža (Fejsbuka i Tvitera, u prvom redu), za šta je određen broj organizatora i osuđen na višegodišnje kazne zatvora, britanski premijer je naveo da se, u saradnji s policijom, razmatra ‘’opcija sprečavanja komunikacije putem ovih internet stranica s obzirom na to da se preko njih organizuje nasilje, neredi i kriminal”.

imajući u vidu da se većina, ako ne i sve društvene mreže, baziraju na ekonomskim principima poslovanja (gdje se omasovljavanje posmatra kao cilj neophodan za globalne marketinške svrhe, od čega se većina društvenih mreža finansira), tehnička (aplikacijska) platforma društvenih mreža je tako koncipirana da od korisnika prikuplja određene podatke neophodne za upoznavanje i komunikaciju sa drugima (što je i suština društvenih mreža), ali isto tako prikupljaju i određene podatke koje, filtriranjem, segmentiraju i koriste u marketinške svrhe. Upravo ova mogućnost zloupotrebe određenih podataka od strane društvenih mreža predstavlja jedan od segmenata narušavanja privatnosti korisnika koji u zadnje vrijeme sve više dobija i određenu globalnu, ali i regionalnu političku i normativnu stranu posmatranja i reagovanja. Usljed navedenog, privatnost na društvenim mrežama je sigurno relativizirana, čemu doprinose kako sami korisnici koji dobrovoljno daju određene podatke o sebi (pristupom i korištenjem društvene mreže), tako i same društvene mreže (prikupljanjem i filtriranjem, te segmentiranjem korisničkih podataka za ciljane marketinške kampanje).

Pored navedenih oblika ispoljavanja određenih kriminalnih aktivnosti na društvenim mrežama ili uz pomoć mogućnosti koje omogućavaju društvene mreže, primijetan je još i cijeli niz kriminalnih aktivnosti koje se ispoljavaju na ovim mrežama. Međutim, pored navedenog, primijetno je da se društvene mreže koriste i u cilju realizacije samo pojedinih faza ili dijelova određene kriminalne aktivnosti, dok se ostatak realizuje na klasičan način. U tom kontekstu, društvene mreže se sve više koriste i u cilju pronalaženja saradnika i samih izvršilaca kriminalne aktivnosti, vrbovanja žrtvi, za pripremanje djela, za prikupljanje relevantnih informacija, za pomaganje u izvršenju određenih aktivnosti, za obezbjeđivanje sredstava...

Izvršioci ili planeri određenih kriminalnih aktivnosti, bez obzira na to da li se radi o tradicionalnim ili savremenim oblicima ispoljavanja ovih aktivnosti, sve više preko društvenih mreža pronalaze saradnike ili i same izvršioce kriminalnih aktivnosti, birajući ih na osnovu afiniteta i sposobnosti koje se mogu zaključiti na osnovu njihovih profila ili postavljenog sadržaja (komentara, snimaka, ličnih podataka). S obzirom na specijalizovanost određenih društvenih mreža (poput *LinkedIna*), razumljivo je da se na tim društvenim mrežama nalaze korisnici koji traže stručnjake za određenu vrstu poslova ili koji imaju određena znanja i vještine. Naravno, činjenica je da dosta korisnika koji posjeduju određena (specifična) znanja i vještine neće pristati na korištenje tih znanja i vještina u kriminalne svrhe, ali je činjenica da će ih određeni broj i pristati, dok određeni broj i neće znati da u potpunosti ili jednim dijelom učestvuje u izvršenju krivičnog djela ili određene kriminalne aktivnosti. Ukoliko se navedenom doda i virtuelni aspekt komunikacije i dogovora prilikom realizacije određene aktivnosti kriminalnog karaktera, činjenica je da ovaj vid kriminalnih aktivnosti u kojima se zahtijeva poznavanje određenih znanja i vještina sve više dobija na značaju pronalaženjem tih izvršilaca preko društvenih mreža.

Imajući u vidu mogućnost filtriranja određenih podataka o korisnicima društvenih mreža (podrazumijevajući ovdje, prevashodno, podatke o starosti, polu, profesiji, mjestu stanovanja...), društvene mreže se koriste i u svrhe vrbovanja žrtvi određenih krivičnih djela ili kriminalnih aktivnosti, primarno za pornografiju i pedofiliju. Naime, pedofili kao savremeni seksualni grabežljivci, koristeći se društvenim mrežama, filtriraju (po polu, starosti i lokaciji stanovanja) podatke o

korisnicima kako bi došli do eventualnih žrtvi, kojom prilikom na razne načine pokušavaju da se zbliže sa potencijalnom žrtvom, a potom da je i neposredno seksualno iskoriste ili u cilju stvaranja pornografskog materijala u pedofilske svrhe.

Korisnici društvenih mreža u ličnoj ili opštoj komunikaciji nesvjesno otkrivaju i određene lične ili zajedničke informacije koje kriminalcima (mogu da) služe prilikom planiranja, organizovanja ili i same neposredne realizacije krivičnog djela ili kriminalne aktivnosti, pa čak im i određeni detalji koje saznaju korištenjem društvenih mreža omogućavaju otežavanje, pa čak i onemogućavanje efikasne ili adekvatne kriminalističke aktivnosti usmjerene u cilju identifikovanja, pronalaženja i hvatanja izvršioca i u cilju rasvjetljavanja cjelokupne kriminalne aktivnosti ili prikupljanja dokaznog materijala. Navedeno je direktna posljedica bezbjednosno-informatičke nepismenosti, odnosno needukovanosti korisnika o bezbjednosnim rizicima društvenih mreža, ali i načina korišćenja društvenih mreža, pogotovo postupanja (dijeljenja) sa određenim ličnim ili sličnim podacima i informacijama.

ZAKLJUČNA RAZMATRANJA

Društvene mreže su postale neizostavan dio naše svakodnevice, a pošto internet projektuje i predstavlja društvo u virtuelnom svijetu, onda se i rizici iz realnog svijeta projektuju u virtuelnom.

Opasnost koja prijeti prilikom korišćenja društvenih mreža jeste u tome što korisnici društvenih mreža objavljuju i otkrivaju veliki spektar informacija o sebi. U zaštiti korisnika na društvenim mrežama neophodna je saradnja svih, primarno samih korisnika, zatim kompanija društvenih mreža i kompanija koje se bave proizvodnjom antivirusa za zaštitu računara i samih krajnjih korisnika usluga.

Jedan od prioritetnih načina borbe protiv ovih pojavnih oblika kriminalnih aktivnosti na društvenim mrežama, a s kojim se korisnici svakodnevno susreću, jeste sve veća emancipacija internauta, pogotovo korisnika društvenih mreža. Najviše pažnje u zaštiti treba posvjetiti korisniku, na način da on odlučuje koje informacije ‘’pohranjuje’’ na internet (društvene mreže), kao i konkretnoj zaštiti ličnih podataka, pogotovo identifikacionih i autentifikacionih podataka. U tom kontekstu, treba omogućiti veću edukaciju i podizanje svijesti korisnika o opasnostima u koje se upuštaju dajući osnovne podatke o sebi, a da se ne pominju drugi detalji privatnosti korisnika. U kontekstu navedenog, neophodno je navesti da se korišćenjem društvenih mreža svaki korisnik odriče dijela svoje privatnosti, tako da sami korisnici trebaju dobro ocijeniti da li će ih neki sadržaj koji daju ili objavljuju ugroziti, te shodno tome odlučiti da ga postave ili ne.

Takođe, kompanije društvenih mreža moraju da misle na svoje korisnike i da obezbijede zaštitu njihove privatnosti, jer je neminovno da će korisnici društvenih mreža početi da traže druge načine umrežavanja, a samim tim kreatori društvenih mreža će gubiti na profitu koji im omogućava upravo masovnost korisnika.

LITERATURA

1. Banović, B., Miladinović, A. (2010). *Kriminološko-fenomenološki aspekt Fejsbuka,* Kriminalističko-forenzička istraživanja, broj 1, Banja Luka: Internacionalna asocijacija kriminalista, dostupno i na: *www.iak-bl.com/images/casopis/volumen1/4.pdf,*
2. Bonneau, J., Preibusch, S. (2009). *The Privacy Jungle: On the Market for Data Protection in Social Networks,* Eighth Workshop on the Economics of Information Security, dostupno na: *www.weis09.infosecon.net/files/156/index.html,*
3. Ivanović, Z., Banović, B. (2010). *Mobilne socijalne mreže – novi rizik visokotehnološkog kriminala,* Zloupotreba informacionih tehnologija i zaštita, Beograd: IT vještak,
4. Miladinović, A., Petričević, V. (2011). *Vršnjačko nasilje na Fejsbuku,* Nasilnički kriminalitet, Banja Luka: Univerzitet Apeiron,
5. Trivić, S. (2011). *Virtuelni zločin i njegovo sankcionisanje,* Strani pravni život, broj 3, Beograd: Institut za uporedno pravo.

Aleksandar Miladinović
MUP RS – Police academy Banja Luka
E-mail: aaleksandarbl@yahoo.com
Vitomir Petričević
MUP RS – Police college Banja Luka
E-mail: vitomir.petricevic@education.muprs.org

CRIMINOLOGICAL ASPECTS OF SOCIAL NETWORKS

Apstrakt: With qualitative and kvanititive expansion of social networks it is noteced that these games cause criminal activites on social networks or tu users these networks. Cause of this is large number of users, security and IT illiteracy, there own non care for security. Environment of social network allows the nearly all phases of certion criminal acts (planning, preparation, finding victims, provision of funds, realization and having the benefits) do from ‘’room’’, using the service over the internet and social networks that is cause of clasic criminal acts (fraud, theft, various forms of violence, terrorism) but also and modern (identity theft, internet piracy, theft of time, various forms of internet violence). In this context, in paper as most frequent (primary on Facebook, Tweetter, YouTube…) we will talk about scams, identity theft, internet piracy, pornography, pedophilia, terrorism, bullying, hate speech.

Kay words: social networks, criminality, identity theft, scams over internet, pedophil

Prethodno saopštenje - UDK 343.326: 004.738.5

INTERNATIONAL ORGANIZATIONS LEGAL STANDARDS FOR COMBATING CRIMINAL ACTS OF HIGH TECH CRIME

Ivana Bodrozic, spec.[1]
Academy of Criminalistic and Police studies, Belgrade
ivana.bodrozic@kpa.edu.rs

Abstract: High tech crime as a form of transnational organized crime can be suppressed only through intensive interstate cooperation, by means of identical or synchronized mechanisms, with clearly harmonized standards for defining, adopting and implementing legal acts related to the suppression of this type of crime. Within the interstate cooperation in this field a number of acts have been issued, of which regional and global regulations have been singled out as significant for the purpose of this essay. The adoption of criminal standards presented in two documents, the Council of Europe's Convention on High Tech Crime and Guide for Fight against the High Tech Crime of the International Telecommunication Union, could create a suitable environment and legal frame for suppression of legal acts of high tech crime.

Key words: High Tech Crime, The Council of Europe's Convention on High Tech Crime, Guide of the Telecommunication Union for Fight against the High Tech Crime for developing countries.

INTRODUCTION

Danger of information-telecommunication technologies misuse have been registered much earlier in the international level than in the Republic of Serbia, since the application of these technologies commenced earlier in other countries and since key segments for their functioning, starting from the state administration itself, through army, institutions for health, education and business, became exposed to attacks and misuses at earlier stage. Apart from preventive protection measures, which were useful but insufficient for prevention of these forms of misuses, numerous countries and their criminal legislations incorporated in their incrimination systems at least several criminal acts for which various types and measures of criminal sanctions are stipulated.

In terms of the high tech crime, one of the priority tasks in the international level is synergic protection of information systems, by use of both preventive and repressive means. Since this is a new type of crime with transnational character, intensive regional and universal interstate cooperation intended for its suppression has been developed within the most significant international organizations and bodies. Each of them, within their own competences, issued relevant legal acts,

[1] Assistant on the Academy of Criminalistic and Police studies, Student of Doctoral studies in the Faculty of Law, Belgrade University.

mainly in form of recommendations, which further channeled stipulating of certain criminal acts in national criminal legislations, the harmonization of which, accompanied by generally accepted operational standards and competences of police and other state authorities, represented good basis for efficient suppression of these illicit behaviors.

THE TERM CYBER SPACE AND STANDARDS OF CRIMINAL LEGAL PROTECTION IN INTERNATIONAL DOCUMENTS

As said by William Gibson[2], cyber space is a digital world in which war for data and information is led among the society in general, multiethnic companies and informatics-pirates. He states that cyber space is: "…a homeland of information age – a place where citizens will live in the future".[3]

According to the online dictionary Webopedia, cyber space is defined as „a metaphor used for describing non-physical terrain created by interconnected computers via telecommunication network for the purpose of communication".[4]

According to David Haken, cyber space is a particular assembly of a number of social and cultural associations established in the moment when people start to use computers and think about those, as well as when computers start functioning as a kind of technology „prosthesis" for human activities.[5]

In our opinion cyber space is a technological space which exists in reality and occurs in a particular moment, the participants of which are real individuals regardless of the possibility for them to adopt new identities. It is not to be strictly separated from the real space, for those are basically two parallel spaces, interconnected and inseparable in many ways, since virtual space is accessed from the so called real one, and since both of them are being used for basically the same activities and operations.

This space is considered to be the fifth most significant domain, apart from the land, sea, air and space. It necessitates the existence of contemporary, internationally accepted legal frame, which would regulate it and in the scope of which uniform standards and codes of conduct would be accepted, as well as the system of sanctions for those disobeying the rules or misusing them. When acknowledged serious threats which this type of criminality poses, numerous international organizations issued and have been issuing legal acts for defining common goals, activities and standards while prescribing and regulating this field in the national legislations.

Interpol is one of the first organizations that started cooperation in suppression of the high tech crime by organizing conferences which defined the

---

[2] Canadian author who used the term cyber space for the first time in 1984 in his science fiction novel Neuromancer, although the usage of prefix cyber is associated with Norbert Winner, a scientist who used it first for the purpose of his research that represented the basis for then new scientific discipline cybernetics.

[3] Gibson, V. (2008), *Neuromancer,* IPS Media, Belgrade.

[4] See Webopedia, http://www.webopedia.com, accessed on May 15, 2011.

5 Panovic, I. (2003): On Cyber Space and Identity, E-volution, no. 1, www.apisgroup.org/ sec.html? id= 29, accessed on December 20, 2011.

international character of this type of criminality and determined legal nature of these criminal acts, characterized by constant change of existing forms and by present element of cross-border organized crime. Primary goal of these conferences was training of regional expert groups in fighting the high tech crime that include international approach. The Interpol made efforts to create, develop and contribute to establishing of international, uniform standards in the field of law, police, investigation and exchange of information on high tech crime. As a necessary assumption in the development of adequate fighting mechanisms for this type of crime, a need is emphasized for better cooperation with Internet providers and creation of legal frame for its functioning, with clearly expressed obligations regarding the availability of certain information, as well as for upgrading the level of their cooperation in electronic evidence exchange.[6]

Organization for Economic Cooperation and Development (OECD) observed the problem of computer crime since 1983, when a Study on international application and harmonization of the criminal law regarding the problems of computer crime and misuses was issued. Subsequently, collections of guidebooks have constantly been published with aim to determine rules and bases for acquiring and maintaining the security of information systems[7]. Such a guide is a Guide for cyber security from 2002, which refers to the application of various standards, the application of which should provide cyber space security for individual users and states. These standards include:

- Awareness of the threatening risks within the computer systems and networks, of their international dimension and of necessity to develop activities for their prevention,
- Responsibility of all sides for security of computer systems and networks,
- Common, coordinate activity for prevention, detection and responding to security challenges,
- Respect of interest of other participants and users of the cyber space,
- Harmonized activities in the cyber space related to security maintenance have to be governed by legal state principles.
- Adequate risk assessment,
- Global activity on harmonization of legal frameworks for suppression of criminal acts in this field,
- Common measures and procedures of gathering and exchange of data and cooperation in criminal matters.

G8 or Group of 8 is the international group comprised of the strongest industrial democratic states: Canada, France, Germany, Italy, Japan, Russia, United Kingdom and United States of America united for the purpose of cooperation in many levels, from international economic affairs, through political and security ones. This group started dealing with issues related to the information-telecommunication technologies and their misuse in cyber space in 1997, by forming subgroups for high tech crime, which adopted first ten standards for fighting the high tech crime that,

[6] See more in: Interpol and cyber crime, www.europol.eu.int

[7] See more in: Putnik, N. (2010): *Cyber Space and Security Challenges,* Faculty of Security Studies, Belgrade, pg. 169.

inter alia, include strengthening of national criminal legislations with aim to adopt uniform illicit behaviors in their own incriminating catalogues, rapid cooperation in investigations related to the Internet and fight against cyber terrorism. G8 continued its activities in various summits on which a common decision had been asserted that unambiguous fight against high tech crime could be carried out only through coordinated activity in the international level, with recommendation to adequately implement regulations from the Council of Europe's Convention on High Tech Crime in national criminal legislations and to leave no space for perpetrators of these criminal acts to escape sanctioning as a consequence of different defining of these forms of criminal acts in different countries.

The Council of Europe started regulating cyber space and cyber crime by adoption of Recommendation on criminal activities related to computer use[8]. The Recommendation presented a list of computer crime offences, which member states should introduce to their national criminal legislations in order to establish harmonized legal regulations[9].

Although prior to the adoption of the Council of Europe's Convention on High Tech Crime, numerous documents have been published on researches from this field[10], the mentioned Convention is appropriately considered to be the most significant regional legal act[11], which is, by its nature, mandatory and which represent the basic guideline for uniform regulation of criminal acts of high tech crime in the member states.

The Convention includes four chapters as follows:

1. Usage of terms;
2. Measures that need to be carried out on the national level – material and process law;
3. International cooperation;
4. Final provisions.

The basic purpose of provisions from the second chapter on material criminal law is to unify provisions of national criminal legislations, in order to make types of illicit behaviors of the same kind recognizable by different legal systems, which enables strong universal fight against this type of national criminality.

---

[8] See more in: The Council of Europe's Recommendation no. (89) 9.

[9] The list included criminal acts of unauthorized computer access, computer fraud, computer sabotage, forging by help of computers, damaging of computer data and programs and, as potentially dangerous, criminalization of criminal acts computer espionage, unauthorized usage and unauthorized alteration of computer data and programs is recommended.

[10] From 1989 to 1995, European committee for criminal law issues published several recommendations concerning the field of criminal-material and criminal-process law. The Recommendation no. 89/9 emphasizes the significance of adequate and timely response to new forms of computer-related criminal acts that usually have transnational character. Upon the Convention's adoption, a Conference on high tech crime took place in 2005 on which a necessity of wider and more rapid implementation of regulations from 2001 Convention was pointed out, while concern was expressed for growing threats and serious harmful consequences of high tech crime in terms of social economic aspect, as well as fear of terrorist activities on the Internet, which is why both private and public sector had been invited to work effectively on further harmonization of the law and its mechanisms.

[11] The extent of Convention's significance is evidenced by the fact that, apart from the member states, non-member states such as USA, Japan, Canada and South Africa also signed and ratified the said Convention.

Four types of criminal acts have been prescribed as follows:

1. ***Criminal acts against confidentiality, integrity and availability of computer data and systems***
   - unauthorized access,
   - unauthorized interception[12],
   - data obstruction,
   - system obstruction and
   - device misuse
2. ***Computer-related criminal acts***
   - Computer-related forging,
   - Computer-related frauds;
3. ***Criminal acts in terms of the content***
   - criminal acts related to children pornography,
4. ***Criminal acts related to violation of copyrights and similar rights***

Apart from the regulations on individual incriminations, each signatory country is obliged to define facilitating and inciting to the perpetration of the said criminal acts as criminal act, while each country is to decide whether the attempt to commit those criminal acts shall be stipulated as punishable.

Responsibility of legal persons is also stipulated as mandatory for criminal acts defined in the Convention when perpetrated by natural person with authorization to represent, make decisions or control.[13]

In terms of sanctions for the mentioned criminal acts, the Convention instructs prescribing of suitable penalties, with mandatory imprisonment sentence and financial fines for legal persons.

Within the ***United Nations Organization*** computer crime is also designated as one of the priority problems of contemporary society in a series of documents, among which the most significant is the Resolution 55-2 from 2000, which determines the need to suppress contemporary technologies misuse and asserts the necessity to unify regulations of criminal acts from this field, which would prevent certain countries to become heavens for perpetrators of criminal acts of high tech crime, due to the lack of incriminations or non-harmonized regulations on international legal assistance in criminal matters.

The International Telecommunication Union (ITU)[14] enacted numerous documents among the most contemporary and the most significant ones is the

---

[12] See more on disharmony between criminal legislation of the Republic of Serbia and the Convention regulations and on barriers for prosecution of perpetrators, as a result of insufficiently extensive definition of the act of perpetration of criminal act from article 298. CC: Kolen-Nikolic, L. (2008): Domestic Legislation Problems in Fight against the High Tech Crime, Magazine for Security, no. 9, Belgrade, pg. 22.

[13] On responsibility of legal persons in the legislation of the Republic of Serbia see more in Stojanovic, Z., Kolaric, D. (2010): *Criminal Legal Response to High Forms of Criminality*, Krimen edition, the Faculty of Law, Belgrade, pgs. 25-34.

[14] The United Nations Organization's Agency dealing with information – telecommunication technologies. It coordinates common global usage of radio spectrum, promotes international cooperation in satellite field, upgrades telecommunication infrastructure by determining common internationally recognized standards of behaviour and business in the mentioned fields. It works on harmonizing views of member states' governments and representatives of industrial sector by continual organizing of regional gatherings worldwide with aim to exchange knowledge, ideas and technologies. It has 191 members and its headquarters is in Geneva. See more in: http://www.itu.int, accessed in December 12, 2011.

Guide on Suppression of High Tech Crime for Developing Countries[15]. This Guide or manual comprises of six chapters dealing with problem to define computer crime concept, its forms, as well as forms of protection and fight against it, with special view on legal frame necessary for regular institutional fight against this type of criminal behavior.

The Guide contains six chapters. ***Introduction*** determines the field of infrastructure and services, advantages and risks, computer data security and computer crime, the international dimension of computer crime and consequences affecting the developing countries.

The second chapter, called ***Phenomenon of computer crime,*** defines computer crime, the existing forms of computer crime, statistical data on criminal acts of computer crime, with special accent on significance of criminal acts against confidentiality, integrity and usage of computer data and systems, as well as criminal acts related to the labels of origin and copyrights, computer-related criminal acts.

The third chapter, called ***Challenges of the fight against computer crime,*** includes three segments dealing with possibilities available in the fight against computer crime, general challenges and legal challenges.

The fourth chapter, ***Strategy for combating cyber crime,*** is composed of four subchapters dealing with problems of legal regulations as strategy segment for fighting computer crime, implementation of the existing strategies, regional differences and significance of computer crime as basis for computer data security.

In line with the very title the chapter, the fifth chapter deals with ***overview of international legal approaches in fight against computer crime***. It gives an overview of international approaches to this problem, regional approaches, scientific approaches, as well as mutual relations between legal and international approaches on one hand, and international and national legal approaches and solutions on the other hand.

The last chapter called ***Legal regulation*** deals with legal framework for fight against computer crime, both from the aspect of material criminal law and processing aspect, marrying it with adopted principles in international cooperation and issues of responsibility of internet service providers.

European Union enacted numerous international acts with aim to suppress high tech crime. The most significant are the Study on legal aspects of computer crime in information society[16], Proposal of the legal framework regarding the attacks on information systems[17], Directive on electronic entrepreneurship[18], Convention on mutual help in criminal matters[19] and Recommendation on strategy for new millennium in protection and control of computer crime[20].

---

[15] ITU Cyber crime guide for developing countries, http://www.itu.int/ITU-D/cyb/cybersecurity/projects/crimeguide.html

[16] Legal Aspects of Computer/ related Crime in the Information Society-COMCRIME, http:// europa.eu.int/ ISPO/ legal/ en/ crime/ crime.htm l

[17] Proposal for a Council Framework Decision on attacks against information systems.

[18] Directive on electronic commerce

[19] Convention on Mutual Assistance in Criminal Matters.

[20] The Prevention and Control of organized crime - A European Union strategy for beginning of the new millennium (OJ 2000 C124, 3.5.2000).

CONCLUSION

All the mentioned international legal acts are the best illustration of how high regional and universal organizations rank the threats posed by high tech crime. This trend has a growth tendency having in mind the increasing development of technology accompanied by a simultaneous development of new forms of misuses.

The registered transnational dimension of this type of criminal activity represents the backbone for cooperation and development of common mechanism for fight against it, primarily through harmonized legal regulations that include organizational-legal and criminal-legal aspect. Adequate and timely response to new forms of high tech crime is possible exclusively by means of harmonized fighting mechanisms, both of preventive and repressive character.

A need to optimize work performance in public and private sector influenced the emergence of a new informatics-technical concept, which is considered to be a feature of new business era and that may appropriately be addressed to as informatics phenomenon of today. The said phenomenon is ***cloudcomputing,*** or SAAS (Software as a Service)[21], which refers to purchasing or renting of the entire information-communication resources from specialized companies[22], which offer those services, for monthly or annual compensation.

The said form of entrepreneurship decreases initial and ongoing expenditures, which is, in time of recession, in the interest of both state and industrial subjects in private sector. Furthermore, it accelerates and facilitates basic functions performance by allowing a specialized company to deal with entire procurement and maintenance of information-communication systems, with dislocating of data to remote servers, which increases, in terms of content and capacity, work space within the internal information systems of subjects that use this type of services.

Apart from indisputable benefits, this type of service leaves space for misuses open because of the very dislocating of data on subject's operational policy and its employees, with absolute digitalization and virtualization, which lessens the possibility of standard, direct control of the existing data. In this digitalized system of processing, safeguarding and updating of data and systems themselves there is a great potential for different forms of misuses regarding the data, secrecy of documents and security in general, which can be perpetrated trough various existing forms of criminal acts, but also by means of some new activities, closely connected with this new type of entrepreneurship.

In that sense, there is a possibility for a programmer to attack software, a possibility of data tampering, from alterations, through deletion and destruction, to their deceptive use for the purpose of obtaining a better competing position on the market or protecting of personal interests, revenge and other motives.[23]

---

[21] See more in: Milasinovic, S. (2010): Optimization of information systems by use of cloudcomputing solution, *Collection of works regarding the misuse of information technologies and protection (ZITEX),* Belgrade-electronic source-cd-rom.

[22] See more in: Microsoftcloud, Googlecloud, Ciscocloud.

[23] A new trend is manifested by misuses of salary lists in enterprises' computer systems, which refer to illicit access to the sector of data on employees, which allows alteration of data on employees, whether by altering the existing or adding new data, in order to transfer the money intended for salaries to other peoples' accounts that could create enormous benefits on yearly bases.

Another danger is posed by activities related to sophisticated computer programs for secret acquiring of information, used for the purpose of espionage, which is not necessarily state operation but can be non-profitable operation as well.

Contemporary technology accomplishments in a car industry, in terms of car networking, which enables incessant 24 hour control of functions by a control center, will enable misuses related to the unobtrusive intrusion to someone else's motor vehicle, without the presence of a direct perpetrator. Those will also enable alteration and tempering with basic functions of a vehicle and their misuse, as means for perpetration of certain criminal acts against the security of public traffic and general security of people and property.

Apart from the mentioned concerns, the number of technical - technological solutions, the misuse of which can potentially be instrument for perpetration of a number of criminal acts, is impossible to observe and accurately state, which in best way illustrates the need to classify these type of criminal acts among the most dangerous ones, for the digitalization of society and dependence to all forms of contemporary information–technological accomplishments is such that we could reasonably say that in the future a great number of criminal acts will, in their certain aspect, be related to computer systems and technology, while the adequate preservation of cyber space security and its participants can be achieved only through adoption and application of a series of legal regulations in the international level, which would represent global contract on cyberspace, cyber security and high tech crime.

LITERATURE:

1. Gibson, V. (2008). *Neuromancer.* Belgrade: IPS Media.
2. Komlen-Nikolic, L. (2008). Domestic Legislation Problems in Fight against the High Tech Crime. *Magazine for Security, no.9,* Belgrade, pp. 20 – 26.
3. Panovic, I. (2003). On Cyber Space and Identity. *E-volution, no. 1*, www. apisgroup.org/ sec.html? id= 29, accessed on December 20, 2011.
4. Polic, V. (2010). Comparative analyses of computer crime in legislation of the Republic of Serbia and some foreign countries. *Collection of works Misuse of information technologies and protection (ZITEX).* Belgrade: Electronic source-cd-rom.
5. Putnik, N. (2010). *Cyber Space and Security Challenges.* Belgrade: Faculty of Security Studies.
6. Stojanovic, Z., Kolaric, D. (2010). ***Criminal Legal Response to High Forms of Crime***. Belgrade. The Faculty of Law. Krimen edition.
7. Schjolbergand, S., Ghernaouti-Helie, S. (2011). *A Global Treaty on Cyber security and Cybercrime*. Second edition.pdf. http://www.cybercrimelaw.net/ documents accessed on February 1, 2012.
8. Chawki, M. (2005). Cyber Crime in France: An Overview. *Cyber Crime Research Center*. http:// www.crime.research.org, accessed on December 10, 2011.
9. Legal Aspects of Computer-related Crime in the Information Society-COMCRIME, http:// europa.eu.int/ ISPO/ legal/ en/ crime/ crime.htm l

10. http:// www.itu.int, accessed on December 12, 2011.
11. http://www.webopedia.com, accessed on May 15, 2011.
12. Interpol and cybercrime, www..europol.eu.int, accessed on January 5, 2012.
13. Legal Aspects of Computer-related Crime in the Information Society-COMCRIME, http:// europa.eu.int/ ISPO/ legal/ en/ crime/ crime.htm l, accessed on January 5, 2012.

REZIME

Visokotehnološki kriminal kao jedan od vidova transnacionalnog organizovanog kriminala može biti suzbijan samo putem intenzivne međudržavne saradnje, upotrebom istih ili usklađenih mehanizama, sa jasno usaglašenim standardima po kojima se pišu, usvajaju i primenjuju pravna akta koja sadrže inkriminacije u vezi sa suzbijnjem ove vrste kriminaliteta. U okviru međudržavne saradnje u ovoj oblasti donošeni su mnogobrojni akti, od kojih su za potrebe ovog rada izdvojeni značajniji regionalni i globalni propisi, koji predviđaju propisivanje krivičnih dela čija će bića po sadržini biti usklađena i onemogućavati stvaranje digitalnog raja za izvršioce ove vrste nedozvoljenih ponšanja. Konvencija Saveta Evrope o visokotehnološkom kriminalu i Priručnik za borbu protiv visokotehnološkog kriminala Međunarodne unije za telekomunikacije predstavljaju dva dokumenta, prihvatanjem čijih pravnih standarda može biti stvoren odgovarajući ambijent i pravni okvir za suzbijanje krivičnih dela visokotehnološkog kriminla.

Prethodno saopštenje - UDK 004.738.5: [341.48+343.326

INTERNATIONAL COOPERATION IN RESPECT OF COMPUTER-RELATED CRIMES

Prof. Anton T. Girginov, PhD
EUPM - Team Banja Luka[1]
anton.girginov@eupmbih.eu

Abstract: The paper addresses the current problems of the international legal assistance in respect of: computer crimes, committed by use of a computer system, and also such ordinary crimes, not committed by use of any computer system, which involve some electronic evidence. International legal assistance in this area is governed primarily by the Council of Europe Convention on Cybercrime. This Convention is intended to supplement existing Council of Europe conventions on co-operation in the penal field in order to make criminal investigations and court proceedings concerning criminal offences related to computer systems and data much more effective, and to enable the successful collection of evidence in electronic form of any other criminal offence. It is designed to strengthen the provision of international support for investigations, prosecutions and trials of computer-related crimes throughout Europe with a specific focus on expeditious preservation and effective transfer of valid electronic evidence. The paper highlights the necessity of fostering professional coordination between international police cooperation activities and international legal assistance, especially when it comes to actions in the delicate and sophisticated cyber crime sphere. The author considers some practical problems of this coordination that limit efficient international cooperation in the fight against computer-related crimes. He recommends that, for the purposes of improving this cooperation, the RS Criminal Assets Recovery Act should be amended to always allow RS authorities to implement the full corpus of international obligations provided for in the Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime.

Key words: cybercrime, international, cooperation, convention, confiscation

INTRODUCTION

1. The fast-paced innovations in communications technology offer organized crime new opportunities for economic and other offences broadly known as Internet, high tech or cybercrime. There is no doubt that such sophisticated organized crime poses a threat to international security and stability in general, and in particular to new, still unconsolidated democracies as well as countries with weak or corrupt governmental and administrative structures. According to estimates by the United Nations, international organized crime has an annual turnover of several hundred billion US dollars. A significant amount of them constitutes a direct or indirect result of committed computer crimes.

[1] E-mail addresses: *agirginov@hotmail.com*.

The Council of Europe's 1990 Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime (ETS No. 141) makes an important contribution to the fight against organized crime. The Council has also been at the forefront of efforts to tackle cyber crime, and its Convention on Cyber Crime (ETS No. 185) signed in Budapest on 23 November 2001 constitutes the first international agreement concerned with fighting this new form of crime. The Convention, together with its Additional Protocol of 01 March 2006 (ETS No. 189), obliges Parties to criminalize certain cyber-related acts, improve their procedural laws for the successful investigation and prosecution of such offences, and provide international legal assistance in respect of them. Bosnia and Herzegovina is a Party to both Conventions: the former entered into force for this country on 01 July 2004 while the latter, together with the Additional Protocol, entered into force on 01 September 2006.

2. As already mentioned, one of the principle aims of the Cyber Crime Convention is to set up a fast and effective regime of international legal assistance in respect of the specific offences defined by this Convention, namely: illegal access, illegal interception, data interference, system interference, misuse of devices, computer-related forgery, computer-related fraud, offences related to child pornography and offences related to copyright and neighbouring rights. The Protocol added the following offences to this list: the dissemination of racist and xenophobic material through computer systems, as well as of racist and xenophobic-motivated threats and insults.

The Cyber Crime Convention focuses on the two leading methods of international legal assistance in criminal matters: extradition and letter rogatory. The legal framework for them has been improved in view of the peculiarities of computer-related crimes.

ACTIVE EXTRADITION

3. Pursuant to Article 24.4 of the Cyber Crime Convention, Parties [such as BiH] that do not make extradition conditional on the existence of a treaty shall recognize the criminal offences, defined by the Convention, as extraditable offences between themselves. BiH may also seek extradition from a country which is not a Party to this Convention. Moreover, BiH may seek extradition from a country with which it has no treaty at all. In this connection it is worth mentioning that very few countries in the world accept the existence of a relevant treaty as the only condition to consider incoming extradition requests. Most of the countries subsidiarily recognize some extra-treaty condition.

Common law countries, in general, extradite on extra-treaty basis to the so-called "designated countries"[2]. Therefore, if BiH is in a common law country's list of designated countries, it may obtain extradition from that country without the existence of any treaty.

When it comes to civil law countries, their extra-treaty condition for extradition is reciprocity. It is noteworthy that there are two ways of invoking

[2] See, for example, Article 40 of the Extradition Act 1999 of New Zealand, Article 45 of the Extradition Act 2003 of Fiji Islands, etc.

reciprocity with such countries, namely: through action or by words. First, any requesting country, including BiH, can invoke **reciprocity by action**. This situation occurs when BiH is requesting extradition from a country whose extradition request it has already considered. The consideration of the request is sufficient to achieve reciprocity; the actual granting of the request is not necessary.

If reciprocity has not been invoked by action, it might be invoked through **reciprocity by words**. This is done by promising (declaring) that the requesting country, including BiH, will undertake to process in good faith future extradition requests from the country being asked to extradite. However, a sole promise is never sufficient. The other country must be certain that law of the requesting country does not prevent its authorities from keeping the promise. Hence, where BiH is that requesting country, it would also be necessary to append to its request a copy of Article 12 (1) of the Law on International Legal Assistance in Criminal Matters which explicitly provides for rendering assistance under reciprocity. Otherwise, the likelihood of honoring the given promice can't be high.

4. According to Article 24.6 of the Cyber Crime Convention, if extradition is refused solely on the basis of the nationality of the person sought, the requested Party shall submit the case at the additional request of the requesting Party to its competent authorities for prosecution and shall report the final outcome to the requesting Party in due course.

Where such case arises in BiH as a requesting country, its competent authorities shall make sure, prior to submitting any such additional request for prosecution, that the requested country has jurisdiction over the criminal offence. If the crime in respect of which extradition is sought has been committed outside the requested country, and the alleged offender has become its national after the commission of the crime, where the crime does not affect interests of that country or any of its nationals, then that country's national criminal law might not be applicable at all. It follows that, on the one hand, the initial request of BiH for extradition of the newly naturalized person, shall be rejected as by the time of the decision on the extradition request [the relevant time for procedural matters] the person in question is already a national of the requested country. On the other hand, the national criminal law of the requested country will not be applicable to the crime of the newly naturalized person crime as by the time of its commission [the relevant time for substantive matters] s/he is not yet a national of that country.

In such case, the requested country's national criminal law would be applicable to the crime committed by the naturalized person wanted for extradition only if that country has: (i) either a rule generally providing, on the grounds of effected naturalization, for retroactivity of the personality principle – to extend the applicability of the foreign country's criminal law to the crimes of all persons who have acquired local nationality in the meantime [e. g. Chapter II, Section 2.2 of the Swedish CC], including the particular crime committed by the naturalized person wanted by BiH for extradition; (ii) or a rule specifically providing, on the grounds of rejected extradition, for exceptional extension of the foreign country's criminal law to the particular crime committed by the naturalized person wanted by BiH for extradition. Thus, according to the former rule, the foreign country's criminal law is applicable to the crime in question because it is one of the crimes committed by persons naturalized afterwards, while according to the latter rule, the foreign

country's criminal law is applicable to the crime in question because it is a crime in respect of which an incoming extradition request has been rejected.

Article 123 (2) CC of RS is similar to the latter rule. It also prescribes such exceptional extension of territorial applicability of local criminal law to make it applicable to the particular criminal offence in respect of which another country has sought the extradition. However, in this Article the wanted person is a foreigner rather than any of its nationals, including those which have acquired BiH/RS nationality by naturalization.

There is also an international rule which provides subsidiarily for the exceptional extension of territorial applicability of the criminal law of a requested country to make it applicable to the particular criminal offence but this rule is found only in the European Convention on Transfer of Proceedings in Criminal Matters [ETS No. 73] - in force for BiH as of 26 July 2005. According to its Article 2.1, for the purposes of applying this Convention, any of its Parties shall have the competence to prosecute under its own criminal law any offence to which the law of the respective requesting country is applicable. Hence, if BiH as the requested country has agreed to take over some criminal proceedings but cannot apply its own criminal law to the offence on the basis of its territoriality principle, or of its personality principle, or of its or reality (protection, passive personality) principle [thus, having no original jurisdiction over it], this country shall, nevertheless, apply its criminal law on the basis provided for in the aforementioned Article 2.1. This conditionally expanded criminal jurisdiction grounded exclusively on this Article is called subsidiary jurisdiction.

At the same time, neither the Cyber Crime Convention, nor any extradition agreement, including the European Convention on Extradition [ECE, ETS No. 24], contains a rule introducing any expanded jurisdiction (unconditional or conditional) over crimes of naturalized nationals of requested countries, regardless of the circumstances. Neither the quoted Article 24.6 of the Cyber Crime Convention, nor the identical Article 6.2 of the ECE ["*If the requested Party does not extradite its national, it shall at the request of the requesting Party submit the case to its competent authorities in order that proceedings may be taken if they are considered appropriate*"] is being interpreted as providing any possible ground for expansion of the extraterritorial jurisdiction of the requested country to the criminal offence in respect of which extradition has been sought. Hence, to avoid efforts in vain (useless if not counterproductive, benefiting fugitive offenders only), the competent authorities should not rely on any foreign country that can't apply its national criminal law to the criminal offence in respect of which extradition is being sought. Although Paragraph 6 of Article 24 applies the principle "*aut dedere aut judicare*" (Latin: "extradite or prosecute"), it does not necessarily guarantee this result automatically. Where the other country cannot exercise any jurisdiction over the criminal offence, the BiH authorities should not send to it any additional request for prosecution. Instead, they would need to consider an alternative approach to dealing with the fugitive offender that could increase likelihood of imposing punishment on him/her, if found guilty.

5. There are also some other tactical problems relating to active extradition. Given the knowledge, skills and information in possession of many cyber crime perpetrators, international searches should be meticulously planned. The issue is

being highlighted because following practices have been observed in some new countries when the whereabouts of the wanted person is not known. In such situations, some police officers (often encouraged by prosecutors and judges) try to locate the person by means of one or more international police requests, and if successful, notify the prosecutor (if the person is a suspect) or the judge (if the person is accused or sentenced) about that person's country of current residence. Then, once the prosecutor or the judge, correspondingly, learns the exact country where the wanted person resides, s/he initiates the procedure for his/her provisional detention pending the official extradition request.

Such an approach shall not be encouraged. On the one hand, any such request for international location is not necessary. Once the active extradition file is ready, the next step should be the request for international search and provisional arrest of the fugitive offender (Article 16 of the ECE). Thereafter, the police may conduct any supporting operation. On the other hand, requests solely for international location are not only unnecessary but are also risky for two reasons.

- Police in other countries are not always careful with foreign cases. When checking the identity of the person sought, they may alert him/her that some other country is interested in obtaining his/her extradition. This may cause the person to flee to another foreign country where his/her extradition to BiH is less possible or impossible.
- Additionally, the request for international location may be mistakenly understood as a request for a provisional arrest. Such mistakes are not uncommon and may be made not only by the police but also by foreign courts. If the person is put under provisional detention pending the extradition request all supporting documentation must be compiled in a very limited period of time, almost never exceeding 40 days – the general deadline for provisional detention. The requesting country will most likely be unable to meet this deadline. Consequently, the time period for detention will expire before the extradition request is received. The person will be released and may flee to another foreign country where his/her extradition to BiH is less possible or impossible.

The released fugitive obviously has no interest in waiting patiently for the BiH authorities to prepare and send the fully documented request for extradition. Instead, it is more likely s/he will flee to a country where extradition to BiH is more difficult or impossible. If this happens several times, even with different persons, other countries are likely to reach the conclusion that BiH authorities do not respect the right to liberty and human rights, in general, which constitutes a sufficient ground for rejecting future requests of BiH for extradition.

- Finally, as most fugitives are identified and apprehended while passing the international border control, it does not make sense to try to discover their place of residence in order to trigger the procedure: the provisional detention procedure and thereafter it the extradition itself. It is sufficient to circulate the request for the provisional arrest via INTERPOL in accordance with Article 16 ECE, where applicable. If there is some spontaneous information of the whereabouts of the person, it might be mentioned in the request without any high expectations that s/he will be found there.

OUTGOING LETTERS ROGATORY

6. As per Article 23 of the Cyber Crime Convention, international legal assistance shall be extended to all criminal offences related to computer systems and data as well as to the collection of evidence in electronic form related to any criminal offence. This means that either where the crime is committed by use of a computer system, or where an ordinary crime not committed by use of a computer system, e. g. murder, involves electronic evidence, the terms of the Cyber Crime Convention on international cooperation are applicable.

The Cyber Crime Convention foresees a Speciality Rule. Unlike the speciality rule in extradition cases (Article 14 of the ECE), this one is not mandatory. It is optional depending on the discretion of the requested country. Pursuant to Article 28.2 of the Convention the requested Party may make the provision of evidence (information or material) in response to a request dependent on conditions which require that the evidence obtained is: (a) kept confidential where the request for mutual legal assistance could not be complied with in the absence of such condition, and/or (b) not used for investigations or proceedings other than those stated in the request. When the requesting Party accepts the condition, it shall be bound by it. This provision guarantees the requested Party that in cases involving the provision of sensitive information or material, its use is limited to that for which the assistance is granted, and the information or material is never disseminated beyond officials of the requesting Party. These restrictions provide safeguards that are available for, *inter alia*, data protection purposes.

7. Taking into account the specific peculiarities of cyber crime and traces left behind, the Convention introduces an innovation which is not inherent in other letters rogatory. This is an innovation which reflects the volatile nature of electronic evidence and carries some similarity to the provisional arrest of persons sought for extradition – Article 16 of the ECE. In cases of ordinary letters rogatory no provisional seizure of any item (or information piece) or any other provisional measure might be requested in advance, even where the item in question will be later requested as physical evidence by means of the letter rogatory. Everything should be requested simultaneously, through this letter rogatory.

In contrast, Article 29 [Expedited preservation of stored computer data] of the Cyber Crime Convention postulates that a Party may request another Party to order or otherwise obtain the expeditious preservation of data stored by means of a computer system, located within the territory of the other Party, in respect of which the requesting Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data. Any preservation in response to such a request shall be for a period not less than sixty days, in order to allow sufficient time to the requesting Party to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data. Following the receipt of the request, the data shall be preserved pending a decision on the request.

Additionally, the requested country is obliged to notify the requesting country if the track leads to a third country and provide sufficient information to the requesting country to enable it to request legal assistance from the third country. According to Article 30 [Expedited disclosure of preserved traffic data] of the Cyber Crime Convention, where, in the course of the execution of a request to preserve

traffic data concerning a specific communication, the requested Party discovers that a service provider in another State was involved in the transmission of the communication, it shall expeditiously disclose to the requesting Party a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted.

Articles 29 and 30 of the Cyber Crime Convention therefore express and confirm the inevitable idea that the urgent measures which are needed to preserve computer data at the national level (see Articles 16, 17 of the Convention) are also necessary at the international level, within the framework of international cooperation. Otherwise, the efficiency of the collection of evidence for almost all crimes mentioned in the Convention would significantly drop. If countries do not share computer data quickly, the electronic trail will simply disappear.

8. As in the case with extradition, international police cooperation activities should not aim to assume the functions of international legal assistance in criminal matters. It has been observed in some countries that, prior to ordering any official investigation, some prosecutors start gathering information from abroad through police officers about criminal offences. The prosecutors gather the information for the purpose of establishing whether they can have, as a result, grounds for suspicion that a reported criminal offence has actually been committed. This information though, being gathered in a non-judicial way, can be used only to substantiate the order for the conduct of the investigation into the crime. Subsequently, if the prosecutor has to prove the crime with some evidence from abroad, s/he will inevitably need a letter rogatory **for the same facts**.

In any case, it is the lesser evil to open an official investigation without sufficient information and resort to a letter rogatory rather than clarify the same facts twice: *first*, in a non-judicial way, and *thereafter*, through a letter rogatory. Otherwise, the requesting authorities are more likely to benefit suspects rather than justice. The reasons are the following.

First of all, any approach of this sort eliminates the element of surprise which should be inherent in any evidence gathering process and may, most probably, warn the criminals and other interested persons of what is likely to be officially requested. This, in turn, can afford them the chance to find the person who made the statement and intimidate him/her as a potential witness when it comes to his/her oral evidence. In relation to documentary evidence, criminals can take the opportunity to destroy, modify or replace the paper whose copy has been obtained through international police cooperation. Second, the abovementioned approach of double work causes serious delays in criminal proceedings with all accompanying negative consequences. Third, the said approach may prepare the grounds for the requested country's refusal to execute your letter rogatory:

- The authorities of the other country may have already regarded the initial non-judicial request as a letter rogatory. In this case (i) if they have denied its execution, they are likely to say: "*We do not need to reject your request again*"; (ii) if the authorities of the other country have already executed the previous request, the non-judicial one, they are likely to say: "*We do not need to execute the same request again*".
- If the requested certified copy is of a bank document or another confidential document, the authorities of the other country may

conclude that BiH has illegally obtained the first copy and any further assistance in relation to the same issue poses danger to the "*security, ordre public or other essential interests of their country*" as such a situation constitutes grounds for refusal to render international legal assistance – see Article 28.4.b of the Cyber Crime Convention, Article 2.b of the European Convention on Mutual Assistance in Criminal Matters [ETS No. 30].

9. Trying to improve the legal framework for letters rogatory, the current HJPC project **"SUPPORT TO JUSTICE IN BiH – STRENGTHENING PROSECUTORS IN THE CRIMINAL JUSTICE SYSTEM, Component "A" (Project component "A2")"** proposes that any obtained evidence shall be considered lawful and admissible only if it has been collected in accordance with procedures of requested countries – Part IV, Proposal No. 1.1[3].

Such an innovation is not recommendable and should not be supported. The domestic law of the requested country is not necessarily applicable to the execution of the letter rogatory. Pursuant to Article 8 [Procedure] of the Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters [ETS No. 182], where letters rogatory specify formalities or procedures which are necessary under the law of the requesting Party, even if unfamiliar to the requested Party, the latter shall comply with the request to the extent that the action sought is not contrary to fundamental principles of its law[4].

Article 28.3 of the Cyber Crime Convention is a replica of the quoted Article 8 of the Second Additional Protocol. Article 28.3 reads: *Mutual assistance requests … shall be executed in accordance with the procedures specified by the requesting Party, except where incompatible with the law of the requested Party.* Therefore, should the newly proposed text on evidence from abroad be drafted with precision, this text must be in the sense that obtained evidence is lawful and admissible if the letter rogatory has been executed in accordance with the applicable procedures in requested countries.

There is a more serious problem to be considered here. So far any requesting country that has received an execution of its letter rogatory presumes without discussions that the judicial authorities of the requested country have complied with the laws applicable in their territory, especially when these laws are their own.

---

[3] Its text literally proposes "*Amendments to article 10 of CPC BiH and corresponding articles of CPC RS, FBiH and BD in the sense of defining lawfulness of evidence obtained through the International legal aid in accordance with procedures of countries where the evidence was obtained (this provision on accepting the evidence gained through the international legal aid and in accordance with the law of the State where they have been gathered can be prescribed by the Law on International Legal Aid and CPC Provisions of entities that regulate these matters)*".

[4] Thus, for example, a requesting Party cannot require the requested Party to execute a search and seizure that would not meet the requested Party's fundamental legal requirements for this measure. In light of the limited nature of the obligation, it was agreed that the mere fact that the requested Party's legal system knows no such procedure is not a sufficient ground to refuse to apply the procedure requested by the requesting Party; instead, the procedure must be incompatible with the requested Party's legal principles. For example, under the law of the requesting Party, it may be a procedural requirement that a statement of a witness be given under oath. Even if the requested Party does not domestically have the requirement that statements be given under oath, it should honour the requesting Party's request [see Council of Europe Explanatory Report to the Convention, p. 267].

But if the aforementioned legislative proposal is accepted, it will, undoubtedly, make the issue a part of the subject of proof. Hence, the innovation is likely to open the way to endless discussions triggered by defense in local courts as to whether the applicable law (whatever it is) has been complied with in the requested county. In some cases, a second letter rogatory to the same foreign country might become necessary to verify that the initial one has been executed properly.

INTERNATIONAL COOPERATION IN CONFISCATION MATTERS

10. Computer-related forgery, fraud and other computer crimes generate, directly or indirectly, enormous amounts of material gain for participants. In turn, this unjust gain gives offenders further powers to commit new crimes. To address this phenomenon and cut the circle, society is in need of a reliable and effective system of confiscation of crime proceeds. The RS has made a remarkable progress with the enactment of the Criminal Assets Recovery Act [CARA] in 2010. This Act provides for confiscation of "unexplainable property" found in the territory of the RS where a crime (specified in Article 2 of the Act) has been committed, local criminal law is applicable to it and, above all, this crime has been ascertained by a local judgment – Article 28 of the Act. The problem is that CARA does not prescribe confiscation if local criminal law is not applicable to the conditioning crime and, therefore, no judgment to ascertain it might be issued. It follows that CARA is not well synchronized with the European Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime (1990) which requires some domestic law "extension" for its actual implementation in all cases where confiscation is appropriate. According to Article 13 of the Convention,"*a Party, which has received a request made by another Party for confiscation concerning instrumentalities or proceeds, situated in its territory, shall: (a) enforce a confiscation order made by a court of a requesting Party in relation to such instrumentalities or proceeds; or (b) submit the request to its competent authorities for the purpose of obtaining an order of confiscation and, if such order is granted, enforce it*". Further on, pursuant to the same Article "t*he procedures for obtaining and enforcing the confiscation shall be governed by the law of the requested Party*"; under Article 15, "*Property confiscated by a (requested) Party …, shall be disposed of by that Party in accordance with its domestic law*".

Obviously, the Convention makes no exception for cases when the requested country's criminal law is not applicable to the crime conditioning confiscation, and does not free from the obligation to confiscate on incoming international request any requested country, including BiH/RS, on the grounds that its national criminal law is inapplicable. The importance of such confiscation, even though conditioned by a crime to which the requested country's law shan't be applied, is beyond reasonable doubt nowadays.

It is true that if the assets wanted for confiscation are located in RS/BiH as a requested country, this usually constitutes a clear indication of money laundering crime committed in its territory substantiating the applicability of its national criminal law. It seems that, once BiH/RS authorities receive an international request for confiscation, they can institute criminal proceedings over money laundering to

obtain a local judgment ascertaining the commission of this crime and proceed with the requested confiscation.

In practice though, such money laundering is hardly provable, let alone ascertainable by a local judgment. It follows that in almost all cases of incoming requests for confiscation conditioned by crimes, committed beyond the territory of RS/BiH to which its criminal law is not applicable its authorities would, inevitably, break the quoted Article 13 of the Convention. To avoid such systematic violations that are counterproductive to domestic budget as well (see the quoted Article 15 of the Convention), the CARA should provide for confiscation procedure that is triggered solely by incoming international requests for confiscation where the conditioning crime does not fall within local jurisdiction but has been ascertained, for example, by a judgment in the requesting country.

LITERATURE:

1. Antinori, A. (2008). Information Communication Technology and Crime: The Future of Criminology. *Rivista di Criminolgia, Vittimologia e Sicurezza* (*In English: Journal of Criminology, Victimology, and Security*), year 2, no. 3, pp. 23–31. http://www.vittimologia.it/ rivista/articolo_ antinori_2008-03.pdf.
2. Cédras, J. (2006). Un aspect de la cybercriminalité en droit français: Le téléchargement illicite d'œuvres protégées par le droit d'auteur. (In English: An aspect of cybercrime in French law: The illicit downloading of works protected by intellectual property rights). *Revue internationale de droit penal.* (*In English: International review of penal law*), no. 3–4, pp. 589–610.
3. Clough, J. (2010). *Principles of Cybercrime*. Cambridge, UK; New York: Cambridge University Press.
4. Kempa, D. (2006). *Angriff auf Netze und Systeme: Hackerkultur zwischen gesellschaftlicher Anerkennung und Kriminalisierung. (In English: Attack on Networks and Systems: Hacker Culture between Social Recognition and Criminalization)*. Dissertation. Germany: University of Hamburg. http://www.sub.uni-hamburg.de/opus/volltexte/2006/ 3025/ index.html.
5. Quéméner, M. (2008). Cybercriminalité: Aspects stratégiques et juridiques. (In English: Cybercrime: Strategic and legal aspects). *Défense nationale et sécurité collective (In English: National defense and collective security)*, no. 5. http://www.droitalenfance.com/ download/Quemener [1].pdf.
6. Sokol, B. (2006). *Achtzehnter Datenschutz- und Informationsfreiheitsbericht. (In English: Eighteenth Data Protection and Information Freedom Report).* Landesbeauftragter für Datenschutz und Informationsfreiheit (In English: State Representative for Data Protection and Information Freedom). Germany: North Rhine – Westphalia. https://www.ldi.nrw.de/mainmenu_Service/ submenu_Berichte/index.php.
7. Vekhov, V. (2004). *Aktual'nyye voprosy rassledovaniya prestupleniy, sovershennykh s ispol'zovaniyem plastikovykh kart. (In English: Current issues in investigation of crimes committed using plastic cards).* Computer Crime Research Center, November 25, 2004. http://www.crime-research.ru.
8. Vetter, J. (2002). *Gesetzeslücken bei der Internetkriminalität. (In English: Gaps*

in the Law regarding Internet Crime). Dissertation. Germany: University of Konstanz. http://www. ub. uni- konstanz.de/kops/volltexte/2002/927/pdf/diss_ vetter.pdf.

9. Vitaline, V. (2006). *Cybercriminalité–Délinquance financière différentes escroqueries liées aux réseaux informatiques. (In English: Cybercrime–Various forms of financial fraud related to data networks).* Master's Thesis. France: Université Paul Cézanne d'Aix-Marseille.
10. Vulpiani, D. (2007). La nuova criminalita informatica. Evoluzione del fenomeno e strategie di contrasto. (In English: New computer criminality: Evolution of the phenomenon and strategies to combat it). *Rivista di Criminologia, Vittimologia e Sicurezza* (*In English*: *Journal of Criminology, Victimology, and Security),* year 1, no. 1, pp. 46–54. http://www.vittimologia.it/ rivista/vulpiani% 202007-01-01.pdf.

SUMMARY

Generally, the methods [forms] of international legal assistance in criminal matters are the basis for the differentiation of the legal framework for this assistance. That is why the methods of the assistance (extradition, letters rogatory, recognition of foreign judgments, etc) are governed by such sets of rules which are very different from one another. Nevertheless, the character of the criminal offences in respect of which the assistance is being requested and rendered also exercises some influence on the legal framework for this assistance. Cybercrime seems so far to be the most typical example. Given the volatile nature of electronic evidence, the legal regulations governing both local criminal proceedings and international legal assistance handling such evidence are in need of significant specialization. In order to ensure prompt preservation and successful collection of necessary electronic evidence, the applicable legal regime (both domestic and international) needs to be strengthened by additional rules, such as the rules described in Articles 16, 17 the Council of Europe Cyber Crime Convention on expedited preservation of stored computer data, and the rules of Articles 29, 30 of the same Convention on urgent provisional measures of international aid. In any case, the urgent measures which are needed to preserve computer data at the national level are also necessary at the international level, within the framework of international cooperation.

It is well known that cybercrime perpetrators are masters in the commission of their crimes and also have knowledge, skills and good current information on avoiding justice. In turn, this makes it necessary for police, prosecutors and judges to avoid mistakes when obtaining the extradition of these offenders, or information and evidence from abroad in relation to their crimes. In many cases, such mistakes are likely to benefit the offenders rather than justice. It is noteworthy that most mistakes come from insufficient coordination between international police cooperation activities and international legal assistance. This requires the authorities to take appropriate action to address and resolve the practical problems of this specific coordination without delay.

It is truly important that domestic law includes all necessary provisions for the execution of incoming international requests for confiscation of proceeds from cybercrime and all other criminal offences as well. Regretfully, the CARA does not allow for the execution of other countries' requests for confiscation in respect of those crimes committed abroad to which local criminal law is inapplicable. This legislative gap prevents the local authorities from always implementing Article 13 of the Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime which makes no difference as to whether the requested country's national criminal law is applicable to the crime in question or not. The filling-out of this gap will provide a good example to the state level lawmakers as to how to improve the text of the draft Criminal Assets Recovery Act of BiH which is actually a replica of the CARA.

Prethodno saopštenje - UDK 343.541/.545-053.2/.6

DJEČIJA PORNOGRAFIJA KAO OBLIK NASILJA NAD DJECOM I VISOKOTEHNOLOŠKOG KRIMINALA

Mirela Jokić
Uprava za policijsko obrazovanje Banja Luka
mirelajokic@rocketmail.com

Apstrakt: Dječija pornografija kao jedan od oblika nasilja nad djecom, usljed stalnog razvoja informacionih i komunikacijskih tehnologija i računarskih mreža, usko je vezana za visokotehnološki kriminal. Internet kao pravno neregulisan prostor omogućava brojna nezakonita djelovanja u vidu distribucije pornografskog sadržaja, naročito putem zatvorenih foruma. Ovim radom se nastoji dati doprinos sagledavanju ozbiljnosti situacije u kojoj se nalazi društvo, a prije svega djeca i maloljetnici, zbog prisutnosti i širenja negativnih pojava vezanih za dječiju pornografiju i visokotehnološki kriminal. Takođe se želi ukazati na odlučnost i nastojanja pojedinih međunarodnih struktura da skrenu pažnju i obavežu nacionalna zakonodavstva da, prije svega, inkriminizuju oblast dječije pornografije i visokotehnološkog kriminala i da urede funkcionalnu organizaciju specijalizovanih državnih organa koji će se preduzimanjem odgovarajućih mjera, u skladu sa svojim nadležnostima, uspješno suprotstaviti ovom obliku kriminala.

Ključne riječi: nasilje nad djecom, dječija pornografija, visokotehnološki kriminal, internet, policijski i pravosudni organi.

UVOD

Nasilje nad djecom, bez obzira da li se dešava unutar porodice ili izvan nje, predstavlja veliki problem cjelokupne zajednice, kako u domaćim tako i u međunarodnim okvirima. Ono se ne može i ne smije posmatrati izdvojeno od problema nasilja uopšte.

Predmet ovog rada jeste oblast dječije pornografije kao jedan od oblika nasilja nad djecom i njegova veza sa visokotehnološkim kriminalom.

Dječija pornografija nastaje i prenosi se najčešće putem računara, internet stranica, foruma i sl., i upravo iz ovih specifičnih uslova u kojima nastaje i prenosi se vidljiva je njena povezanost sa visokotehnološkim kriminalom. Isto tako, ta činjenica predstavlja problem gotovo svim državama i njenim strukturama, koje se bave ovom problematikom, da otkriju i sprječe pojedina djela dječije pornografije. Ipak, većina država, poštujući međunarodne standarde i propise, izrazila je spremnost da se suoči sa problemom kakav je dječija pornografija, i počele su od onog najprioritetnijeg, a to je pravno uređenje materije nasilja nad djecom i dječije pornografije, pa do stvaranja specijalizovanih timova sa posebno obučenim kadrom za borbu u toj oblasti.

POJAM NASILJA NAD DJECOM SA ISTORIJSKIM OSVRTOM

Iako se radi o pojavi koja traje od najstarijih vremena i prisutna je u gotovo svim državama i vremenskim epohama, određivanje pojma nasilja nad djecom nije jednostavno, pa se u tom smislu u literaturi i javnom komuniciranju koriste različiti izrazi kao: zanemarivanje djece, zlostavljanje, zapostavljanje, vaspitno zapuštanje, seksualna zloupotreba djece, iskorišćavanje djece, itd.

Ako bismo sve ove izraze pokušali da obuhvatimo jednim opštevažećim pojmom nasilja nad djecom, prilikom definisanja ove pojave opet se nalazimo pred teškim zadatkom, jer kao što ne postoji opšteprihvaćena definicija nasilja uopšte, tako ne postoji jedinstven stav ni oko pojmovnog određivanja nasilja nad djecom.

Pošto ne postoji tačno određen pojam nasilja nad djecom, to su pojedine države u svojim zakonodavstvima objašnjavale ovaj pojam kroz pojedina krivična djela, što je slučaj i u zakonodavstvu Republike Srpske, gdje se nasilje nad djecom povezuje sa sljedećim krivičnim djelima:

- vanbračne zajednice sa maloljetnim licem;
- oduzimanja maloljetnog lica;
- zapuštanja i zlostavljanja maloljetnog lica;
- nasilja u porodici;
- izbjegavanja davanja izdržavanja;
- rodoskvrnjenja;
- polnog nasilja nad djetetom;
- iskorišćavanje djece i maloljetnih lica za pornografiju;
- proizvodnja, posjedovanje i prikazivanje dječije pornografije (Babić i Marković, 2009: 387).

Ukratko, kada se sagledaju krivična djela vezana za nasilje nad djecom, može se reći da nasilje nad djecom predstavlja bilo koje djelo kojim se nanosi fizička, psihička i seksualna patnja djeci ili ekonomska šteta po njih, kao i prijetnje takvim djelima ili propuštanje činjenja dužne pažnje prema djeci.

Kada se govori o nasilju nad djecom, mora se uzeti u obzir činjenica da ta pojava postoji od davnina, jer mnogi podaci ukazuju na to da su djeca oduvijek bila predmet određenog negativnog djelovanja od strane odraslih, pa je tako u antičkom periodu i u starom Rimu zabilježeno da novorođenčad nisu imala pravo na život dok im to pravo nisu formalizovali očevi, a djeca rođena sa deformitetom nerijetko su bila ubijana odmah po rođenju, kao što se dešavalo u Sparti, i takvo stanje je trajalo sve do pojave hrišćanstva (Faktopedija, 2005: 380).

Nasiljem nad djecom i u ranijim periodima, kada ova pojava nije privlačila toliku pažnju javnosti, bavili su se psiholozi, sociolozi, istoričari, ljekari, pisci, itd., pa se u tom smislu posebno ističe francuski doktor Pol Bernard, autor djela "Des Attentats a la pudeur sur les petites filles" (Nasrtaji na nevinost malih djevojčica), u kojem se on bavi seksualnim zlostavljanjem djece u 19. vijeku u Francuskoj, i posebno naglašava seksualna zlostavljanja djevojčica i zataškavanje tih djela od javnosti, koje je, nažalost, prisutno i danas, ne samo u Francuskoj već i u drugim državama. Ipak se mora naglasiti da su ove pojave zataškavanja i skrivanja nasilja nad djecom i njihovih počinilaca, a posebno nasilja nad ženskom djecom, češće u nerazvijenim zemljama, gdje je odnos prema ženskoj populaciji uopšte praćen određenim predrasudama koje su nerijetko izražene negativnim i omalovažavajućim stavom prema ženama.

Uprkos nastojanjima društava, posebno onih u savremenim državama, da skrenu pažnju na problem nasilja nad djecom i da pokušaju da zaštite djecu i njihove interese, svakodnevno smo svjedoci sve sofisticiranijih vidova nasilja nad djecom, a posebno u tim istim savremenim državama sa visokim životnim standardom stanovništva.

Da je u današnjim uslovima došlo do porasta nasilja nad djecom, govore i podaci Međunarodne unije za zaštitu djetinjstva, koji kažu da u visokorazvijenim zemljama više djece strada od svojih roditelja nego od tuberkuloze, dječije paralize, boginja i sl.[1], što je samo po sebi podatak koji treba da bude alarm svim državama da se ozbiljno počnu baviti ovom problematikom i da koriste sva raspoloživa sredstva u borbi sa nasiljem nad djecom i za njegovo iskorjenjivanje.

POJAM VISOKOTEHNOLOŠKOG KRIMINALA

Većina definicija odnosno pojmova visokotehnološkog kriminala svodi se na to da visokotehnološki kriminal obuhvata skup krivičnih djela gdje se kao objekat izvršenja i kao sredstvo za izvršenje krivičnog djela javljaju računari, računske mreže, računski podaci, kao i njihovi produkti u materijalnom i elektronskom obliku. Ova definicija uključuje veliki broj zloupotreba informacionih tehnologija, kao i oblast zloupotreba u radio-difuznim tehnologijama.

Ipak, još uvijek ne postoji opšteprihvaćena definicija visokotehnološkog kriminala. U najširem smislu može se reći da je visokotehnološki kriminal svaka kriminalna djelatnost koja se vrši uz upotrebu računara i računarskih sistema i mreža, a opseg ovih radnji je veoma širok i raznovrstan i podrazumijeva različite vrste nedozvoljenih radnji, od neovlaštene distribucije piratizovanih autorskih djela, uključujući i dječiju pornografiju do višemilionskih krađa, koje se vrše putem neovlaštenog korišćenja računarskih sistema i pristupa bankarskim računima (Jerković, 2009). Broj i vrste krivičnih djela iz oblasti visokotehnološkog kriminala, kao i ekonomsku štetu koja nastaje izvršenjem ovih djela veoma je teško procijeniti. Međutim, broj izvršenja ovih krivičnih djela u stalnom je porastu, a načini njihovog izvršenja, zbog same prirode savremenih informacionih tehnologija, veoma su raznoliki i sve sofisticiraniji (Jerković, 2009).

Imajući u vidu brojnost i raznovrsnost radnji kojima se vrše djela kvalifikovana kao kompjuterski kriminal, precizno definisanje ove pojave zahtijeva izdvajanje određenih zajedničkih karakteristika koje se odnose i na radnju izvršenja i na objekat napada, pa se kao sveobuhvatna definicija može prihvatiti ona koja kompjuterski kriminal definiše kao radnju koja se vrši uz pomoć računara i drugih sličnih tehnologija usmjerenih na:

- neovlašćen pristup zaštićenom računaru;
- neovlašćeno presretanje elektronskih podataka koji su upućeni sa računara ili ka drugom računaru;
- uništavanje, izmjenu i brisanje elektronskih podataka;
- ometanje funkcionisanja računarskog sistema putem oštećenja, brisanja ili mijenjanja elektronskih podataka;

[1] dostupno na: http://www.njcap.org/, 10. marta 2009.

- distribuciju nedozvoljenih sadržaja i
- stvaranje i širenje virusa (Jerković, 2009).

Visokotehnološki odnosno komjuterski kriminal, kao što je već naglašeno, vrši se uz upotrebu računara, računarskih sistema i iz različitih pobuda, a može biti sistematizovan i kao:

1. Politički
   - sajber špijunaža;
   - hakovanje;
   - sajber sabotaža.
2. Ekonomski
   - internet prevare;
   - hakovanje;
   - piraterija softvera;
   - sajber industrijska sabotaža.
3. Proizvodnja i distribucija nedozvoljenih i štetnih sadržaja
   - dječija pornogrfija;
   - pedofilija;
   - zloupoteba žena i djece;
   - vjerske sekte.
4. Povreda privatnosti
   - nadgledanje pošte;
   - prisluškivanje i snimanje;
   - praćenje.

DJEČIJA PORNOGRAFIJA KAO OBLIK VISOKOTEHNOLOŠKOG KRIMINALA

Dječja pornografija, kao vid visokotehnološkog kriminala, predstavlja svaki sadržaj koji vizuelno predočava dijete uključeno u stvarno ili simulirano seksualno eksplicitno ponašanje ili bilo kakvo prikazivanje dječijih polnih organa, prvenstveno za seksualne svrhe. Prema članu 20. Konvencije Savjeta Evrope o zaštiti djece od seksualnog iskorišćavanja i seksualnog zlostavljanja, prestupi povezani sa dječijom pornografijom uključuju sljedeće namjerno bespravno ponašanje, kao što je:

- stvaranje dječije pornografije;
- nuđenje ili omogućavanje dostupnosti dječije pornografije;
- distribucija ili prenošenje dječije pornografije;
- nabavljanje dječije pornografije za sebe ili druge;
- posjedovanje dječije pornografije;
- svjesno pristupanje, preko informacijskih i komunikacijskih tehnologija, dječijoj pornografiji (Ajduković, 2012: 254).

Visokotehnološki kriminal, upravo iz razloga što nastaje korišćenjem savremenih kompjuterskih sistema i mreža, predstavlja dobro zaštićenu i skrivenu bazu za mnoge zloupotrebe tih i takvih sistema, od kojih se posebno izdvajaju djela vezana za dječiju pornografiju. Ono što je karakteristično za djela dječije pornografije, jeste da se ona najčešće dešavaju od strane trećih lica, koja se koriste

savremenim računarskim sistemima i nerijetko posjeduju određena znanja iz te oblasti, što je posebno izraženo u savremenim društvima, gdje je korišćenje savremene tehnologije jednostavno rutina i svakodnevnica.

Dječija pornografija, kao što je rečeno, najčešće se širi putem zatvorenih foruma na internet stranicama i to predstavlja veliki problem policijskim i bezbjednosnim organima, koji zbog nedostatka odgovarajuće obučenog i stručnog kadra i opreme nisu u stanju da u svakom momentu preduzmu odgovarajuće mjere na otkrivanju i sprečavanju takvih radnji, pa je iz tih razloga još uvijek veliki broj neriješenih slučajeva dječije pornografije.

Premda se sa sigurnošću ne može utvrditi tačan broj izvora dječije pornografije na internetu, nesporno je da svakodnevno raste broj djela vezana za dječiju pornografiju. Tom širenju pridonose i mnogi razlozi kao što je anonimnost korisnika te razvoj multimedijalnih tehnika kojima i osobe bez posebnog znanja mogu izraditi i distribuisati nedozvoljene sadržaje (Derenčinović, 2003: 8).

Isto tako, činjenica je da je većina djela dječije pornografije otkrivena sasvim slučajno kada su policijski organi vršeći istragu zbog nekih drugih izvršenih djela npr. krađe, prevare ili utaje i sl. došli do saznanja o djelima i licima vezanim za dječiju pornografiju.

Iz ovih razloga i ozbiljnosti same situacije, u borbu protiv nasilja nad djecom morale su se uključiti gotovo sve međunarodne strukture, a rezultat toga je donošenje niza propisa, preporuka, protokola, konvencija i sl. koje imaju za cilj da aktiviraju nadležne organe, prije svega državne, da se pripreme za borbu protiv nasilja nad djecom uopšte, uključujući dječiju prostituciju i pornografiju, od kojih se ističu neke značajnije kao što su:

- Konvencija UN o pravima djeteta;[2]
- Protokol o prodaji djece, dječijoj prostituciji i dječijoj pornografiji;[3]
- Okvirna odluka Savjeta Evropske unije o borbi protiv seksualne eksploatacije djece i dječije pornografije.[4]

Posebna pažnja u ovom radu data je Okvirnoj odluci Savjeta Evropske unije o borbi protiv seksualne eksploatacije djece i dječije pornografije, koja daje smjernice svim državama – članicama kako da se pripreme za postupanja u slučajevima vezanim za seksualnu eksploataciju djece, dječiju pornografiju i visokotehnološki kriminal, misleći prije svega na normativno uređenje ove oblasti, što bi u svakom slučaju bio pokazatelj državama i njihovim institucijama da se adekvatno pripreme za određena postupanja koja slijede u borbi protiv stvaranja i širenja dječije pornografije.

U ovoj Odluci je rečeno da je dječija pornografija, sem što je vezana za visokotehnološki kriminal, posebno ozbiljan vid seksualne eksploatacije djece i predstavlja povredu ljudskih prava i osnovnog prava djeteta na harmonično odrastanje i razvoj.

Radi što boljeg sagledavanja ove problematike od strane država i njihovih institucija, njihove pripreme za dalja djelovanja u borbi protiv stvaranja i širenja dječije pornografije i visokotehnološkog kriminala, u pomenutoj Odluci su

---

[2] "Službeni glasnik BiH", br. 2/92 i 13/94.

[3] Isto.

[4] "Službeni glasnik Evropske Unije", 20. januar 2004. godine.

objašnjeni pojedini termini, od kojih se kao najvažniji izdvajaju termini: "dijete" i "dječija pornografija".

Za termin "dijete" je rečeno da podrazumijeva svako lice ispod 18 godina starosti.

Za termin "dječija pornografija" se kaže da podrazumijeva svaki pornografski materijal koji vizuelno opisuje ili predstavlja sljedeće:

- pravo dijete koje prisustvuje ili učestvuje u seksualno eksplicitnom ponašanju, uključujući i lascivno prikazivanje genitalija ili pubične oblasti djeteta;
- pravu osobu koja se predstavlja kao dijete koje prisustvuje ili učestvuje u seksualno eksplicitnom ponašanju uključujući i lascivno prikazivanje genitalija ili pubične oblasti;
- realne slike nepostojećeg djeteta koje prisustvuje ili učestvuje u seksualno eksplicitnom ponašanju, uključujući i lascivno prikazivanje genitalija ili pubične oblasti.

Istom Odlukom sugerisano je svim državama – članicama da do januara 2006. godine preduzmu neophodne mjere koje moraju biti u skladu sa Okvirnom odlukom i o tome da podnesu izvještaj Generalnim sekretarijatu Savjeta, iz čega će se vidjeti u kojoj mjeri su državne članice postupile u skladu sa ovom Odlukom i na koji način su uredile zakonsku regulativu shodno obavezama iz Odluke, a u cilju sprečavanja bespravno počinjenih radnji, bez obzira da li su ostvarene putem kompjuterskog sistema ili ne, kao što su:

- proizvodnja dječije pornografije;
- distribucija, širenje ili prenošenje dječije pornografije;
- nabavljanje i činjenje dječije pornografije dostupnom;
- sticanje ili posjedovanje dječije pornografije.

U tom smislu, mnoge države su odlučile da preduzmu određene konkretne mjere u borbi protiv visokotehnološkog kriminala, uključujući samim tim i borbu protiv stvaranja i širenja dječije pornografije, koristeći se svim raspoloživim kapacitetima. Počelo se, uglavnom, od pravnog uređenja ove materije u skladu sa međunarodnim propisima, preporukama i standardima, pa do stvaranja specijalizovanih odjeljenja u okviru policije, tužilaštva i sudova, sa posebno obučenim kadrom koji će raditi i djelovati u skladu sa tim propisima.

Takve aktivnosti su dovele do toga da se u skoro svim državama dječija pornografija i djela u vezi sa tim, zakonski određena kao krivična djela, kao što su npr. u Krivičnom zakonu Republike Srpske, u kojem su ova djela svrstana u krivična djela protiv polnog integriteta, u koje spadaju djela kao što su:

- iskorišćavanje djece i maloljetnih lica za pornografiju, čija zakonska formulacija glasi: "Ko zloupotrebi dijete ili maloljetno lice za izradu slika, audio-vizuelnog materijala ili drugih predmeta pornografske sadržine ili dijete i maloljetno lice zloupotrijebi za pornografsku predstavu, kazniće se kaznom zatvora od jedne do osam godina" (član 199);
- prozvodnja, posjedovanje i prikazivanje dječije pornografije**,** čija zakonska formulacija glasi: "Ko posjeduje, nudi, distribuira, prikaže ili javnim izlaganjem ili na drugi način učini dostupnim spise, slike, audio-vizuelne ili druge predmete koji predstavljaju dječiju

pornografiju ili ko takve materijale radi toga proizvodi, nabavlja ili drži ili ko prikaže dječiju pornografsku predstavu, kazniće se kaznom zatvora do tri godine", a "ako je ovo djelo izvršeno prema licu mlađem od 16 godina, kazniće se zatvorom od šest mjeseci do pet godina". Isto tako je naznačeno da "ako su ova djela izvršena putem sredstava javnog informisanja ili putem interneta, učinilac će se kazniti zatvorom od jedne do osam godina" (član 200).[5]

Što se tiče posjedovanja materijala vezanog za dječiju pornografiju, ono je novina u mnogim zakonodavstvima i kažnjiva je u sljedeća tri oblika:

- obično posjedovanje;
- posjedovanje radi komercijalne distribucije i
- posjedovanje radi ličnih promocija i zahtjeva.

Zahtjevi za kriminalizaciju posjedovanja dječije pornografije polazi od pretpostavke da se represivnim nastupom prema klijentima, odnosno osobama koje se koriste takvim materijalom može na odgovarajući način suzbiti prizvodnja takvog materijala i njegova dalja distribucija i tako zbog ograničenja ponude utiče se i na smanjenje potražnje za tom robom. Čak i mnoge države, kao npr. Holandija, koje su vrlo tolerantne prema prostituciji odraslih, s međunarodnim propisima su uskladile svoja zakonodavstva, a radi potpune zaštite osoba mlađih od osamnaest godina. Prema navodima onih koji se zalažu za kriminalizaciju posjedovanja dječije pornografije, povezanost dječije online pornografije, povezanost seksualne zloupotrebe djece i dječije pornografije najbolje se vidi upravo kod posjedovanja materijala vezanog za dječiju pornografiju (Derenčinović, 2003).

Ipak postoje i protivnici kriminalizacije posjedovanja dječije pornografije, koji tvrde da se u tom slučaju uglavnom radi o licima koja nemaju direktnu vezu sa proizvođačima dječije pornografije, a uz to mogu poslužiti kao ključni svjedoci u postupcima prema proizvođačima i distributerima ovakvih sadržaja.

Međutim, preovladao je stav u većini zemalja o kažnjivosti posjedovanja dječije pornografije s obzirom na to da su mnogobrojna iskustva u slučajevima iskorišćavanja i zlostavljanja djece pokazala da su lica koja posjeduju materijal vezan za dječiju pornografiju isto tako sklona zlostavljanju djece odnosno njihovom seksualnom iskorišćavanju, što je bio samo jedan od argumenata za kriminalizaciju posjedovanja dječije pornografije, a drugi argument je taj da je to pogodan način suzbijanja proizvodnje dječije pornografije (Isto).

S obzirom na težinu ovakvih djela, njihove posljedice, brojnost i raznovrsnost radnji čijim preduzimanjem se čine ova djela, borba protiv visokotehnološkog kriminala, koja podrazumijeva i borbu protiv dječije pornografije, zahtijeva sveobuhvatnu reakciju cjelokupnog društva, a posebno policijskih, bezbjednosnih i pravosudnih struktura.

Kao pozitivan primjer angažovanja države i državnih organa u borbi protiv visokotehnološkog kriminala i dječije pornografije na ovim prostorima, ističe se, između ostalih, i Republika Srpska, u kojoj se, sem normativnog uređenja ove oblasti, otišlo i dalje, pa je tako u Ministarstvu unutrašnjih poslova osnovano posebno Odjeljenje za sprečavanje visokotehnološkog kriminaliteta, koje se bavi isključivo djelima iz te oblasti.

---

[5] "Službeni glasnik RS", br. 49/03, 73/10 i 1/12.

Pomenute mjere su već dale određene rezultate, koji se ogledaju u uspješno obavljenoj akciji hapšenja jednog lica iz Dervente, zbog osnovane sumnje da je počinilo krivično djelo "proizvodnje i prikazivanja dječije pornografije". Tom prilikom zaplijenjen je obiman materijal sa pornografskim sadržajima vezanim za dječiju pornografiju, a po podacima Ministarstva unutrašnjih poslova Republike Srpske, to je do sada najveća količina zaplijenjenog materijala dječije pornografije u BiH i radi se o 2 miliona slika i 7.000 video klipova.[6]

Pojedine države regiona, kao što su Republika Srbija i Hrvatska, isto tako ozbiljno su shvatile problematiku visokotehnološkog krimanaliteta, pa su u okviru svojih nadležnosti preduzele potrebne mjere i aktivnosti, od kojih u Republici Srbiji pominjemo kao najznačajnije donošenje Zakona o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala 2005. godine[7], na osnovu kojeg je država Srbija ažurirala policijske, bezbjednosne i pravosudne organe da preduzmu konkretne mjere u borbi protiv visokotehnološkog kriminaliteta, što je dalo osnova za uspostavljanje Specijalizovane jedinice u okviru Ministarstva unutrašnjih poslova Republike Srbije, zatim Posebnog tužilaštva u okviru Okružnog javnog tužilaštva u Beogradu i Posebnog sudskog odjeljenja u Okružnom sudu u Beogradu, čiji je prevashodni cilj borba protiv svih vidova visokotehnološkog kriminala, kao i njegovo otkrivanje i sprečavanje (Jerković, 2009).

Takođe, kao veliki doprinos ovoj borbi, moraju se naglasiti aktivnosti Ministarstva unutrašnjih poslova Republike Srbije na angažovanju građana u provođenju akcije pod nazivom "Armagedon". Naime, ova akcija je pokrenuta isključivo radi suzbijanja dječije pornografije uz učešće građana, koji dajući potrebne informacije, pomažu policijskim organima u identifikovanju tzv. "internet predatora", a rezultat ove akcije, u toku 2011. godine, jeste hapšenje 23 lica iz Beograda, Gornjeg Milanovca, Zaječara, Novog Sada, Sombora, Bora i mnogih drugih gradova širom Srbije, što je za 50% više u odnosu na 2010. godinu. Upravo zbog ovakvih podataka reakcija javnosti na ovu akciju je bila više nego povoljna, pa je ona nastavljena i u 2012. godini.

Podaci Ministarstva unutrašnjih poslova Republike Srbije govore da je među uhapšenim licima tokom akcije "Armagedon", bilo ličnosti različitih profesija i obrazovanja, kao što su npr. sveštenici, direktori, advokati, nastavnici, itd., i ono što je karakteristično za sva djela vezana za dječiju pornografiju, jeste da su izvršena uz pomoć računara, koji su oduzeti od vlasnika radi dalje istrage i vještačenja. [8]

U Republici Hrvatskoj ova oblast je, takođe, pravno regulisana i njihova pojedina zakonska rješenja se izdvajaju po određenim specifičnostima jer, npr., idu dotle da djeluju "povratno preventivno", tačnije utiče se na potražnju za internetskim sadržajem dječije pornografije, a poenta takvih zakonskih rješenja jeste da se pronađu osobe koje posjeduju i distribuišu pornografski materijal dok još samo gledaju i dok nisu "napravile štetu". U tom smislu osnovan je i Odsjek

---

[6] Dostupno na: http://www. novosti.rs/vesti/planeta.70.html:323623-Derventa-Pedofil-imao dva – miliona snimaka.

[7] "Službeni glasnik Republike Srbije", broj: 61/05.

[8] dostupno na: http://www.dw.de/dw/article/0,,15462460,00.html?maca=ser-Blic%2520Online-2569-xml-mrss, 14. oktobar 2011. godine

za kompjuterski kriminal unutar Ministarstva unutrašnjih poslova Republike Hrvatske, koji tijesno sarađuje sa međunarodnim policijskim strukturama u cilju razješnjenja ovih i sličnih slučajeva i, što je važno istaći, a što je proisteklo iz ovih aktivnosti, jeste 120 procesuiranih slučajeva iz oblasti dječije pornografije do danas (Grković, 2007).

ZAKLJUČAK

Razvoj tehnologije u savremenim uslovima omogućio je u većem obimu proizvodnju i distribuciju dječije pornografije, kao i pornografskog materijala uopšte. Nepostojanje jedinstvenog stava u određivanju i definisanju pojma dječije pornografije dovelo je do teškoća vezano za određivanje pravnog okvira i zakonskog regulisanja te materije, a posebno u dijelu koji se odnosi na inkriminacije pojedinih djela iz oblasti dječije pornografije. I pored navedenih poteškoća, jedna od osnovnih obaveza države i njenih institucija jeste obaveza da zaštite svoje građane i njihova prava, što naravno uključuje i prava djece i maloljetnika. U tom smislu, od strane zvaničnih međunarodnih institucija doneseno je niz propisa i uputstava koja su većini država poslužila kao svojevrsni putokaz, prilikom normativnog uređenja oblasti vezane za zaštitu prava djece i maloljetnika.

Mnoge države su tako u svojim zakonodavstvima dale odgovarajući prostor djelima vezanim za visokotehnološki kriminal i dječiju pornografiju i većina tih djela je inkriminisana i zakonski određena kao krivična djela.

Međutim, samo pravno uređenje ovih oblasti je nedovoljno, jer borba protiv bilo koje vrste kriminaliteta, pa tako i ovih navedenih, zahtijeva mnogo veće angažovanje drugih organa i institucija s odgovarajućim stručnim kadrom, kako bi dala što pozitivnije rezultate. Upravo zbog poteškoća koje počinju od definisanja dječije pornografije, pa do posebnih uslova u kojima ona nastaje i širi se, teško je ući u trag licima koja posjeduju, proizvode ili distribuišu dječiju pornografiju. Većina država su iz tih razloga pribjegle metodama uključivanja javnosti na otkrivanju ovih djela i pružanja pomoći nadležnim policijskim i bezbjednosnim organima, a počelo se od prijava građana – korisnika interneta, do uključivanja internet industrija.

Primjer takve saradnje jeste osnivanje Inhope (Internet Hotline Providers i Europe) organizacije, koja predstavlja mrežu nacionalnih hotline operatera čija je uloga da samim korisnicima omoguće da prijave ono što smatraju nepoželjnim sadržajem na internetu i funkcioniše kao neprofitabilna organizacija koja se većinom finansira od strane EU.

Takve i slične aktivnosti nas dovode i do potrebe stalnog jačanja svih vidova međudržavne i međupolicijske saradnje koja bi se ogledala ne samo u razmjeni važnih informacija i podataka vezanih za pomenutu problematiku, već i u zajedničkom djelovanju policijskih i bezbjednosnih struktura, kao i pružanju odgovarajuće pomoći kako u kadrovskim kapacitetima, tako i u nekim drugim aktivnostima, od kojih vrijedi pomenuti zajedničke edukacije, seminare za osposobljavanje kadrova za efikasnu borbu protiv visokotehnološkog kriminala i dječije pornografije.

Isto tako treba imati na umu i činjenicu da internet stranice nisu uvijek način na koji se širi dječija pornografija i da puko brisanje dostupnih sadržaja i

blokada određenih stranica mogu dati samo trenutne rezultate koji se dalje moraju koristiti kao dio sveopšte strategije u borbi protiv visokotehnološkog kriminala i dječije pornografije, pa iz tih i drugih razloga međunarodna saradnja treba da se odnosi, prije svega, na:

- sprečavanje svih oblika nasilja nad djecom;
- zaštitu djece;
- krivično gonjenje počinilaca djela vezanih za nasilje uopšte, ali sa posebnim akcentom na djelima nasilja nad djecom i
- izradu programa za razvoj i pomoć trećim zemljama u borbi protiv svih oblika nasilja nad djecom.

LITERATURA

1. Ajduković, M. (2012). Preporuka CM/Rec(2009)10 Odbora ministara zemljama članicama o integriranim nacionalnim strategijama za zaštitu djece od nasilja. *Dijete i društvo (1/2),* str. 237–256.
2. Babić, M. i Marković, I. (2009). *Krivično pravo – posebni dio*. Banja Luka: Univerzitet u Banjoj Luci.
3. Bernard, P. (1886). *Des Attentats a la pudeur sur les petites filles* . Lion: IMP.
4. Grković, B. (2007). Zlostavljači iz anonimnosti, *Vreme (840)*.
5. Derenčinović, D. (2003). Dječija pornografija na internetu – o kažnjivosti posjedovanja i virtuelnoj dječijoj pornografiji. *Hrvatski ljetopis za kazneno pravo i praksu(10)*
6. Faktopedija, 3. izdanje (2005). Novi Sad: Mladinska knjiga.
7. Jerković, R. (2009). Borba protiv visokotehnološkog kriminaliteta u Srbiji. *Telekomunikacije 3.*
8. http://en.wikipedia.org/wiki/Computer_crime
9. http://www.justice.gov/criminal/cybercrime/reporting.htm
10. http://www.cybercrime.gov/reporting.htm

SUMMARY

Child pornography as a type of violence against children, due to development of informational and communicational technologies and computer networks, is in close connection with high-tech crime. The internet as a space with no legal regulation allows unlawful activities like distribution of child pornography, especially through closed forums. This study tries to contribute to reviewing of serious situation in which society currently is, especially minors, due to presence and expansion of negative phenomenon in relation to the child pornography and high-tech crime. Also, the aim of this study is to point out determination and activities of some international structures in drawing attention to the obligation of national legislative, the incrimination of child pornography and high-tech crime and functional organisation of specialized public authorities and their jurisdiction, in fighting against this tipe of crime.

Stručni rad - UDK 004.738.5: :343.533

PROBLEM SAVREMENE DOBI
OBLICI KRAĐE I ZLOUPOTREBE IDENTITETA I MJERE PREVENCIJE

Slobodanka Milićević, diplomirani pravnik unutrašnjih poslova
Visoka škola unutrašnjih poslova, Banja Luka, bobam2010@live.com
Srđan Vujović, diplomirani kriminolog
Fakultet za kriminalistiku, kriminologiju i sigurnosne studije, Sarajevo, srdjanvuja@yahoo.com

Apstrakt: Savremeni svijet je nezamisliv bez infirmacionih tehnologija, ali nekada sve dobre i loše strane toga snosi pojedinac, upravo zbog sofisticirane tehnologije, čija je primjena velikim dijelom pravno neregulisana oblast. Problemi nastaju kada dođe do krađe identiteta, odnosno ličnih podataka koji se mogu zloupotrebljavati na različite načine. Sa druge strane i sama krađa identiteta vrši se na različite načine, a najčešće pominjani su Phishing, Spoofing, Skimming i sl.

Shodno tome, zbog napretka infirmacionih tehnologija i osoba koje ih zloupotrebljavaju, sve su češće izmjene propisa koji regulišu ove oblasti, kako bi se na taj način bar malo doprinijelo sprečavanju ovog globalnog problema.

Ovim radom će se nastojati ukazati na ozbiljnost problematike krađe identiteta, jer je iz dana u dan sve zastupljenija. Krivična djela visokotehnološkog kriminala, u koja ubrajamo i krađu identiteta, veoma je teško otkriti, još teže pronaći izvršioca, a i veoma teško ih je dokazati. Zbog toga, potrebno je djelovati prije izvršenja delikta (ante delictum), sa ciljem sprečavanja da do njega dođe. Mi smatramo da adekvatne preventivne mjere moraju biti preduzete kako na individualnom/ličnom, tako i na globalnom/kolektivnim nivou.

Ključne riječi: Visokotehnološki kriminal, krađa identiteta, zloupotreba, prevencija.

UVOD

Identitet[1] je skup svojstava vezanih za pojedinca, koji ga karakterišu i po kojim se taj pojedinac razlikuje od drugih osoba. Svojstva po kojima se jedna osoba razlikuje od drugih, mogu biti: 1. Pravna svojstva (lično ime, prezime, ime oca, državljanstvo, bračno stanje, prebivalište i slična svojstva promjenjiva tokom života) 2. Faktička svojstva (dan, mjesec i godina rođenja, mjesto rođenja, matični broj, nacionalnost i druga svojstva koja su nepromjenjiva), 3. Fizička svojstva (pol, otisci prsta, lični opis i sl.) (Modli, Korajlić, 2002: 158) 4. Virtuelna svojstva (Lozinka, pin-kod, šifra, korisničko ime).

Pomenuta svojstva predstavljaju privatne podatke osobe, tako da ih svaka osoba ima pravo čuvati u tajnosti i objelodaniti samo onda kada je to dužna učiniti

[1] **Identitet** (lat: *identitas* = karakteristična jedinica) je individualna karakteristika, odnosno osobina po kojoj je predmet ili osoba prepoznatljiva ili znana. Preuzeto sa: http://bs.wikipedia.org/wiki/Identitet, Pregledano 02.03.2012.

prema važećim zakonima ili drugima propisima. O pravu na privatnost govori nam i član osam[2] Evropske konvencije za zaštitu osnovnih ljutskih prava i osnovnih sloboda. U cilju zaštite ovog, ali i drugih ljudskih prava i sloboda u BiH postoji Zakon o zaštiti ličnih podataka. Međutim, u savremenim uslovima života pravo na privatnost je sve ugroženije. Razvojem nauke i tehnologije, posebno razvojem savremenih komunikacija, uvođenjem novih informacionih sistema i stvaranjem baza podataka u svim oblastima, uz nesporno korisne efekte, stvaraju se i pretpostavke za nove oblike ugrožavanja prava na privatnost, odnosno zloupotrebu privatnih podataka. Podaci na osnovu kojih se utvrđuje ili se može utvrditi identitet određenog lica mogu biti zloupotrijebljeni za nadziranje i usmjeravanje ponašanja i navika tog lica, za trgovinu i razmjenu baza podataka o ličnosti, za krađu identiteta, kao i za razne druge oblike zloupotrebe.[3]

Krađa identiteta[4] je takvo **krivično djelo**[5] kod kojeg se neko lice lažno predstavlja kao drugo lice u namjeri pribavljanja protivpravne imovinske koristi ili druge lične koristi. (Teri Bidwell, 2002: 3) Iako su sve aplikacije na socijalnim mrežama zamišljene kao jedan od oblika lakše komunikacije, odjednom dolazimo do jedne granice, gdje se oni u velikoj mjeri zloupotrebljavaju u različite svrhe. Neki od razloga koji bi se mogli navesti kao osnovni, zašto je ova vrsta kriminaliteta sve zastupljenija, jesu sljedeći: veliki profit, ogroman broj potencijalnih žrtava, širok spektar manipulativnog prostora, te ih je teško otkriti i dokazati. Na zabrinjavajući porast broja krađa identiteta upozorila je američka organizacijea ITCR (*Identity Theft Resource Center*), iznoseći alarmantne podatke do kojih je došla na osnovu svojih istraživanja. Ove podatke trebamo shvatiti kao upozorenje, jer lako može da se rasplamsa već "inficirano" područje BiH.

O prevenciji krađe identiteta i značaju zaštite privatnosti govori se dugi niz godina. Ipak, preventivno djelovanje po pitanju ove problematike nije ozbiljno shvaćeno, kako od strane pojedinca tako i od strane organa formalne socijalne kontrole. Značaj ovog rada se sastoji u isticanju problema krađe identiteta i ukazivanju na poželjan način borbe protiv ovog sve učestalijeg neprihvatljivog ponašanja. Ovaj problem moguće je svesti na prihvatljiv nivo jedino ako mu pristupimo organizovano i sistematski, poštujući i uvažavaući sve preporuke i kodekse vezane za prevenciju manipulacije ličnim podacima.

POJAVNI OBLICI KRAĐE IDENTITETA

„Krađe identiteta na osnovu pribavljenih informacija o ličnosti mogu se ostvariti na različite načine, najčešći u 2007. god.[6] bili su u okviru tri glavne

---

[2] U članu osam Evropske konvencije za zašitu ljudskih prava i osnovnih sloboda se navodi: "Svako ima pravo na poštovanje svog **privatnog** i **porodičnog života**, **doma** i **prepiske**.", "Država se neće miješati u vršenje ovog prava, osim ako to nije predviđeno zakonom i ako je neophodno u demokratskom društvu u interesu nacionalne sigurnosti, javne sigurnosti ili ekonomske sigurnosti zemlje, radi sprječavanja nereda ili kriminala, radi zaštite zdravlja ili morala ili radi zaštite prava i sloboda drugih" (Sadiković, 2006)

[3] Preuzeto sa: http://www.zakon.co.rs/podaci-o-licnosti-i-pravo-na-zatitu-kao-osnovno-ljudsko-pravo.html Pregledano: 20.01.2012.

[4] Hack Proofing Your Identity in the Information Age Syngress Publishing, Teri Bidwell, Preuzeto sa: http://www.pdfbooksdownload.net/hack-proofing-your-identity-by-teri-bidwell/ Pregledano: 20.01.2012.

[5] Ipak do danas krađa identiteta nije propisana kao krivično djelo niti u jednom krivičnom zakonu u BiH

[6] Preuzeto sa: www.ftc.gov/opa/2006/12/fyi0688.htm Pregledano: 06.02.2012.

kategorije: stvaranje novih računa (kreditnih kartica, tekućih bankovnih računa, podizanje kredita), zloupotreba postojećih računa (na kojima nisu izdate kreditne i platne kartice) i zloupotreba postojećih uz korišćenje debitnih i kreditnih kartica. Govoreći o tome, krađa identiteta se javlja u sledećim oblicima: Spoofing, phishing i skimming."

Spoofing[7] pretstavlja zloupotrebu podataka da bi se došlo do drugih važnih podataka ili da bi se ostvario neautorizovan pristup nekoj web-lokaciji. Cilj ovog neprihvatljivog ponašanja jeste umjesto prave staviti lažnu IP adresu i na taj način prikupiti i zloupotrijebiti podatke. Izvršioci spofinga se prvobitno predstavljaju kao kakve povjerljive osobe koristeći se prethodno prikupljenim podacima. Ovaj možda i najšire shvaćen oblik krađe identiteta moguće je izvršiti na tri načina, i to u vidu E-mail spofinga (korisnik odgovara na sebi poznatu e-mail adresu koja je, međutim, lažna i zlonamjerna), IP spofinga (korištenje lažne IP adrese) i URL spofing (zlonamjeran URL se prikazuje kao pouzdan).

Phishing napadi su najbrojniji pojavni oblik krađe identiteta, ali to su i najštetniji napadi prevaranata. Tako je i u BiH, tvrdi A. Husrep[8]. Phishing se ostvaruje nasumičnim slanjem elektronske pošte, a kao osnovni cilj javlja se prikupljanje privatnih podataka osoba kako bi se oni mogli zloupotrijebiti. Sadržaj elektronske pošte najčeće je u obliku formulara koji navodno šalje matična kuća u cilju provjere podataka, u svrhu sigurnosti ili zaštite, otklanjanja greške i sl. Formular dobijen u mailu zahtijeva upisivanje podataka poput korisničkog imena, lozinke, pin-koda, broja računa, JMBG i slično. Pored toga često takvi formulari sadrže i dodatna pitanja, ali koja najčešće služe kao dio taktike da bi se postigo krajnji cilj. Kako su najčešći izvršoci profesionalci u svom poslu, veoma je teško uočiti da se ne radi o kući sa kojom smo povezani (npr. banka), jer se sama internet-adresa pošiljaoca može razlikovati u jednom slovu ili jednoj karakteristici od oficijelne. Ovaj način krađe identiteta najbolje pokazuje primamljivost visokotehnološkog kriminala, jer je očigledno da se bez ikakvog fizičkog kontakta može nešto ukrasti od drugog lica, a to izvršiocu može donijeti korist. Primjer korištenja podataka (koji se odnose na kreditne kartice) pribavljenih phishingom jeste upotreba kreditne kartice naknadno ukradene od vlasnika ili kupovina "bijelih kartica" i štampanje kopija.

Skimming *je* ***kartična prevara***. Ova vrsta krađe identiteta vlasnika kartice može se vršiti na više načina, međutim, osnovni cilj je snimanje magnetnog zapisa sa kreditne kartice. Takve radnje najčešće se vrše preko posrednika (saučesnika), npr. prilikom plaćanja kreditnom karticom zaposleno osoblje vrši skimming, te zapise sa kartica prodaje. Ovdje treba istaći veoma prisutnu pojavu nazvanu "carding", koja je vezana za upotrebu podataka nakon što se do njih dođe.[9] Sa druge

---

[7] ***Spoofing*** je pojam koji označava falsifikovanje podataka relevantnih za osiguranje povjerljivosti na Internetu, Preuzeto sa: http://www.carnet.hr/tematski/sigurnost/problemi_ostali.html Pregledano: 05.03.2012.

[8] Vidi intervju sa A. Husrep na http://www.dnevniavaz.ba/vijesti/teme/73512-strucnjaci-upozoravaju-na-opasnost-na-internetu-hakeri-u-bih-udaraju-na-kreditne-kartice.html pregledano 02.03.2012.

[9] „Karding se koristi kada haker dođe u posjed podataka s kreditne kartice, koje može pročitati u svakom trenutku ako ne pokrijete karticu prilikom plaćanja. Dakle, nije mu potrebno ništa drugo osim da pročita 16-znamenkasti kod s kartice i ima sve što mu treba. Nakon toga obavit će kupnju putem interneta da bi provjerio da li je kartica validna." citirano sa http://www.dnevniavaz.ba/vijesti/

strane, ugrađivanje čitača magnetnih zapisa u bankomate, odnosno lažne otvore na bankomatima, veoma je čest način skimminga.

Da je krađa identiteta prisutna u BiH, i to u svim svojim pojavnim oblicima, neće nam pokazati zvanični podaci. Međutim, stručnjaci kažu drugačije. Niko ne prijavljuje ovakve vrste napada, pa se oni nalaze u "apsolutnoj tamnoj brojci kriminala", kaže Budimlić[10]. Da je to tačno, ukazuje nam praksa. Kada se desi krađa identiteta i dođe do zloupoterebe, npr. korištenja tuđe kreditne kartice, oni koji to prvi otkriju jesu vlasnik i banka. Vlasnik nakon pregledavanja snimka sa sigurnosne kamere veoma često prepozna počinioca pa pravdu preuzima u svoje ruke[11]. Sa druge strane, u interesu banke je da se ne sazna za takvo (ne)djelo zbog reputacije banke. Menadžment banaka ima takvu politiku da će nadoknaditi štetu svom klijentu[12], ali neće obavijjestiti nadležne organe o zloupotrebi. Potvrda gore navedenog dolazi i od strane američke organizacije ITCR (*Identity Theft Resource Center*)[13], koja navodi da se pored SAD i Kanade, krađa identiteta velikim obimom pojavljuje i širi u Evropi. Istraživanja koja je proveo ITCR pokazala su da je 2006. godine u SAD zabilježeno 446 slučajeva krađe identiteta, prilikom čega je razotkriveno 128.000.000 ličnih podataka Amerikanaca, a predviđena šteta je oko 2.000 milijardi dolara[14]. Oni ističu činjenicu da se prikuplja mnogo veći broj ličnih podataka od strane kradljivaca nego što se može zloupotrijebiti. To nam treba biti indicija da i ako nemaju zagarantovanu materijalnu korist, hakeri pribavljaju tuđe podatke. Motivi[15] za to su različiti.

ZAKONSKA RJEŠENJA

Za pravnika, kriminologa ili kriminalistu najvažnije je pravno određenje nekog termina. Sa druge strane, u BiH krađa identiteta nije pravno definisana, pa je teško zamisliti i čitavu borbu protiv nje. "Krivičnopravnu zaštitu treba osigurati na planu zaštite ličnih podataka građana, koja predstavlja zaštitu tzv. intimiteta, bilo kroz postojeće inkriminacije ili donošenjem novih." (Tanović, 2002) Pravnu definiciju krađe identiteta ne pronalazimo ni u regionu. U BiH postoji Zakon o zaštiti ličnih podataka, međutim, on ne prepoznaje institut krađe identiteta. Takođe, kršenje ovog zakona predstavlja prekršaj, za koji je propisana novčana kazna, a ne krivično djelo.

Kako postojeći zakoni nisu dovoljni da bi se kroz njih efikasno suprotstavili krađi identiteta, ona treba biti propisana krivičnim zakonom kao posebno krivično

---

teme/73512-strucnjaci-upozoravaju-na-opasnost-na-internetu-hakeri-u-bih-udaraju-na-kreditne-kartice.html, pregledano 02.03.2012.

[10] Ministar unutrašnjih poslova Kantona Sarajevo. Intervju za Dnevni avaz 02.03.2012.

[11] Preuzimanje pravde u svoje ruke je negativna pojava koja može izazvati teške posljedice. Primjer nalazimo u SAD, gdje su „građani zapalili zgrade iz kojih se trgovalo drogom". (Ignjatović, 2005: 329)

[12] Ako se radi o manjem iznosu. U BiH ako je zloupotrebom otuđeno do 1.000 KM, banka neće prijaviti slučaj nadležnim organima.

[13] Preuzeto sa: http://www.idtheftcenter.org/artman2/publish/a_history/The_History_of_the_Identity_theft_Resource_Center.shtml Pregledano: 21.01.2012.

[14] Preuzeto sa: http://dalje.com/hr-hrvatska/kako-se-mozete-zastititi-od-kradje-identiteta/131778 Pregledano: 28.02.2012.

[15] Vidi više u Budimlić, Puharić (2009) str. 16.

djelo[16]. Razlog tome je što inkriminisanjem nekog neprihvatljivog ponašanja predviđamo kaznu za potencijalnog učinoca, a ako pogledamo KZ BiH član 39[17], vidjećemo da je svrha kažnjavanja upravo generalna i specijalna prevencija. Istina, neki članovi krivičnog zakona načelno imaju dodirnih tačaka sa krađom identiteta. Kao primjer možemo navesti čl. 176. KZ RS, a koji se odnosi na neovlašteno korištenje ličnih podataka. Ovaj član krivičnog zakona ujedno je najbliži opisu krađe identiteta. U stavu 1.[18] ovog člana vidimo da se štite lični podaci. Šta je to lični podatak? Prema članu 3. Zakona o zaštiti ličnih podataka "lični podatak" je definisan kao: "Bilo koja informacija koja se odnosi na fizičko lice na osnovu koje je utvrđen ili može da se utvrdi identitet lica". Ako bi se pod ovim smatrala sva svojstava identiteta (pravna, fizička, faktička i virtuelna), to bi bilo prilično dobro rješenje. Međutim, ovaj se član u praksi odnosi na pravna i faktička svojstva ličnih podataka. U Krivičnom zakonu Federacije Bosne i Hercegovine najbliža inkriminacija ili član kroz koji se može suprotstaviti krađi identiteta jeste "kompjuterska prevara" i "neovlašteni pristup zaštićenome sistemu i mreži elektronske obrade podataka"[19].

Već poznata problematika u BiH je neusklađenost entitetskih zakona međusobno, kao i njihova neusklađenost sa Krivičnim zakonom BiH, pa ona i ovoga puta dolazi do izražaja. Stoga u slučaju inkriminacije krađe identiteta najbolje je to uraditi jednako i istovremeno u svim krivičnim zakonima u BiH.

Vidimo da i pored preporuka o suprotstavljanju kompjuterskog kriminaliteta koje su donesene od strane najvažnijih međunarodnih organizacija, BiH nema dobra zakonska rješenja za visokotehnološki kriminal. Tako i krađa identiteta, koja je najčešće vezana za njega, nije propisana kao krivično djelo. Ono što možemo (moramo) uraditi je pogledati kako to izgleda u drugim državama, koje se već duži niz godina bore sa izraženim problemom krađe i zloupotrebe identiteta.

Prema dokumentu[20] (iz materijala 12. kongresa UN u vezi s prevencijom kriminala i krivičnog pravosuđa održanog u Brazilu) navedeno je da se u novom zakonodavstvu Kraljevine Norveške (u Kaznenom zakoniku iz 2009. god.) izbjegava termin "krađa" i koristi supstitucioni termin „zloupotreba identiteta". Naprijed pomenuti Zakonik u čl. 202. navodi da djelo postoji ukoliko lice koje neovlašćeno drži sredstva identifikacije drugog lica ili koristi identitet na takav način da se on može lako zamijeniti sa drugom osobom u cilju:

- pribavljanja protivpravne imovinske koristi sebi ili drugome ili
- nanošenja štete ili nelagodnosti drugom licu.

---

[16] Inkriminacijom krađe identiteta uticalo bi se na suzbijanje drugih krivičnih djela, jer se krađa identiteta najčešće koristi da bi se izvršilo primarno krivično djelo. Kao primjer možemo navesti prevaru, lažno predstavljanje, falsifikovanje isprava i sl.

[17] "Svrha kažnjavanja je: a) da se izrazi društvena osuda učinjenog krivičnog djela; b) da se utiče na učinioca da ubuduće ne čini krivična djela; c) da se utiče na ostale da ne čine krivična djela; d) i da se utiče na svijest građana o pogibeljnosti krivičnih djela i o pravednosti kažnjavanja učinilaca." (KZ BiH čl. 39)

[18] KZ RS Čl. 176. St. 1. "Ko suprotno uslovima određenim u zakonu bez saglasnosti građana pribavlja, obrađuje, saopšti drugom ili koristi njihove lične podatke, kazniće se novčanom kaznom ili zatvorom do jedne godine."

[19] Vidi KZ Federacije BiH.

[20] Preuzeto iz materijala za 12. Kongres UN u vezi prevencije kriminala i krivičnog pravosuđa održan u Brazilu 12-19.04.2010., na str. br. 6.

Prema Zakonu[21] o krađi identiteta (u SAD), kao ista se smatra: „Svaki akt lica koje svjesno transferuje ili neovlašćeno koristi bilo koje ime ili broj, koji se može koristiti, samostalno ili u sprezi sa nekom drugom informacijom, kako bi identifikovalo određenu osobu, u namjeri da izvrši, pomogne u izvršenju ili navede na neku nezakonitu aktivnost koja predstavlja kršenje federalnog zakona, ili predstavlja krivično djelo prema nekom zakonu države članice".

Čl. 18. U.S.C. § 1028 (a) (7) definiše krađu identiteta kao: „svjesno transferisanje, posjedovanje ili korišćenje identifikacionih sredstava druge osobe (drugog lica) u namjeri vršenja ili pomaganja ili podstrekavanja na vršenje ili u drugoj vezi sa nezakonitim aktivnostima kojima se stiču okolnosti za izvršenje nekog krivičnog djela propisanog federalnim zakonom ili zakonima država SAD"[22].

Druga definicija koju daje Federalna trgovinska komisija SAD 15. U.S.C. § 1681a (q) (3) označava krađom identiteta: „korišćenje identifikacione informacije drugog lica". Osnovna razlika je: da li se misli na prevaru i da li se djelo vezuje, u svojoj osnovi, za prevaru. Upravo ovo ograničava inkriminaciju i domet u realnom životu kada izvršilac koristi informacije u druge svrhe, koje se ne odnose na prevaru.

Poslednja inkriminacija obuhvata korišćenje informacija, a ne i njihovo pribavljanje, čime, recimo, phishing i farming otpadaju iz primjene ove norme. Pitanjem određivanja pojma krađe identiteta se bave se i naši naučnici. Oni u svom radu govore o krađi lika i identiteta i drugim vidovima (ne)zakonitog ponašanja[23]. U svom radu na temu krađe identiteta pogrešno je identifikuju kao phishing (engl.), koji definišu kao "preuzimanje "uloge" nekog lica na Internetu, redovno u cilju sticanja neke materijalne ili druge koristi". (Prlja, Reljanović, 2009: 161–184) Kategorizuju ga i kao: najdrastičniji atak na privatnost ličnosti, jer se učinilac, nakon što je prevarom ili na drugi način došao do vitalnih podataka za preuzimanje nečijeg identiteta (internet i druge šifre, brojevi platnih kartica, i sl.) predstavlja u njegovo ime, zaključuje poslove ili ostvaruje društvene kontakte, ispravno primećujući i da tako može vršiti krivična djela na ovaj način, prikriven iza tuđeg identiteta. Pružajući i sopstvenu definiciju, po kojoj: krađa identiteta pretpostavlja prethodno izvršenje nekog drugog krivičnog djela (prevare, upada u tuđi računar ili računarski sistem, postavljanje virusa ili drugog štetnog softvera), ovi autori veoma korektno primjećuju da postoje i drugi načini upada u privatan život ljudi, koje oni karakterišu kao "manje ili više kažnjive"[24]. (Prlja, Reljanović, 2009: 161–184)

Prilikom inkriminacije krađe identiteta treba obratiti pažnju na sljedeće:

-*Korišćenje tuđih (javnih) podataka* podrazumijeva korištenje tuđih ličnih podataka koji su svima dostupni, a u svrhu stavaranja nekog fiktivnog lika. Međutim, i ova ponašanja znaju biti opasna, jer se takvi podaci mogu zloupotrijebiti. Možda manje za sticanje materijalne koristi, ali često se koriste kod pedofilije ili kao

[21] Preuzeto sa: http://www.ftc.gov/os/statutes/itada/itadact.pdfI, Identity Theft Assumption and Deterrence Act (the Identity Theft Act; U.S. Public Law 105-318), Pregledano: 18.01.2012.

[22] Preuzeto sa: Internet related Identity theft, a discussion paper, prepared by Gercke, M. kao dio projekta: Project Cybercrime, Council of Europe, ECD, Directorate General of Human Rights and Legal Affairs. http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/default_en.asp Pregledano: 20.02.2012. god.

[23] Uporedna iskustva, u Strani pravni život, br. 3/09, str. 161–184. Beograd, str. 169.

[24] Neki od njih su inkriminisani; neke zakoni ne navode i kao takvi predstavljaju samo moralno neprihvatljivo ponašanje. Više u Prlja, Reljanović (2009).

priprema za krađu identiteta. Najčešće se ovo ponašanje ogleda u vidu preuzimanja tuđih slika sa interneta. „Ova vrsta aktivnosti (za sada) nije kažnjiva ni u jednoj državi – osim ukoliko se ne radi o silovatelju ili pedofilu, koji na taj način pokušava da pronađe svoju žrtvu, ali je i tada riječ o drugim krivičnim djelima, a korišćenje tuđih podataka se javlja samo kao jedno od prethodnih sredstava pripreme za izvršenje." (Prlja, Reljanović, 2009: 161–184)

-*Korišćenje elektronskih podataka o aktivnosti lica.* U BiH postoji zakon o zaštiti ličnih podataka koji se djelimično odnosi i na ovu problematiku. To je standard koji upotrebljavaju skoro sve države, a odnosi se na upotrebu bilo kojih podataka koji upućuju na određenu osobu, u skladu sa propisima. Primjer je praćenje transakcija na računima osoba ili kopiranje računa.

-*"Prodaja" e-mail adresa i spamovanje.* Svim korisnicima e-mail pošte poznata je problematika prijema sumnjivih ili nepoželjnih e-mail poruka. To svakako ne znači slučajnost ili zalutali e-mail. Ovakav modus operandi često je korišten od strane organizovanih grupa koje za cilj imaju različita neprihvatljiva ponašanja poput protivzakonitih reklama, prevare[25], ili krađe identiteta. Iako je ovakvo ponašanje teško otkriti, a dokazati još teže, Australija je prva država koja je inkriminisala „spamovanje". Irska[26] joj se nedavno pridružila, a s obzirom na trendove narastanja neželjene pošte i na prognoze da će ona u najskorijoj budućnosti imati udio u ukupnom e-mail saobraćaju preko 90%, što čini preko milijardu poruka dnevno, moguće je da će i druge države slijediti ovaj novozapočeti trend inkriminacije". (Prlja, Reljanović, 2009: 161–184)

-*Korišćenje opreme za nadzor i obezbjeđenje.* I ako je na polju sigurnosti veoma doprinijela, visoka tehnologija predstavlja opasnost za jedno od osnovnih ljudskih prava, a to je pravo na privatnost. Ipak sigurnosne kuće koje su dužne djelovati u skladu sa određenim propisima svoju opremu instaliraju tako da je što manja mogućnost ugrožavanaja privatnosti (npr. postavljanje sigurnosnih kamera tako da se ne vidi tastatura na bankomatu). Sa druge srane postoji veliki broj nelegalno instaliranih kamera koje se mogu koristiti putem internet veze (npr. *Google Street View).*

NEOPHODNOST PREVENCIJE KRAĐE IDENTITETA

Krajem XX vijeka najveći kriminološki autoriteti zauzimaju čvrsto stajalište da je najefikasniji način borbe protiv kriminaliteta upravo prevencija. Iako nemjerljiva, prevencija u XXI vijeku mora biti prioritet, jer veliki broj kažnjivih ponašanja ostaje neotkriven, tj. povećava se tamna brojka pojedinih oblika kriminaliteta. Ovo se ponajprije odnosi na tzv. krivična djela visokotehnološkog kriminaliteta. "Brzina kojom se može izvršiti kompjuterska zloupotreba, s velikih udaljenosti, uz anonimnost počinitelja i teškoće njihova otkrivanja veliki su poticaj i čest motiv pojedinca da takvo djelo izvrši, a posebno kada se tome doda mogućnost brzog i lakog bogaćenja, tj. sticanja nezakonite imovinske koristi." (Budimlić, Puharić, 2009: 46)

[25] Prlja, Reljanović, (2009) navode poznati primjer „Nigerijsko pismo"
[26] Preuzeto sa: http://www.junk-o-meter.com/stats/index.php, Pregledano: 07.02.2012.

Prevencija kriminaliteta ne smije biti stihijska. To je posebno važno istaći kada govorimo o prevenciji krađe identiteta, jer kao takva u BiH nije pravno definisana. "Prevencijom možemo smatrati ukupnost planski osmišljenih i organizovano poduzetih mjera kojima se nastoji ukloniti, ili barem smanjiti direktni ili indirektni uzroci kažnjivih ponašanja." (Horvatić, Cvitanović, 1999)

O potrebi prevencije visokotehnološkog kriminala i zaštite informacionih sistema svjedoči uspostavljanje posebnog državnog odbora u Velikoj Britaniji još 1970. godine. Ovaj odbor, poznat pod nazivom Youngerov odbor, završava sa radom 1972. godine i donosi niz važnih načela[27] za prevenciju manipulacije ličnim podacima. Da je prevencija kompjuterskog kriminaliteta neophodna, ukazuje i veliki broj svjetskih organizacija, poput Organizacije za ekonomsku saradnju i razvoj, Evropske unije, Organizacije ujedinjenih nacija, Međunarodnog udruženja za krivično pravo, Interpola, a posebno treba istaći napore Vjeća Evrope, koje je na konferenciji održanoj 1989. godine donijelo važne preporuke. Tom prilikom predložen je veći broj aktivnosti, poput primjene dobrovoljnih mjera od strane kompjuterskih korisnika, nametanja obaveznih sigurnosnih mjera u pojedinim sigurnosnim sektorima, razrada profesionalnih pravila ponašanja prilikom postupka obrade podataka, uključujući i primjenu disciplinskih mjera i sl.[28]

Nosioci prevencije krađe identiteta moraju biti tradicionalna tijela zadužena za borbu protiv kriminaliteta, a to su policija[29], tužilaštvo i sudovi. Ova tijela su dužna djelovati preventivno jer raspolažu najkvalitetnijim informacijama. Sa druge strane, kako bi se postigao cilj efikasnog preventivnog djelovanja, potrebno je provesti kriminološka istraživanja sa ciljem utvrđivanja etiologije i fenomenologije krađe identiteta. To je neophodno, jer u suprotnom napravila bi se početnička greška, koja se često ogleda u prepisivanju strategija za prevenciju od drugih država. „Prema učenjima Pawsona i Telleya iz 1997. godine, nije dovoljno zaključiti da jedan program prevencije djeluje i koristiti tu činjenicu za njegov „izvoz" u druge države. Prema njima, važno pitanje za prevenciju kriminaliteta osim „what works?" (šta djeluje) jeste i „what works for whom in what circumstances" (šta djeluje za koga i u kojim uslovima?)" (Sherman i Strang, 2004, citirano prema Muratbegović, 2008).

Uzrok krađe identiteta najčešće je motiv za sticanje nezakonite koristi na lak način. Ovo dolazi do izražaja sa razvojem tehnologije, a prvenstveno tzv. kompjutera treće generacije. Sa druge strane fenomenologija krađe identiteta je raznolika i teško predvidiva, a što je dodatni motiv za potencijalnog učinioca. Kada pogledamo cjelokupnu situaciju, sigurno bismo trebali da je pokušamo razumjeti kroz kriminološku Teoriju racionalnog izbora[30]. Osnovno rješenje

---

[27] 1) Svaki podatak u kompjuterskom sistemu mora se koristiti za posebnu namjenu i bez odgovarajuće dozvole ne smije biti upotrijebljen u druge svrhe; 2) pristup podacima treba biti dostupan samo ovlaštenim osobama koje ih moraju koristiti isključivo u svrhe zbog okojih su prvobino prikupljeni; (...) 11)za radnike u kompanijskim centrima treba izraditi poseban kodeks profesionalne etike. Više u Šelih (1981).

[28] Više u Budimlić, Puharić (2009: 195).

[29] Jedna od najprimjenjivanijih policijskih aktivnosti koja ima karakter preventivnih mjera je patroliranje. U virtuelnom svijetu to ne znači ništa drugo do tzv. kompjuterske analize.

[30] Prema ovoj teoriji, osnovni elementi kriminalnog fenomena jesu: Motivisan učinilac, ranjiva žrtva, mjesto (pogodno za zločin).

koje nudi ova teorija ponovo se odnosi na prevenciju kriminaliteta. Naime, kako navodi Boba (2005), prvenstveno je potrebno učiniti težim izvršenje krivičnog djela za učinioca, odnosno navesti ga na zaključak da se izvršenje krivičnog djela neće isplatiti. To je upravo veliki problem sa visokotehnološkim kriminalom i krađom identiteta. Prema Budimliću i Puhariću (2009), osnovne zasluge za visoku tamnu brojku jesu 1. Mala vjerovatnoća otkrivanja; 2. Neurednost u izvještavanju o izvršenim djelima; 3. Neodgovorna zaštita; 4. Porastom broja kompjutera i njihovih korisnika raste i mogućnost za počinjenje krivičnih djela iz ove oblasti. Upravo sa ciljem neutralizacije ovih faktora i takoreći poskupljivanja krađe identiteta, predlažemo prevenciju, kako pojedinačnu, tako i onu na globalnom nivou.

Podjela prevencije krađe identiteta

Krađa identiteta podrazumijeva krađu ličnog identiteta osobe, u smislu krađe pravnog svojstva (ime, prezime, ime roditelja, bračno stanje, državljanstvo i sl.) i/ili faktičkog svojstva (matični broj, mjesto rođenja, godina rođenja). Međutim, krađa identiteta je i krađa virtuelnog identiteta osobe, u smislu pin-koda, lozinke, korisničkog imena i slično, a kada se takvi podaci zloupotrebljavaju.

Podjela prevencije krađe identiteta moguća je prema nivoima, i to:

1. Individualni ili lični nivo koji se može izvesti u vidu:
   a) *Fizičke prevencije*
   b) *Logičke prevencije*
2. Generalni ili kolektivni nivo

Individualna prevencija treba da obuhvati sve mjere preduzete od strane pojedinca s ciljem da osoba zaštiti svoj pravni, faktički, fizički i virtuelni identitet. Što smo više zatvoreni, to je manja šansa da postanemo žrtva krađe identiteta. Ipak, veliki broj građana neopravdano zanemaruje čuvanje privatnih podataka[31], ne znajući da je takozvani socijalni inženjering najčešće korišteni način pribavljanja tuđih podataka[32].

Fizička prevencija na individualnom nivou je neophodna, jer veliki broj osoba postaje žrtva isključivo zbog svoje nepažnje i indiferentnosti, tj. osobe svojom nepažnjom postaju latentne žrtve, odnosno osobe koje teži ka vlastitoj viktimizaciji. Često vidimo lozinke zalijepljene po stolovima ili monitorima računara, pin-kod se drži uz kreditnu karticu, koriste se jednake lozinke na više mjesta, a sve više je prisutno instaliranje nepotrebnih programa koji su najčešće zabavnog karaktera. Pored toga, često nepotrebno, dobrovoljno dajemo lične podatke. Dobar primjer je Facebook, gdje se često ostavlju tačni podaci o datumu rođenja, mjestu rođenja,

[31] "Istraživanje MCSI je sprovedeno u 27 zemalja na uzorku od 11.000 korisnika, od kojih je njih 78% pokazalo znanje o osnovama zaštite za internet, ali su puno manje upoznati sa načinima zaštite od cyber kriminala kao što su krađa identiteta ili otvaranje nametnutih linkova koji se pojave dok su na internetu. Više od pola ispitanika, čak njih 56%, nije upoznato sa načinima prevencije krađe identiteta, a čak 73% ispitanika nisu svjesni značaja zaštite njihove online reputacije". Više na http://www.microsoft.com/bih/press/Dan-sigurnijeg-interneta-2012.mspx

[32] Najpoznatiji haker na svijetu, Kevin Mitnick, najviše je koristio metod *pozivanja novih zaposlenih, lažno predstavljanje i zahtijevanje da mu povjere svoje lozinke* (Budimlić, Puharić, 2009).

nadimku, prebivalištu i slično[33]. Sa druge strane, lične podatke, u bilo kojem obliku, ne bismo smjeli učiniti lako dostupnim, pa ne smije izostati prikrivanje tastature pri unošenju koda na bankomatima, provjera da li ima nelegalno instaliranih kamera ili lažnih otvora na bankomatima, praćenje vlastitih kartica prilikom kupovine zbog mogućnosti skeniranja, znati kome smo dužni pokazati identifikacioni dokument i sl.

Logička prevencija ogleda se ponajprije u pravilnom korištenju sigurnosnog koda, lozinke ili šifre. Budimlić i Puharić (2009) navode niz preporuka neophodnih za kreiranje sigurnosne politike i pravilno korištenje lozinke.

a. *Maksimalna starost lozinke – vrijeme nakon kojeg korisnik mora promijeniti lozinku (od 28 do 42 dana je dovoljna vrijednost)*
b. *Minimalna starost lozinke – vrijeme nakon kojeg korisnik može promijeniti lozinku*
c. *Minimalna dužina lozinke – što je lozinka duža, eksplicitno je teže otkriti (osam karakteristika je dovoljno u većini slučajeva[34])*
d. *Kompleksnost lozinke (kombinacija velikih slova, malih slova, te brojeva)*
e. *Obavezno prijavljivanje korisnika prije promjene lozinke*
f. *Blokiranje naloga*
g. *Trajanje blokade (preporuka je isključiti automatsko isključivanje, jer time omogućujemo napadaču da pokuša par lozinki, a zatim sačeka da se nalog deblokira i pokuša ponovo nekoliko lozinki)*
h. *Vrijeme nakon kojeg se broj pokušaja vraća na nulu (najbolje postaviti na duže vrijeme, jer to sprečava napadača na sličan način kao i prethodna opcija)*

Phishing kao jedan od najčešćih pojavnih oblika krađe identiteta neophodno je prevenirati. Potrebu za tim uvidjele su i velike poslovne kuće poput banaka[35]. Sa druge strane, ono što je veoma jednostavno i dostupno u BiH se veoma rijetko koristi. Prije svega mislimo na značajan broj softverskih paketa i uređaja. Kao primjere možemo navesti Open DNS paket ili uređaj WS1000

---

[33] 87 of the 200 Facebook users responded to "friend requests" from Sophos' fake profile
1. 72% revealed their e-mail address
2. 84% published their full date of birth
3. 87% provide detailes about education and work places
4. 78% unveiled their current address or location
5. 23% listed their current phone number
6. 26% gave their IM screen name

Više na http://www.zdnet.com.au/facebook-users-fall-foul-of-fake-frog-id-thief-339281228.htm dostupno 25.02.2012.

[34] To nam omogućuje 167.961.600.000.000 kombinacija.

[35] Upustvo koje šalje jedna od poznatih banaka u BiH glasi: "Raiffeisen banka Vam nikada neće slati e-mail poruke"

• u kojima se zahtijeva da saopštite Vaše korisničko ime, lozinku ili druge lične informacije. Banka nikada ne koristi e-mail za pribavljanje ličnih ili povjerljivih informacija od klijenata.
• koje sadrže linkove ka E-banking aplikaciji
• u kojima od Vas traži da pozovete call centar banke na broj telefona koji se nalazi u poruci i ostavite Vaše lične podatke"

Više na https://rol.raiffeisenbank.rs/Retail/docs BezbednosnaPravilaZaUpotrebuRaiffeisenOnLineAplikacije. dostupno 23.02.2012.

koji veoma dobro štiti od npr. phishinga, trojanskog konja, spyware i svih oblika napada sa interneta[36].

Generalna prevencija krađe identiteta najprije bi se trebala ogledati u zakonskoj zaštiti pojedinca. Pored toga, prema Budimliću i Puhariću (2009), mjere koje se najčešće pojavljuju u stručnim i naučnim analizama i raspravama jesu:

9. Mjere tehnološke zaštite
10. Edukacijske mjere
11. Korištenje kompjutera u skladu sa etičkim i profesionalnim principima.

Dragičević (1999) navodi niz sredstava i načina koje možemo svrstati u mjere tehnološke zaštite, a koje služe za zaštitu krajnjeg korisnika. To su:

1. Metode fizičke zaštite 2. Provjera pristupa 3. Pravilno postavljanje i zaštita lozinki 4. Kriptografske metode, 5. Kerberos[37], 6. Vatreni zidovi[38], 7. Digitalni potpis, 8. Digitalni vremenski bijeg, 9. Steganografija, 10. Izdvajanje podataka iz mreže, 11. Sigurnosne kopije, 12. Zaštite od virusa, 13. Nadzor rada i korištenje kompjuterskog mrežnog sistema.

Ovdje treba posebno naglasiti dva procesa koji su različiti, a koji se često izjednačavaju od strane laika. Naime, radi se o autentifikaciji[39] i autorizaciji[40]. Takođe, kada govorimo o mjerama tehnološke zaštite, neophodna je kontrola pristupa prostorijama u kojima su smješteni kompjuterski sistemi, uređaji i terminali, kao i ograničeno davanje ovlaštenja korisnicima. (Karvan, 1993)

Što se tiče edukacije prema Petroviću (2001), prvenstveno je potrebno obratiti pažnju na osposobljavnje državnih organa zaduženih za suzbijanje kriminaliteta: policije, sudstva i tužilaštva, sa ciljem njihovog što efikasnijeg rada. Međutim, edukacija svih korisnika mora biti prisutna u smislu da se ažurira i usavršava. Da je edukacija jedan od ključnih faktora prevencije krađe identiteta i kompjuterskog kriminaliteta uopšte, dokazuju i međunarodne organizacije u svojim preporukama. "Ako obratimo pažnju, vidjećemo da je edukacija jedan od ključnih resursa za borbu protiv kompjuterskog kriminaliteta Vijeća Evrope." (Kovač, 1995)

Poštovanje etičkih i profesionalnih principa odnosi se prvenstveno na pojedinca. Mnoge institucije, a prvenstveno državne, imaju izgrađene kodekse ponašanja. O njihovoj neophodnosti govori nam pomenuti Youngerov odbor. Budimlić i Puharić (2009) ističu visoku odgovornost proizvođača. Oni uvijek na svijesti moraju imati mogućnost zloupotrebe proizvoda. U tom smislu kroz odgovoran intelektualan i stvaralački rad treba dati svoj maksimalni doprinos kako bi se rizik neregularnog korištenja sveo na što niži nivo.

---

[36] Vidi http://sophos.com

[37] "Kerberos je mrežni identifikacijski protokol, namijenjen da bi osigurao visok stepen provjere identiteta sudionika mrežnog komuniciranja, korištenjem kriptografske metode tajnog ključa". (Budimlić, Puharić, 2009)

[38] "Vatreni zid je jedan od načina zaštite u kompjuterskim mrežama sa svrhom da spriječi neovlašten pristup podacima i programima. Koristi se da bi sudionicima omogućio pristup internetu bez opasnosti za podatke na lokalnoj mreži s koje se pristupa, kao i kada se želi zaštititi veza između javnog Web servera preduzeća, dostupnog svima, i interne mreže sa kojom je povezan." (Budimlić, Puharić, 2009)

[39] Proces provjere identiteta.

[40] Dodjeljivanje prava autentificiranom korisniku.

REZIME

Identitet osobe treba se shvatiti u pravnom, faktičkom, fizičkom i virtelnom smislu. U svakom slučaju to znači da se radi o privatnim podacima koji moraju biti pravno zaštićeni. Krađa identiteta kao sofisticirana negativna pojava izaziva velike finansijske i druge štete, ali i ugrožava jedno od osnovnih ljudskih prava i sloboda, pravo na privatnost. Krađa identiteta se može izvršiti na veliki broj načina, a otkrivanje učinioca je veoma teško. Sve to je uzrokovalo masovnost ove pojave, kako u svijetu tako i kod nas, a to dokazuju rezultati istraživanja. U već "inficiranom" području BiH, krađa identiteta je prisutna u svim svojim pojavnim oblicima (najčešće kao: Phishing, Spoofing, Skimming), pa smatramo neophodnim da se u svim krivičnim zakonima u BiH nađe kao posebno krivično djelo. Ona je propisana kao krivično djelo u mnogim državama, poput SAD, Kanade, Norveške i sl., međutim u BiH ovo neprihvatljivo ponašanje nije inkriminisano ili je djelimično obuhvaćeno drugim zakonima. Inkriminacijom krađe identiteta doprinijeli bismo, između ostalog, smanjenju drugih krivičnih djela, prvenstveno iz oblasti visokotehnološkog kriminala. Ipak, kako inkriminacija nije nešto što se može uraditi za jedan dan, predlažemo mjere prevencije koje se mogu primijeniti u svakom trenutku. One trebaju da se ogledaju u individualnoj prevencuji, i to kroz fizičku i logičku prevenciju, i kolektivnoj prevenciji, zasnovanoj na mjerama tehnološke zaštite, edukacijskim mjerama, kao i korištenju kompjutera u skladu sa etičkim i profesionalnim principima.

Emil Dirkem je bio ubijeđen da kriminalitet ima korisnu ulogu u društvu, jer podstiče društvo ka razvoju različitih oblika obrade kriminaliteta. (Petrović, Meško, 2008) Prema zvaničnim podacima u BiH krađa identiteta nije izražen problem, pa se nadamo da će reakcija, i to u vidu prevencije ali i kao inkiminisanje, doći ranije nego što nas visoka stopa krađe identiteta natjera na reakciju.

LITERATURA

1. Boba, R. (2005). Crime Analysis and Crime Maping, Thousand Oaks, CA: Sage,
2. Budimlić, M., Puharić, P., (2009). Kompjuterski kriminalitet, Sarajevo, Fakultet za kriminalistiku kriminologiju i sigurnosne studije.
3. Dragičević, D. (1999). Kompjuterski kriminalitet i informacijaski sustavi. Zagreb: Informator.
4. Horvatić, Ž., Cvitanović, L. (1999). Politika suzbijanja kriminaliteta, Zagreb.
5. Ignjatović, Đ. (2005). Kriminologija, Službeni glasnik, Beograd.
6. Karvan, D. (1993). Kompjuterski kriminal, kompjuteri i pravo, Vol. 1, br. 1–2.
7. Kovač, Z. (1995). Savremeni pogledi na kompjuterski kriminalitet i strategije zaštite informacija, Zagreb, Policija i sigurnost, br. 4.
8. Krivični zakon Bosne i Hercegovine Službeni glasnik BiH, broj 37/03.
9. Krivični zakon Republike Srpske, Službeni glasnik Republike Srpske, broj 49/03.
10. Krivični zakon Federacije Bosne i Hercegovine, Službene novine Federacije Bosne i Hercegovine broj 36/03.

11. Modli, D., Korajlić, N., (2002). Kriminalistički riječnik, Centar za kulturu i obrazovanje, Tešanj.
12. Muratbegović, E. (2008). „Evidence Based Crime Prevention: šta (ne)djeluje a šta obećava u kontekstu savremene prevencije kriminaliteta“, Kriminalističke teme, Sarajevo, str. 173–178.
13. Petrović, B., Meško, G. (2004). Kriminologija, Pravni fakultet, Sarajevo.
14. Petrović, S. (2001). Kompjuterski kriminal, Beograd: MUP RSrbije.
15. Prlja, D., Reljanović, M., (2009). Visokotehnološki kriminal – uporedna iskustva, Institut za uporedno pravo, Beograd.
16. Sadiković, L. (2006). Ljudska prava, Fakultet kriminalističkih nauka, Sarajevo.
17. Šelih, A. (1981). Problemi krivičnopravne zaštite privatnosti pri primjeni kompjuterske tehnike, Policija i sigurnost, Zagreb.
18. Tanović, R. (2002). Kaznenopravna zaštita informacijskih sustava, Sarajevo, Kriminalističke teme broj 3–4.
19. Zakon o zaštiti ličnih podataka, Službeni glasnik Bosne i Hercegovine br. 49/06.

Internet izvori:
20. http://conventions.coe.int/Treaty/EN/treaties/Html/201.htm. dostupno 07.09.2009.
21. http://databank.worldbank.org/ddp/home.do dostupno 17.01.2012.
22. http://sophos.com - Sophos Plc dostupno 23.02.2012.

RESUME

The identity of a person should be perceived in legal, factual, physical and virtual sense. In any case, that means that these are private data that have to be legally protected. Identity theft is a sophisticated negative phenomenon that causes great financial and other damages, and also threatens one of the basic human rights and freedoms, the right to privacy. Identity theft can be performed in many ways, and discovering the perpetrator is very difficult. All these things caused mass appearance of this phenomenon, both worldwide and in our country, which can be seen in the research results. Identity theft is present in the ‘’infected’’ area of Bosnia and Herzegovina in all its forms (most often as: Phishing, Spoofing, Skimming), and it is our opinion that it should be a part of all the criminal laws of Bosnia and Herzegovina as a particular criminal offence. Identity theft is considered a particular criminal offence in many states, such as USA, Canada, Norway and others, but in Bosnia and Herzegovina this unacceptable behaviour is not incriminated or it is only partly covered with other laws. Among other things, incrimination of identity theft would contribute to decrease in other criminal offences, mainly in the area of high-tech crime. However, since incrimination is not something that can be finished in a day, we suggest some prevention measures that can be applied at any time. These measures should be carried out through individual prevention, i.e. physical and logical prevention, as well as collective prevention based on technological security measures,

educational measures, and using computers in compliance with ethical and professional principles.

Emile Durkheim was convinced that crime has a beneficial role in the society, since it encourages the society to develop different forms of crime processing (Petrović, Meško, 2008). According to the official data, identity theft is not a great problem, so it is our hope that the reaction, in the form of prevention and incrimination, would come before the high percentage of identity theft forces us to react.

Prethodno saopštenje - UDK 004.738.5: 343.9.02

INTERNET U FUNKCIJI TEORIZMA

Dragan Ranđelović,
Mladen Bajagić,
Bojana Carević
Kriminalističko-policijska akademija Beograd
dragan.randjelovic@kpa.edu.rs

Apstrakt*:* Autori istražuju evoluciju interneta kao nezaobilazne svakodnevne potrebe čoveka u današnjem informatičkom društvu sa posebnim osvrtom na trenutnu terorističku korist od mreže i sve mogućenosti s obzirom na kontrateroristično delovanje. Ono što je počelo kao MIT doktorska disertacija 1961. godine, na US Defense Odeljenju za eksperimente u komunikacijama (*Department for Experiments in Communications*), u godinama koje su sledile evoluiralo je u tehnološku revoluciju sada poznatu kao internet. Internet je postao medij za sve – dobro i loše, pa ni prisustvo terorista na Internetu nije izuzetak. Baš kao ni u proteklim godinama, kada su se teroristi oslanjali na druge tehnologije: telefon, radio, poštu itd., što im se nije moglo sankcionisati, danas im se ne može zabraniti ni pristup internetu. Evidentno je da je savremeno društvo postalo zavisno od novih pre svega za komunikacije najbitnijih informacionih tehnologija zasnovanih na mikrokompjuteru i internetu kao mreži svih računarskih mreža koja im , nažalost, svojim burnim razvojem početkom 21. veka pruža sve veće mogućnosti.

Ključne reči*:* Internet, kiber kriminal, kiber terorizam.

UVOD

Upotreba interneta nije odlika samo bogatog i razvijenog sveta, već je svakodnevna pojava i u siromašnim područjima, a korisnici su ljudi svih uzrasta i iz svih sfera život – uključujući i teroriste. Jedan analitičar je napisao: "*Cyberspace* nije samo početni forum za političke ekstremiste i propagandno širenje poruka, nego i medij za strateške i taktičke inovativnosti u borbi protiv neprijatelja". Opisati i proučiti sintezu ove dve pojave, interneta i terorizma je veoma teško, jer ih gotovo nije moguće svesti pod jednu definiciju. Osnovna karakteristika istraživanja fenomena terorizma razlog je nepostojanja takve definicije, kao i dijametralno suprotna, polazna merila pri shvatanju njegove suštine, naročito kada je reč o njegovim nosiocima i motivima, i drugim elementima koji ga opredeljuju kao akt političkog nasilja (granice dozvoljenog i nedozvoljenog u politici, nivo organizovanosti, stepen učinjene materijalne štete i sl.). Zbog toga je u literaturi prisutno mnoštvo definicija terorizma; odsustvo jedne jedinstvene, opšteprihvatljive definicije, postoji pre svega jer se radi o višedimenzionalnom društvenom i političkom fenomenu[1],[2].

Osnovni zadaci pri definisanju pojma terorizma jesu *njegov opis* (*description*), *objašnjenje* (*explanation*) i *predlog mera* (lekovi) *za njegovo suzbijanje* (*prescription*), odnosno:

1. utvrđivanje pojma i konstitutivnih elemenata terorizma;
2. utvrđivanje uzroka koji određene entitete navode da svoje ciljeve nastoje ostvariti (i ostvaruju) terorističkim aktima, i
3. utvrđivanje preventivnih i represivnih mera za suzbijanje terorizma na globalnom planu.[1]

Internet i slični umreženi sistemi idealni su za terorističke aktivnosti i poslovanje. U najopštijem sličaju, oni pružaju mogućnost sigurne komunikacije sa veoma niskim troškovima. Ovaj koncept zasigurno nije nikakva tajna, i nedavne analize pokazuje široku upotrebu interneta od strane raznih terorističkih organizacija širom sveta.

Analiza je fokusirana na korišćenje (i zloupotrebu) interneta u četiri glavna područja:

1. korišćenje interneta za komunikaciju obezbeđuje tajnost tj. anonimnost komunikacije,
2. pristup informacijama putem interneta i *World Wide Web* (*www*), uključujući i dostupnost informacija o mogućim ciljevima, kao i tehničke podatke u područjima, kao što je oružje,
3. korišćenje interneta kao platforme za širenje propagande o terorističkim grupama, u cilju regrutovanja novih članova, i
4. teroristički napadi na internetu, kiber-ratovanje.

Na Bliskom Istoku, na primer, i sekularne i islamske terorističke organizacije imaju zaposlene na računarskim sistemima, što ne samo da pruža teroristima veću fleksibilnost i bezbednost, nego im otvara širok spektar mogućnosti za ciljane napade, zbog difuzije komande i kontrole.[2]

KORIŠĆENJE INTERNETA ZA TAJNU TERORISTIČKU KOMUNIKACIJU

Većina modernih terorističkih organizacija stvorena je kao veza ćelija međusobno često nepovezanih i raširenih na velikom geografskom prostoru. Ovakva struktura zahteva određeni stepen zaštite grupa prilikom potrebe da se komunicira na daljinu. Takve grupe treba da budu povezane kada planiraju i predvode napade. Potreba za komunikacijom predstavlja izazov kada treba zadržati lokaciju i planove grupe na skrivenom mestu. Opstajanje i uspeh tih organizacija zavisi od dobrih komunikacija koje onemogućavaju obaveštajnim službama praćenje njihove aktivnosti [3],[4].

Internet i srodne tehnologije pružaju ekstremno dobre uslove takvim grupama da ostanu skrivene i sigurne prilikom kontakta. Korišćenje kriptovane komunikacije putem javnih internet servisa pruža mogućnost članovima raznih ćelija da budu u stalnom kontaktu čineći njihovo otkrivanje, tumačenje veoma teškim. Bilo bi zaista teško naći idealniji medijum za terorističke komunikacije od modernog interneta[3][5],

---

[1] Mladen Bajagić, *Osnovi bezbednosti,* Beograd: Kriminalističko-policijska akademija, 2007.

[2] Michael Whine, *"Cyberspace: A New Medium for Communication, Command and Control by Extremists,"* May 5, 1999, Internet 10/01/2010, www. ict.org.il.

[3] Mobilni telefoni i GSM mreža su dobar dodatak komunikaciji koju obezbeđuje internet, ali nemaju isti nivo bezbednosti i mogućnosti koje pruža internet

[6]. Kao i svim drugim korisnicima, internet nudi i teroristima uslugu globalnog pristupa. Pošiljalac i primalac e-pošte može biti bilo gde, u bilo kom trenutku. Kako bilo koji terorista može tražiti više? Istovremeno, internet usluge su besplatne i na dohvat ruke a dostupni propusni opseg je praktično neograničen. Na primer, teroristička organizacija Hamas je niz godina koristila internet za slanje datoteka zaštićenih lozinkom svojim članovima, koje su se ticale napada, uključujući: mape, fotografije, uputstva, kodove i tehničke detalje za razne operacije[4]. Međutim, i sami teroristi se sreću sa preprekama da sasvim bezbedno prenesu svoje podatke; slično kao i kod drugih operativaca, poput onih u obaveštajnim službama ili vojsci, postoji potreba da komuniciraju pouzdano i efikasno.

Pristup Internetu teroristi ostvaruju na više načina, uključujući i najčešće komercijalne metode:

1. *High banduidth*, direktne veze: dokazi pokazuju da sami teroristi imaju dostupnost DSL ili sličnim vrstama direktnih pristupa internetu koji oni koriste za prikrivene komunikacije.Ovde je važno da se napravi razlika između operativaca terorističkih komunikacija i onih koji održavaju terorističke veb sajtove i imaju servere i direktne internet veze.

2. *Dial-up* servis: u najvećem broju slučajeva teroristi se pretežno oslanjaju na ovaj vid pristupa. Pored malih troškova i činjenice da je veoma dostupan, ovaj metod pruža dodatnu bezbednost. Moguće je da pozovete lokalni broj pristupa tzv. "Pop. POP je malo više nego modem sa telefonskom linijom, koji ne snima telefonske brojeve dolaznih poziva. Praktično, terorista može da pristupi POP-u u skoro svakom gradu.

3. Internet kafei: javni pristup internetu, uglavnom u internet kafeima, pokazao se kao popularan među teroristima na Bliskom istoku, Africi i drugde. Ovaj metod odlikuje niska cena i relativno je bezbedan. Postoje neka ograničenja u pogledu veličine datoteka, štampača itd., ali su vrlo korisni za manje kompleksne komunikacije.

4. Bežični (*wireless*) internet je sistem povezivanja računara ili računarske mreže sa internetom bez potrebe za telefonskom linijom ili iznajmljenim vodom. Komunikacija se obavlja bežično, radio-talasima. Uređaji rade po međunarodnom standardu IEEE 802.11b i koriste frekvenciju od 2,4 GHz, koja je u celom svetu namenjena za civilne potrebe, odnosno za njenu upotrebu nije potrebna nikakva dozvola. "Bežični pristup" je vrlo brz i dostupan na mnogim javnim mestima, kao što su kafići, aerodromi i drugo. Anonimni pristup daje korisniku trenutni pristup svakom nalogu na bilo koji komercijalni servis.

PRONALAŽENJE TERORISTIČKIH E-MAIL

Velik deo rasprava usmeren je na činjenicu da su internet i *e-mail* idealani mediji za terorističke komunikacije. Postavlja se pitanje, kako ih obaveštajne službe i službe za sprovođenje zakona mogu pronaći, odnosno odvojiti od mora drugih komunikacija. To je zaista glavni problem obaveštajnog rada, i područje gde

[4] Sami Barak, *"Between Violence and 'e-jihad': Middle Eastern Terror Organizations in the Information Age,"* Stockholm, Swedish National Defence College, 2004.

su limitirane informacije dostupne javnosti. U opštem slučaju, moguće je primetiti da su obavještajne službe SAD i zapadnih zemalja ovu činjenicu veoma kasno prepoznale kao ozbiljan problem. Potencijalno kažnjavanje terorističke zloupotrebe novih tehnologija, kao što su internet i mobilna telefonija, bilo je u velikoj meri zanemareno sve do poslednjih desetak godina, ali, i ono što sada postoji se može okarakterisati kao nedovoljno.

Postoji krivica obavještajnih službi za neadekvatanu pažnju i nedostatak ulaganja u tom području, što se može odraziti na dugoročno rešenje ovog problema. Tu je osnovni nedostatak u američkom pristupu, koji kaže da svaki problem mora imati rešenje, a da to rešenje uključuje tehnologije i novac[5]. U slučaju ako je učinjeno "ispravno", gotovo da je nemoguće otkriti prikrivene terorističke komunikacije ostvarene putem e-pošte Ovde "ispravno" znači da teroristi znaju i pridržavaju se operacija sigurnosti tj. (*Open Platform for Security- OPSEC*)[6] procedure. Pristup takvim terorističkim komunikacijama u budućnosti verovatno će zavisiti od greške, neuredne procedure, obaveštajnih podatka.[7] Primeri uključuju sljedeće:

Informativni podaci o nalogu: U slučaju ako se podaci o nalogu menjaju u malim vremenskim razmacima s velikim pravilnostima, biće jako teško provaliti nalog i naći mesto sa kog je poslata pošta, ali ako postoji ljudski izvor, ili neki drugi obavještajni izvor, koji može osigurati takve informacije, pristup materijalima na nalogu postaje manje problematičan, mada informacije na nalogu tj. elektronskom pismu mogu biti šifrirane, što uzrokuje dodatno opterećenje.

Presretanje e-mail saobraćaja u ciljanim područjima: Jedna od tehnika koja je bila predložena jeste da se u ciljanim područjima pregledaju svi paketi (IP) čiji se promet odvija preko komercijalnih *basebands*[8]. Bez opsežne tehničke diskusije, može se zaključiti da je to je proces koji neće dati značajne rezultate u kratkom roku.

UTICAJ KODOVANJA (ŠIFROVANJE – DEŠIFROVANJE)

U većem delu skorašnje istorije upotreba kodiranja je bila ograničena na vladu i vojne komunikacije, pa je ulaganje u razvoj ove oblasti bilo komercijalno neisplativo. Postoji nekoliko očitih razloga za to. U "analognom dobu" bilo

---

[5] Mark Last, Abraham Kandel Fifhting, *Terror in Cyberspace,* World Scientific Publishing, 2005. Aktuelni programi u ovoj oblasti su veoma osetljivi i vladini zvaničnici nerado razgovaraju o njima (misli se na vladu SAD-a).

6 OPSEC je bezbednosna integraciona platforma koja administratorima mreže omogućava upravljanje svim aspektima bezbednosti u otvorenom okruženju. OPSEC je prvobitno stvorila kompanija Cherc Point softver, što je kasnije preraslo u veliki industrijski standardni bezbednosni okvir. Preko 150 partnera nude OPSEC u okviru svojih proizvoda. OPSEC nudi kompletan skup interoperabilnih bezbednosnih komponenti koje mogu da zadovolje potrebe bezbednosti preduzeća. Bilo koji proizvod koji se pridržava OPSEC specifikacija može biti integrisan. Tom Sheldon and Big Sur Multimedia http://www.linktionary.com/o/opsec. html

[7] Postoje velike tehničke, zakonske i političke poteškoće da se pretraže svi nalozi na AOL**,** Yahoo, ili Hotmail, naročito ako su podaci na nalogu šifrovani, kako se navodi SAD ne bi imao dovoljno električne energije da dešifruje sve šifrovane poruke.

[8] *Baseband* je tip prenosa podataka, gde se digitalni ili analogni podaci šalju preko jednog demultipleksiranog kanala, kao što su Ethernet LAN. Baseband prenos u osnovnom pojasu koriste TDM za slanje simultanih bitova istovremeno uz punu propusnost prenosnog kanala.

koji "*high-grade encryption*" sistem je: (a) skup, i (b) korisniku je nametnuta administracija i logistika bez koje enkripcija ne bi bila moguća. Ozbiljno šifrovanje zahtevalio je hardversko rešenje koje je ujedno i analogno-digitalni pretvarač i digitalni uređaj za šifrovanje, što taj hardver čini kompjuterom specijalne namene [7],[12].

"Digitalna revolucija" je unela neke radikalne promene u ovaj koncept. Glas, podaci i svaki drugi tip medija sada su u digitalnom oblik, i u računaru su spojeni na snažan, *high-speed* procesor. Sve što je sada stvarno potrebno za enkripciju jeste pristojan algoritam šifriranja. [9] U isto vreme, korisnički zahtevi su se dosta promenili. Komercijalne firme i privatna lica, podjednako, postali su sofisticiraniji korisnici računara, a zahtevi za privatnost i sigurnost su povećani upotrebom interneta za komercijalne transakcije, poslove koji uključuju kreditne kartice, kao i ubrzano širenje kompjuterskih prevara. Sve to je veoma uvećalo osetljivost u ovoj oblasti i samim tim upotreba bezbednosnih internet protokola (npr. *https://*) kao i kodiran fajl transfer[10] postaju opšte pojave. Nekolicina kritičkih trendova u ovoj oblasti je dostojna napomene:

1. Nema marginalnih troškova za korisnike: korisnici bezbednih internet protokola, pa čak i sigurnosnih sertifikata za internet transakcije, nisu izloženi stvarnim troškovima. Dok neki bezbednosni sertifikati treba da se kupe na godišnjoj osnovi, za nominalne cene, drugi su dostupni na internetu besplatno – sa kvalitetom jednakim tipu koji se prodaje.

2. Nema dodatnih napora: bezbedna upotreba interneta zahteva malo ili čak nikakav dodatni napor od strane korisnika. Sigurnosni internet protokoli funkcionišu automatski, a kada su instalirani sigurnosni sertifikati, njihovo korišćenje je u velikoj meri automatsko.

3. Razvoj bezbednosnih aplikacija: svet se ubrzano kreće ka eri u kojoj će enkripcija biti integralni deo većine aplikacija (na primer: obrada teksta, komunikacije, itd.), a fajlovi će biti čuvani i transportovani u šifrovanom obliku. Bezbednost će biti objedinjen proces u velikoj meri transparentan za korisnika.

4. Bezbednost na više nivoa: u ne tako dalekoj budućnosti, bezbednost će se održavati na više nivoa. Fajlovi generisani primenom softvera će biti "čuvani" na hard diskovima i drugim medijima u šifrovanom obliku, prenos podataka preko interneta i drugih lokalnih mreža će biti kodiran, uz bezbednosne sertifikate ili druge sigurne protokole, šifrovanje će biti integrisan proces. A velikih tehničkih, ekonomskih ili

---

[9] Kriptografski algoritmi zasnovani su na matematičkoj funkciji koja se koristi za šifrovanje i dešifrovanje. Razlikuju se dve vrste algoritama. 1. Ograničeni algoritmi – bezbednost se zasniva na tajnosti algoritma (istorijski interesantni). 2. Algoritmi zasnovani na ključu – bezbednost se zasniva na ključevima, a ne na detaljima algoritma koji se može publikovati i analizirati (algoritam je javno poznat, a ključ se čuva kao tajna).

[10] Jedan od programa za kriptovanje (dekriptovanje) fajlova koji podržava sve tipove fajlova (ekstenzije), zove se Digit Secret. Između ostalog, algoritmi koji se nalaze u ovome programu su među poznatijim: Blowfish (448 bitni ključ), Twofish (256 bitni ključ), CAST (128 bitni ključ), i da ne zaboravimo jedan od poznatih AES (Rijndael, 256 bitni ključ). Kompresije koje su omogućene za enkripciju fajlova izvode se po nivoima 1, 2, 3 itd. sve do snažne (*strong*) enkripcije (kompresije). Tu je i podrska slanju enkriptovanih podataka putem imejla, ili drugog tipa slanja drugom korisniku. Slanje se izvodi na sledećem principu: izvršava se enkripcija fajla u određenoj ekstenziji sa lozinkom koju pošiljalac odredi, korisnik koji prima fajl moze da otvori fajl jedino ukoliko ima instaliran ovaj program i dostupna mu je lozinka (šifra) za pristup fajlu sa podacima.

pravnih barijera nema. Era šifrovanja svih podataka se brzo približava. Za obaveštajne službe i agencije za sprovođenje zakona, pronalaženje terorista, špijuna, kriminalaca i ostalih u budućnosti bi moglo biti problematično. To više nije svet gde postoji samo mali broj šifrovanih komunikacija. Sve će biti šifrovano. Dva preostala pitanja jesu:

1. da li šifrovane komunikacije ili datoteke od interesa uopšte mogu biti locirane?
2. da li će biti moguće dešifrovanje terorističkih komunikacija blagovremeno i na ekonomičan način, tako da te informacije uopšte budu od koristi?

To je još uvek veoma malo prostora za rešavanje ovih kritičnih pitanja na ozbiljan način. Prvo, nalaženje bilo koje komunikacije od interesa u moru kodiranih digitalnih bitova i paketa će postati obeshrabrujući zadatak. Korišćenje žive sile za pristup i pretraživanje mase podataka iz mreže operatera neće biti visoko produktivno[11]. U najmanju ruku, biće neophodno da postoji neka "spoljna" naznaka izvora i primaoca podataka. U julu 2004. godine, na primer, oduzimanje nekoliko računara koje je koristila Al Kaida u Pakistanu omogućilo je da se ispitaju hard diskovi sa sačuvanim porukama i datotekama. Odgovor na drugo pitanje još je problematičniji. Zaista nekvalitetno šifrovanje je stvar prošlosti; tome je doprinela široka dostupnost moćnih digitalnih procesora i dobrih algoritama za šifrovanje. Stvarni problem u "razbijanju" šifrovane datoteke ili bilo koje poruke se odnosi na specifične algoritme i dužine ključa koji se koristi. Čak i kada je pristup tehnički moguć, potrebni su resursi u smislu računara, vremena i ljudstva.

NE E-MAIL TEHNIKE

Gore navedena analiza je u velikoj meri fokusira na imejl kao glavni način tajne komunikacije za teroriste, preko interneta, i zaista, dokazi ukazuju da je mejl najpoželjniji metod za takve komunikacije. Postoje, međutim, i druge tehnike za ostvarivanje takve komunikacije i prenos podataka preko interneta, a koje ne uključuju korišćenje imejla. To su:

1. Podaci ugrađeni u slike (*Steganographi*): metod koji je bio popularan neko vreme jeste ugradnja podataka u digitalne slike. Trenutno postoji doslovno milijarde slika dostupnih na internetu, hostovanih na veb sajtovima i računarima širom planete. Tako terorista (pošiljalac) može da ugradi podatke na slike postavljene na internetu, ili da zameni već postojeću sliku jednom koja već sadrži podatke. Terorista primalac zatim može preuzeti slike sa interneta, i ekstrahovati podatake, bez vidljivog linka pošiljaoca. Ovo je nezgrapan pristup "komunikaciji" putem interneta, ali obezbeđuje značajan stepen sigurnosti za teroriste, a izbegava mogućnost detekcije.

2. Internet "*Dead Drop*" je druga tehnika za tajni prenos informacije putem interneta; ovde se kao pošiljalac koristi (pojavljuje) mesto na serveru, na primer pomoću FTP protokola, a zatim se ukloni primalac datoteka. Moguće je da se za tu svrhu, kao host, koristiti neki nepoznat server, ime fajla ostaje na serveru, ali ne i njegov sadržaj. Ovo je moderna, elektronska verzija "mrtvih kapi", tehnike koju koriste obaveštajci dugi niz godina.

[11] Vrlo teško se može naći dobar način procene digitalnih podataka na internetu; neke procene kažu da se radi o nekoliko exabta, ovaj broj se povećava velikom brzinom.

Pored ova dva ilustrovana korišćena interneta za prikriven prenos podataka, svakako postoje i mnogi drugi, a i novi se svakodnevno razvijaju. Važno je primetiti da se internet može koristiti za komunikaciju i tajni transfer na različite načine, i da takve tehnike nisu tajna i, što je još važnije, obezbeđuju veliki stepen sigurnosti i slobode.

PRISTUP INFORMACIJAMA PUTEM INTERNETA

Pored toga što teroristi koriste internet za komunikaciju, internet je vrlo brzo postao najveći svetski izvor informacija, koji ne pravi razliku među svojim korisnicima. Zaista, ima čvrstih dokaza da su teroristi širom sveta redovni korisnici interneta, gde dobijaju informacije za razne operacije. U mnogim slučajevima, za terorističku organizaciju ovaj način dobijanja informacija o potencijalnim ciljevima iz izvora dostupnih na internetu je daleko efikasnije i jeftiniji. Jasno je da fizički nadzor bilo kog cilja, od strane terorističkih operativca, uglavnom uključuje putovanja, moguće otkrivanje namera, kao i značajne troškove. Korišćenjem interneta, teroristi mogu dobiti ogromnu količinu informacija za vrlo širok spektar ciljeva. Pristup ovim informacijama je jednostavan i u većini slučajeva pretraživač informacije ne može biti identifikovan[12]. Za mnoge potencijalne mete veliki broj bitnih podataka je dostupan na internetu To često uključuje: fotografije, planove, informacije o satnici rada, kao i druge geografske i operativne podatake od značaja. Čak i kada takvi podaci nisu detaljni ili potpuni, ipak mogu da pruže teroristima prednost, npr. za jednostavno sortiranje potencijalne mete, ili u velikoj meri smanjuju količinu podataka koja treba da se prikupi od strane lokalnih operativaca. Pristup sajtovima često nije ograničen i generalno je dostupan bez troškova korisnika. Osim toga, pristup najvećem broju sajtova je zasnovan na "anonimnoj" bazi, tj. server sajta ni na koji način ne prati aktivnosti korisnika sajta. Iako mnogi sajtovi, u stvari, snimaju IP adrese korisnika, sofisticiranim teroristima korisnicima interneta nije teško da se povežu sa adrese koja se ne može lako pratiti [8],[9].

S razvojem društva zasnovanog na informacionoj tehnologiji i internetu, priroda meta terorista se promenila. Velika gužva na takvim sistemima (E-poslovanje, E-trgovina) dovodi do situacije u kojoj će nove mete biti informacioni sistemi i mreže. Npr., do kraja 2003. godine ukupan promet B2C (*Business to Consumer*), V2V (*biznis-tu-biznis*)[13] i E-trgovanja[14] (*E-kom*) je bio oko jedan trilion (1.000

[12] Moguće ja na pretraživanje određenih podataka staviti alarm. Npr. kada je grupa studenata arhitekture pretraživala nove građevine, među kojima i Kamp David, koji služi za predsedničke potrebe, česta poseta ovim podacima je alarmirala bezbednosne službe.

[13] B2C (Business to Consumer) i B2B (Business to Business), poslovanje B2C predstavlja prvi primenjen način e-poslovanja. Potrošači određuju koje informacije žele da dobiju, za koje ponude su zainteresovani i koju cenu su spremni da plate. Ključni izazovi u oblasti B2C poslovanja jesu: naterati one koji krstare internetom da kupe proizvod/uslugu; stalni doprinos lojalnosti potrošača (personalizacija sajta); zadovoljstvo potrošača. B2B poslovanje je sad najrasprostranjenije. Uticaj B2B sajtova čini tržišta efikasnijim jer danas, korištenjem interneta, pristup informacijama je znatno olakšan.

[14] Internet je postao glavni kanal prodaje za različite industrije. Najranije interesovanje za internet bilo je rezultat želje da se bolje komunicira i bude ispred ostalih. Uzroci sporog rasta elek. trgovine jesu: sigurnost i privatnost, troškovi infrastrukture i pitanja vezana za porez kod poslova koji se

milijardi) američkih dolara. Većina vodećih banaka u svetu objedinjuje sada onlajn formu bankarskih usluga i korišćenje elektronskih kreditnih kartica kako bi povećale broj korisnika i mogućnost korišćenja takvih usluga. Vladine službe idu ka tome da postanu ‘’umrežene’’ u pokušaju da povećaju svoju efikasnost i pruže brži i bolji pristup svojim uslugama.

Razne javne i privatne usluge koje postoje na internetu atraktivne su mete za teroriste. U trci sa tehnologijom mnogi postojeći sistemi sa onlajn uslugama imaju manje nego zadovoljavajuću kontrolu obezbeđenja. Takvi sistemi vrše funkcije kao što su berzanska i bankarska poslovanja, kontrola nuklearnog naoružanja, vođenje i kontrola vazdušnog saobraćaja i drugih hitnih službi. Vlade počinju da prepoznaju nedostatke takvih sistema i definisale su potrebu za boljim stepenom zaštite. Kritičnim tačkama sistema je označeno sledećih pet oblasti, potencijalnih meta terorista:

- informatika i komunikacije;
- bankarstvo i finansije;
- energija (nafta, gas, struja);
- dostava trgovinskih proizvoda;
- usluge od vitalnog značaja za čoveka.

Internet je ‘’lepak’’ u povezivanju različitih infrastruktura. On može biti okarakterisan kao mreža svih mreža – povezuje milione privatnih kompjutera i mreža zajedno. U isto vreme on služi javnoj, naučnoj, poslovnoj i državnoj namena i svrsi. Kao što ne postoje geografske (fizičke) granice interneta, tako ne postoje jasne linije razdvajanja između poslovanja, vojnih, javnih ili naučnih sistema. Takođe, internet nikada nije bio osmišljen za poslovnu i komercijalnu upotrebu i zbog toga nije bilo predviđeno da bude siguran i obezbeđen. Povezane i zajedničke slabosti interneta čine zaštitu ključnih sistema teškom, a ostavljaju otvorena vrata za terorističke napade.

Mogućnost za usmerenje napada koji imaju veliki uticaj na javnost, sada ne dovodi do nepotrebnog gubitka života ljudi i daje terorizmu sasvim novu formu. Tradicionalni terorizam je koristio nasilje da zaplaši javnost i privuče svetsku pažnju. Ekstremno nasilje je u pojedinim slučajevima dovodilo do žestoke kontrareakcije u javnosti protiv terorističkih grupa i u nekim slučajevima štetilo njihovim ciljevima. Simpatije prema određenim grupama mogu biti potkopane javnim besom zbog gubitka života nedužnih. Terorističke grupe koje traže simpatije, kao i pordšku i zaštitu od ljudi za svoja delovanja, naučile su da budu veoma selektivne u svojim napadima, kako ne bi izgubile pristalice. Terorističke grupe koje opstaju na osnovu podrške određenih zemalja, takođe treba da budu pažljive kako ne bi izgubile podršku tih zemalja, privatnih donatora i drugih nevladinih organizacija širom sveta.

---

obavljaju elektronski. Intranet omogućuje povezanost svih jedinica, ujedinjuje računare u jedinstven sistem, koji može poslužiti integraciji različitih procesa i sistema koji postoje u kompaniji. Osnovna svrha ovakvog sistema je da se omogući ažuriranje informacija kada god je to potrebno. Kompanije koriste intranet da bi povezale različite grupe, projekte, aktivnosti u organizaciji. Intranet omogućuje prikupljanje operativnih podataka o aktivnostima u oblasti finansija i računovodstva i povezuje ih sa procesom donošenja odluka i merenja performansi. Osnovni zadaci odeljenja za ljudske resurse su obaveštavanje zaposlenih o osnovnim zbivanjima u kompaniji i pružanje informacija o zaposlenima. Intranet se koristi i za oblast koordinacije rada prodajnog odeljenja, jer pripadnici ovog odeljenja uvek traže ažurirane informacije o cenama, promociji, potrošačima i konkurenciji. Intranet se koristi i za informisanje u proizvodnji.

LOGISTIKA ZA TERORISTIČKE OPERACIJE

Postoji značajan broj dokaza da teroristi sve više koriste internet kao logistiku za svoje aktivnosti. Rezervacije aviona i vozova se vrše preko interneta i većina terorista koji su učestvovali u napadima je rezervisala karte preko interneta. To je činjenica savremenog života, jer se internet baziran na veb sajtovima koristi za raspored, rezervacije, prodaje karata, i druge vidove putovanja. Ove usluge pružaju veliku efikasnost i za operatera i za putnike. Ali, ovaj način takođe pruža teroristima mogućnost za organizovanje rute i drugu logistiku, kao što je prenos pošiljke, na način koji obezbeđuje značajnu anonimnost. Kao i sa imejlom terorista može biti izgubljen, tj. pomešan sa velikim brojem legitimnih internet korisnika.

Jedini put kada teroristi postanu "vidljivi" jeste kada se pojave na aerodromu, gde se vrše samo površne provere njihove identifikacije. Pošto je malo verovatno da će svet prestati da koristi ove načine, i da će se vratiti na stare tehnologije, ostaje pitanje šta se zaista može uraditi, za otkrivanje korišćenja interneta od strane terorista. "Dobra vest" je da su sve takve transakcije zapisane u digitalnom obliku i da se čuvaju u bazama podataka; koriste se kreditne kartice, uglavnom, i organi za sprovođenje zakona će imati odgovarajući pristup. Sa ovim u vezi, DARPA je, recimo, pokušala da pokrene jedan rogram "rudnik", tj. da obeleži podatke koji bi mogli da se vežu za terorističke aktivnosti. Bez obzira na pitanje o privatnosti, ozbiljno tehničko pitanje je kako će biti moguće otkrivanje nezakonitog korišćenja ili korišćenja internet baze u terorističke svrhe.

TEHNIČKI PODACI ZA TERORISTIČKE OPERACIJE

S obzirom na sve veću važnost koja se daje borbi protiv terorizma, obraća se pažnja na veliku količinu tehničkih podataka koji su slobodno dostupni na internetu a koji su od koristi teroristima. Iako je mnogo pažnje javnosti, u ovoj oblasti, usmereno na nuklearne tehnologije i razvoj oružja, na internetu je i ogromna količina korisnih informacija o dizajnu drugih oružja: hemijsko oružje, biološko oružje i drugi oblici oružja. Najgori slučaj bi bio da nuklearna tehnologija, tj. informacije o izradi nuklearnog oružja procure u javnost, i nađu se na internetu. Međutim, i pod pretpostavkom da neke terorističke grupe dobiju informacije, zapravo, sama tehnologija izrade nuklearnog oružja je veoma složena i teška i postoji veliki broj prepreka koje se moraju savladati a za koje internet ne može dati odgovore. Više je problematično to što su pitanja koja se tiču oblasti hemijskih i bioloških agenasa dostupna, jer njihova upotreba nije komplikovana kao u slučaju nuklearnog oružja, pa korist podataka od izvedenih iz interneta može biti velika. Ovde se govori o informacijama koje se prikupljaju putem veba, iz tehnički legitimnih izvora.

Kao praktično oružje terorističkih organizacija u ovom trenutku najčešće se koriste dosta grube tehnologije. Popularni termin je „improvizovane eksplozivne naprave" ili IEDs, koji uglavnom znači oružja koja su sastavljena korišćenjem delova i eksploziva dobijenih od drugih oružja ili granata. Jedan primer klasičog IEDs je „haubica 155 mm, koja je oličenje improvizacije. Ovo nije uvek slučaj. Visokosofisticirani IEDs su izgrađeni od naoružanja s konvencionalnom municijom ili se jednostavno kupe elektronske komponente, preporučene putem interneta.

Stepen sofisticiranosti zavisi od pronicljivosti dizajnera, alata, kao i materijala koji je na raspolaganju. Danas su IEDs izuzetno raznovrsni i mogu da sadrže bilo koji tip dela za pucanje ili inicijator uređaja, kao i razne komercijalne, vojne ili neprirodne hemijske ili eksplozivne delove. IEDs se uglavnom nalaze u Izraelu i okupiranim teritorijama, Iraku i Palestini.

KORIŠĆENJE INTERNETA KAO PLATFORMA ZA ŠIRENJE PROPAGANDE O TERORISTIČKIM GRUPAMA TERORISTIČKI WEB SAJTOVI[15]

Pojava interneta, tj. veb (www) protokola, dovela je do najznačajnije revolucije medija. Po prvi put u istoriji svako sa internet pristupom može lako da pretražuje i pristupi ogromnom broju informacija. Informacije, publikacije, evidencije i podaci bilo kog tipa su sada "*online*", sa velikom količinom dodatnih informacija koje se povećavaju na dnevnom nivou. Nekoliko ključnih tačaka jesu:

1. pristupačnost: sve što je potrebno je relativno jednostavan računar i pristup internetu. Ovo može biti u kući, kancelariji, ili čak i javnom objektu. Istraživanje više ne zahteva odlazak u biblioteku, pa je logistički problem donekle eliminisan.

2. simbolični troškova za korisnike: kada neko ima pristup internetu, može se pretraživati ili "surfovati" beskrajno bez dodatnih troškova

3. simbolični troškovi za publikovanje: troškovi osnivanja veb sajt su mali, sadržaj stavljen na veb sajt je dostupan neograničenom broju potencijalnih korisnika širom sveta, bez velikih troškova. Nema drugih medija koji imaju takav sklad ekonomičnosti, efikasnosti i dostupnosti.

4. inteligentni interfejs i alati za pretraživanje: rani internet protokoli su zamenjeni veb pretraživačima (kao što su *Internet Eksplorer* i *Google Chroma, Mozilla Fireox*), dok je izuzetno moćan pretraživač Google omogućio internet korisnicima da pretražuju internet materijale lako i brzo. Ove "činjenice" savremenog života nisu nedostupne ni terorističkim organizacijama. Kao i druge organizacije i grupe, brzo su uspostavile veliki broj sajtova sa ciljem širenja informacija, regrutovanja članova, prijema sredstava i dr.

Zajedno sa satelitskom televizijom, internet je odličan medij za širenje terorističkih "informacija", uključujući: vesti, propagandu, i druge podatke koje teroristi žele da učine dostupnim, opseg materijala je prilično širok, i obuhvata audio-transkripte, video snimake i druge oblike hiper-teksta. Hezbolah organizacija, na primer, održava višejezični veb sajt (*www.hizballah.org*) koji pokušava da legitimno pruži vesti kao i druge materijale za međunarodnu upotrebu. Vebmaster, Alija Ayoub je izjavio: "Hezbolah nikada neće odustati od interneta. Uspešno je korišćen u prošlosti kada smo pokazali video snimke i slike šteta od izraelskog bombardovanja u Libanu". Slično tome, Hamas, teroristička organizacija, osnovala je sopstvenu internet prezentaciju. Njihov sajt (*www.palestine-info.org*) obezbeđuje i arapske i engleske linkove za širok spektar Hamas resursa, uključujući i statut Hamasa, i izjave vođe vojnog krila *Izz al-Din al Kassam* brigade[16]. Hamas resursi

[15] Pogledati: http://www.jihadwatch.org/ i http://jarretbrachman.net/ Internet> 15.03.2010.
[16] Vidi http://www.muslimedia.com/ARCHIVES/special99/izz-din.htm , Internet 15.03.2010.

su takođe dostupni kroz sajt "Udruženje studenata Muslimana" u SAD-u; sajt Islamske asocijacije Palestine, kao i zvanični sajt Hamasa[17].

MEDIJSKA PAŽNJA

Mediji igraju značajni ulogu kada je u pitanju terorizam. Ova činjenica je naglašena i posvedočena u praksi, a najbolji primer je neprestano ponavljanje snimaka koji prikazuju udar dva aviona na kule Svetskog trgovinskog centra u Njujorku, koji su iskorišćeni da se medijska pažnja u tom momentu prenese na Osamu Bin Ladena i pokret Al-Kaide. Teroristi koriste medije kako bi prosledili svoje poruke širokom audutorijumu, povećavajući tako strah od svoga delovanja. Javnost i mediji daju terorističkim napadima posebnu pažnju. Ako je nasilje ili neka destruktivna kriminalna aktivnost rezultat neke globalne pojave, to tada ne izaziva toliko veliku pažnju. Međutim, ako su dešavanja rezultat delovanja terorista, to postaje glavna meta interesovanja. Pažnja koja se daje teroristima u suprotnosti je sa merljivim efektima njihovih napada. Istorijski gledano, mali broj ljudi godišnje gine od direktnih ili indirektnih posledica terorističke aktivnosti, prirodne katastrofe i nesreće donose mnogo više ljudskih i materijalnih gubitaka.

PLATFORME ZA TERORISTIČKO REGRUTOVANJE I PRIKUPLJANJE SREDSTAVA

Blisko povezana aktivnost sa terorističkim korišćenjem interneta kao platforme za širenje vesti i drugog propagandnog materijala jeste i korišćenje ovog medija, kao sredstva za regrutovanje i prikupljanje sredstava. U pogledu regrutovanja članova i terorističkih operativaca putem veb sajtova, još uvek ne postoji onlajn prijava i obrazac za prijavljivanje, ali, praktično, sve ostalo je onlajn. Veliki deo propagandnog materijala postavljenog na islamskim terorističkim sajtovima u suštini je fokusiran na islamsku omladinu, i potencijalne regrute. Izraelci i njihove pristalice su prikazani u najgorem mogućem svetlu, a dela islamskih mučenika se pominju u herojskom kontekstu. Još uvek nema značajnih istraživanja ili tačnih statističkih podataka o tome koliko je internet efikasan kao alat za regrutovanje terorista, ipak, nema sumnje da mu je uloga značajna.

Hezbolah, Hamas, PIJ *(Palestinian Islamic Jihad)* i druge terorističke organizacije na Bliskom Istoku koriste Internet za različite načine prikupljanja sredstva. Ove aktivnosti se odnose i na transfer novca preko elektronskih *kurira* i legitimnog bankovnog računa, koji se potom koristi za finansiranje aktivnosti organizacija. U ove transfere su uključene islamske dobrotvorne ustanove, profesionalna udruženja, i slične institucije za socijalne i obrazovne projekte. Svi transferi su legitimni i rade se elektronski preko bankovnih računa u SAD, Evropi i Bliskom Istoku. Hezbolah je, na primer, prikupljao novac u SAD preko sajta Podrška Islamskom udruženju otpora[18], sajt gde korisnici imaju priliku za finansiranje operacija protiv "nacionalnih neprijatelja". Isto tako, Hamasova

[17] Višejezični sajt, vidi http://www.palestine-info.info/, Internet 10.03. 2010.
[18] http://en.wikipedia.org/wiki/Islamic_Resistance_Support_Organization, Internet 12.03 2010.

Fondacija za pomoć i razvoj Svete Zemlje pružala je posetiocima sajta mogućnost da kreditnom karticom ili preko elektronske uplate izvrše donaciju. Ovaj sajt je zatvoren od strane SAD 2002. godine.[19] Međutim, zatvaranje tetorističkih sajtova nije trajno rešenje, jer se svakodnevno pojavljuju novi, što nije moguće kontrolisati. Terorističke organizacije su u više navrata pokazale sposobnost da se kreću po veb serverima i alternativnim lokacijama izvan SAD-a. U najboljem slučaju, takva nastojanja mogu se pokazati kao kratkoročno a ne kao trajno rešenje.

Za mnoge terorističke grupe pitanje preživljavanja u određenom vremenskom periodu znači da one moraju da imaju metode za regrutovanje. Prosek postojanja jedne grupe jeste manji od jedne godine. Ako žele da opstanu određeno vreme, grupe moraju da popune svoje redove, koji se osipaju usled hapšenja, smrti, napuštanja članova. Internet postaje zgodan medij za privlačenje potencijalnih regruta. Pretpostavlja se da je do kraja 2003. godine oko 200 miliona ljudi koristilo mrežu interneta. To je veoma velika grupa potencijalnih kandidata. Činjenica je da teroristi mogu koristiti mrežu kako bi pronašli članove i delovali u svojim napadima. Čak i veliki broj terorističkih grupa ima zvanične prezentacije svojih aktivnosti i ciljeva, te kako ne postoji kontrola pristupa i objavljivanja sadržaja na mreži, simpatizeri prostom pretragom ključnih reči na svakom globalnom pretraživaču mogu naći takve grupe i pristupiti im (primeri: Kju Kluks Klan, Hamas, Hezbolah, Tamilski tigrovi). Grupe promovišu svoje aktivnosti sa otvorenim pozivom na delovanje koje može privući čak i mnoštvo tzv. ‘’mekih sledbenika’’ – primer demonstracija u Sijetlu 1999. godine protiv politike Svetske trgovinske organizacije.

TERORISTI I KIBER TERORIZAM

Na listu mogućih terorističkih zloupotreba interneta treba staviti i mogućnost napada na samu mrežu, ili “kiber-terorizam”. U skladu sa tim, često se vode debate oko realne opasnosti od kiber terorizma. Mnogo je učesnika sa obe strane ovog pitanja, iako su mnogi od onih koji učestvuju u raspravi, uključujući i vladine zvaničnike, vojno osoblje kao i novinare sa ograničenim ili nikakavim realnim tehničkim ekspertizama, pa vide dve relativno različite pojave (terorizma i kibernetike), ali logično je da se one ukrštaju u nekom trenutku. Ostavljajući po strani Hezbolah i Al-Kaidu, moguće je razmotriti izvore kiber-napada [10], [11], [13]:

1 Hakeri: Do sada je velika većina kiber napada došla od “hakera”. U većini slučajeva hakeri su najbolje opisani kao zlonamerni, ali ne i kao teroristi. Oni ne žele ni novac ni kraj SAD (ili izraelske vlade). Rade iz ličnog zadovoljstva i satisfakciju im pruža činjenica da su sposobni da upadnu u strogo čuvane kompjutere, mreže, da mogu da raširе virus koji će zaraziti što više korisnika itd.

2. Kriminalci: Od kada su poslovi banaka, trgovina, plaćanje itd. prešli na mreže, sasvim je prirodno da su se i kriminalci preselili u ovaj prostor. Od kada je grupa ruskih sajber kriminalaca napala njujoršku Siti banku[20], komercijalne firme su više zainteresovane za zaštitu svojih resursa.

---

[19] Vidi na: http://www.ustreas.gov/offices/enforcement/key-issues/protecting/charities_execorder_13224-e.shtml, 10.03.2010.

[20] Opširnije na : http://www.reuters.com/article/idUSTRE5BL0I320091222, Internet 15.03 2010.

3. Nezadovoljni radnici: Statistički, najveći broj problema i napada na računarski sistem još uvek dolazi od strane bivših zaposlenih (na primer, administratori sistema), koji su ljuti na svoje poslodavce, a ne na nacije. U većini slučajeva to su sadašnji ili bivši "insajderi" s nekim tehničkim veštinama, i ljudi koji su upućeni u kritične podatke kao što su administrativne lozinke, itd.

Do sada je bilo nedovoljnih dokaza da bilo koja teroristička grupa ima nameru da napadne internet ili računare koji podržavaju poslovanje. Američke obaveštajne službe, vojska i policija su zaplenjivale računare i hardvere teroristima širom sveta, a zaključak koji se može izvući, jeste da su oni korisnici a ne napadači na internetu. U SAD 1998. godine Ministarstvo odbrane je izvelo vežbe pod nazivom "PRAVO prijemnika" i "Crveni tim"; 35 stručnjaka iz Agencije za nacionalnu bezbednost dobilo je tri meseca da vrše elektronski napad na informacioni sistem Ministarstva odbrane i elemenate nacionalne infrastrukture koje podržavaju Ministarstvo odbrane. [21] Koristeći samo javni pristup internetu i običan hardver i softver, Crveni tim je pokazao da može da "obori" telekomunikacijski sistem koji je kičma Ministarstva odbrane, kao i veliki deo nacionalne mreže električne energije i 911 sistema. Godine 2002. održana je vežba "DIGITALNI Perl Harbur" u američkom pomorskom vojnom koledžu, gde je grupa stručnjaka ocenila da je sajber teroristički napad moguć, ali bi bilo potrebno 200 miliona dolara i pet godina da se ostvari.[22]

LITERATURA

1. Bajagić, Mladen i Kešterović, Želimir (2002), *Borba protiv međunarodnog terorizma, pravni aspekat*, zbornik radova „Terorizam u savremenim uslovima", VŠUP, Banja Luka
2. Bajagić, Mladen (2007), *Osnovi bezbednosti*, Beograd: Kriminalističko-policijska akademija
3. Gabriel Weimann (2005), *Terror on the Internet*, Washington, DC: USIP Press
4. Daglas Comer (2006), *The Internet Book: Everything You Need to Know About Computer Networking and How the Internet Works* (3rd Edition), The Internet Book.
5. Douglas E. Comer (2008), *Computer Network and Internet*, Indiana: Purde Universety
6. John R. Vacca (2007), *Practical Internet Security*, Ohio: Pomeroy.
7. Kahn, D. (1996). *The Codebreakers*, New York: Scribner.
8. Preston Gralla (2007), *How to Internet Works*, Indianapolis, IN : Que Pub
9. Ranđelović, Dragan, S. Jaćimovski (2011), *Policijska informatika*, Beograd: KPA
10. Ranđelović, D.: Sigurnost računarskih mreža kao osnove za povezanost policije, bezbednosti i visokotehnološkog kriminala, Tematski zbornik Policija, bezbednost i visokotehnološki kriminal, pp 133–174, (2010), KPA Beograd

[21] Vidi: http://www.nsa.gov/ Internet,15.03.2010.

[22] Opširnije: poglavlje 4 – Digital Perl Harbor, knjiga-Guarding your Business, A menagment Aproach to Security, Sumith Gosh, Manu Manel, and Edvard A. Stork, Kluwer Academy, Plaenum Publisher, New York, 2004.

11. Ranđelović, D. (2011.), Poređenje komercijalnih i nekomercijalnih alata digitalne forenzike i njihova upotreba, Naučnotehnička informacija, Vojnotehnicki institut Beograd.
12. Ferguson Niels, Bruce Shneier (2003), *Practical Crictografhy,* Indianapolis: Wily Publishing.
13. Council of Europe (2008), *Cyberterrorism – The use of the Internet for terrorist purposes*. Council of Europe Publications

SUMMARY

We live in an time-period which is crisscrossed with many informations and, as some scholars say, they became the number one resource. To make this informations to be properly transferred it is necessary supply suitable support ,using modern information and communication technologies, for theirs transfer and use . Also, modern business can not be imagined without the orderly system of information and communication which is implemented in the business process. The fundamental importance of the underlying structure modern business is not just exclusive to this part of human activity, but applies to all areas of human action from education, health care, through social and fiscal functions to the functioning of the government and administrative bodies.

Internet has its advantages, which make it to be almost indispensable in everyday life and business, but it is also suitable medium for use by criminals and terrorists from this reason.

Multiplicity various tools available on the Internet and the ease of their utilization determines that any who knows computers and who has a personal computer connected to the Internet and has a motive, can become a cyber-criminal, and as cyber-crime is essentially a classic crime was committed in the information environment to be in a narrow set of his best-known forms that are listed in this work of: theft, fraud, forgery, extortion, blackmail, sabotage, espionage, pornography, especially is considered the terrorism.

The terrorists are free to use websites, to propagate their ideas and recruit new supporters, the Internet is used for recruiting new members, fundraising, and Collection of intelligence sharing and to coordinate the execution of their actions. Information resources used by terrorists as a handy material for planning and organizing their work program and carried the other ‘’minor’’ activities and functions. For the secure exchange of operational information, terrorists can use cryptographic protection of digital tools. Messages can be protected using passwords of cryptographic public key. This technology is accessible to all who want even in the source code, which allows sophisticated users to perform the testing and make changes to make sure that they are not deceived. Cyber-terrorists and information resources are used as a means to carry out its terrorist activities, any unauthorized access (Hacking), or by using information warfare weapons (viruses, worms, Trojan horse, ...). In addition to the tool, information technology can be the goal of a terrorist attack. Potential targets may be all that linking, running and servicing computers.

Prethodno saopštenje - UDK 341.48: [343.326: 004.738.5](497.6 RS)

PRAVNI OKVIR ZA EFIKASNU BORBU PROTIV KOMPJUTERSKOG KRIMINALITETA U REPUBLICI SRPSKOJ

Darko Jokić
Visoka škola unutrašnjih poslova Banja Luka
jokic.darko@yahoo.com

Apstrakt: Ubrzan i permanentan razvitak informacionih i telekomunikacionih tehnologija, kao i interneta, krajem XX i početkom XXI vijeka značajno je uticao na mnoge oblike i procese društvenog i ekonomskog života. Kao i brojna druga tehnička i tehnološka dostignuća kompjuteri su, od svog nastanka do danas, postali predmet i sredstvo brojnih zloupotreba, posredno ili neposredno mijenjajući fenomenologiju kriminaliteta, što je primoralo međunarodne i nacionalne institucije na reakciju u cilju definisanja, suzbijanja i otkrivanja ove nove vrste kriminala. U ovom radu predstavljen je kraći prikaz nastanka i razvoja međunarodne pravne regulative, kao i krivičnog zakonodavstva u Republici Srpskoj kojim je izvršeno inkriminisanje zloupotrebe kompjutera, kompjuterskih tehnologija, sistema i mreža.

Ključne riječi: kompjuterski kriminalitet, međunarodni propisi, krivični zakon.

UVOD

Kompjuter, kao jedno od najznačajnijih otkrića u istoriji čovječanstva, našao je brojne primjene u skoro svim oblastima života i rada, pa čak i u svakodnevnom životu, a da njegove uloge ponekad nismo ni svjesni. Od pojave prvog kompjutera[1] pa do danas, došlo je do rapidnog širenja upotrebe kompjutera, tako da se omasovila proizvodnja i korišćenje personalnih računara,[2] a samim tim došlo je do stvaranja povoljnih uslova za različite vrste zloupotreba kompjutera i stvaranja jednog novog oblika kriminaliteta koji se najčešće naziva kompjuterski kriminalitet. Kompjuterski kriminalitet je jedan od najbrže rastućih vidova kriminaliteta, jer kriminalci iskorištavaju brzinu, praktičnost i anonimnost koje moderne tehnologije nude kako bi se počinila raznolika krivična djela. To uključuje napade na kompjuterske podatke i sisteme, krađu identiteta, distribuciju pornografskog sadržaja djece, internetske prevare, pirateriju u oblasti kompjuterskih softvera

[1] Prvi računar, nazvan ENIAC, pušten je u eksperimentalni pogon februara 1944. godine, da bi konačno bio završen tek 1946. godine. Njegova je osnovna funkcija bila da u ratne svrhe izračunava putanje artiljerijskih granata, a njegova izrada je koštala oko 400.000 tadašnjih dolara, što je u to vrijeme bila značajna svota. (Aleksić i Škulić, 2010: 380).

[2] Broj korisnika interneta u Kini je u decembru 2011. godine dostigao cifru od 513 miliona, a broj onih koji internetu pristupaju putem mobilnih telefona i tablet računara iznosi 356 miliona. Skoro 250 miliona Kineza koristi Veibo društvenu mrežu (mikroblog servis sličan Tviteru) koja je zabranjena u Kini. dostupno na: http://www.frontal.rs/index.php?option=btg_novosti&catnovosti=16&idnovost=16950, 16. januar 2012.

i drugih kompjuterskih proizvoda i druge oblike, a globalna priroda interneta omogućuje da se nezakonite aktivnosti sprovode bilo gdje u svijetu. Korištenje interneta od strane terorista, posebno za regrutovanje lica i podsticanje istih na radikalne akcije, sve više predstavlja ozbiljnu prijetnju nacionalnoj i međunarodnoj bezbjednosti.

POJAM KOMPJUTERSKOG KRIMINALITETA

Kompjuterski kriminalitet, kao jedan od najnovijih vidova kriminalnog ponašanja, nije se još u potpunosti izdiferencirao u odnosu na druge vidove kriminaliteta i njegovo definisanje i precizno zakonodavno uređivanje i sistematizovanje je izuzetno teško i prolazi kroz stalne promjene i prilagođavanja.[3] Razlozi ovakvim nejedinstvenim i nepreciznim pojmovnim određenjima jesu prvenstveno u činjenici da je riječ o jednom relativno novom obliku kriminalnog ponašanja, kao i u činjenici da kompjuterski kriminalitet ispoljava veliku fenomenološku raznovrsnost koja se ne može obuhvatiti jednom definicijom. Pored toga, važno je napomenuti da se, donedavno, u većini zakonodavstava, oblici djela koji obuhvataju ovu vrstu kažnjivih ponašanja postavljaju dosta široko (ekstenzivno) i razvrstani su i različite zakonske glave, a da ne postoje kompjuterski delikti kao posebna krivična djela.[4]

Prvi pokušaj određenja kompjuterskog kriminaliteta je izvršen 1979. godine u Priručniku o komjuterskom kriminalitetu *(The Criminal Justice Resource Manual on Computer Crime)* od strane ministarstva pravde SAD, kada je kao kompjuterski kriminal određen svaki ilegalan akt (zločin) za koji je nužno znanje kompjuterske tehnologije (Hebert & Pilon, 1984).

Organizacija za ekonomsku saradnju i razvoj (*Organisation for Economic Cooperation and Development* – OECD) prva je organizacija koja je nastojala da se sveobuhvatno pozabavi problemom i da inicira harmonizovanje propisa iz oblasti kompjuterskog kriminaliteta i 1986. godine je donijela preporuke u kojima

---

[3] Kako nema potpune saglasnosti u definisanju, tako i nema potpune saglasnosti u nazivu ove vrste kriminaliteta i u upotrebi je više naziva kao što su: kompjuterski, kibernetički, sajber, kiber, visokotehnološki, elektronski, informatički, računarski kriminalitet. Sam naziv nekada dovodi do terminološke zabune. Termin kompjuterski kriminalitet je najprepoznatljiviji zbog činjenice da se kompjuteri pojavljuju kao sredstvo i/ili objekt izvršenja, ali kako postoje i krivična djela u čijem se načinu izvršenja pojavljuju elementi nezakonitog korišćenja interneta, ovaj naziv nije sveobuhvatan. S obzirom na to da je riječ kibernetika nastala kao prevod engleske riječi *cibernetik* (čiji korijen potiče iz grčke riječi *kybernáō* – upravljam, vladam, kormilarim), a mogli bi je definisati kao sistemsko proučavanje komunikacije i upravljanja u organizacijama svih vrsta, očigledno je da termin kibernetički kriminalitet unosi dodatne zabune. U posljednje vrijeme se koristi termin visokotehnološki kriminalitet, ali se može postaviti pitanje šta se sve podrazumijeva pod pojmom visoke tehnologije. Mislimo da je najadekvatniji termin sajber kriminal (*cybercrime*), kakav je i izvorni naziv u *The European Convention on Cybercrime* i pod tim pojmom se podrazumijevaju tradidicionalna djela učinjena putem kompjutera, djela učinjena putem interneta, tako i djela kojima je cilj specifična kompjuterska tehnologija. O pojmu sajber i kompjuterskog kriminaliteta vidjeti Vagner, S. (2002). Cybercrime. U: *Enciclopedia of Crime and Punishment,* (455–462) Volume 1, editor David Levinson. Thousand Oaks, CA: Sage Publications.

4 Zakonom o izmjenama i dopunama Krivičnog zakona Republike Srpske („Službeni glasnik Republike Srpske“ broj 73/10) uvrštena su krivična djela protiv bezbjednosti računarskih podataka.

je definisala kompjuterski kriminal kao svaku ilegalnu, neetičnu ili neovlašćenu radnju koja se odnosi na automatsku obradu i prenos kompjuterskih podataka.

Prema listi OECD-a kao krivična djela protiv kompjuterskog sistema mogu se smatrati sljedeća krivična djela:

- neautorizovani pristup, tj. neovlašćeni i protivpravni upad u kompjuterski sistem ili mrežu kršeći mjere zaštite (hakovanje);
- neovlašćeno uništenje, brisanje, oštećenje kompjuterskih programa ili podataka,
- računarska sabotaža, u smislu unosa, uništenja, izmjene, oštećenja, brisanja, kompjuterskih podataka ili programa sa namjerom potkopavanja funkcionisanja kompjuterskih ili telekomunikacionih sistema;
- neovlašćeno sprečavanje i ograničavanje komuniciranja ka kompjuterskom sistemu ili mreži, iz njih i unutar njih;
- kompjuterska špijunaža, u smislu bespravnog i uz pomoć nedozvoljenih sredstava otkrivanja, prenošenja ili korišćenja komercijalnih tajni i to sa namjerom da se izazove ekonomski gubitak lica koje posjeduje tu tajnu ili za sebe ili drugog ostvarenja nezakonite imovinske koristi (Ghosh & Turrini, 2010: 326–327).

Savjet Evrope je 1989. godine donio Preporuku broj (89)9, u kojoj je na funkcionalan način usvojen katalog kompjuterskih krivičnih djela i državama članicama je preporučeno da u svojim nacionalnim zakonodavstvima inkriminišu navedena djela. U Preporuci je navedena minimalna lista krivičnih djela (kompjuterska prevara, krivotvorenje, oštećenje i uništenje kompjuterskih podataka i programa, kompjuterska sabotaža, neovlašćeno kopiranje programa), kao i opcijska lista sa sljedećim djelima (neovlašćeno mijenjanje podataka i podataka, kompjuterska špijunaža, neovlašćeno korišćenje kompjutera i neovlašćeno korišćenje kompjuterskog programa) (Scholjberg, 2008). Savjet Evrope je 1995. godine donio Preporuku za krivično procesno pravo broj R (95)13, u kojoj se koristi termin "zločini povezani sa informacionom tehnologijom" (*Offences connected with Information Tehnology- IT offences or IT crimes*) i navodi se da, u fazi istrage za bilo koje krivično djelo povezano sa informacionom tehnologijom, ovlašćeni organi moraju dobiti pristup svim informacijama koje se obrađuju ili prenose u kompjuterskim sistemima. Preporuku je odobrio Evropski odbor za probleme kriminaliteta (CDPC) na svojoj 44. plenarnoj sjednici održanoj od 29. maja do 2. juna 1995. godine.[5]

Na desetom kongresu Ujedinjenih nacija za prevenciju kriminaliteta i tretman delinkvenata u Beču 2000. godine definisan je kompjuterski kriminalitet (*cybercrime*) kao opšti pojam koji obuhvata krivična djela koja se vrše posredstvom kompjuterskog sistema ili mreže, u komjuterskom sistemu ili mreži, ili protiv komjuterskog sistema ili mreže, a obuhvata u principu bilo koji kriminal počinjen elektronskim putem, ili je počinjen u dijelu ili u cijelosti u elektronskom okruženju (ambijentu). Sajberkriminal se ovom prilikom od strane UN-a dijeli u dvije kategorije i u užem smislu predstavlja svako ilegalno ponašanje obavljeno elektronskim putem koje za cilj ima sigurnost kompjuterskih sistema, kao i podataka koje oni obrađuju. U širem smislu sajberkriminal (kriminal vezan za kompjutersku tehnologiju) je svako ilegalno

[5] Vidjeti: http://cm.coe.int/ta/rec/1995/95r13.htm

ponašanje obavljeno pomoću ili u vezi sa kompjuterskim sistemom ili kompjuterskom mrežom, uključujući i takve aktivnosti kao što su ilegalno posedovanje i/ili nuđenje i distribucija informacija pomoću kompjuterskog sistema ili kompjuterske mreže.[6]

U daljem definisanju kompjuterskog kriminaliteta susrećemo se sa prijedlogom Međunarodne konvencije o kibernetičkom kriminalu i terorizmu, sačinjene od strane Stanford univerziteta 2000. godine, gdje se pod komjuterskim (*cyber*) kriminalitetom podrazumijeva ponašanje koje je, s obzirom na sajber sistem, klasifikovano kao krivično djelo po ovoj Konvenciji.

U članu 3. prijedloga ove Konvencije radnje inkriminisane kao kompjuterska krivična djela su svako nezakonito i namjerno preduzimanje bilo koje od sljedećih radnji (ukoliko učinilac ne posjeduje zakonito ovlašćenje, dopuštenje ili pristanak):

a) stvaranje, pohranjivanje, izmjena, brisanje, prenošenje, skretanje, manipulisanje ili ometanje podataka ili programa u kompjuterskom sistemu s ciljem izazivanja, ili znajući da bi takve aktivnosti bile uzrok da taj ili neki drugi kompjuterski sistem prestaje funkcionisati onako kako je predviđen da funkcioniše, ili obavljanje funkcije ili aktivnosti za koje nije namijenjen i smatra se nelegalnim na temelju ove Konvencije;
b) stvaranje, pohranjivanje, izmjena, brisanje, prenošenje, skretanje, manipulisanje ili ometanje podataka ili programa u kompjuterskom sistemu u svrhu pružanja lažnih informacija u cilju da uzrokuje znatnu štetu po lica ili imovinu;
c) ulaženje u kompjuterski sistem za koji je pristup ograničen na vidljiv i nedvosmislen način;
d) neovlašćeno ometanje mehanizama za detekciju i provjeru autentičnosti,
e) proizvodnja, prodaja, korišćenje postova ili na drugi način distribuisanje bilo kojeg uređaja ili programa namijenjenog u svrhu počinjenja bilo kojeg ponašanja zabranjenim članovima 3. i 4. ove Konvencije;
f) korištenje kompjuterskog sistema za počinjenje nezakonite ili zabranjene radnje bilo koje od sedam taksativno nabrojanih konvencija;
g) bavljenje bilo kojim ponašanjem koje je zabranjeno prema članovima 3. i 4. ove Konvencije s ciljem usmjeravanja kritične infrastrukture bilo koje države članice.

Pod kompjuterskim sistemom u ovom prijedlogu se podrazumijeva bilo koji kompjuter ili mreže kompjutera koje se koriste za obezbjeđenje, prenos, koordinisanje ili kontrolu komunikacija podataka ili programa.[7]

U saopštenju Komisije Evropske unije iz 2001. godine ponovo je definisan kompjuterski kriminal i navedeno je da se radi o kriminalu koji, u najširem smislu riječi, na bilo koji način uključuje korišćenje informacionih tehnologija.[8]

George Mohay, Alison Anderson, Bayron Collie, Oliver de Vil i Rodney McKemmish (2003: 1–9) trostruko posmatraju kompjuter, i to: a) kao objekt (metu)

---

[6] Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, Viena, 10–17 April 2000, Background paper for the workshop on crimes related to the computer network: Crimes related to computer networks, Chapter III – Categories of cyber crime, para. 9. dostupno na: http://www.uncjin.org/Documents/congr10/10e.pdf, 20. decembar 2011.

[7] http://iis-db.stanford.edu/pubs/11912/sofaergoodman.pdf

[8] Vidjeti saopštenje Komisije Vijeća, Evropskom parlamentu, Ekonomskom i socijalnom odboru i Odboru regija, od 26.01.2001. godine, dostupno na: http://europa.eu.int.

izvršenja krivičnog djela, b) kao spremište u kojem se nalaze informacije važne za postupak i c) kao sredstvo (alat) za izvršenje krivičnog djela (Mohay, Anderson, Collie, de Vel, McKemmish, 2003: 9–10). Ove podjele se među sobom ne isključuju, što je navedeno i u izvještaju predsjednika Radne grupe za nezakonito poslovanje na internetu koju je formirala vlada SAD.

Eoghan Casey (2000) kompjuterski kriminal definiše kao poseban dio sveobuhvatnog pojma kibernetičkog kriminala, koji se odnosi na navedene tri kategorije, jer dokazi se mogu pronaći kako na kompjuteru koji je predmet izvršenja, tako i na kompjuteru kojim je izvršeno djelo ili je uvezan u neki sistem za deponovanje podataka.

Đorđe Ignjatović (1991: 142) pod pojmom kompjuterskog kriminala podrazumijeva poseban vid inkriminisanih ponašanja kod kojih se računarski sistem (shvaćen kao jedinstvo hardvera i softvera) pojavljuje kao sredstvo izvršenja ili kao objekt krivičnog djela, ukoliko se djelo na drugi način, ili prema drugom objektu, ne bi moglo izvršiti ili bi ono imalo bitno drugačije karakteristike.

Milo Bošković (1999: 139) za kompjuterski kriminalitet navodi da je vrsta delinkvencije i tipologija kriminalnih pojava uzrokovanih zloupotrebom kompjuterske tehnike i tehnologije, a ogleda se u neovlašćenim izmjenama, uništavanju ili krađi programa i tehnologije i njenih komponenti. Isti autor smatra pod kompjuterskim kriminalom i slučajeve kada se uređaji za elektronsku obradu podataka koriste kao sredstvo izvršenja kažnjivih radnji ili kao cilj kriminalne aktivnosti.

Branislav Simonović (2004: 665) kompjuterski kriminalitet definiše kao društvenoopasnu pojavu za čije se ostvarenje učinilac koristi znanjima kompjuterske (informatičke) tehnologije, tako što se kompjuterski sistem shvaćen u najširem smislu (hardver, softver, njihovo jedinstvo; jedan komjuter ili mreža kompjutera) koristi kao sredstvo ili kao objekt kriminalnog napada ili i jedno i drugo.

Živojin Aleksić i Milan Škulić (2010: 381–382) pod kompjuterskim kriminalitetom podrazumijevaju oblik kriminalnog ponašanja, kod koga se korišćenje kompjuterske tehnologije i informatičkih sistema ispoljava kao način izvršenja krivičnog djela, ili se kompjuter upotrebljava kao sredstvo ili cilj izvršenja, čime se ostvaruje neka u krivičnopravnom smislu relevantna posljedica.

Slobodan R. Petrović (2000) pod kompjuterskim kriminalom određuje nedozvoljene aktivnosti u kojima je kompjuter objekt ili sredstvo izvršenja krivičnog djela, a kojima je cilj uništenje ili otuđenje kompjuterskog sistema ili njegovih komponenti; uništenje, oštećenje, otuđenje i neovlašćena izmjena, objavljivanje ili korišćenje softverskih i programskih proizvoda; uništenje, oštećenje, otuđenje i neovlašćena izmjena, objavljivanje ili korišćenje podataka; izvršavanje krivičnih djela; neovlašćeno korišćenje kompjuterskih resursa; narušavanje ili probijanje sistema zaštite.

Dragan Jovašević (2002: 208) kompjuterski kriminalitet definiše kao oblik kriminalnog ponašanja kod koga se korišćenje kompjutera, kompjuterske tehnologije i uopšte informacionog sistema ispoljava kao način izvršenja krivičnog djela, ili kao sredstvo ili cilj vršenja krivičnih djela ili pak kao objekat napada.

Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala Republike Srbije u članu 2. definiše visokotehnološki kriminal „kao vršenje krivičnih dela kod kojih se kao objekat ili sredstvo izvršenja

krivičnih dela javljaju računari, računarske mreže, računarski podaci, kao i njihovi proizvodi u materijalnom ili elektronskom obliku".[9]

KARAKTERISTIKE KOMPJUTERSKOG KRIMINALITETA

Kompjuterski kriminalitet postao je stvarna prijetnja za društvo, jer stalno evoluira i ima veliku fenomenološku raznovrsnost, tj. pojavljuje se u velikom broju formi. Radnja krivičnog djela ogleda se, po pravilu, u manipulacijama na kompjuteru, tako da je kriminalna radnja, gledajući spolja, neprepoznatljiva. Štetne posljedice kompjuterskog kriminaliteta, po pravilu, jesu veoma velike, a ispoljavaju se kako u nastupanju imovinske štete za fizička ili pravna lica (korporacije, državne ili međunarodne institucije),[10] tako i u nematerijalnoj ili neznatnoj šteti koja se ogleda u pravljenju šaljivog sadržaja na tuđim web stranicama. Učinioci ove vrste djela često ne ostvaruju nikakvu imovinsku korist (hakerisanje, kompjuterske sabotaže, dječija pornografija), tako da je njihovo otkrivanje, zbog nedostatka spoljnjih manifestacija, dodatno otežano. Budući da mnoge korporacije, zbog negativne reklame i pogoršanja svog položaja na tržištu, ne prijavljuju slučajeve kada su oštećene raznoraznim zloupotrebama uz pomoć kompjutera, evidentna je velika tamna brojka ove vrste krivičnih djela. Postoji procjena da se manje od 1% kompjuterskih pronevjera otkrije, a da više od 90% svih slučajeva kompjuterskog kriminaliteta ostaje neobjavljeno (Petrović, 2000: 90).

U praksi je evidentan čitav niz problema i teškoća sa dokazivanjem prijavljenih krivičnih djela kompjuterskog kriminala. Dokazivost se teže ostvaruje zbog sve većeg broja izvršilaca ovih krivičnih djela koji pripadaju svim starosnim strukturama (uz napomenu da je starosna struktura sve niža),[11] njihovog nejedinstvenog profila, koji vrlo često ne pripadaju nasilnim i socijalno neprilagodljivijim kategorijama, i sve je manja potreba za njihovim dodatnim obrazovanjem i specijalizacijom. Profil izvršioca se razlikuje od amatera, koji povremeno vrše ova krivična djela, do profesionalaca koji vrše djela u vidu zanimanja. U organizacionom smislu izvršioci se najčešće pojavljuju pojedinačno, ali su česti slučajevi organizovanog djelovanja.[12]

Kada govorimo o kompjuterskom kriminalitetu, sve je manji značaj vremenskih okvira, jer su nebrojene mogućnosti da se radnja djela može izvršiti u

---

[9] "Službeni glasnik Republike Srbije" broj 61/2005.

[10] Prema podacima Interpola, procjenjuje se da su u 2007. i 2008. godini štete od kompjuterskog kriminala širom svijeta iznosile oko 8 milijardi dolara, a što se tiče korporativne sajber špijunaže i krađe intelektualnog vlasništva, procjenjuje se da ukupna šteta za isti period iznosi oko 1 bilion dolara. Vidi: http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime, 12. januar 2012.

[11] 28. aprila 2004. godine, na svoj 18-ti rođendan, Sven Jaschan iz Rotenburga, Njemačka, kreirao je i unio u kompjutersku mrežu više verzija virusa SASER. Virus SASER je napravio enormne štete u bankama, bolnicama, željeznicama i drugim korporacijama, a angažovanjem njemačkih istražitelja, uz pomoć FBI i CIA agenata, S. J. je otkriven i kasnije osuđen na kaznu od 21 mjesec uslovno. Naknadno je angažovan od strane jedne njemačke korporacije kao programer za unapređenje kompjuterskih bezbjednosnih sistema.

[12] O karakteristikama, motivima i tipovima izvršilaca kompjuterskog kriminaliteta više vidjeti u: Mesarović, S. (2006) Motivi i profili izvršilaca. U zborniku: *Zloupotreba informacionih tehnologija i zaštita,* Tara: ZITEH 06. dostupno na: http://www.singipedia.com/content/1013-Motivi-i-profili-izvrilaca.

jednom trenutku, a da se nastupanje posljedice odloži za neko buduće programirano vrijeme. Zbog tehničkih mogućnosti da izvršilac sa svog personalnog računara ili mobilnog telefona izvrši napad na računare ili računarske sisteme na više lokacija u svijetu, sve se manje može govoriti o prostornom okviru kompjuterskog kriminaliteta, a sve više o njegovoj internacionalizaciji.

KOMPJUTERSKA KRIVIČNA DJELA U KRIVIČNOM ZAKONU REPUBLIKE SRPSKE

Usvajanjem Krivičnog zakonika Republike Srpske 2000. godine[13] normirano je više krivičnih djela vezanih za zloupotrebu kompjutera. Ova krivična djela su razvrstana u više glava. Tako je u glavi 16 – Krivična djela protiv slobode i prava građana, u članu 155. stavu 3. (neovlašćeno korišćenje ličnih podataka) predviđeno da se radnja izvršenja ovog djela može izvršiti neovlašćenim ulaskom u tuđu zaštićenu kompjutersku bazu podataka, sa namjerom da njihovim korišćenjem za sebe ili drugoga pribavi kakvu korist ili da drugom nanese kakvu štetu. Za ovo djelo je propisana kazna zatvora do dvije godine, a kažnjiv je i pokušaj krivičnog djela.

U grupu krivičnih djela kompjuterskog kriminaliteta može se svrstati i krivično djelo proizvodnja i prikazivanje dječije pornografije iz člana 190. (glava 90 – Krivična djela protiv polnog integriteta). Prema stavu 1. navedenog člana djelo postoji ako izvršilac nudi, distribuira, prikaže ili javnim izlaganjem ili na drugi način učini dostupnim spise, slike, audiovizuelne i druge predmete koji predstavljaju dječiju pornografiju ili ko takve materijale radi toga proizvodi, nabavlja ili drži ili ko prikaže dječiju pornografsku predstavu. Za ovo djelo je zaprijećena novčana kazna i kazna zatvora do jedne godine, a prema stavu 2, ako je radnja iz stava 1. izvršena prema licu mlađem od šesnaest godina, učinilac će se kazniti zatvorom do tri godine. Može se konstatovati da se djela iz prethodnih stavova mogu izvršiti i na drugi način, koji nema veze sa zloupotrebom kompjutera, što se za radnju iz stava 3. ne može reći, jer je eksplicitno navedeno da ukoliko su djela iz stava 1. i 2. izvršena putem interneta, učinilac će se kazniti zatvorom od šest mjeseci do pet godina.

Neovlašćeno ulaženje u zaštićenu kompjutersku bazu podataka jeste krivično djelo predviđeno u članu 228. u glavi 23 – Imovinska krivična djela. Prema stavu 1, djelo čini ko neovlašćeno uđe u tuđu zaštićenu bazu podataka i unese izmjene, uništi, kopira, upotrijebi, sakrije, objavi ili unese kakav svoj podatak ili kompjuterski virus, ili na neki drugi način učini neupotrebljivim tuđe kompjuterske podatke i programe. U stavu 2. predviđen je teži oblik djela koji postoji ako je djelom iz stava 1. pribavljena velika imovinska korist ili je prouzrokovana znatna imovinska šteta. Za osnovni oblik ovog krivičnog djela propisana je kazna zatvora do dvije godine (pokušaj je kažnjiv), a za teži oblik kazna zatvora od jedne do osam godina.

Sljedeće kompjutersko krivično djelo predviđeno je u članu 260. pod nazivom upad u kompjuterski sistem. Ovo djelo spada u grupu krivičnih djela protiv privrede i

[13] „Službeni glasnik Republike Srpske“ broj 22/2000 i 37/01.

platnog prometa (glava 24), a razlikuje se od krivičnog djela iz člana 228. (neovlašćeno ulaženje u zaštićenu kompjutersku bazu podataka) prvenstveno u tome što se ovo djelo vrši u oblasti privrede, odnosno što djelo iz člana 228. može da postoji i bez namjere pribavljanja imovinske koristi. Za ovo djelo propisana je kazna zatvora do tri godine, a pokušaj djela je kažnjiv. Zavisno od visine pribavljene imovinske koristi ili visine prouzrokovane imovinske štete, zakon razlikuje dva teža, kvalifikovana oblika ovog krivičnog djela. Prvi teži oblik za koji je propisana kazna zatvora od šest mjeseci do pet godina postoji kada visina pribavljene imovinske koristi ili prouzrokovane imovinske štete prelazi 10.000 KM, a ako ova visina imovinske koristi ili štete prelazi iznos od 50.000 KM, propisana je kazna zatvora od jedne do deset godina.

Posljednje djelo u ovom Zakoniku koje, u užem smislu, spada u grupu kompjuterskih krivičnih djela predviđeno je u stavu 3. člana 386. (izrađivanje i nabavljanje oružja i sredstava namijenjenih za izvršenje krivičnih djela) i normirano je u grupi krivičnih djela protiv javnog reda i mira (glava 30). Radnja izvršenja ovog djela sastoji se u izradi, pribavljanju, prodaji ili davanju na korišćenje uputstva ili sredstva koje je namijenjeno za ulaženje u komjuterski sistem, a za učinioca je propisana kazna zatvora do jedne godine.

U širem smislu možemo svrstati u komjuterska krivična djela i brojna druga djela normirana u ovom Zakoniku, kao što su: prevara iz člana 229, neovlašćeno iskorišćavanje autorskog prava iz člana 164, kockanje iz člana 388, kao i sva druga djela gdje se kompjuter može iskoristiti kao sredstvo izvršenja.

Do sada najsveobuhvatniji pravni instrument koji jasno definiše vrste kriminalne aktivnosti na globalnim mrežama komunikacija, kao i uvođenje dodatnih procedura i ovlašćenja državnim organima u cilju efikasnijeg otkrivanja i procesuiranja djela visokotehnološkog kriminala, jeste Konvencija o kompjuterskom kriminalu (*Convention on Cybercrime)*, koju je u Budimpešti 23. novembra 2001. godine donio Savjet Evrope, a podržale su je i neke neevropske države kao što su SAD, Kanada, Japan i Južna Afrika, koje su i učestvovale u njenoj izradi. Navedenom Konvencijom, kao i Dodatnim protokolom koji se odnosi na inkriminaciju djela rasističke i ksenofobične prirode izvršenih preko kompjuterskih sistema, koji je sačinjen u Strazburu 28. januara 2005. godine, u državama koje su ih ratifikovale, pokrenut je niz aktivnosti u cilju inoviranja zakonskih propisa i uspostave organa koji će se specijalizovati za otkrivačku funkciju ove vrste kriminala.

Budući da je Bosna i Hercegovina 9. maja 2005. godine potpisala Konvenciju o kibernetičkom kriminalu (ETS br. 185) i Dodatni protokol uz konvenciju o kibernetičkom kriminalu o inkriminisanju djela ksenofobične i rasističke prirode izvršenih preko kompjuterskih sistema (CETS br. 189), te da ih je ratifikovala 19. maja 2006. godine, nakon njihovog stupanja na snagu 1. septembra 2006. godine[14] izvršena je implementacija u domaćem zakonodavstvu, tj. u zakonodavstvu Republike Srpske, Federacije BiH i Brčko Distrikta BiH.

Zakonom o izmjenama i dopunama Krivičnog zakona Republike Srpske[15] implementirana su kompjuterska krivična djela koja možemo podijeliti u tri grupe.

U prvu grupu spadaju krivična djela iz Glave 24A koja za grupni zaštitni objekat imaju bezbjednost računarskih podataka, a među njima su: oštećenje

[14] „Službeni glasnik Bosne i Horcegovine“ – Međunarodni ugovori broj 6/06.
[15] „Službeni glasnik Republike Srpske“ broj 73/10.

računarskih podataka i programa (član 292a.), računarska sabotaža (član 292b.), izrada i unošenje računarskih virusa (član 292v.), računarska prevara (član 292g.), neovlašćeni pristup zaštićenom računaru, računarskoj mreži, telekomunikacionoj mreži i elektronskoj obradi podataka (član 292d.), sprečavanje i ograničavanje pristupa javnoj računarskoj mreži (član 292đ.) i neovlašćeno korišćenje računara ili računarske mreže (član 292e.).

U drugu grupu kompjuterskih krivičnih djela možemo svrstati djela koja su na sličan ili identičan način bila riješena u Krivičnom zakoniku Republike Srpske iz 2000. godine, a sistematizovana u drugim glavama, i u kojima se kao sredstvo izvršenja eksplicitno navodi zloupotreba kompjutera ili interneta. Kao prvo krivično djelo navodimo proizvodnju, posjedovanje i prikazivanje dječije pornografije (član 200), gdje je, za razliku od ranijeg rješenja iz KZ-a iz 2000. godine, sankcionisano i posjedovanje pornografskog sadržaja, a i zaprijećene su veće kazne, i to: za djelo iz stava 1. kazna zatvora do tri godine, za djelo iz stava 2. kazna zatvora od šest mjeseci do pet godina, a za djelo iz stava 3. (ukoliko je radnja izvršena preko sredstava javnog informisanja ili putem interneta) kazna zatvora od jedne do osam godina. U ovu grupu spadaju i krivična djela neovlašćeno korišćenje ličnih podataka iz člana 176. (riješeno na identičan način kao u KZ RS iz 2000. godine) i izrađivanje i nabavljanje oružja i sredstava namijenjenih za izvršenje krivičnih djela iz člana 398, za koje je na identičan način propisana radnja izvršenja, ali su zaprijećene veće kazne zatvora, i to za djelo iz stava 1. kazna zatvora od dvije do pet godina, a za djela iz stava 2. i 3. kazna zatvora do tri godine.

U treću grupu kompjuterskih krivičnih djela možemo, u širem smislu, svrstati brojna djela normirana u ovom Zakonu, gdje se kompjuter izričito ne navodi, ali se s obzirom na određene pojavne oblike može iskoristiti kao sredstvo izvršenja (razni oblici prevara, falsifikovanje kreditnih kartica i kartica za bezgotovinsko plaćanje, terorizam i sl.).

Ovdje moramo napomenuti da su u Krivičnom zakonu BiH[16] normirana druga kompjuterska krivična djela kao što su: neovlašteno prisluškivanje i zvučno ili optičko snimanje (član 147a.), neovlašteni promet oružjem i vojnom opremom te proizvodima dvojne upotrebe (član 193), nedozvoljeno korišćenje autorskih prava (član 243), nedozvoljeno korišćenje prava proizvođača zvučnog snimka (član 244). U istom zakonu je normirano krivično djelo izazvanje nacionalne, rasne i vjerske mržnje, razdora i netrpeljivosti (član 145a.), što je direktna implementacija Dodatnog protokola koji se odnosi na inkriminaciju djela rasističke i ksenofobične prirode izvršenih preko kompjuterskih sistema.

ZAKLJUČAK

Danas je skoro nezamislivo poslovanje privrednih subjekata, funkcionisanje državnih i međudržavnih institucija i odvijanje životnih aktivnosti građana uopšte bez korišćenja kompjutera i kompjuterskih tehnologija. Budući da je ubrzani razvoj informacionih tehnologija doveo do novih pojavnih oblika kriminaliteta koji

[16] „Službeni glasnik Bosne i Hercegovine" broj 3/03, 32/03, 37/03, 54/04, 61/04, 30/05, 53/06, 55/06, 32/07, 8/10.

se ogledaju u upotrebi kompjutera i drugih sofisticiranih uređaja, kompjuterskih programa, kompjuterskih mreža kao sredstava i objekata izvršenja krivičnih djela, početkom ovog vijeka je, u cilju sankcionisnja ovih nezakonitih radnji, došlo do međunarodne saradnje u krivičnoj oblasti. Sagledavajući potrebu da se osigura ravnoteža između potrebe za provođenjem zakona i poštovanja osnovnih ljudskih prava, a da se donese krivičnopravna regulativa koja će dati okvire za stvaranje efikasnih institucija za borbu protiv ove pojave, došlo je do pokušaja definisanja, i stvaranja međunarodnih, a potom i nacionalnih propisa kojima se inkriminišu kompjuterska krivična djela. Tako se i naša zemlja pridružila velikom broju zemalja koje su u svom krivičnom zakonodavstvu predvidjele različite oblike i vidove kompjuterskog kriminala. Nakon ratifikovanja Konvencije o kompjuterskom kriminalu i Dodatnog protokola koji se odnosi na inkriminaciju djela rasističke i ksenofobične prirode izvršenih preko kompjuterskih sistema došlo je do noveliranja krivičnog zakonodavstva. Međutim, s obzirom na sve moguće pojavne oblike, ovo noveliranje je samo jedan korak ka daljem konstituisanju posebne vrste kompjuterskog krivičnog zakonodavstva.

LITERATURA

1. Aleksić, Ž., Škulić, M. (2010). Kriminalistika. Beograd: Pravni fakultet.
2. Bošković, M. (1999). Kriminološki leksikon. Novi Sad: Matica srpska.
3. Casey, E. (2000). Digital Evidence and Computer Crime: Forensic Sciene. San Diego, CA: Academic Press.
4. Ghosh, S., Turrini, E. (2010). *Cybercrimes: A Multidisciplinary Analisis.* London: Springer.
5. Hebert, M., Pilon, M. (1984). Computer Crime. Canada: Law and Government Division dostupno na: http://publications.gc.ca/Collection-R/LoPBdP/BP/bp87-e.htm
6. Ignjatović, Đ. (1991). Pojmovno određenje kompjuterskog kriminaliteta, *Anali Pravnog fakulteta u Beogradu,* broj 1–3/1991.
7. Jovašević, D. (2002). Leksikon krivičnog prava. Beograd: Službeni list SRJ.
8. Mohay, G., Anderson, A., Collie, B., de Vel, O., McKemmish, R. (2003). *Computer and Instrusion Forensic.* Boston: Ertech House.
9. Petrović, S. R. (2000). Kompjuterski kriminal. Beograd: MUP Republike Srbije.
10. Plesser, R. L., Halpert, J. J., Cividanes, E. W. (2002). *The USA Patriot Act for internet and communication companies,* The Computer and Internet Lawyer 19(3). dostupno na: http://cyber.law.harvard.edu/privacy/Presser%20article--redacted.htm. 15.decembar 2011.
11. Scholjberg, S. (2008). *The History of Global Harmonization on Cybercrime Legislation – The Road to Geneva.*dostupno na: http://www.cybercrimelaw.net/documents/cybercrime_history.pdf. 20.januar 2012.
12. Simonović, B. (2004). Kriminalistika, Kragujevac: Pravni fakultet.
13. Vagner, S. (2002). Cybercrime. U: *Enciclopedia of Crime and Punishment,* (455–462) Volume 1, editor David Levinson. Thousand Oaks, CA: Sage Publications

SUMMARY

Rapid and permanent development of informational and telecommunicational technologies, as well as the internet, by the end of XX and beginning of XXI century had a great influence on many forms and processes of social and economic life. As many other tehnical and technological achievements computers, from their beginning and today, are subjects and tools of many abuses, directly or indirectly changing the phenomenology of crime, which forced international and national institutions reaction in defining, preventing and discovering a new tipes of crime. By ratification of the Convention on Cybercrime and Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems, there have been made preconditions for amending B&H and Republic of Srpska criminal codes. In that way, by incrimination of this tipe of crime there have been made necessary precondition for further organization of legislative and institutional fight against this tipe of unlawful activity. This study represents short review of beginning and development of international legal regulations, as well as Republic of Srpska criminal legislation which have incriminated misuse of computers, computer technologies, sistems and networks.

SUZBIJANJE KRIMINALA I EVROPSKE INTEGRACIJE

Pregledni rad - UDK 316.334.3: 316.7(4-664)

SOCIOLOŠKO-DEFENDOLOŠKI ASPEKTI REGIONALIZACIJE I KLEPTOKRATIJA U HODU KA EVROPSKIM INTEGRACIJAMA

Prof. dr Duško Vejnović,[1*]
Visoka škola unutrašnjih poslova
Banja Luka

Apstrakt: Pitanja i problemi regiona, regionalizacije, organizovanog kriminala, suzbijanja kriminala i „zamišljene“ evropske integracije predstavljaju jednu od najaktuelnijih debata u savremenoj društvenoj nauci. **Naravno, kao i u slučaju većine ostalih tema koje se tiču savremenih društvenih promjena, sociologija i defendologija više nemaju ekskluzivno pravo na diskurs o regionu, regionalizaciji, kleptokratiji, dakle strukturalnom kriminalu i korupciji kao rakrani tranzicijskih društava u zamišljenom hodu ka evropskim integracijama. U okviru novih evropskih odnosa na liniji evropskih integracija i između partikularnih interesa velikih sila, prije svega SAD i** „njemačke Evrope”, **u okviru regionalnih strategija, ovaj dio, region Balkana mora prihvatiti evropske obaveze**[2] **i zadržati svoj tradicionalni geopolitički i geostrateški značaj i ulogu** „zemlje graničara u procjepu svjetova”. **Ovu debatu podjednako mogu da dijele filozofija, pravo, istorija, psihologija, geografija, geopolitika, političke ili neke druge nauke. Kad se danas govori o globalnim odnosima u svijetu, obično se razlikuju dva osnovna pristupa. Jedan je** sociološki pristup**, kojim se ukazuje na globalizaciju modernih razvojnih procesa do svjetskih razmjera, čiji je rezultat stvaranje** modernog demokratskog svjetskog društva**. Drugi pristup je** politikološki, **i on se usredsređuje na vojne, političke i ekonomske odnose moći među državama, kakvi se uspostavljaju u tzv.** novom svjetskom poretku**. Posebno se sagledavaju razlike između opredjeljenja za evropske integracije i stvarnih obrazaca i stilova ponašanja subjekata prava u međunarodnim odnosima opterećenim kleptokratijom (strukturalnom korupcijom i kriminalom), te potrebom njihovog suzbijanja.**

Ključne riječi: regionalizacija, kleptokratija, evropske integracije, suzbijanje korupcije i kriminala,

OPŠTA RAZMATRANJA

Sociološki uvid u najglobalnije, složene i protivrječne razvojne procese (tzv. megatrendove) u savremenom svijetu širi je od politikološkog i bazira se na cjelovitom sagledavanju uzajamnih uslovljavanja i međuuticaja **industrijalizacije**, **rada** i **proizvodnje**, **urbanizacije** društvenog prostora i **modernizacije** kulturnih

[1] * Autor je redovni profesor na Univerzitetu u Banjoj Luci na predmetima sociologija, sociologija sporta, poslovna kultura i komunikacija i defendologija, predsjednik je Udruženja nastavnika i saradnika Univerziteta u Banjoj Luci, Evropskog defendologija centra, i glavni i odgovorni urednik časopisa Defendologija. Kontakt *tin@blic.net,* 0038765526793.

[2] Strategijske osnove saradnje između država, borbu protiv organizovanog međunarodnog kriminala, posebno otkrivanje i sprečavanje trgovine drogom, oružjem, bijelim robljem itd.

obrazaca i sveukupnog načina društvenog života ljudi. Opšti je zaključak da su sva posebna nacionalna društva, u raznim krajevima svijeta i na različitim stepenima razvoja, zahvaćena istim razvojnim procesima (trendovima), da su međusobno sve povezanija i sve sličnija. Zato se danas sve više može govoriti o novom **„svjetskom društvu"**, koje nastaje sa novim sredstvima međusobne komunikacije ljudi, naroda i država koju obezbjeđuje savremena elektronsko-informatička **komunikativna tehnologija**.

Globalizacija kao proces nejednakog razvoja, koji istovremeno fragmentiše i koordiniše donosi nove oblike međuzavisnosti u svijet u kojem ne postoje „drugi". Ti oblici stvaraju nove rizike i opasnosti, pa i opasnosti od kriminala, terorizma, isto tako kao što unapređuju dalekosežne mogućnosti globalne sigurnosti. Globalizacija je jedna od fundamentalnih posljedica modernosti i ona znači više od difuzije zapadnih institucija širom svijeta koja slama druge kulture. Međutim, ono što je još važnije, diskurs o regionima, regionalizaciji, organizovanom kriminalu i terorizmu se transformisao u regionalne socijalne diskurse veoma različitih društvenih grupa i pokreta, koji mogu zastupati veoma različite politike. **Ovi socijalni supstrati regionalizacije, organizovanog kriminala i terorizma kao vida organizovanog kriminala mogu konstruisati svoje socijalne pozicije zastupanjem veoma različitih politika identiteta: nacionalnih, religijskih, etničkih, jezičkih, geografskih, ekonomskih, polnih itd.** Ali upravo to što više nema tradicionalnih ekskluzivnih prava na određenu vrstu diskursa, jeste odraz regionalizacije organizovanog kriminala i terorizma.

Gotovo u istoj mjeri koliko se sociologija i defendologija bave problemima regionalizacije, organizovanog kriminala i terorizma, regionalizacija, organizovani kriminal i terorizam se reflektuju na sociologiju i defendologiju, odnosno ne samo da sociologija i defendologija prate trendove regionalizacije, organizovanog kriminala i terorizma kao vida organizovanog kriminala, već se **i sama sociologija i defendologija regionalizuju**.

Konačno, **samo pitanje regiona, regionalizacije, organizovanog kriminala i terorizma je regionalizovano**, tj. decentrirano u odnosu na nekadašnje diskurse povlašćenih epistemoloških elita, kakve su predstavljali sociolozi, defendolozi, politikolozi, odnosno naučnici uopšte.

GEOSTRATEŠKI REGIONALNI NESPORAZUMI – NASILJE, ILI DIJALOG I TOLERANCIJA

Naslijeđenu i aktuelnu svjetsku stvarnost u najopštijem smislu na početku XXI vijeka karakterišu suprotstavljene tendencije ekonomske prirode između Sjevera i Juga i političke prirode između Zapada i Istoka. Ključ ove pometnje predstavljaju međuetnički nesporazumi i neriješeni granični problemi između država, tendencije u stvaranju nacionalnih država, problemi funkcionisanja tržišta i tradicionalna vojna garancija nacionalne bezbjednosti.[3]

[3] Svjetski ekonomski problemi danas se rješavaju u trouglu – SAD, Japan, Njemačka. U slučaju svjetskih političkih i bezbjednosnih pitanja, opet je u pitanju moćna trojka, samo ovoga puta: SAD, Velika Britanija i Francuska. A kao kruna postojećih odnosa snaga u svijetu, dominiraju institucije kao što su Savjet bezbjednosti Ujedinjenih nacija i Međunarodni monetarni fond. (potcrtao D.V.)

U svakom pokušaju pomirenja geografskih i istorijskih, političkih, ekonomskih i bezbjednosnih problema na istoku i jugu Evrope ili transformisanja država u stabilna multietnička društva, kao odgovor na njih ispoljavaju se regionalni nacionalizmi i šovinizmi s fragmentacijskim tendencijama. **Tako se Evropa našla u dvojakoj ulozi, u ulozi širenja integrativnih ideja i uticaja na zapadnom dijelu i sprečavanja dezintegrativnih tendencija na njenom istočnom dijelu.**

Početak XXI vijeka u Evropi je pružio nadu da će biti prevaziđene ekonomske suprotnosti između Sjevera i Juga i političke između Istoka i Zapada. Od kada su jednopartijski sistemi zemalja evropskog istoka zamijenjeni višepartijskim sistemima zapadnog tipa, politička podjela na liniji Istok–Zapad praktično je postala prošlost. Međutim, ekonomske i druge suprotnosti i dalje su ostale kao problemi na čije prevazilaženje će se morati čekati još izvjesno vrijeme. U najopštijem smislu, njihovo rješenje stoji kao uslov za stvaranje cjelovite geopolitičke slike nekonfliktne **„druge Evrope".**

Od „nove", „druge" hipotetičke ili stvarne Evrope se očekuje da bude zajednica tolerantnih i kooperativnih država, zajednica građana za dijalog i toleranciju. Svi subjekti u međunarodnoj zajednici trebaju se učiti dijalogu i toleranciji, jer sve nevolje proističu iz činjenice što mi ne umijemo da komuniciramo jedni sa drugima. Biti spreman na razgovor, znači odbaciti svaku pomisao na nasilje. Sve dok ljudi razgovaraju, oni su izvan svakog nasilja, nesreće i zla. „U razgovoru se svaki nasilni odnos svodi u okvire spora ili sukoba sa kojim se može izaći na kraj bez težih posljedica. Onog trena kada pojedinci i grupe odbace nasilje kao način rješavanja sporova i sukoba, njihova mašta i duh otvaraju se za iznalaženje novih puteva, jer se više ne mogu oslanjati na stari put dolaska do cilja, put nasilja. Izlaz iz dugog i teškog nasilja može biti samo u jednoj drugoj metodi rješavanja sukoba. Ta metoda jeste dijalog, sporazumijevanje, dogovaranje". (Šušnjić,Đ.1994). Nenasilje, s obzirom na svoj cilj, podrazumijeva prikrivenu moć, a s obzirom na sredstva, ono je blago, ma kakav bio oblik nenasilnog djelovanja, štrajk glađu, pasivan otpor u obliku obustave rada, građanska neposlušnost itd. – on je u stvari moćan oblik djelovanja.

Samo vaspitanjem i obrazovanjem za dijalog i toleranciju može se steći svijest da su drugi čovjek i naša kultura naša dopuna, a ne naš pakao. Ko nije trpeljiv, ne može biti savremen čovjek: još nije dorastao do čovjekove visine! Da bi to postigao, on mora da osluškuje različite glasove vremena i različite načine govora, jer samo tako ima mogućnosti da upoređuje, bira i stvara. **Jedan uistinu dijaloški način mišljenja i življenja imao bi za posljedicu da među misliocima ne bi bilo dogmatika, među vjernicima ne bi bilo fanatika, a među političarima ne bi bilo tirana.**

Zapadna Evropa je kroz trgovinu i integracione procese čak i nekadašnje neprijatelje preobrazila u političke partnere i dobre susjede, a kroz vojno-političku organizaciju uspjela je da se integriše i preko Evropske zajednice stvori nadnacionalne organizacije koje je vode ka projektu „Sjedinjenih Evropskih Država"[4]. I ostale evropske zemlje, posebno istočne, s tržišnom ekonomijom i parlamentarnim demokratskim institucijama ubrzo bi potpuno trebale da se priključe tom projektu.

[4] Najznačajnije nadnacionalne organizacije jesu: Savjet ministara evropskih zemalja, Centralna banka EZ, Evropska investiciona banka i mnoge druge organizacije u oblasti ekonomije, privrede i kulture.

Međutim, na tom putu, bar prema strateškim analizama i procjenama, uz još nesređenu balkansku međuetničku i civilizacijsku pometnju otvaraju se i nova pitanja koja bude nadu za realizaciju regionalne strategije, a po nekima i sumnju za bolju budućnost.

U prekomponovanoj Evropi regionalna strategija bazira se na: mjerama bezbjednosti i borbe protiv organizovanog kriminala, tranzitu robe i putnika, ekonomičnosti mreže energetskog snabdijevanja u okviru Pakta za stabilnost Evrope i Jugoistočne Evrope, osposobljavanju Dunava kao transevropskog koridora, saradnji između međunarodnih finansijskih institucija stabilizacije, regionalnog povezivanja i asocijacije balkanskih zemalja sa Evropskom unijom, zatim ostvarivanje „Regionalne strategije svjetske banke" o Balkanu (The World Bank, 2000)[5]**, poštivanje i sprovođenje međunarodnih sporazuma itd.**

U sagledavanju problema stabilnosti u međunarodnim odnosima treba uzeti u obzir posljedice geopolitičkih i geostrategijskih promjena.

Za evropske odnose i posebno balkanske zemlje, neophodno je sagledavanje karaktera odnosa (saradnje i razlika) između SAD i Evropske unije u cjelini, i posebno odnosa između SAD i Njemačke, kao i odnosa Njemačke sa Rusijom, Ukrajinom i zemljama Srednje Evrope, novih evropskih energetskih projekata, sa jedne strane, i posebna oblast interesa vezanih za aktuelna i potencijalna krizna žarišta na Balkanu i Sredozemlju.

Strategijsku poziciju Balkana i Bosne i Hercegovine karakteriše odnos i politika velikih sila prema ovim područjima na globalnom planu, međusobni odnosi i granični problemi novonastalih država na regionalnom planu. Za stabilnost Balkana značajna je strategija, politika i pozicija SAD u Sredozemlju, uticaj Evropske integracije na politiku Albanije i Bugarske u regionu, kao i Grčke i Turske.

U odnosima između novih država – bivših jugoslovenskih republika, na stabilnost u regionu uticaće otvoreni određeni teritorijalni sporovi, u vezi s kojima će se ukrštati i identifikovati interesi velikih sila. Ove interese bitno će determinisati odnosi sa novonastalim državama, a sigurno će „oživjeti" stare geopolitičke i strategijske nastupe kroz podršku pojedinim narodima i novim državama. Posebna transparentnost takve politike može se očekivati prema Bosni i Hercegovini, Srbiji (albanski i mađarski nastup) i Makedoniji. Međunacionalne suprotnosti i oživljavanje geopolitičkih pretenzija moguće su na lokalnim civilizacijskim razdjelnicama Sandžak, Kosovo, BiH, odnosno Crna Gora i Srbija.

U okviru novih evropskih odnosa na liniji evropskih integracija i razmeđu partikularnih interesa velikih sila, prije svega SAD i „njemačke Evrope", u okviru regionalnih strategija ovaj dio, region Balkana, mora prihvatiti evropske obaveze[6]

---

[5] Po tom projektu razvoj regiona bazira se na ostvarivanju pet osnovnih pretpostavki:

- problemi Balkana definisani su kao problemi tranzicije i razvoja, dok su prijedlozi reformi po prvi put usklađeni s potrebom regionalne i evropske integracije,
- subregionalna integracija je važan aspekt političkog okvira uz neka ograničenja,
- prednost se daje evropskoj integraciji u odnosu na subregionalnu integraciju,
- preporučuje se reforma institucija kao prioritet za vlade i donatore,
- naglasak se stavlja na očuvanje ljudskog društvenog kapitala.

[6] Strategijske osnove saradnje između država, borbu protiv organizovanog međunarodnog kriminala, posebno otkrivanja i sprečavanja trgovine drogom, oružjem, bijelim robljem itd.

i zadržati svoj tradicionalni geopolitički i geostrateški značaj i ulogu „zemlje graničara u procjepu svjetova".

U globalnoj politici velikih sila najpresudniju ulogu igraju nafta i religija. Jedno od spornih balkanskih pitanja jeste i ono civilizacijsko. Na globalnom planu čovječanstvo se kreće ka dobu u kome će različite civilizacije morati da nauče da žive jedna pored druge u mirnoj razmjeni, da uče jedna od druge, da jedna drugoj istražuju istoriju, ideale, umjetnost i kulturu, i da se tako međusobno obogaćuju. Alternativa tome, u ovom prenatrpanom malom svijetu, jeste nerazumijevanje, napetost, sukob i katastrofa. Religija kao složena pojava, u vrijednosnom i u institucionalnom smislu, različito je uticala na čovjeka kroz čitavu njegovu istoriju. Ona je, sociološki posmatrano, dio čovjekove kulture. Na južnoslovenskom prostoru, kroz čitavu njegovu istoriju, osnovne nacionalne religije (pravoslavna, katolička, islamska) bile su značajan činilac nacionalne identifikacije. Istovremeno, religije su doprinosile podjelama i otežavale koegzistenciju više naroda u istom društveno – pravnom okviru. U vremenu kada je Evropa ušla u jednu od svojih najvećih kontradiktornosti, integracija i dezintegracija, civilizacijske pretpostavke tolerancije manifestovale su se u svojim suprotnostima.

Saznanja ukazuju da će budućnost razvoja međunarodne zajednice u miru i prosperitetu na globalnom i regionalnom planu, zavisiti od razumijevanja i saradnje između političkih, duhovnih i intelektualnih vođa, od dijaloga, tolerancije i ekonomskog razvoja.

Međutim, u mnogim dijelovima svijeta danas su u toku borbe različitih kulturnih i rasnih grupa, a neke od njih posebno su ogorčene i veoma krvave. Krvavi ratovi ovakvog porijekla vodili su se, između ostalog, u Bosni i Hercegovini, Etiopiji (u Africi) i Gruziji (dio bivšeg SSSR-a).

U isto vrijeme, talasi izbjeglica i useljenika neprekidno prelaze preko raznih regiona planete bježeći od sukoba ili tražeći bolji život. Često se, došavši u novu sredinu, suočavaju sa odbojnošću onih koji su, nekoliko generacija ranije, i sami bili doseljenici.

To je, na primjer, slučaj sa mnogim narodima koji su došli u SAD. Ta zemlja je u kulturnom pogledu najraznovrsnije društvo na svijetu. To je, u stvari, društvo doseljenika: prvobitno stanovništvo – američki Indijanci – čine manje od 1% ukupnog broja stanovnika SAD. Međutim, i Britanija i Evropa uopšte i same brzo postaju kulturno izmiješane. Evropljani kao prvi useljenici u Sjevernu Ameriku, donedavno su bili najbrojnija grupa u SAD i Kanadi. Danas, pak, ima novih talasa legalnog i ilegalnog useljavanja u Zapadnu Evropu, a useljenici dolaze iz Istočne Evrope, Afrike, sa Bliskog istoka i iz Azije, tako da Evropa već doživljava mnoge dileme i sukobe, ali i koristi, kroz koje su nekada prolazile SAD.

Evropa postaje **etnički heterogena** više no što je ikada bila. **Problem usklađivanja etničkih različitosti postao je problem od fundamentalnog značaja za globalno društvo.**

BORBA PROTIV KRIMINALA U EVROPSKOJ UNIJI

Organizovani kriminal predstavlja prijetnju ekonomskom osnovu Evropske unije i takođe ugrožava sigurnost njenih građana. Evropska unija kao svjetski najintegrisanije i najdinamičnije tržište predstavlja plodno tlo za sve

vrste kriminalnih aktivnosti, pa tako i organizovani kriminal. Neka praktična iskustva mjera koje doprinose olakšanom poslovanju, prometu ljudi, dobara i kapitala, poreske, administrativne i mnoge druge olakšice namijenjene upravo ubrzanju ekonomskog prometa, doprinijele su razvoju i jačanju kriminalnih grupa i stvorile okruženje idealno za njihovo djelovanje. Organizovani kriminal odnosi se na aktivnosti koje imaju mnoge osobine redovnog poslovanja, ali su u stvari nezakonite. On najčešće obuhvaća ilegalno kockanje, prostituciju, krađu na veliko, reketiranje i druge nezakonite aktivnosti. Vlade evropskih zemalja sarađuju na planu borbe protiv međunarodnog kriminala na mnogo načina, kao što su potpisani međunarodni standardi u sklopu UN-ove konvencije protiv organizovanog transnacionalnog kriminala, zatim redovni sastanci unutar Savjeta Evrope, tijela koje ne pripada Evropskoj uniji, u cilju dijeljenja primjera dobre prakse u oblasti pranja novca i posebno u oblasti sajber-kriminala.

Da li se za državne organe uopšte može reći da mogu biti počinioci krivičnih djela? Ako se krivično djelo definiše šire nego do sada i obuhvati kršenje moralnih normi sa štetnim posljedicama, odgovor je sasvim jasan. Države su počinile mnoge strašne zločine u istoriji, kao što su uništenje čitavih naroda, bezobzirna masovna bombardovanja, nacistički holokaust i Staljinovi koncentracioni logori. Državni organi često ignorišu ili krše one zakone koje su inače dužni da poštuju. Društvo koje je blagonaklono prema devijacijama u ponašanju ne mora da pati od socijalnog razaranja. Do nekog rješenja se, međutim, može doći jedino ako se **ličnim slobodama priključi socijalna pravda** – u jednom društvenom poretku u kome nema pretjeranih nejednakosti i u kome narod kao cjelina ima mogućnosti da živi pun i zadovoljavajući život. Ako sloboda nije dovedena u sklad sa jednakošću, i ako mnogi ljudi smatraju da je život prazan i jadan, prestupničko ponašanje će se najvjerovatnije usmjeriti prema društveno destruktivnim ciljevima.

Organizovani kriminal, kao društveno negativna pojava, ima izuzetnu sposobnost da koristi povoljne uslove za svoje infiltriranje i da se vješto prilagođava konkretnoj društveno-političkoj i ekonomskoj situaciji, ne samo unutar jedne države, nego i na međunarodnom planu. Internacionalni karakter organizovanog kriminala upravo i podrazumijeva nužnost međunarodne saradnje na planu otkrivanja konkretnih krivičnih djela i učinilaca i obezbjeđenja valjanih materijalnih i ličnih dokaza. Veoma je bitno da svaka država sagleda kakvo je stanje na njenim prostorima u oblasti organizovanog kriminala i da nakon izvršene analize identifikuje uzroke i oblike ispoljavanja ovih negativnih pojava i analogno tome preduzme i odgovarajuće mjere na efikasnijem suprotstavljanju tim pojavama. Ponekad je teško konstatovati o kojem obliku kriminaliteta se radi, što stvara i opasnost da mnogi oblici ne budu otkriveni. To takođe ukazuje na opasnost od tamne brojke kod ovih kriminalnih pojava, što svakako nije zanemarljivo, naročito kada se radi o krivičnim djelima iz oblasti privrednog kriminaliteta.

Organizovani kriminal podrazumijeva, pored postojanja kriminalne organizacije sa visokim stepenom organizovanosti, hijerarhijom, podijeljenim zadacima, disciplinom i planiranjem kriminalne djelatnosti, čiji cilj je ostvarivanje dobiti i stvaranje profita, **obuhvata i određenu vezu kriminalne organizacije sa državom i pojedinim njenim organima**. Ta veza se može ostvariti u vidu saradnje organa za primjenu zakona sa onima koji ne poštuju i žele da izigravaju zakon, u vidu neutralizacije policije i pravosuđa i korumpiranja vlasti, kako bi organizovani

kriminal neotkriven ušao u legalni poslovni svijet, vršenjem uticaja na politiku, sredstva javnog informisanja, javnu upravu, pravosuđe i privredu, i nasiljem i korupcijom policije, sudstva i političke i izvršne vlasti.

Kriminalna organizacija vrši određenu kriminalnu djelatnost kao što je reketiranje, trgovina ljudima, prostitucija, kocka, krijumčarenje ili se radi o kriminalnoj organizaciji sa čvrstom strukturom, podjelom posla, odgovornošću i planiranjem kriminalne djelatnosti, odnosno da se radi o imovinskom kriminalu koji nastoji da se ugradi u legalnu ekonomiju, koristeći nasilje, ali i pribjegavajući, u posljednje vrijeme, prefinjenim metodama uticaja, ili da je to djelatnost neke grupe koja ima za cilj profit i širok dijapazon kriminalnih postupaka, često međunarodnih po svojoj prirodi.

Veza sa državom i njenim organima organizovanom kriminalu daje određenu sigurnost i pruža odgovarajuću zaštitu od krivičnog gonjenja, ali i pojedine privilegije i ustupke koje ne bi mogao da ostvari bez uspostavljenih adekvatnih kriminalnih veza. Dosadašnja iskustva na našem području ukazuju na činjenicu da organizovanom kriminalu određenu zaštitu i koncesije donosi i veza uspostavljena sa velikim privrednim i finansijskim sistemima i političkim strankama, naročito onim parlamentarnim, pa stoga i tu vezu treba smatrati za relevantni element organizovanog kriminala u onim oblicima u kojima se kod nas ispoljava. Organizovani kriminal ne može da opstane i da nastavi svoju aktivnost, makar bez pasivnog dopuštanja svojih operacija od strane organa javne prisile. Ako hoće da opstane, organizovani kriminal mora da neutrališe prijetnje koje dolaze od javne prisile, a to se upravo vrši korumpiranjem javnih službenika, uključujući policijske službenike, njihove nadzornike, javne tužioce, sudije, novinare, izdavače i političare na svim nivoima.

Raspoloživa saznanja i zapažanja o pojavnim oblicima organizovanog kriminala ukazuju na činjenice da je on po svom karakteru i specifičnosti radnji zaista organizovan, a s obzirom na prostor i mjesto izvršenja, u pravilu međunarodni.

Organizovani međunarodni kriminal ne poznaje i ne poštuje granice, nacionalnu i vjersku pripadnost, pol, životnu dob, uz osnovni motiv organizatora za pribavljanje velike materijalne dobiti. Suprotstavljanje organizovanom međunarodnom kriminalu, pojednostavljeno gledano, jeste borba državnih – vladinih institucija, tj. legalnog – zvaničnog pravnog sistema koji poštuje propise – pozitivne zakone i međudržavne ugovore protiv veoma organizovanih lica i grupa ilegalnog sistema koji bez ikakvih ustezanja i skrupula nastoje što prije, tajnije i ne birajući sredstva ostvariti cilj – planiranu materijalnu dobit.

Nerijetko su u pojedinim državama iz kojih se organizuje ili čiji se prostor koristi za organizovani međunarodni kriminal pojedinci iz struktura vlasti umiješani u organizovani kriminal na način tzv. „upoznat sa problemom, a za novac ćuti i ne smeta posao", te i hijerarhijski čvrsto organizovane vladine institucije, kao npr. obavještajne službe, MUP, ministarstvo inostranih poslova itd. Napred istaknute činjenice opet su motivisane materijalnom dobiti. Kada su u pitanju obavještajne službe, one osim materijalne dobiti međunarodni kriminal koriste kao sredstvo za ostvarenje svojih ofanzivnih ciljeva i u smislu ciljanog operativnog prodora, što ukazuje na bezbjednosni značaj problema i složenosti u pristupu navedenom fenomenu.

Osim navedenih podataka koji se vežu za pojam organizovanog kriminala, treba imati na umu da je svaka radnja za sebe klasično krivično djelo, prekršaj

carinski i finansijski, i da se kriminalističkom obradom i presijecanjem pojedinog slučaja ne suzbija organizovani kriminal čija je društvena opasnost znatno veća od pojedine radnje, te da rješavanje jednog lica u lancu međunarodnog kriminala ne znači potpuno kidanje tog lanca već samo preusmjeravanje na drugi pravac.

Među najčešćim pojavnim oblicima organizovanog kriminala na prostoru Bosne i Hercegovine i regiona jesu: ilegalna proizvodnja i promet narkotika posebno na pravcu iz evroazijskih zemalja i zemalja Jugoistočne Evrope, preko prostora bivše Jugoslavije prema zapadnoevropskim državama, ilegalni promet naoružanja i vojne opreme iz područja bivše Jugoslavije u kojima su vođeni ratovi prema zapadnoevropskim državama, Albaniji, Kosovu, Crnoj Gori, Čečeniji itd., trgovina ljudima, krijumčarenje ilegalnih emigranata, krijumčarenje radioaktivnog materijala i skladištenje nuklearnog otpada i opasnih materija, te za područje istočne Evrope i Balkana specifično krijumčarenje dragog kamenja i plemenitih metala, skupocjenih automobila i visokoakcizne robe.

U pomenutim oblicima međunarodnog kriminala nerijetko se isti kanal ili pravac (u kom se učesnici po hijerarhiji ugrađuju u cijenu) koristi za dva oblika organizovanog kriminala. Na primjer, droga iz Albanije i sa Kosova preko Srbije, Crne Gore, Bosne i Hercegovine, pa dalje preko Hrvatske u pravcu zapadnoevropskih zemlja postiže dva do tri puta veću cijenu „na veliko kod velikih šefova", da bi se ponovo „na malo" uz još veću cijenu vraćala u Bosnu i Hercegovinu, Hrvatsku i tako dalje. Slično tom pojavnom obliku, „veliki trgovci" iz zapadnoevropskih zemalja (uz znanje ili pokroviteljstvo moćnih i za određeno područje zainteresovanih službi) kupuju ilegalno sabrano oružje „na veliko" iz zemalja nastalih raspadanjem Jugoslavije i Sovjetskog Saveza, pa to isto oružje plasiraju u krizna područja (na primjer, Kosovo, Čečenija, Crna Gora i slično), uz uvećanu cijenu „na male količine", kao kod droga ili ga „u paketu" kompenzuju za drogu iz spomenutih područja i slično.

Za period od 2007. do 2013. godine Evropska unija je predvidjela djelovanje definisano programom **„Prevencija i borba protiv kriminala"** donesenim 2007. godine. Ovaj program postoji unutar okvirnog programa **„Sigurnost i očuvanje slobode".** Time se zamjenjuje okvirni sporazum o policijskoj i pravosudnoj kooperaciji u kriminalnim stvarima. **Njegova uloga je da suzbije kriminal sa naglaskom na terorizam, trgovinu ljudima i zlostavljanje djece, nelegalnu trgovinu oružjem, narkoticima, te korupciju i razne vidove prevare.** Ovaj se program sastoji iz **četiri glavne oblasti:**

- **sprečavanje kriminala i kriminologija,**
- **sprovođenje zakona,**
- **zaštita i podrška svjedocima,**
- **zaštita žrtava.**

Unutar četiri oblasti djelovanja, ovaj program **ima za cilj da**:

- **razvije koordinaciju među agencijama za sprovođenje zakona, ostalih nacionalnih institucija i organa EU,**
- **promoviše i unaprijedi primjere dobrog djelovanja u cilju zaštite žrtava kriminala kao i svjedoka kriminalnog djela,**
- **osnaži sprovođenje metoda neophodnih za strateško suzbijanje kriminala i očuvanje sigurnosti.**

Ovi se ciljevi izvršavaju u skladu sa djelovanjem Europola i Cepola (European Police College – Koledž evropske policije), u sklopu akcija koje se kreću

od operativne kooperacije i koordinacije, analitičkih, nadglednih i evaluacijskih aktivnosti, razmjene tehnologija i metodologija, obuke, razmjene osoblja i stručnjaka, te ocjene uspješnosti posebnih aktivnosti i akcija.

U skladu sa ovim ciljevima, 2009. godine je pokrenuta inicijativa za sprečavanje kriminala oličena u **Evropskoj mreži za suzbijanje kriminala**. Ova mreža djeluje kao okvir za saradnju evropskih zemalja u toj oblasti, i to kroz:

- **uspostavljanje saradnje, komunikacije i razmjene informacija između strana u istrazi na posebnom slučaju,**
- **sakupljanje, ocjenjivanje i dijeljenje informacija iz oblasti suzbijanja kriminala,**
- **organizovanje konferencija i aktivnosti za razvoj suzbijanja kriminala,**
- **pružanje usluga stručne pomoći organima EU,**
- **razvoj i primjenu raznih programa koji se bave određenim prijetnjama iz oblasti kriminala.**

Kao dodatak mreži i inicijativi definisane su i posebne oblasti koje predstavljaju prioritete kad su borba protiv organizovanog kriminala u pitanju, i to: krijumčarenje oružja, pranje novca, financijski kriminal, sajber-kriminal i zaštita prirodne sredine.

ZAKLJUČAK

- U skladu sa osnovnom tezom, **planovi regionalizacije** u varijantama koje se karakterišu političkim preopterećenjima manje zavise od autoriteta date države, zato što spadaju pod nadležnost globalne supersile, tako da daleko više zavise od njenih **geostrateških planova i političkih zahtjeva**, a ne od lokalnih „specifičnosti" ili životne „potrebe za decentralizacijom". U tom kontekstu, može se pretpostaviti da se mi u Bosni i Hercegovini i regionu suočavamo sa **„svijetlom perspektivom demokratije" po cijenu „nestajanja" države kao njenog prvog garanta**. Dok je koncept nacionalne države počivao na ideologiji teritorijalne jedinstvenosti i monolitnih identiteta nacije, koncept regiona i regionalne decentralizacije počiva na pretpostavkama polifrenih socijalnih identiteta koji jedinstveni prostor transformišu u pluralizam mjesta. **Savremena ideja regiona i regionalizacije može se smatrati jednim od najbitnijih tranzicijskih fenomena moderne u postmodernu epohu.**
- **Organizovani kriminal**, kao društveno negativna pojava, ima izuzetnu sposobnost da koristi povoljne uslove za svoje infiltriranje i da se vješto prilagođava konkretnoj društveno-političkoj i ekonomskoj situaciji, ne samo unutar jedne države, nego i na međunarodnom planu. **Internacionalni karakter organizovanog kriminala, trgovine ljudima i terorizma** kao vida organizovanog kriminala upravo i podrazumijeva nužnost međunarodne saradnje na planu otkrivanja konkretnih krivičnih djela i učinilaca i obezbjeđenje valjanih materijalnih i ličnih dokaza.
- **Pravac kretanja razvoja saradnje u cilju borbe protiv organizovanog kriminala ne primorava EU da stvara paralelne policijske strukture sa eksplicitnim nadležnostima na teritoriji cijele Unije. Saradnja i kooperacija već postojećih snaga i resursa je mnogo bolja i efikasnija**

alternativa, posebno ako se izvede profesionalno, temeljno i predano cilju.

- U radu je pokazano da **društveni faktori** utiču na pojave trgovine ljudima i terorizma, zatim je ukazano na **naučna shvatanja** koja trgovinu ljudima i terorizam izučavaju i tumače s pozicija **determinacije društvenih i socijalnih faktora**.
- Nauka je podbacila zbog svojih oštrih političkih podjela i ideoloških opredjeljenja u istorijskoj prilici tranzicije i korupcije i kriminala (kleptokratije) u analizi i predviđanju događaja. Društvene promjene i razvitak su osnovni zadaci za proučavanje društvenog razvoja.
- Postkomunistička tranzicija političko-ekonomskih institucija i kulturnih obrazaca suočava se sa brojnim aspektima klasičnog problema interakcije kulture i političke strukture, te iz tih razloga povećava se prisustvo kriminala i korupcije (kleptokratija) u društvima u tranziciji. To znači da priroda socioekonomskih, istorijsko-etničkih, kulturnovrijednosnih, i ideološko-političkih rascjepa u društvima u tranziciji i dalje se zadržava u zoni tzv**. „teških društava za demokratiju“**. (Satori)
- Globalizacijski procesi su nametnuli raspodjelu rizika, umjesto ranijih unutardruštvenih procesa koji su se odvijali u okvirima raspodjele dobara (i usluga) između aktera u procesima tranzicije i rada. Transformacija organizacija rada se odvija u pravcu njihove sve veće promjenljivosti, prilagodljivosti i privremenosti (tzv. „3P“). U tu transformaciju procesi globalizacije su „unijeli“ neke dominantne novoliberalne vrijednosti sa novolibaralnim ideologijama, a to se ne može zanemariti, tim više što u pozadini svake ideologije stoji „zaštitnička“ funkcija odgovarajućih društvenih aktera u čijem središtu je **borba za profit.**
- U društvima u tranziciji traženo je uvođenje demokratije, bez obzira na konkretne političke i ekonomske uslove, a zanemarena je briga za izgradnju institucija.
- Nedostatak odgovarajućeg institucionalnog okvira omogućio je još jednu nesreću više, i to da slobodno tržište nužno dobije oblik crne berze, **kleptokratija** postaje dominantan društveni odnos, obrazac i stil ponašanja, privatizacija postaje velika pljačka kao „prvobitna akumulacija kapitala“, a umjesto kapitala (kojeg nema) imamo spremnost političkih elita da rasprodaju „naciju“, državu i resurse, do spremnosti da stanovništvo uvedu u tzv. dobrovoljno ropstvo.
- **Antinarodna i antidržavna koalicija** „novih – starih“ tajkuna u društvima u tranziciji uništila je državu, stvorila bogatu manjinu i masovno osiromašila građane – stanovništvo i projektovano ih gura u društveno štetna ponašanja (teorija devijantnosti).
- Smatramo da se tranzicija kao put ka slobodi u većini postsocijalističkih zemalja danas ostvaruje putem osiromašenja naroda i njihovim uvođenjem u tzv. dobrovoljno ropstvo.
- Maksimalizacija profitne orijentacije u društvima u tranziciji u navedenim uslovima otvorila je vrata za prodor nelegalnog kapitala i za jačanje mafije, organizovanog kriminala i korupcije. **Kriminalizacija državnih struktura** i dominantna kleptokratija i kod nosioca funkcija vlasti postaje pitanje od posebnog značaja.

- Rješenja za društva u tranziciji treba tražiti u **jačanju uloge socijalne države**, u moralnom preporodu svih subjekata, da bi se mogli rješavati nagomilani problemi u sferi svakodnevnog života i društvenih servisa, umjesto njenog sve većeg ograničavanja koje izaziva otklon građana ka desničarskim opcijama. Treba uspostaviti održivu ravnotežu sukoba i konsenzusa u društvima u tranziciji.
- Zemlje EU su po prvi put razvile sposobnost da zajedno planiraju kako će i koje kriminalne mreže biti spriječene da djeluju, te koje će se strukture donošenja odluka upotrijebiti za zajedničku akciju protiv njih. Na pripadnicima policijskih struktura zemalja članica je da iskoriste puni potencijal ovih novih struktura i da ih razviju u skladu sa potrebama.

LITERATURA:

1. Janjević, M. (2003). *III stub Evropske Unije*. Beograd: Službeni list SCG.
2. Prokopijević, M. (2009). *Evropska unija*. Beograd: JP Službeni glasnik.
3. The World Bank, (2000). *The Road to Stability and Prosperity in South East Europe*. Washington: The World Bank.
4. Šušnjić, Đ. (1994). *Dijalog kao metoda mišljenja i načina življenja*. Zbornik radova, Novi Sad: Filozofski fakultet – Institut za filozofiju i sociologiju.

Prof. Dr. Duško Vejnović[7*]
Advanced School of Internal Affairs
Banja Luka

SOCIOLOGICAL-DEFENDOLOGICAL ASPECTS OF REGIONALIZATION AND KLEPTOCRACY ON THE WAY TO EUROPEAN INTEGRATIONS

Abstract: Issues and problems in the region, regionalization, organized crime, suppression of crime and "imaginary" European integrations represent of the most current debates in modern social science. Of course, as is the case with most modern social changes, sociology and defendology have no more an exclusive right on the discussion about the region, regionalization, kleptocracy, i.e. structural crime and corruption, as an eye sore of transitional societies on the imaginary way to European integrations. Within the framework of new European relations on the course of European integrations and division of particular interests of big powers, such as the USA and "**German Europe**", within the framework of regional strategies, this area, the Balkan region has to accept European commitments[8] and maintain its traditional geopolitical and geostrategic importance and the role of "**the bordering country in the rip of worlds**". This issue can be addressed by other sciences, such as philosophy, law, history, psychology, geography, geopolitics, political and other sciences. Two main approaches are applied when global relations in the world are concerned. One of them is **a psychological approach**, which points to the globalization of modern developmental processes, with worldwide proportions, whose result is the creation of **a modern democratic world society**. The second approach is **a politicological one**, and it focuses on military, political and economic relations of power between countries, which can be found in the so called **new world order**. Special emphasis is given to differences between the commitment to European integrations and real patterns and styles of behavior of law subjects in international relations **burdened with kleptocracy** (structural corruption and crime), and the need for the suppression of the same ones. The European Union has provided an action plan defined by the program "**Prevention and combat against crime**".

Key words: regionalization, kleptocracy, European integrations, suppression of corruption and crime, European Union

---

[7 *] The author is a full professor at the University of Banja Luka on the subjects Sociology, Sociology of Sports, Business Culture and Communication and Defendology. He is the chairman of the Association of Professors Assistants at the University of Banja Luka, European Defendology Center and Editor-in-Chief of the journal Defendology. Contact addresses: email: tin@blic.net, phone: 00387 65 526 793.

[8] Strategic basics of cooperation between countries, combat against organized international crime, especially detection and prevention of trafficking in drugs, weapons, white slavery, etc.

Pregledni rad – UDK 340.134: 343.13(497.6)

O PREDSTOJEĆOJ REFORMI ZAKONA O KRIVIČNOM POSTUPKU BOSNE I HERCEGOVINE U KONTEKSTU DALJEG POŠTOVANJA EVROPSKIH STANDARDA

Akademik prof. dr Miodrag N. Simović,
redovni profesor Pravnog fakulteta u Banjoj Luci i
predsjednik Ustavnog suda Bosne i Hercegovine
Mr Marina M. Simović-Nišević,
Uprava za indirektno oporezivanje BiH, doktorand

Sažetak: Nakon uvodnih napomena, rad sadrži pregled najznačajnijih rješenja koja donosi predstojeća dugo pripremana reforma Zakona o krivičnom postupku Bosne i Hercegovine koji je stupio na snagu 1. marta 2003. godine. Autori posebno analiziraju nova rješenja dogovorena u okviru Radne grupe za izradu Nacrta Zakona o izmjenama i dopunama Zakona o krivičnom postupku Bosne i Hercegovine (dostavljen Savjetu ministara Bosne i Hercegovine u decembru 2011. godine) koja predstavljaju usklađivanje ovog zakona sa međunarodnim standardima ili je dosadašnja primjena pokazala nedostatke, odnosno inicirala unapređenje pojedinih odredbi. To se, prije svega, odnosi na ukidanje obligatornog pritvora, na odlučivanje u sjednici vijeća ili pretresu pred drugostepenim sudom, ukidanje prvostepene presude, odredbe o novom vanrednom pravnom lijeku – zahtjevu za zaštitu zakonitosti, i nepravo ponavljanje krivičnog postupka. I najnovije novele koje su tokom posljednjih mjeseci u središtu interesa bh. stručne, ali i šire javnosti, donose neke suštinske i temeljne promjene krivičnog postupka, prvenstveno glavnog postupka i postupka pravnih lijekova, između ostalog i time što predviđaju da vijeće drugostepenog suda, uvažavajući žalbu, može ukinuti prvostepenu presudu i vratiti predmet vijeću prvostepenog suda na ponovno suđenje. Uz to, Sudu Bosne i Hercegovine se daje mogućnost da po službenoj dužnosti preispituje presudu u smislu povreda krivičnog zakona na štetu optuženog. Cilj ovog rada nije sveobuhvatna i produbljena analiza, nego osvrt na neke odrednice predložene zakonodavne reforme.

Ključne riječi: Zakon o krivičnom postupku Bosne i Hercegovine, Sud Bosne i Hercegovine, pritvor, ukidanje presude, zahtjev za zaštitu zakonitosti.

UVODNE NAPOMENE

Krivični postupak u Bosni i Hercegovini prolazi kroz značajne reforme još od 2003. godine, kada su doneseni novi Zakon o krivičnom postupku Bosne i Hercegovine[1] i zakoni o krivičnom postupku entiteta i Brčko distrikta. S jedne strane, i pod snažnim uticajem prakse Evropskog suda za ljudska prava, zakonodavci su nastojali ojačati jemstva pravičnog postupka.[2] S druge strane, usljed ekspanzije

[1] Službeni glasnik BiH" br. 3/03, 32/03, 36/03, 26/04, 63/04, 13/05, 48/05, 46/06, 76/06, 29/07, 32/07, 53/07, 76/07, 15/08, 58/08, 12/09, 16/09 i 93/09.

[2] Vid. B. Pavišić, "Novi hrvatski Zakon o krivičnom postupku", *Hrvatski ljetopis za krivično pravo i praksu,* Zagreb, vol. 15, 2/2008, 489–602.

međunarodnog organizovanog kriminaliteta, te s obzirom na obaveze iz sve brojnijih međunarodnopravnih konvencija, zakonodavci nastoje osigurati efikasniji krivični postupak, između ostalog i jačanjem procesne uloge tužioca.[3] Time je i Bosna i Hercegovina slijedila trend koji je posljednjih decenija zavladao u pravnim sistemima koji pripadaju evropskoj kontinentalnoj pravnoj tradiciji.[4]

Važeći Zakon o krivičnom postupku[5] Bosne i Hercegovine, od svog stupanja na snagu do danas, bio je podvrgnut brojnim izmjenama i dopunama. Riječ je o zakonskim reformama kojima se nastojala uravnotežiti, s jedne strane, potreba za unapređenjem učinkovitosti krivičnog postupka, a s druge strane, o nastojanjima na zaštiti osnovnih prava osumnjičenog, odnosno optuženog u krivičnom postupku, s obzirom na to da je bh. krivični postupak trebalo uskladiti sa standardima koje su pred zakonodavca postavljali brojni međunarodnopravni dokumenti, u prvom redu Evropska konvencija za zaštitu ljudskih prava i osnovnih sloboda[6], te judikatura Evropskog suda za ljudska prava.

Najavljena i dugo pripremana zakonodavna reforma ima više aspekata.[7] Zasigurno jedna od najvećih novina u Zakonu o krivičnom postupku biće uvođenje zahtjeva za zaštitu zakonitosti, shodno čemu se dopunjava važeći član 24. Nadalje, Odlukom Ustavnog suda Bosne i Hercegovine[8] u predmetu broj AP 498/11, povodom apelacije Tokalić Pere od 15. jula 2011. godine, utvrđena je povreda prava propisanih Ustavom BiH i Evropskom konvencijom kada je u pitanju odredba o određivanju obaveznog pritvora nakon izricanja prvostepene presude.[9] Radi toga se predloženom izmjenom i dopunom član 138 stav 1 Zakona o krivičnom postupku usklađuje sa navedenom odlukom. Dakle, u prvoj rečenici se fakultativno postavlja određivanje, odnosno produžavanje pritvora, jer važeća formulacija „će biti produžen“ ukazuje na obligatornost određivanja pritvora. U istoj rečenici se briše pozivanje na neophodnost nesmetanog vođenja postupka zbog stvarne potrebe za postojanjem ovakvog osnova nakon završetka prvostepenog postupka.

---

[3] Najdetaljnije se o tim pitanjima raspravljalo u istraživanju koje je rezultiralo izradom nacrta *Corpus Juris portant disposition pour la protection des intérêts fi naciers de l'Union européenne* (Delmas-Marty – Vervaele), Antwerpen, 2001). Taj projekt je namijenjen krivičnopravnoj zaštiti finansijskih interesa Evropske unije i izvorno je nastao 199., a revidiran je u Firenci 1999. godine. U čl. 18–35 uređuje pitanja krivičnog postupka.

[4] Za stanje u Francuskoj vid. E. Ivičević Karas, „O glavnim značajkama reformi savremenog francuskog krivičnog postupka“, *Hrvatski ljetopis za krivično pravo i praksu,* Zagreb, 1/2010, 109─124.

[5] U daljnjem tekstu: Zakon o krivičnom postupku.

[6] U daljnjem tekstu: Evropska konvencija.

[7] U iznalaženju i usaglašavanju najpovoljnijih zakonskih rješenja učestvovali su predstavnici izvršne i sudske vlasti svih nivoa u Bosni i Hercegovini, istaknuti profesori pravnih fakulteta u Bosni i Hercegovini, te predstavnici advokatskih komora koji su članovi Tima za praćenje i ocjenu primjene krivičnih zakona, kao tijela formiranog u okviru Ministarstva pravde Bosne i Hercegovine, koje je uspostavljeno 2003. godine. Tim kontinuirano prikuplja podatke iz prakse, prati i analizira primjenu zakona, te predlaže rješenja kojim se uklanjaju uočeni zakonski nedostaci i uvode norme usaglašene sa najboljim pravnim standardima. Prvopotpisani autor ovog referata je kopredsjedavajući ovog tima.

[8] U daljnjem tekstu: Ustavni sud.

[9] Vid. D. Krapac, Pretpostavke za pokretanje i vođenje ustavnosudskog postupka zaštite individualnih ustavnih prava i sloboda: pravni okviri i stvarne granice ("procesnost") hrvatskog modela ustavne tužbe, *Hrvatsko ustavno sudovanje de lege lata i de lege ferenda,* Zagreb, Hrvatska akademija nauka i umjetnosti, 2009, 169–207.

SASTAV SUDA

Predlaže se promjena vezana za član 24 Zakona o krivičnom postupku. S obzirom na uvođenje novog vanrednog pravnog lijeka – zahtjeva za zaštitu zakonitosti, o njemu će odlučivati Vijeće Krivičnog odjeljenja Suda BiH, sastavljeno od pet sudija (novi stav 6 člana 24).

ODREĐIVANJE PRITVORA NAKON IZRICANJA PRESUDE

Predlaže se da se član 138 stav 1 izmijeni tako da glasi: „Kada izrekne presudu na kaznu zatvora, Sud BiH može optuženom odrediti, odnosno produžiti pritvor uzimajući u obzir sve okolnosti vezane za izvršenje krivičnog djela, odnosno ličnost učinioca. U ovom slučaju donosi se posebno rješenje, a žalba protiv rješenja ne zadržava njegovo izvršenje."

Iako navedena odluka Ustavnog suda nije donesena u postupku ocjene ustavnosti zakona, već u postupku apelacije, očigledno je da mišljenje Ustavnog suda izraženo u toj odluci ima posebnu težinu i da po samoj svojoj logici i argumentaciji nameće obavezu da se slijedi. Budući da je Ustavni sud u pomenutoj odluci ukazao na potrebu izmjene, a ne brisanja sporne odredbe, bilo je neophodno sagledati mogućnost formulisanja odredbe člana 138 stav 1 na način koji bi zadovoljio postavljeni standard, odnosno, kojim bi se Sudu BiH dala mogućnost individualizacije izrečene mjere pritvora, u smislu ocjene posebnih okolnosti konkretnog slučaja, umjesto sadašnje odredbe o „obligatornom pritvoru".

Isto pravno pitanje Ustavni sud je razmatrao u odluci broj AP 573/07[10]. U navedenoj odluci Ustavni sud je usvojio apelaciju podnesenu protiv rješenja redovnih sudova o pritvoru, te utvrdio povredu člana II/3.d) Ustava Bosne i Hercegovine i člana 5 stav 1 Evropske konvencije. Naime, navedenim rješenjima apelantu je određen pritvor u skladu s odredbama člana 348 stav 1 tada važećeg Zakona o krivičnom postupku Federacije Bosne i Hercegovine kojima je bilo propisano da "kada sud izrekne presudu kojom se optuženi osuđuje na pet godina zatvora ili težu kaznu, vijeće će odrediti pritvor ako se optuženi već ne nalazi u pritvoru". U vezi s tim, Ustavni sud je ukazao da je nesporno da je apelantu određen pritvor u skladu s domaćim zakonom. Međutim, Ustavni sud je ukazao da je Evropski sud konzistentno ponavljao da je to nespojivo s Evropskom konvencijom i da je svaki pritvor koji je zasnovan na takvoj odredbi nezakonit.[11] S obzirom na to, Ustavni sud je zaključio da navedene odredbe domaćeg zakona koje propisuju "obligatoran pritvor" nisu u skladu s članom 5 stav 1 Evropske konvencije.

Ako pogledamo krivičnoprocesne odredbe država u okruženju, slijedi da Republika Hrvatska ima identičnu odredbu (član 123 stav 3 Zakona o krivičnom postupku[12]) o obligatornom pritvoru koja glasi: "Pri izricanju presude uvijek će se

---

[10] Vidi Ustavni sud, Odluka o dopustivosti i meritumu od 29. aprila 2009. godine, objavljena u "Službenom glasniku BiH" broj 75/09, dostupna na web-stranici Ustavnog suda *www.ustavnisud.ba*.

[11] Vidi Evropski sud, *Fox Campbell i Harley protiv Ujedinjenog Kraljevstva,* presuda od 30. avgusta 1990. godine i 27. marta 1991. godine, serija A broj 182.

[12] „Narodne novine Republike Hrvatske" broj 152/08.

odrediti ili produžiti istražni zatvor[13] protiv okrivljenog kojem je izrečena kazna zatvora od pet godina ili teža kazna."

Za razliku od Republike Hrvatske, Republika Srbija postavlja dodatne uslove za slučaj kada je sud izrekao kaznu zatvora od pet godina ili težu kaznu, pa relevantna odredba (član 142 stav 1 tačka 6 Zakonika o krivičnom postupku Republike Srbije[14]) glasi: „Pritvor se može odrediti protiv lica za koje postoji osnovana sumnja da je učinilo krivično delo, ako je: ... 6) presudom prvostepenog suda licu izrečena kazna zatvora od pet godina ili teža kazna i ako je to opravdano zbog posebno teških okolnosti krivičnog dela."

Zakoni o krivičnom postupku Slovenije i Crne Gore ne sadrže odredbu o obligatornom pritvoru, niti se određivanje, odnosno produženje pritvora veže za visinu izrečene kazne zatvora, nego se radi o identičnom rješenju kakvo je postojalo u Zakonu o krivičnom postupku BiH prije izmjena iz 2009. godine[15], kada je uveden obligatorni pritvor.

Treba primijetiti i da je apelaciono vijeće Suda BiH, u svojoj praksi, već uvelo obavezu ocjene i drugih okolnosti konkretnog krivičnog djela u slučaju kad je optuženom izrečena kazna zatvora u trajanju od pet godina ili teža kazna.[16] Time je postavilo upravo one standarde o kojima je bilo riječi u odluci Ustavnog suda broj AP 498/11, odnosno utvrdilo da na strani optuženog, osim činjenice da je nepravnosnažno osuđen na kaznu zatvora u trajanju od pet godina, „egzistiraju i posebni pritvorski razlozi propisani odredbom člana 132 stav 1 tač. a) i d) Zakona o krivičnom postupku ... te je mjeru pritvora kao najstrožu mjeru za obezbjeđenje prisustva optuženog i uspješno vođenje krivičnog postupka, našlo jedinom adekvatnom mjerom u konkretnom slučaju."[17]

U izdvojenom mišljenju o neslaganju sudije Ustavnog suda Tudora Pantirua navodi se, između ostalog, da je očigledno da je apelant bio pritvoren nakon što ga je Sud BiH osudio na kaznu lišavanja slobode u trajanju od pet godina. U rješenju o pritvoru izričito se navodi da je apelant pritvoren u vezi s konačnom presudom Suda BiH, kojom je osuđen na kaznu zatvora u trajanju od pet godina. Uz to, ističe se da član 5 stav 1a Evropske konvencije dozvoljava „zakonito lišavanje slobode po presudi nadležnog suda". S druge strane, apelant nikad nije osporavao u svojoj žalbi zakonitost presude Suda BiH kojom je osuđen, niti nadležnost tog suda. Apelant nije precizirao u svojoj žalbi šta je bilo pogrešno u vezi s „načinom na koji je određen pritvor". Njegova glavna pritužba se zapravo tiče nemogućnosti da se žali protiv rješenja o pritvoru u skladu s članom 5 stav 4 Evropske konvencije.

Sudija Pantiru podsjeća da je u svojoj presudi *Iribarne Perez protiv Francuske* od 24. oktobra 1995. godine (tačka 30-1) Evropski sud smatrao da: „Preispitivanje koje zahtijeva član 5 stav 4 inkorporirano je u odluci kojom se osoba lišava slobode kada tu odluku donese sud po okončanju sudskog postupka; ovo je, na primjer, slučaj kada se kazna zatvora odredi po `presudi nadležnog

[13] Zakon koristi termin „istražni zatvor" umjesto „pritvor", ali jasno je da se radi o istom institutu.
[14] "Službeni list SRJ" br. 70/01 i 68/02 i „Službeni glasnik Republike Srbije" br. 58/04, 85/05, 115/05, 49/07, 20/09, 72/09 i 76/10.
[15] „Službeni glasnik BiH" broj 93/09.
[16] Rješenje Suda BiH, broj S1 1 K 002590 11 Krž. od 27. septembra 2011. godine.
[17] *Ibid.*

suda' u smislu člana 5 stav 1a Evropske konvencije." Imajući to u vidu, smatra se neopravdanim zaključak Ustavnog suda da je član 5 stav 1 Evropske konvencije bio povrijeđen zbog toga što je „…rješenjem Suda BiH broj Kpž. 13/10 od 24. januara 2011. godine apelantu određen pritvor u skladu s odredbama člana 138 stav 1 Zakona o krivičnom postupku koji propisuje `obligatorni pritvor`, jer je prema navedenoj odredbi jedini uslov za određivanje pritvora – postojanje presude kojom je izrečena kazna zatvora u trajanju od pet godina ili teža kazna."

Član 5 stav 1 Evropske konvencije dozvoljava pritvor osobe po presudi nadležnog suda, bez nametanja ograničenja koja se odnose na dužinu zatvorske kazne koju određuje sud u presudi. Stoga, smatra sudija Pantiru, član 138 stav 1 Zakona o krivičnom postupku, kojim se zahtijeva hapšenje samo onih lica koje su osuđena na kaznu zatvora u trajanju od pet godina i duže, nameće viši standard zaštite od onog koji je sadržan u članu 5 stav 1 Konvencije i ne može dovesti do povrede ovog člana, kao što je to zaključio Ustavni sud u svojoj odluci.

ŽALBA NA PRVOSTEPENU PRESUDU

U članu 305 Zakona o krivičnom postupku bi se promijenio stav 2 propisivanjem da će Sud BiH prije svega u sjednici vijeća donijeti odluku o tome da li žalbeni navodi ukazuju na to da je potrebno održati pretres pred drugostepenim vijećem, dok stav 3 propisuje uslove za održavanje pretresa pred vijećem apelacionog odjeljenja. Uslovi su postavljeni kumulativno. Opravdani razlozi predstavljaju faktično pitanje koje će se ocjenjivati u svakom pojedinačnom predmetu. Nadalje, stav 4 propisuje učesnike pretresa pred vijećem apelacionog odjeljenja[18], prihvatanjem načela neposrednosti i kontradiktornosti[19] vođenja krivičnog postupka. Naposlijetku, stavom 5 ovog člana nalaže se obaveza predsjedniku apelacionog vijeća da osigura dovođenje optuženog iz pritvora na pretres, a stavom 6 da će se isti rokovi za izradu odluke na sjednici vijeća primjenjivati i za odluku koja je donesena na pretresu.

Novim članom 305a Zakona o krivičnom postupku regulišu se pravila održavanja pretresa pred vijećem apelacionog odjeljenja, zasnovana na načelu neposrednosti i adversarnosti postupka. Na ovom pretresu će se razmatrati samo ona pitanja zbog kojih je pretres otvoren. Pretres pred vijećem počinje izvještajem izvjestioca koji izlaže stanje stvari ne dajući svoje mišljenje o zasnovanosti žalbe. Po prijedlogu stranaka ili po službenoj dužnosti pročitaće se presuda ili dio presude na koji se odnosi žalba, a po potrebi i zapisnik o glavnom pretresu. Stranke i branilac mogu na pretresu iznositi nove dokaze i činjenice. Tužilac može, s obzirom na rezultat pretresa, u cjelini ili djelimično odustati od optužnice ili izmijeniti optužnicu u korist optuženog.

Dopunom člana 306 Zakona o krivičnom postupku daje se Sudu BiH mogućnost da po službenoj dužnosti preispituje presudu u smislu povrede

[18] Optuženi i njegov branilac, tužilac, oštećeni, zakonski zastupnici i punomoćnici oštećenog, kao i oni svjedoci i vještaci za koje Sud BiH odluči da se saslušaju.

[19] O kontradiktornosti, kao četvrtom modelu krivičnog postupka, vidjeti Chiavario, u *Procedure penali d'Europa* (a cura di Delmas-Marty – Chiavario), Padova, 2001.

Krivičnog zakona BiH[20] na štetu optuženog. Ova dopuna predstavlja propisivanje *de facto* usvojene prakse Suda BiH da se kod ovakvog preispitivanja presude poziva na Evropsku konvenciju. Zbog nepostojanja jasno propisane odredbe koja će omogućiti preispitivanje presude u smislu povrede Krivičnog zakona BiH na štetu optuženog – Sud BiH se poziva na Evropsku konvenciju i time popunjava prazninu koja postoji u domaćem zakonodavstvu (npr. dekriminalizacija krivičnog djela, odnosno promjena bića krivičnog djela nakon podnošenja žalbe, te zastara krivičnog gonjenja na koju niko ne ukazuje u žalbenom postupku).

Izmjena i dopuna stava 1 člana 310 Zakona o krivičnom postupku usklađuje ovu odredbu sa odredbama o vrstama odluka koje može donijeti vijeće apelacionog odjeljenja povodom žalbe na prvostepenu presudu – uvođenjem mogućnosti jednog vraćanja predmeta vijeću krivičnog odjeljenja na ponovno suđenje. Inače, potreba za uvođenjem ove odredbe se ukazala nakon što je osmogodišnja praksa primjene Zakona o krivičnom postupku pokazala da postojeće rješenje ne uspostavlja balans između efikasnosti postupka i kvaliteta suđenja i presude. Vijeća apelacionog odjeljenja su nerijetko pretvorena u prvostepena krivična vijeća koja razmatraju činjenice i provode postupak u cijelosti. Ovakva praksa je dovela do toga da ne postoji jasna veza između prvostepenih i drugostepenih odluka, izostaje edukativni karakter presuda, a i uspostavlja se manjkava i nedosljedna sudska praksa.[21]

Nadalje, novim članom 315 Zakona o krivičnom postupku jasno se preciziraju razlozi i postupanje vijeća apelacionog odjeljenja kod ukidanja presude i vraćanja predmeta vijeću krivičnog odjeljenja. Osnovi za vraćanje predmeta vijeću krivičnog odjeljenja na ponovno suđenje se od osnova za održavanje pretresa pred vijećem apelacionog odjeljenja razlikuju samo u dijelu koji se odnosi na izvođenje novih dokaza. Takođe, stavom 2 se propisuje mogućnost da vijeće apelacionog odjeljenja naredi da se pretres održi pred izmijenjenim vijećem – ukoliko će takva odluka doprinijeti efikasnom i kvalitetnom rješavanju predmeta.

Novi član 316 Zakona o krivičnom postupku propisuje sadržaj presude, odnosno rješenja vijeća apelacionog odjeljenja kojim se ukida prvostepena presuda. Precizira se da presuda, odnosno rješenje mora jasno ukazati na nedostatke kada su u pitanju bitne povrede krivičnog postupka i pogrešno ili nepotpuno utvrđeno činjenično stanje. Ovakva odredba ima za cilj stavljanje akcenta na kvalitetno obrazlaganje presuda i rješenja, te isticanje značaja tog uslova koji postavlja Zakon o krivičnom postupku, a koji se u praksi ponekada pokazao kao manjkav.

Postupanje vijeća krivičnog odjeljenja nakon donošenja drugostepene odluke propisuje novi član 316a Zakona o krivičnom postupku. Vijeće apelacionog odjeljenja vratiće sve spise vijeću krivičnog odjeljenja s dovoljnim brojem ovjerenih prepisa svoje odluke – radi predaje strankama i drugim zainteresovanim licima. Vijeće krivičnog odjeljenja kome je predmet upućen na suđenje uzeće za osnovu raniju optužnicu. Ako je presuda vijeća krivičnog odjeljenja djelimično ukinuta, vijeće krivičnog odjeljenja će za osnovu uzeti samo onaj dio optužbe koji se odnosi na ukinuti dio presude. Odredba stava 3 izričito propisuje mogućnost iznošenja

[20] „Službeni glasnik Bosne i Hercegovine" br. 3/03, 32/03, 37/03, 54/04, 61/04, 30/05, 53/06, 55/06, 32/07 i 8/10.

[21] Vid. S. W. Becker, "Žalba u kaznenom postupku u SAD: preispitati ili ne preispitati presudu", Hrvatski ljetopis za kriviično pravo i praksu, Zagreb, vol. 15, 1/2008, 343–356.

novih činjenica i dokaza, a stavom 4 se nalaže obaveza vijeću krivičnog odjeljenja da postupa po uputama vijeća apelacionog odjeljenja. Na ovaj način se osigurava edukativna svrha rada apelacionog vijeća i smanjenje mogućnosti ponavljanja istih grešaka. Takođe se olakšava usklađivanje prakse rada prvostepenih vijeća, te osigurava dosljednost stavova vijeća apelacionog odjeljenja u istim ili sličnim predmetima. Stav 5 predstavlja dodatni naglasak na zabranu *reformatio in peius*[22].

Novi član 317 Zakona o krivičnom postupku propisuje obavezu vođenja pretresa pred vijećem apelacionog odjeljenja ako je presuda već jednom bila ukinuta u drugostepenom postupku. Ako vijeće apelacionog odjeljenja ustanovi da je potrebno ponovo izvesti već izvedene dokaze u prvostepenom postupku, iskazi saslušanih svjedoka i vještaka i pisani nalaz i mišljenje biće prihvaćeni kao dokazni materijal ukoliko su ti svjedoci i vještaci prilikom svjedočenja bili unakrsno ispitani od suprotne stranke ili branioca ili nisu bili unakrsno ispitani od suprotne stranke ili branioca iako im je to bilo omogućeno, te ukoliko se radi o dokazima iz člana 261 stav 2 tačka e)[23] ovog zakona. U tom slučaju njihovi iskazi na pretresu mogu se čitati. Pri izricanju nove presude vijeće apelacionog odjeljenja je vezano zabranom propisanom u članu 307 ovog zakona (zabrana *reformatio in peius*).

Nije iznenađujuće što su o odredbama Nacrta o ukidanju prvostepenih presuda i vraćanju predmeta prvostepenom sudu na ponovni postupak i odlučivanje zauzeli nepovoljan stav i Tužilaštvo BiH[24] i Sud BiH[25]. Predložene izmjene nisu prihvatljive za Sud BiH iz sljedećih razloga: (1) ukidanje presuda i vraćanje prvostepenom sudu na ponovni postupak znatno će uticati na dužinu trajanja krivičnog postupka u krivičnim stvarima, čime se dovodi u pitanje standard suđenja u razumnom roku iz člana 6 Evropske konvencije i pravo optuženog iz člana 13 stav 2 Zakona o krivičnom postupku; (2) u znatnoj mjeri će se povećati troškovi krivičnih postupaka i sudskog budžeta; (3) izmjene će se štetno odraziti na efikasnost suđenja u predmetima ratnih zločina koji zbog prirode postupaka zahtijevaju efikasno procesuiranje; (4) u predmetima ratnih zločina nova suđenja pred prvostepenim sudom bi ugrozila sistem zaštite svjedoka i zaštićene svjedoke izložila dodatnoj viktimizaciji; (5) povećaće se obim poslova u prvostepenim sudovima i automatski uticati na ažurnost sudova i kompletnog sudskog sistema i (6) to je korak nazad u reformi krivičnog procesnog zakonodavstva koji će biti loše ocijenjen od strane međunarodnih institucija (UN) koje su sačinile analizu sistema i predložile principe reforme radi prevazilaženja evidentiranih problema. Iako se kao razlozi za promjene navode loš kvalitet suđenja i izrađenih odluka i izostanak edukativnog djelovanja odluka žalbenog suda, ti razlozi ne bi smjeli biti argumenti za vraćanje na stari model. Žalbeni sud nema zakonska ovlašćenja za edukaciju nižestepenih sudija. Za otklanjanje ove vrste problema (čije postojanje se ne dovodi u sumnju) postoje drugi institucionalni mehanizmi (centri za edukaciju,

---

[22] Međunarodni izvori ljudskih prava, kao ni Ustav BiH, ne predviđaju izričito tu zabranu. Međutim, ona se danas uzima kao neizostavna komponenta vladavine prava. Vid. Petranović, "Primjena načela zabrane *reformatio in peius* u ponovnom suđenju", *Hrvatska pravna revija*, 7–8/2005, 203–205 i I. Kramarić, "Drugostepeni krivični postupak i zabrana *reformatio in peius*", *Glasnik Advokatske komore Vojvodine*, Novi Sad, 5/1985.

[23] Dokazi čije je izvođenje naredio sudija, odnosno vijeće.

[24] Mišljenje Kolegija Tužilaštva BiH, broj A-218/10 od 7. juna 2010. godine.

[25] Mišljenje Krivičnog odjeljenja Suda BiH od 17. februara 2010. godine.

sjednice odjeljenja). Osim toga, odluke apelacionih sudova su dostupne svim sudijama preko Centra za sudsku dokumentaciju, a ovaj projekat upravo ima za cilj samoedukaciju sudija.

Tužilaštvo BiH je, između ostalog, istaklo da bi predložene izmjene Zakona o krivičnom postupku u znatnoj mjeri opteretile rad Tužilaštva BiH, budući da bi tužioci morali provesti dodatno vrijeme prisustvujući pretresima u ponovnom suđenju.[26] Izmjene bi značajno opteretile i rad svih drugih tužilaštava u BiH – ukoliko bi predloženo rješenje bilo prihvaćeno i na entitetskom nivou i nivou Brčko distrikta. Osim toga, ozbiljno bi se doveo u pitanje jedan od ciljeva reforme pravosuđa koji se odnosi na racionaliziranje tužilaštava, tj. ukidanje opštinskih (osnovnih) tužilaštava, odnosno njihovo sjedinjavanje sa okružnim (kantonalnim) tužilaštvima. Usvajanjem mogućnosti ukidanja prvostepenih presuda i vraćanja predmeta na ponovno suđenje, znatno bi se povećali troškovi krivičnog postupka iz razloga što bi tužioci ponovno morali prisustvovati suđenjima u osnovnim (opštinskim) sudovima koji se nalaze van mjesta sjedišta okružnog (kantonalnog) tužilaštva, a isti troškovi bi se povećali i na strani odbrane.

VANREDNI PRAVNI LIJEKOVI

U članu 324a Zakona o krivičnom postupku (nepravo ponavljanje krivičnog postupka) predlaže se da se promijeni stav 2 tako da ako je od izrečenih dvije ili više presuda, između ostalog, jednu od pravnosnažnih presuda izrekao Sud BiH, za donošenje nove presude nadležan je taj sud, bez obzira na okolnost da li je u drugoj ili u više drugih presuda kao najstrožu vrstu kazne ili najveću kaznu kod istovrsnih kazni ili kod jednakih kazni posljednji izrekao nadležni entitetski sud ili sud Brčko distrikta BiH.

Radi pravilnog tumačenja razloga za ovakav prijedlog treba ukazati i na neke druge zakonske odredbe. Naime, u članu 6 Zakona o izvršenju krivičnih sankcija Federacije BiH[27] navodi sa da se o premještaju osobe osuđene od strane Suda BiH može odlučiti isključivo po Zakonu Bosne i Hercegovine o izvršenju krivičnih sankcija, pritvora i drugih mjera[28]. U članu 12 istog zakona navedeno je da će se u pogledu uslovnog otpusta osuđenih osoba prema nadležnosti Bosne i Hercegovine u krivičnim stvarima u pogledu primjenjivog zakona konsultovati Sud BiH i Ministarstvo pravde BiH, što iskazuje namjeru i entitetskog zakonavca da u ovakvim slučajevima primat ima zakon Bosne i Hercegovine. Takođe, istu namjeru slijedi i zakonodavac Republike Srpske u svojim izmjenama i dopunama Zakona o izvršenju krivičnih sankcija[29], i to u čl. 47 i 51, koji isključivo ukazuju da će se o premještaju takvog lica odlučivati po zakonu Bosne i Hercegovine, a u pogledu uslovnog otpusta da će se konsultovati Sud BiH i Ministarstvo pravde BiH.

---

[26] Prosječno vrijeme trajanja jednog pretresa koji se vodi po Zakonu o krivičnom postupku BiH je godina dana.

[27] „Službene novine Federacije BiH“ broj 12/09.

[28] „Službeni glasnik BiH“ br. 13/05, 53/07 i 97/07.

[29] Objavljenim u „Službenom glasniku Republike Srpske“ broj 67/07.

Navedenu nadležnost potvrdio je i Zakon Bosne i Hercegovine o pomilovanju[30], koji je u članu 2 ugradio nadležnost za postupanje „drugog organa ili drugog suda" kada je propisao da će Predsjedništvo BiH odlučivati o molbama za pomilovanje i za krivičnopravne sankcije koje je izrekao drugi sud u Bosni i Hercegovini kada je na njega Sud BiH prenio vođenje postupka, kao i za krivičnopravne sankcije koje nije izrekao Sud BiH a izvršavaju se u Bosni i Hercegovini.

Na važnost ovog pravnog pitanja ukazao je i jedan krivični postupak koji je vođen pred Opštinskim sudom u Sarajevu, gdje je osuđenom licu (od strane Suda BiH na kaznu zatvora u trajanju od 12 godina) nakon toga Opštinski sud Sarajevo izrekao kaznu zatvora u trajanju od dvije godine i šest mjeseci zbog nasilničkog ponašanja. Tom prilikom, Opštinski sud u Sarajevu je odbio zahtjev odbrane osuđenog da taj sud izrekne jedinstvenu kaznu zatvora, s obzirom na to da je to bio posljednji sud koji je izrekao kaznu zatvora, jer se u konkretnom slučaju radilo o pravnoj situaciji u kojoj je od strane Suda BiH bila izrečena veća kazna zatvora od kazne izrečene od strane Opštinskog suda. Međutim, ukoliko bi se pojavile pravne situacije gdje je Sud BiH izrekao blažu vrstu kazne ili ako je kod istovrsnih kazni Sud BiH izrekao manju kaznu ili ako je u slučaju izricanja jednakih kazni, Sud BiH takvu kaznu izrekao prije drugog nižeg nadležnog suda, u praksi bi u takvim slučajevima jedinstvenu kaznu izricao entitetski sud ili sud Brčko distrikta BiH. To bi uticalo da osuđeno lice od strane Suda BiH mijenja status zatvorenika, tj. iz statusa zatvorenika koji bi izdržavao kaznu po propisima Bosne i Hercegovine, prešao bi u status zatvorenika gdje bi kaznu izdržavao po propisima entiteta ili po propisima Brčko distrikta BiH.

Predlaže se, takođe, da se iza člana 333 Zakona o krivičnom postupku doda Odjeljak 2 i čl. 333a, 333b, 333c, 333d, 333e, 333f, 333g i 333h kojim se uređuje novi vanredni pravni lijek – zahtjev za zaštitu zakonitosti. Cilj je ovog zahtjeva da se obezbijedi sprovođenje načela zakonitosti sudskog rada i istovremeno da se postigne jednoobrazna primjena prava kada su u pitanju krivična djela iz nadležnosti Suda BiH. Zahtjev za zaštitu zakonitosti je vanredno pravno sredstvo u nadležnosti Suda BiH koje mogu koristiti tužilac[31], osuđeni i branilac[32]. Osnovi za ulaganje ovog pravnog lijeka su restriktivno određeni i svode se na povredu prava na odbranu kao bitnu povredu odredaba krivičnog postupka, te na povredu krivičnog zakona. Zbog ovako usko ograničenih mogućnosti ulaganja ovog pravnog lijeka, njegovo uvođenje neće uzrokovati značajno povećanje broja predmeta, niti potrebu za povećanjem postojećeg broja sudija, a pri tome je veliki značaj ovog pravnog sredstva sa aspekta ujednačavanja prakse Suda BiH.

Zahtjev za zaštitu zakonitosti se podnosi u roku od tri mjeseca od dana prijema pravnosnažne presude. Podnošenje zahtjeva nije dozvoljeno ni protiv odluke Suda BiH kojom je odlučeno o zahtjevu za zaštitu zakonitosti. Prilikom odlučivanja o zahtjevu, Vijeće Apelacionog odjeljenja će se ograničiti samo

---

[30] „Službeni glasnik BiH" broj 93/05.

[31] Vid. D. Novosel, M. Pajčić, "Državni advokat kao gospodar novog prethodnog krivičnog postupka", *Hrvatski ljetopis za krivično pravo i praksu,* Zagreb, vol. 16, 2/2009, 427–474.

[32] Nakon smrti osuđenog mogu u njegovu korist podnijeti zahtjev za zaštitu zakonitosti lica iz člana 293 stav 2 Zakona o krivičnom postupku (zakonski zastupnik, bračni, odnosno vanbračni drug optuženog, roditelj ili dijete i usvojilac, odnosno usvojenik).

na ispitivanje onih povreda zakona na koje se poziva podnosilac zahtjeva. Ako Vijeće Apelacionog odjeljenja utvrdi da razlozi zbog kojih je donijelo odluku u korist osuđenog postoje i za nekog od saosuđenih u pogledu kojeg nije podnesen zahtjev, postupiće po službenoj dužnosti kao da takav zahtjev postoji. Ako je zahtjev podnesen u korist osuđenog, vijeće apelacionog odjeljenja je pri donošenju odluke vezano zabranom predviđenom u članu 307 ovog zakona. Osim toga, ako je pravnosnažna presuda ukinuta i predmet vraćen na novo odlučivanje, za osnovu će se uzeti ranija optužnica ili onaj njen dio koji se odnosi na ukinuti dio presude.

QUO VADIS?

Iznesene promjene nameću čitav niz dilema, poput, primjera radi, pitanja kako i tokom glavnog postupka osigurati nužna jemstva pravičnog postupka, prateći i uporednopravne trendove i judikaturu Evropskog suda. Naročito je zanimljiv kvalitet novih promjena i s aspekta uloge stranaka i branioca, te posebno zaštite žrtava krivičnih djela i međunarodne saradnje u krivičnom gonjenju transnacionalnog kriminaliteta. Ne treba, naravno, zaboraviti da jedan od ključnih preduslova za uključivanje Bosne i Hercegovine u krug država članica Evropske unije jeste i učinkovit progon ratnih zločina, uravnotežen sa zahtjevima zaštite osnovnih ljudskih prava lica protiv kojih se takvi postupci vode.

LITERATURA

1. Beziz-Ayache, A., Dictionnaire de droit penal general et procedure penale*,* 2e edition, Paris 2003;
2. Bejatović, Stanko, Efikasnost krivičnog postupka kao međunarodni pravni standard, Zbornik „Krivično zakonodavstvo Srbije i standardi Evropske unije“, Srpsko udruženje za krivičnopravnu teoriju i praksu, Beograd, 2010;
3. Bejatović, Stanko, Međunarodni pravni standardi u oblasti krivičnog procesnog prava i način njihove implementacije i Zakonik o krivičnom postupku, Zbornik „Zakonodavni postupak i krivično zakonodavstvo“, Srpsko udruženje za krivičnopravnu teoriju i praksu, Beograd, 2009;
4. Brkić, Snežana, Racionalizacija krivičnog postupka i uprošćene procesne forme, Pravni fakultet u Novom Sadu, Novi Sad, 2004;
5. *Damaška, Mirjan, "*O nekim učincima stranački oblikovanog pripremnog postupka", Hrvatski ljetopis za krivično pravo i praksu, Zagreb, vol. 14, 1/2007;
6. *Damaška, Mirjan, "*Sudbina anglo-američkih procesnih ideja u Italiji", Hrvatski ljetopis za krivično pravo i praksu, Zagreb, vol. 13, 1/2006;
7. Đurđević, Zlata, "Primjerovnik", Zagreb, Narodne novine, 2010;
8. Đurđić, Vojislav, Krivičnoprocesno zakonodavstvo kao normativna pretpostavka efikasnosti postupanja u krivičnim stvarima, Zbornik *Krivično zakonodavstvo, organizacija pravosuđa i efikasnost postupanja u krivičnim stvarima*, Srpsko udruženje za krivičnopravnu teoriju i praksu, Beograd, 2008;
9. Fischer, T., Strafgesetzbuch und Nebengesetze*,* 56. Auflage, *Verlag C.H. Beck*, München, 2009;

10. *Horvatić, Željko,* Cvitanović, Leo, "Politika suzbijanja kriminaliteta", Zagreb, Ministarstvo unutrašnjih poslova Republike Hrvatske, Policijska akademija, 1999;
11. *Krapac, Davor, "*Zakon o krivičnom postupku i drugi izvori hrvatskog procesnog prava", Narodne novine, Zagreb, 2008;
12. Krapac, Davor, "**Reforma mješovitog krivičnog postupka: potpuna zamjena procesnog modela ili preinaka prethodnog postupka u stranački oblikovano postupanje",** Zbornik radova Pravnog fakulteta u Zagrebu i Pravnog fakulteta Univerziteta "Justinijan prvi" u Skoplju, posvećen prof. dr Franji Bačiću, 2007;
13. *Pavišić, Berislav,* Novi hrvatski Zakon o krivičnom postupku", Hrvatski ljetopis za krivično pravo i praksu, Zagreb, vol. 15, 2/2008;
14. Pavlović, Šime, "Poznavanje i primjenjivost ustavnih i konvencijskih načela o pravičnom postupku", .Hrvatski ljetopis za krivično pravo i praksu, Zagreb, vol. 16, 2/2009;
15. Radulović, Drago, Reforma krivičnog procesnog zakonodavstva Crne Gore, „Revija za kriminologiju i krivično pravo", Beograd, 2/2010;
16. Roxin, C., Strafrecth, Allgemeiner Teil, Band I, 4. Auflage, *Verlag C. H. Beck*, München, 2006;
17. *Sijerčić-Čolić, Hajrija,* Krivično procesno pravo, knjiga II, Pravni fakultet Univerziteta u Sarajevu, Sarajevo, 2008;
18. Sijerčić-Čolić, Hajrija, „Specifični instituti u razvoju novog krivičnog postupka u BiH", *Revija za kriminologiju i krivično pravo*, Beograd, 1/2010;
19. Simović, Miodrag, Krivično procesno pravo, knjiga prva, Pravni fakultet, Bihać, 2009.
20. Simović, Miodrag, O nekim iskustvima u funkcionisanju novog krivičnog procesnog zakonodavstva Bosne i Hercegovine, Zbornik *Nove tendencije u savremenoj nauci krivičnog prava i naše krivično zakonodavstvo*, Udruženje za krivično pravo i kriminologiju Srbije i Crne Gore, Beograd, 2005;
21. *Van Dijk, Van Hoof, "Theory and Practice of the European convention on human rights",* Kluwer, 1998.

Academician Miodrag N. Simović,
Full Professor of the Faculty of Law of Banja Luka and President of the Constitutional Court of Bosnia and Herzegovina
Marina M. Simović-Nišević, M.A.,
the Indirect Tax Administration of BiH, doctoral candidate

ON THE UPCOMING REFORM OF THE CRIMINAL PROCEDURE CODE OF BOSNIA AND HERZEGOVINA IN THE CONTEXT OF FURTHER COMPLIANCE WITH THE EUROPEAN STANDARDS

SUMMARY

After the introductory remarks, the paper contains a review of the most significant solutions that are introduced by the upcoming extensively prepared reform of the Criminal Procedure Code of Bosnia and Herzegovina which became effective on 1 March 2003. The authors particularly analyze solutions agreed upon within the Working Group for Draft Law on Amendments to the Criminal Procedure Code of Bosnia and Herzegovina (submitted the Council of Ministers of Bosnia and Herzegovina in December 2011) that represent harmonization of this law with international standards or the current application has shown some flaws or in fact it has initiated improvement of certain provisions. That primarily relates to annulment of obligatory detention, decision-making in the session of the panel or hearing before the second instance court, annulment of first instance judgment, provisions on new non-contentious legal remedy – request for review of legality and quasi-renewal of criminal proceedings. Even the newest amendments that were the focus of interest of BH professional but also general public for the past months, bring some essential and fundamental changes to the criminal proceedings primarily to main proceedings and proceedings upon legal remedies, *inter alia*, by providing that a panel of the second instance court, by granting the appeal, can annul first instance judgment and refer the case back to the panel of the fist instance court for renewed trial. In addition, the Court of BiH gives possibility to *ex officio* review judgment within meaning of violation of criminal law to the detriment of the accused. The goal of this work is not an all-inclusive and extensive analysis but rather a review of some points of reference of the proposed legislative reform.

Keywords: Criminal Procedure Code of Bosnia and Herzegovina, the Court of Bosnia and Herzegovina, custody, revoking verdict, request for review of legality.

Pregledni rad - UDK 343.3/.7: 343.21

NE/EFIKASNOST AKTUELNOG KRIVIČNOG ZAKONODAVSTVA U SUZBIJANJU KRIMINALITETA, SA POSEBNIM OSVRTOM NA ISTRAGU

Prof. dr Mile Matijević
Internacionalna asocijacija kriminalista Banja Luka
Dragan Mitrović
Direkcija za koordinaciju policijskih tijela Bosne i Hercegovine

Apstrakt: Približava se deset godina od uspostave novog krivičnog procesnog zakonodavstva na području Republike Srpske – Bosne i Hercegovine. Od donošenja Zakona o krivičnom postupku Republike Srpske – Bosne i Hercegovine 2003. god. očekivalo se značajno unapređenje efikasnosti u suzbijanju kriminaliteta, a posebno onih najtežih oblika, tj. organizovanog i transnacionalnog kriminaliteta, kojima se ugrožavaju najznačajnije društvene vrijednosti. Izmjene „starog“ ZKP su bile u sferi uspostavljanja „novog“ koncepta istrage (objedinjavanje policijske i tužilačke istražne djelatnosti), uz ukidanje klasične policijske kriminalističke obrade, te „predaju“ istrage u nadležnost tužilaštvu. Policijskim organima su oduzeta neka decenijama posjedovana ovlašćenja (policijski pritvor, rad sa osumnjičenim bez prisustva branioca, podnošenje krivične prijave i sl.). Novim ZKP uvedene su veoma moćne operativne metode i sredstva „posebne istražne radnje“ u pribavljanju dokaza kod najsloženijih oblika kriminalne djelatnosti. Pojedine analize u proteklom periodu pokazuju da je došlo do određenih promjena u realiziaciji i shvatanju nadležnosti organa i načina vršenja poslova. Međusobni odnosi i saradnja policije, tužilaštva, sudija, advokata i drugih subjekata u prethodnom i glavnom krivičnom postupku značajno je izmijenjena. Ocjena rezultata primjene novog zakonodavstva veoma je različita. Neki smatraju da je unapređena efikasnost svih organa, drugi da je ovaj model totalno neefikasan i nefunkcionalan, a ima i onih daju djelimičnu vrijednost aktuelnom modelu, zakonskoj određenosti i efikasnoti pojedinih mjera i radnji. U radu će se analizirati kretanje kriminaliteta, počev od prijavljivanja, otkrivanja NN učinioca, razjašnjavanja krivičnog djela, preduzimanja radnji dokazivanja – istražnih radnji, pa do krivičnog procesuiranja, presuđivanja. Prezentiraće se određeni komparativni podaci i dati mogući zaključci u vezi sa kvalitetom, efikasnosti nadležnih organa u pojedinim fazama prethodnog i glavnog krivičnog postupka.

Ključne riječi: Kriminalitet, krivično procesno zakonodavstvo, istraga, efikasnost, otkrivanje, razjašanjavanje, presuđivanje, tamno polje kriminala, saradnja, profesionalizam.

AKTUELNI OBLIK ISTRAGE U BOSNI I HERCEGOVINI

Istraga[1] predstavlja fazu prethodnog krivičnog postupka u kojoj policijski

[1] Istraga apsorbovala i kriminalističku obradu, zbog čega se u slobodnoj verziji može nazivati i kriminalističkom istragom.

organi – agencije u zajedničkoj djelatnosti sa tužilaštvom preduzimaju planirane mjere i radnje radi pronalaženja i obezbjeđenja dokaza za uspješno vođenje krivičnog postupka.

Sukladno načelu akuzatornosti i legaliteta, istragu može jedino pokrenuti – narediti javni tužilac[2]. Međutim, postoji i situacija kada pripadnici policijskih agencija mogu samostalno pokrenuti i preduzeti pojedine istražne radnje i bez obavještavanja javnog tužioca.[3]

U zemljama regiona (Srbija, Hrvatska[4]) tek u 2011. godini sprovedena je višegodišnja inicijativa koja je kroz zakonodavnu proceduru donijela "nove" zakone o krivičnom – kaznenom postupku. Donesenim zakonima ustanovljava se "tužilačka – odvjetnička istraga". Međutim, model tužilačke istrage, pored toga što ima izvjesne sličnosti sa "BiH modelom", ima i određene razlike. Osnovna razlika se sastoji u tome što se i u novim ZKP Srbije i Hrvatske zadržava tzv. predistražni policijski postupak (otkrivanja krivičnog djela isključivom policijskom djelatnošću[5]), što doprinosi kompletnijem i kvalitetnijem operativnom i otkrivačkom zahvatanju osumnjičenika od strane policije, prije ulaska u "tužilačku" istragu. Time se nadalje zadržava krivična – kaznena prijava, koja je u BiH ZKP izgubila pravni i stvarni konstituens[6].

U ovom radu razmatraće se značaj i doprinos tužilačke istrage u otkrivanju, razjašnjavanju i dokazivanju krivičnih djela organizovanog kriminaliteta[7]. Tužilac je dužan u skladu sa načelom legaliteta krivičnog gonjenja da preduzme krivično gonjenje, ako postoje osnovi sumnje za krivično djelo i učinioca. U kontekstu ove zakonske odredbe postavlja se pitanje kako tužilac dolazi do osnova sumnje koja ga opredjeljuje za pokretanje postupka otkrivanja i krivičnog gonjenja učinilaca krivičnih djela. Kako je Zakon o krivičnom postupku iz 2003. godine dao u nadležnost javnom tužiocu i djelatnost otkrivanja krivičnog djela, za razliku od ranije nadležnosti u sferi gonjenja, smatramo da je tužilac ovim ovlašćenjima dobio značajniju kriminalističko-istražnu fukciju, koja ga ovlašćuje, ali i obavezuje, da se već od prvog saznanja i poimanja osnova sumnje neposredno uključi u procjenjivanje postojanja osnova sumnje o krivičnom djelu i učiniocu.[8]

Upravo je to jedno od bitnih pitanja o kome se tokom cjelokupne strategije tužilačke istrage vodi tužilačko-policijska saradnja, koja bi morala rezultirati višim kvalitetom početnih informacija, saznanja, koja će opredijeliti tužilaštvo da inicira, tj. naredi početak istrage.

---

[2] Ovakvo rješenje sadrže sva četiri zakona o krivičnom postupku (ZKP BiH, ZKP Republike Srpske, ZKP Federacije Bosne i Hercegovine i ZKP Brčko Diskrikta BiH)

[3] Za krivična djela za koja je predviđena kazna zatvora do 5 godina, potrebno je obavijestiti javnog tužioca u roku do 7 dana. Ovakvu odredu predviđaju sva četiri ZKP-a u BiH.

[4] Pavišić, B. (2008). „Novi Hrvatski zakon o kaznenom postupku", *Hrvatski ljetopis za kazneno pravo i praksu*, vol. 15, broj 2/2008, Zagreb, str. 489–60.

[5] Komentar Zakona o krivičnom postupku Srbije.

[6] I nakon skoro decenijske primjene već „iskusnog" ZKP, u komunikacijama, pa i zvaničnika, ostaje tradicionalni pojam „krivična prijava".

[7] Otkrivanje krivičnih djela organizovanog kriminaliteta je u nadležnosti tužilaštva Bosne i Hercegovine, što ne isključuje određene aktivnosti i djelovanje i entitetskih tužilaštava i policijskih agencija, kao i policije i tužilaštva Distrikta Brčko.

[8] Značajno je da postoji saglasnost tužioca i policije u pogledu postojanja osnova sumnje, kao početnog kvalitativnog sadržaja za otpočinjanje istrage o krivičnom djelu i učiniocu.

U sferi organizovanog kriminaliteta kao svojevrsne nadgradnje klasičnih oblika kriminala, neophodno je potrebno da tužilaštvo u odnosu na policijske organe ima izvjesnu naredbodavnu i koordinativnu ulogu i zadatak. Takav zadatak se posebno ogleda u neophodnosti blagovremenog uključivanja u razmatranje i fiksiranje početnih saznanja o pripremanju i izvršavanju krivičnih djela organizovanog kriminaliteta. U takvim situacijama tužilačko učešće i odlučivanje o konstituisanju osnova sumnje je veoma značajno u smislu ključnih načela israge (akuzatornosti i legaliteta krivičnog gonjenja).

Takva situacija, koja je obezbijeđena odredbama Zakona o krivičnom postupku, ničim ne umanjuje operativno-kriminalistički kapacitet i snagu kriminalističko-obavještajne djelatnosti policije. Ona mora da svojim brojnim i ofanzivnim sistemima detekcije početnih podataka, informacija,[9] te njihovim svrsishodnim procjenjivanjem i sistematizovanjem doprinese stvaranju početnog kvantuma činjenica koje bi mogle uvjeriti tužioca o opravdanosti naređivanja i početka istrage u konkretnom slučaju.

Kod krivičnih djela organizovanog kriminaliteta, veoma je bitno iz niza razloga pravnopolitičke i druge prirode da se javni tužilac blagovremeno obavijesti o postojanju osnova sumnje o kivičnom djelu i učiniocu. Naime, policijske agencije, ako samostalno prikupljaju takve podatke i obavještenja, te ako ih duže drže i čuvaju u svojim oprativnim dosijeima, na takav način ne omogućavaju tužiocu ostvarivanje njegove ustavne i zakonske funkcije u vezi s otkrivanjem i gonjenjem učinilaca najtežih krivićnih djela.

Zbog toga, policijski organi bi morali redovno, a u određenim situacijama i neizostavno[10] da informišu tužioca o dinamici prikupljanja, raspolaganja početnim podacima, a posebno kada i sami smatraju da postoje osnovi sumnje za krivično djelo odnosno učinioca. U svim slučajevima kada postoje indicije za krivična djela organizovanog krimanala, tj. kada je predviđena kazna zatvora preko pet godina, odredbe Zakona o krivičnom postupku su obavezale policijske agencije[11] da neizostavno tj. odmah obavijeste tužioca o svim raspoloživim podacima, te da mu predlože otvaranje istrage.

SARADNJA TUŽILAŠTVA I POLICIJE U ISTRAGAMA KRIVIČNIH DJELA ORGANIZOVANOG KRIMINALITETA

U teorijskom smislu saradnja policije i tužilaštva je neophodna. Ona je značajna za uspjeh i kvalitet istrage. U praktičnom smislu, pored ustanovljenih relacije saradnje (nadzor tužioca, mogućnost povjeravanja pojedinih istražnih radnji policiji i dr.), javlja se i niz problematičnih situacija, u vezi s međusobnom saradnjom, ili nesaradnjom, što može imati negativne posljedice i po ukupan kvalitet i rezultat istrage. Kako je Zakon o krivičnom postupku jasno istakao, u slučaju krivičnih djela za koja je zaprijećena krazna zatvora preko pet godina tužilac je neophodno

[9] Matijević, M., Mitrović, D. (2011). *Kriminalistika operativa*. Banja Luka: IAK.

[10] U slučajevima postojanja osnova sumnje za krivična djela za koja je predviđena kazna zatvora preko pet godina, policija je dužna odmah obavijestiti tužioca, i predložiti mu pokretanje istrage.

[11] Ovlaštena službena lica unutar policijskih agencija.

potreban da se neposrednije uključi u sve faze istrage, što znači da svojevrsno i rukovodi istragom, izdajući naloge policiji i drugim subjektima – učesnicima istrage. Posebno se to odnosi na potrebu stručnog nadzora tužioca nad karakterom, kvalitetom istrage. Ovakva zakonska odredba je jasna i sasvim svrsishodna[12]. Smatra se da će tužilac svojim znanjem, autoritetom doprinijeti nezavisnosti, snazi istrage koja će biti efikasnija, kvalitetnija u odnosu na samostalno vođenje od strane policije[13]

Međutim, postoji shvatanje da je tužilačko učešće nepotrebno, nedovoljno ili da se stvaraju problemi, dualitet rukovođenja, i nejasnoća ko je glavni autoritet, akter istrage. Zakoni o krivičnom postupku dali su dosta jasne odredbe, koje nisu detaljnije razrađene, ali se iz njih može vidjeti relacija odnosa i saradnje policije i tužilaštva[14]. Najbolji model saradnje jeste stvaranje zajedničkih istražnih timova u koje ulazi tužilac ili više njih, i policijske agencije, gdje se jasno utvrđuju zadaci i relacije saradnje. U poslu je potrebno da postoji jedinstvo akcije, koordinacija, a ne i u personalnoj odgovornosti. Jasno je da policija i dalje zadržava samostalnost i odgovornost u svojoj hijerarhijskoj liniji, ali i strukovnu odgovornost i obavezu prema tužiocu kao svojevrsnom ruovodiocu akcije[15].

Poseban značaj imaju zajedničke akcije pri primjeni pojedinih radnji dokazivanja, kao što su: uviđaj, rekonstrukcija događaja, vještačenje, pretresanje u svim oblicima, privremeno oduzimanje predmeta, ispitivanje osumnjičenih, saslušanje svjedoka, lišavanje slobode i pritvaranje, kao i druge mjere i radnje.[16] Na osnovu mjerodavnih teorijskih analiza ovlašćenja, sposobnosti, efikasnosti policije i tužilaštva, smatramo da je policiji potrebno dati dovoljno operativne slobode, inicijativnosti u otkrivačkoj djelatnosti, tj. u sferi prikupljanja podatka, obavještenja, koja se moraju stalno prezentirati nadležnom tužiocu, radi njegove ocjene njihove validnosti i potrebe uključivanja u cjelokupnu strategiju istrage[17].

Neprihvatljivo je da policija samostalno i duže vrijeme, a posebno kod težih krivičnih djela organizovanog kriminala, primjenjuje mjere i radnje koje moraju biti pod nadzorom tužioca. Javni tužilac mora da bude apsolutno u toku primjene posebnih istražnih radnji[18]. Tu se posebno misli na procjenu zakonitosti primjene u

---

[12] Zakonodavac je upravo želio da pojača kvalitet istrage neposrednim učešćem tužioca od prvog momenta njene realizacije, a posebno kroz radnje naređivanja, nadzora, praćenja.

[13] Upravo su ključne zamjereke prethodnog ZKP bile u vezi s tzv. policijskom nezakonitosti u primjeni pojednih istražnih radnji.

[14] U praksi policije i tužilaštva različito se ponekada tumači međusobni odnos, relacije saradnje ova dva subjekta istrage. Shvatanja idu od nivoa potpune nezavisnosti organa do potpune integrisanosti po principu nadređenosti i podređenosti, a u suštini nijedno shvatanje nije pravilno.

[15] Dobri primjeri osmišljene saradnje i koordinirane akcije policije i tužilaštva u posljednjim akcijama na području Bosne i Hercegovine dali su pozitivne rezultate, a javnosti pokazali ukupnu moć policijsko-tužilačke saradnje. (Akcija Kastel, Maoča, i još neke).

[16] Neke od ovih radnji tradicooonalno kvalitetno vrše policiski organi, ali u njihovom učešću je takođe bitno učešće tužioca (npr. uviđaj kod teških krivičnih djela, saslušanje i ispitivanje osumjičeng, bitnih svjedoka i dr.).

[17] Ovakav postupak je posebno značajan kod procjene potrebe postupanja u slučaju postojanja osnova sumnje kod krivičnih djela organizovanog kriminaliteta (krijumčarenja, finansijskih delikata, krivičnih djela gdje se indicira učešće lica iz vlasti, politike).

[18] Zakon o krivičnom postupku je precizirao uslove za primjenu posebnih istražnih radnji, dok instruktivna akta policije konkretizuju način, tehnologiju realizacije u konkretnoj kriminalističkotaktičkoj situaciji (Detaljnije u: Matijević, M., Mitrović, D. (2011). *Kriminalistika operativa*. Banja Luka: IAK.)

vezi sa prikupljanjem tj. obezbjeđenjem dokaza u svakoj konkretnoj situaciji. Veća je operativna, ali i dokazna šteta ako policija i u dobroj namjeri preduzme pojedine posebne istražne radnje, ali suprotno odredbama Zakona o krivičnom postupku, i time onemogući dalju upotrebu kvalitetnih dokaza koji su pribavljeni na nezakonit način[19]

ISKUSTVA U TUŽILAČKOJ ISTRAZI

U proteklim godinama veoma su različita iskustva u organizaciji i vođenju istrage u skladu sa odredbama aktuelnih Zakona o krivičnom postupku. U odnosu na očekivanja na početku primjene zakona smatralo se da će istraga dobiti novi kvalitet, time što će je tužilac naređivati, nadgledati, tj. nadzirati, a posebno što će u stručnom tužilačkom pogledu integrisati policijsko-tužilačku aktivnost,[20] koja bi morala donijeti novi sveukupni kvalitet.

Tužilačka istraga krivičnih djela organizovanog kriminala može biti veoma efikasna ako se kvalitetno i dobro koordinira od strane tužioca, kao vrhovnog organizatora i menadžera istrage[21]. Učešće tužioca, specijalnih tužilaca u Republici Srpskoj[22] bez potpunijeg uključivanja policije, i nije najbolji model istrage kod složenijih krivičnih djela organizovanog kriminala. Naime, ma koliko pripadnici tužilaštva bili mobilni i aktivni, pripadnici policije raspolažu velikim ljudskim kapacitetom, a time i operativnim potencijalom za vođenje sveobuhvatne pa i kvalitetne istrage, gdje je neophodno učešće i tužilaštva, što samo tužilaštvo mora na određeni način razumjeti i iskoristiti.

Samostalnost tužilaštva u neposrednoj operativno-istražnoj djelatnosti može biti nepotpuno, nedovoljno, čak i kontraproduktivno, i time može umanji ukupan efekat istrage. Zbog toga, potrebno je i korisno aktivirati i zadužiti i policiju da participira u istrazi složenijih slučajeva, tj. organizovanog kriminala, čime će se zasigurno zahvatiti širi dijapazon kriminogenih problema. Istovremeno će se svi učesnici istrage (policija, tužilaštvo) učiniti odgovornijim za konkretni istražni predmet.

U okviru ukupne strategije suzbijanja organizovanog kriminaliteta, izmjenama Zakona o krivičnom postupku 2003 godine ustanovljene su brojne posebne istražne radnje, koje u ranijem zakonu nisu uopšte postojale, ili su bile u nadležnosti drugih organa. Kako se shvatilo da se u ofanzivniju borbu protiv

---

[19] Javljanju se slučajevi gdje pripadnici policije bez obzira na poznavanje ZKP u žaru operativne žurbe prekorače neka ovlašćenja i time „ pokvare“ perspektivne dokaze, bez kojih će se teško dalje voditi istrga, a posebno teško formirati i zastupati optužnica na sudu.

[20] U ranijem ZKP postojao je posebno tzv. pretkrivični (policijski) postupak, nakon čega se provodila sudska istraga, što je u suštini bio dupli – sličan posao, što se željelo novom koncepcijom istrage prevazići.

[21] Nekoliko slučajeva istraga teških krivičnih djela organizovanog krimanala u BiH, gdje se neposredno angažovao i državni tj. glavni tužilac u BiH pokazalo je veću ozbiljnost i efektivnost u odnosu ne parcijalne i samostalne policijske istrage.

[22] Učešće i djelovanje Specijalnog tužilaštva RS u istragama krivičnih djela organizovanog kriminala je dosta upitno, s obziorom da činjenicu da se pripadnici policije značajno isključuju iz takve aktivnsti, što kasnije rezultira odgovornošću samog specijalnog tužilaštva u daljem toku i nošenju tereta istrage.

savremenih oblika i vidova kriminaliteta (organizovani kriminalitet) ne može ići „staromodnom“ tehnologijom, zakonodavac je omogućio policijskim agencijama da u skladu sa zakonom primjenjuju radnje i metode koje su već bile uveliko „oprobane“ u razvijenim zemljama, kao npr. efikasna metoda u pribavljanju i fiksiranju dokaza za najteža krivična djela, a koja se nisu na drugi način mogla pribaviti.

U okviru kriminalističke obrade krivičnih djela organizovanog kriminaliteta, primjena posebnih istražnih radnji ima veoma značajnu ulogu u pronalaženju i obezbjeđenju dokaza koji se na drugi način ne mogu obezbijediti. Tu se posebno misli na pribavljanje dokaza u vezi sa međusobnim tajnim kontaktiranjem osumnjičenih lica, zaticanje na mjestu izvršenja krivičnog djela, zaticanje u primopredaji predmeta krivičnog djela, skrivanju predmeta i tragova krivičnog djela[23]

U okviru primjene posebnih istražnih radnji, teorijska razrada i zakonska regulativa je utvrdila pravila u primjeni ovih veoma “osjetljivih” metoda i sredstava. U praksi policije i tužilaštva poznati su primjeri veoma kvalitetne primjene ovih metoda i sredstava, ali i slučajevi primjene suprotno zakonskim osnovama i normama. Naime, u primjeni metoda i sredstava ponekada se ne vodi dovoljno računa o neophodnosti prethodne detaljne pripreme izvršilaca za primjenu posebnih istražnih radnji, metoda tajne primjene, potrebi čuvanja ljudskih prava i sloboda lica, problemu provociranja krivičnog djela, problemu vremenskog ograničenja primjene, neophodnosti postojanja naredbe nadležnog organa, i drugim okolnostima. U slučajevima prekoračenja ovlašćenja ili primjene posebnih istražnih radnji suprotno Zakonu o krivičnom postupku, dokazi pribavljeni na ovaj način neće se moći upotrebiti u daljem krivičnom postupku[24]

Primjena odredaba Zakona o oduzimanju imovine stečene krivičnim djelom

Odredbe Zakona o oduzimanju imovine stečene izvršenjem krivičnog djela[25] primjenjuju se za krivična djela propisana u KZ Republike Srpske. Imovinom koja je stečena izvršenjem krivičnog djela smatra se ona imovina učinioca krivičnog djela, vlasnika imovine, koja je stečena prije pokretanja postupka za krivično djelo iz čl. 2 zakona, a koja je u očiglednoj nesrazmjeri sa njegovim zakonitim prihodima. Ovdje se trasira put za uvođenje istog zakona na nivou Bosne i Hercegovine odnosno Federacije BiH i Brčko Distrikta BiH. Donošenjem navedenog zakona i pokretanjem aktivnosti na pronalaženju, procesuiranju takve imovine u Bosni i Hercegovini se počinju primjenjivati svjetska iskustva u efikasnijoj borbi protiv organizovanog kriminaliteta. Naime, radi se o sasvim novom krivičnopravnom institute, koji u svijetu daje veoma značajne efekte i rezultate.

Uloga policije i tužioca u otkrivanju takve imovine i provođenju istrage je neizostavna i ključna za dalji postupak njenog obezbjeđenja tj. privremenog

[23] Metode posebnih istražnih radnji imaju veoma dragocjenu svrhu kod dokumentovanja koruptivnih krivičnih djela u „in flagranti“ situacijama, kako se jedino i mogu obezbijediti kvalitetni dokazi. (npr. Afera indeks u Kragujevcu)

[24] Šikman, M. (2011). *Organizovani kriminalitet*. Banja Luka: Visoka škola unutrašnjih poslova, str. 441–548.

[25] *Zakon o oduzimanju imovine stečene izvršenjem krivičnog djela* („Sl. Glasnik Republike Srpske“, br. 12/10) od 01. 07. 2010. God.

oduzimanja, i na kraju, konačnog postupanja s njom[26] U slučajevima kada se dođe do osnova sumnje o postojanju takve imovine, tužilac je nadležan da naredi finansijsku istragu. Istragom rukovodi tužilac, a kriminalističko-istražni postupak vodi Ministarstvo unutrašnjih poslova – posebna organizaciona jedinica u čijoj je nadležnosti otkrivanje imovine stečene izvršenjem krivičnog djela. U cilju obezbjeđenja takve imovine, tužilac može podnijeti zahtjev za privremeno oduzimanje takve imovine. O zahtjevu odlučuje nadležni sud, a upravljanje privremeno oduzetom imovinom preuzima Agencija za upravljanje privremeno oduzetom imovinom. Konačnu odluku o statusu imovine donosi sud po zahtjevu tužioca. Ovaj novi, još neisproban krivičnopravni institut na ovim prostorima će se sigurno u narednom periodu afirmisati na prostoriu cijele države, jer je to jedina perspektivna metodologija kojom se može značajnije stati na put nekontrolisanom i nezakonitom bogaćenju lica kroz vršenje krivičnih djela. Tradicionalni metodi su se pokazali apsolutno neefikasnim, što dovoljno govori o potrebi hitnog aktiviranja svih mehanizama ovakve krivično pravne zaštite interesa države i građana, u čemu zemlje u okruženju već pokazuju evidentne rezultate.

ASPEKTI ISTRAGE POJEDINIH VRSTA KRIVIČNIH DJELA ORGANIZOVANOG KRIMINALA

U istrazi pojedinih krivičnih djela organizovanog kriminala različita su iskustva u modalitetima angažovanja policije i tužilaštva, sa stanovništa zajedničkog procjenjivanja postojanja osnova sumnje, i potrebe zajedničke djelatnosti, što je osnova početka istrage. Zajednička aktivnost policije i tužilaštva nalazi se u učešću tužioca već od prvnih radnji. kao i kod krajnje ocjene kvaliteta istrage i njenog završetka, tj. stvaranja uslova za podizanje optužnice.

Istrage **nasilničkih delikata** kao mogućih oblika organizovanog kriminaliteta posebno su složene kada su u pitanju teška ubistva, pod složenim motivima (naručena ubistva), i drugi vidovi nasilja, gdje je prinuda osnovni oblik radnje izvršenja, a povezuje se sa organizovanom kriminalnom djelatnošću. Kod teških krivičnih djela organizovanog krimanala nasilnički delikati[27] obavezuju tužioca da se posebno zainteresuje i uključi u sve faze istrage, počev od donošenja hitne naredbe za istragu, preko nadzora nad radom ovlašćenih službenih lica, kao i neposrednog saslušanja pojedinih lica, a posebno osumnjičenog. Posebno je bitna pravilna procjena prihvatanja inicijative policije u preduzimanju tzv. hitnih istražnih radnji (pretresa, lišenja slobode, pritvora, primjene posebnih istražnih radnji). Svaki tužilac koji posmata suštinu efikasnog otkrivanja ovakvih krivičnih djela poprimiće izvjesnu policijsku psihologiju istrage i intenzivno će podržati policiju u preduzimanju radnje čije preduzimanje ne trpi odlaganje[28].

---

[26] *Ibid*.

[27] Najteži oblici nasilničkih delikata koji imaju karakter organizovanog kriminaliteta (specifična ubistva, otmice, reket, ratni zločini, teroristički akti), zahtijevaju tijesnu saradnju policije i tužilaštva u svim fazama prethodnog I krivičnog postupka.

[28] Pored primjera dobre zajedničke aktivnosti i saradnje, poznati su slučajevi nerazumijevanja i suprotstavljenih shvatanja, pa i odluka policije i tužioca (određivanje pritvora, pretresanje i dr.).

Privredna krivičnih djela, a posebno ona koja po svojim fenomenološkim sadržajima imaju karakter organizovanog kriminala, predstavljaju veoma čestu i posebno složenu problematiku u nadležnosti istraga. Takvi delikti su uglavnom u obliku delikata: Zloupotreba položaja i ovlašćenja, Zloupotrebe ovlašćenja u privrednom poslovanju, tzv. "finansijskih delikata," pranja novca, poreskih utaja i sl. Uloga tužioca mora biti veoma stručna, oprezna, ali i strpljiva. Posebno stručna procjena postojanja osnova za otvaranje istrage umnogome će opredijeliti dalju dinamiku, tok, pa i samu zakonitost istražnih radnji[29]. Vrlo je značajno da postoji koordinirana djelatnost sa policijom u realizaciji mjera prvog zahvata, kao što su hapšenja, pritvor, privremeno oduzimanje predmeta, saslušanje lica.

Iskustva proteklih istraga kod krivičnih djela privrednog kriminala u Bosni i Hercegovini često ukazuju na dosta neusklađenu, nesinhronizovanu istražnu djelatnost policije i tužilaštva, što je rezultiralo značajnim "odugovlačenjem" istrage, nepotpunim preduzimanjem dokaznih radnji, čiji rezultati su se na glavnom pretresu vrlo brzo "raspršili" pod jakim udarom odbrane.

Poreska krivična djela potpadaju pod nadležnost poreskih institucija[30], ali i policijskih agencija. Sveukupne inicijative, nastojanja u državi da se uredi poreski sistem nisu dovoljna, pa je potrebna aktivnost nadležnih organa na otkrivanju i dokumentovanju konkretnih krivičnih djela. Ovdje se posebno ostvaruju obilježja krivičnih djela organizovanog kriminaliteta (poreske utaje, kao prethodnog djela pranja novca), gdje je neophodna potpunija saradnja nadležnih organa, uz izrazitu rukovodno-nadzornu ulogu tužioca. Pored saradnje policije, tužilaštva, neophodno je potpunije akativranje drugih subjekta istrage (stručna lica, finansijski stručnjaci)[31], od kojih istražne ekipe moraju dobiti kvalitetne informacije koje bi opredijelile dalji tok istrage. Nije preporučljivo da se prethodno preduzimaju čak ni represivne mjere (lišavanje slobode, pritvaranje lica), a tek onda da se vrše preliminarne finansijske kontrole, koje pokažu nekada i „svu apsurdnost" istrage.

Pribavljanje prljavog novca i imovine u BiH je u porastu. Od stupanja na snagu Zakona o sprečavanju pranja novca 2004. godine, Državna agencija za istrage i zaštitu je podnijela više od 80 izvještaja tužilaštvima, a prema njihovim procjenama, u BiH se godišnje opere oko 70 miliona KM. Prljavi novac, prema podacima Tužilaštva BiH, najčešće se pribavlja poreskim utajama, krijumčarenjem ljudi, trgovinom droge i ljudi, organizovanjem prostitucije, trgovinom oružja, cigareta i alkohola, te zloupotrebama u bankarskom i kartičnom poslovanju. Pranje novca, prema podacima iz prakse tužilaštava, najčešće radi jedno preduzeće, odnosno njegov direktor, za desetine drugih firmi. Novac koji potiče iz utaje poreza firme su prale preko zajedničke, najčešće fiktivne firme. Recept je jednostavan: dokumentacijom se lažno prikaže da je između preduzeća postojao kupoprodajni odnos, i to u veleprodaji, odnosno bez poreza na prodaju, iako posla uopšte nije bilo.

---

[29] Tužilac ne bi smio odugovlačiti otvaranje istrage ako su očigledni osnovi sumnje, ali ni ulaziti u nju na svaki "mig", nekada jakih faktora u vlasti, politici. (Poznati su slučajevi oba oblika, koji su se uglavnom neslavno završili).

[30] UINO BiH, PU RS, PU FBiH, PU BD BiH.

[31] Hasanspahić, S. (2010). „Saradnja i koordinacija djelovanja policijsko istražnih i tužilačkih organa u otkrivanju, dokumentovanju i procesuiranju poreznih krivičnih djela", u: *Zbornik radova*. Kelebija: IAK, str. 568.

Prema državnom Zakonu o sprečavanju pranja novca u BiH, koji je usvojen 2009. godine, za otkrivanje, sprečavanje i istraživanje pranja novca i finansiranje terorističkih aktivnosti zadužen je Finansijsko-obavještajni odjel (FOO) koji pripada Državnoj agenciji za istrage i zaštitu. Bosna i Hercegovina se, sudeći prema prema broju pravosnažnih sudskih presuda, nalazi u samom vrhu liste zemalja koje se efikasno bore protiv pranja novca, oblika kriminalnog djelovanja putem kojeg određene grupe traže način da transformišu sredstva stečena kriminalnim radnjama u legitimno zarađeni novac.

Posebna dinamičnost istrage ostvaruje se kod raznih oblika kriminalnih radnji **krijumčarenja** (lica, droga, vozila, i sl.). Značaj operativnog sadejstva tužioca i policije ogleda se u blagovremenom predlaganju adekvatnih mjera i radnji u istrazi (primjena posebnh istražnih radnji, lišenje slobode, saradnja sa drugim policijskih agencijama, saradnja sa Interpolom, i dr.). U proteklom periodu značajan pozitivan napredak su učinili istražni organi u organizovanju, realizaciji kriminalističkih obrada kod ovih krivičnih djela. Dobra tehnička opremljenost, kvalitetna operativna priprema i uvezanost sa drugim policijskim, istražnim strukturama daje rezultate u sve uspješnijem suzbijanju ovih oblika kriminaliteta.[32]

Posebno je značajno ukazati na značaj efikasne istrage kod **korupcijskih krivičnih** djela, kao i svu složenost preduzimanja mjera i radnji u obezbjeđenju dokaza za uspješno vođenje krivičnog postupka. Poznato je da postoje brojne strategije, planovi za uspješnije suzbijanje korupcije, što uglavnom ostaje u sferi „praznih" strategija, i neproduktivnih konkretnih akcija. Pored insistiranja na razvijanju preventivnih mehanizama, zahtijeva se energičnija akcija policijsko-tužilačkih organa, koji imaju zadatak da u ovoj sferi kriminaliteta, primjenjujući najsuptilnije operativno-istražne metode, pribave kvalitetne dokaze za uspješno vođenje krivičnog postupka**.**

U proteklom periodu su malobrojni istražni postupci u ovoj oblasti bili uspješni, i pored brojnih ukazivanja na postojanje kriminalnih radnji, gdje se posebno ističe koristoljubljivost, korumpiranost, zloupotreba službenog polažaja i ovlašćenja. Ključni problem neefikasnosti istrage nalazi se u neobezbjeđenju kvalitetnih dokaza i njihovom „naknadnom" nestajanju, čime se ne obezbjeđuje neophodan uslov za podizanje optužnice. Osuđujuće presude za ovakva krivična djela su rijetkost.[33]

OSTVRT NA REZULTATE ISTRAGA U BOSNI I HERCEGOVINI

Rezultati istraga u proteklom periodu na prostorima BiH, pa i šire, u vezi sa suzbijanjem krivičnih djela organizovanog kriminala, pokazuju izvjesne

[32] Procjena relevantnih međunarodnih institucija jeste da su nadležni organi Bosne i Hercegovine unaprijedili rad u ovoj oblasti.

[33] Prema statistici državnog tužilaštva, entitetskih policija i tužilaštva mogu se pronaći poneki procesuirani, pa i presuđeni slučaj, što je svakako zanemarljivo u odnosu na ukupne procjene o prisutnosti ovog vida kriminala.

tendencije napretka. Međutim, vidljivo je da istraga krivičnih djela organizovanog kriminaliteta na prostorima Bosne i Hercegovine, posebno u vezi sa deliktima protiv privrede, korumptivnim deliktima, nije dala očekivane rezltate[34]. Uzroci takvog stanja su veoma složeni i različiti. Počev od nedovolje zajedničke procjene početnih podataka – osnova sumnje o krivičnom djelu i učiniocu, nesinhronizovanih aktivnosti nadležnih organa, nedovoljne uključenosti tužioca, ili policije. Posebno je pitanje u ne/prihvatanju zajedničke odgovornosti u vezi s kvalitetom ukupnih rezultata istrage[35].

Evidentno je da se „poznate afere" uglavnom neslavno završavaju, što ne ide u prilog kvalitetu i efikasnosti istrage krivičnih djela oganizovanog kriminaliteta. Takvi rezuzltati u suštini devalviraju kvalitet i snagu istrage, kao bitnu fazu prethodnog krivičnog postupka, kojom se obezđjeđuju ključni dokazi za uspješno vođenje krivičnog postupka[36]. Mora se anlazirati gde se nalaze uzroci takvog stanja, te ih u narednim koracima ispravljati, doprinoseći efiksnijem radu i boljim rezultatima.

Bez detaljnije analize konkretnih krivičnih predmeta, odnosno događaja, može se konstatovati da su sudovi u donošenju validnih sudskih odluka limitirani kvalitetom dokaza koji su ponuđeni na glavnom pretresu, i da presude donose skladno načelima krivičnog postupka. [37] Na osnovu prethodnih analiza mogu se istaći bitne karakteristike dobre aktivnosti, kao i karakteristični problemi u okviru organizacije, vođenja istrage u vezi sa otkrivanjem i dokazivanjem krivičnih djela organizovanog kriminaliteta: zajednička aktivnost tužilaca – policije ojačava istragu, jedinstvo istrage je snažnije, skraćeno je vrijeme istrage; ekonomičnost istrage, primjena efikasijih istražnih metoda i sredstava su pozitivne karakteristike istražnog postupka, dok se problemi javljaju u vezi sa: nedovoljnom saradnjom policije i tužilaštva, nejasnosti zakona, nedovoljnom stručnosti, neodgovornosti u radu.

Da bi se dobio cjelovit odgovor na pitanja sveukupnih karakteristika istrage krivičnih djela organizovanog kriminaliteta u proteklom period, neophodno bi bilo projektovati kvalitetno naučnostručno istraživanje. Predmet istraživanja bi bila tužilačka istraga u proteklom periodu primjene.

---

[34] Ostvariti detaljniji uvid u statističke podatke o odnosu pokrenutih istraga, podignutih optužnica i osuđujućih presuda.

[35] Nakon obustavljanja krivičnog postupka, događaju se međusobna optuživanja policije – tužilaštva, u cilju „skidanja" odgovornosti za neuspjeh u konkretnom slučaju.

[36] Poznata konstatacija prof. Vodinelića je upravo istakla „kakva istraga – takvo i suđenje".

[37] Načelo slobodnog sudijskog ocjenjivanja dokaza, i načelo *in dubio pro reo* obavezuju sudsko vijeće da svestrano razmotri svaki dokaz pojedinačno, a onda sve dokaze u međusobnoj vezi, i da osuđujuću presudu zasnuje isključivo na odlučnim činjenicama koje su dokazane.

PRIKAZ PRIVREDNOG KRIMINALITETA PREMA PODACIMA SVIH TUŽILAŠTVA U BIH (PRIJAVA, ISTRAGA, OPTUŽNICA, PRESUDA)

Godina	**Naziv institucije**	**Ukupno zaprim. prijava**		**Ukupno naređeno istraga**		**Ukupno podign. optužnica**		**Uku. pod. opt. sa kriv. nalogom**		**Ukupno doneseno presuda**	
		predmeta	osobe	predmeta	osobe	predmeta	osobe	predmeta	osobe	predmeti	osobe
2007.	Tužilaštvo BiH	358	632	174	324	111	169	19	21	75	113
	Kan.tužilaš. FBiH	907	1.552	410	606	270	354	50	59	245	285
	Okružno tužil. u RS	691	1.200	462	744	300	463	89	130	316	412
	Javno tužil. Brčko Dist.	23	47	23	27	14	27	0	0	13	17
	Ukupno	**1.979**	**3.431**	**1.069**	**1.781**	**695**	**1.013**	**158**	**210**	**649**	**827**
2008.	Tužilaštvo BiH	343	559	116	193	68	96	11	16	65	95
	Kan. tužil. FBiH	1015	1.839	469	735	266	365	62	80	224	320
	Okružno tužil. u RS	685	1.222	402	678	306	429	127	163	251	347
	Javno tužil. Brčko Dist.	7	10	7	10	10	22	1	1	13	16
	Ukupno	**2.059**	**3.630**	**994**	**1.616**	**650**	**914**	**201**	**260**	**553**	**777**
2009.	Tužilaštvo BiH	387	629	239	424	134	207	18	24	89	132
	Kan. tužil. FBiH	962	1.462	472	780	315	468	154	294	284	398
	Okružno tužil. u RS	606	1.091	423	749	133	214	42	70	261	378
	Javno tužil. Brčko Dist.	37	48	**18**	**25**	**7**	**10**	**0**	70	8	13
	Ukupno	**1.992**	**3.230**	**1.152**	**1.978**	**589**	**899**	**214**	**389**	**642**	**921**
∑	**2007, 2008. i 2009.**	***6.021***	**10.291**	***3.215***	**5.375**	***1.934***	**2.226**	**573**	**854**	***1.844***	**2.525**

Tabela daje osnovne pokazatelje u trogodišnjem periodu (2007–2009) u vezi sa aktivnošću nadležnih organa (policija, tužilaštvo, sudovi) u fazama prijavljivanja krivičnih djela, naređivanja istrage, optuženja, i presuda. Pokazatelji se odnose na sva četiri postupajuća tužilaštva u Bosni i Hercegovini (Tužilaštvo BiH, Tužilaštvo Brčko Distrikta, kantonalna tužilaštva F BiH, i okružna tužilaštva RS).

Iz prezentirane tabele o nekim faktima iz oblasti privrednog kriminaliteta u Bosni i Hercegovini vidljive su interesantne karakteristike, iz kojih se mogu izvući određeni zaključci. Tako je vidljivo da je ukupan broj prijava koje je zaprimilo tužilaštvo na području BiH u posmatranom period 6.021, protiv 10.291 lica. U odnosu na broj zaprimljenih prijava, broj otvorenih – naređenih istraga je tek iznad

50% u odnosu na prijave. Navedena konstatacija govori u prilog činjenici da se prijavljuju "razni" slučajevi, koji veoma često nemaju obilježja krivičnog djela za koje se goni po službenoj dužnosti, ili da tužilaštvo "ipak" ne otvara istragu skladno načelu *ex ocifio*.

Ova konstatacija je svakako preliminarna, i trebalo bi je tek istražiti kroz sveobuhvatno analiziranje i sintetiziranje raspoloživih podataka, ali i analizu konkretnih prijava, predmeta istraživanja. Takođe je za posebnu analizu i zaključivanje u odnosu na broj naređenih istraga i broj podignutih optužnica, gdje je vidljivo da jedna trećina istražnih predmeta ne "doživi" optuženje. Ovakva situacija u vezi sa neoptuživanjem znatnog broja lica u odnosu na istragu, zahtijeva analiziranje i zaključivanje u vezi sa odnosom broja otvorenih istraga i podignutih optužnica.

Na kraju treba istaći odnos broja podnesenih prijava za krivična djela privrednog kriminaliteta i broja presuda (6021: 184). Ovaj odnos govori o nizu mogućnosti tumačenja efikasnosti prethodnog i glavnog krivičnog postupka u okviru sveukupne aktivnosti na suzbijanju kriminaliteta, a posebno kroz krivično procesuiranje krivičnih djela i učinilaca.

ZAKLJUČAK

Na osnovu teorijskih analiza istrage krivičnih djela organizovanog kriminaliteta na području Bosne i Hercegovine u određenom periodu može se steći izvijestan utisak o nekim karakteristikama, tendencijama ovog kriminaliteta. Posebno se dobija saznanje o sadržaju, karakteristikama i sveukupnim dometima tužilačke istrage u otkrivanju, dokumentovanju krivičnih djela organizovanog kriminaliteta. U zavisnosti od vrsta kriminaliteta, stiče se utisak da je tužilačka istraga u izvjesnim oblastima unapredila kvalitet, efikasnost tužilačko-policijske djelatnosti, koja rezultira kvalitetnim osudama.

Međutim, takođe je vidljivo da je aktuelni model istrage još nedovoljan i neefikasan da se energičnije suprotstavi najsloženijim oblicima organizovanog kriminaliteta, posebno krivičnim djelima sa elementima korupcije, kada se kao učinioci u svim oblicima saučestvovanja pojavljuju organizovane kriminalne grupe, a posebno pod uticajem jakih struktura vlasti, politike.

Zbog svega navedenog potrebno je sveobuhvatno analizirati stanje istrage kod krivičnih djela organizovanog kriminaliteta, a posebno u kontekstu zahtjeva za efikasnije zahvatanje „tamnog polja" najsloženijih oblika kojima se ugrožavaju ključne društvene vrijednosti, posebno u obliku enormnih protivpravnih prisvajanja materijalnih dobara građana i države.

U nastojanju da se zadovolje proklamovani zahtjevi evropskih standarda, istražni, sudski organi u Bosni i Hercegovini moraju permanentno raditi na unapređenju metoda sopstvene djelatnosti, kroz jačanje preventivnih metoda u suprotstavljanju organizovanom kriminalu, ali i kroz sve ofanzivnije i organizovanije otkrivanje, razjašnjavanje, dokumentovanje i dokazivanje kriminalnih radnji u toj oblasti.

Posebno bi bilo značajno da se u okviru zajedničke, koordinirane aktivnosti policije i tužilaštva unaprijede slijedeća pitanja, oblasti istražne djelatnosti:

- Operativnija i kvalitetnije kriminalističko-obavještajna djelatnost policije, koja prethodi sticanju „osnova sumnje“ kao potrebnog kvalitativnog stepena sumnje za otvaranje istrage,
- Zajednička procjena postojećih saznanja, podataka, obavještenja u momentu predlaganja i iniciranja otvaranja istrage, da bi se izbjegli kasniji suprotstavljeni stavovi i ocjene kvaliteta početnih podataka i obavještenja,
- Jasnije i neposrednije učešće tužilaca u „težim“ predmetima organizovanog kriminala, gdje bi se vidljivije manifestovao “tužilački“ nadzor, kontrola i stručna pomoć,
- Operativniji pristup tužilaca u pripremanju i preduzimanju pojedinih istražnih radnji, sa ciljem „zadovoljavanja principa“ brzine i efikasnosti otkrivanja i gonjenja osumnjičenih,
- Zajednička procjena dostignutog kvaliteta prikupljenih dokaza u fazi istrage da bi se izbjegle kasnije suprostavljenosti u ocjeni rezultata istrage i doprinosa, i odgovornosti tužilaštva i policije,
- Postistražna analiza pojedinih slučajeva radi ocjene kvaliteta prethodnog rada i „eventualnog“ ispravljanja pogrešaka u prethodnim istražnim predmetima.

Da bi odgovorili postavljenom zahtjevu, nadležni organi moraju svoja zakonska ovlašćenja, koja su manifestovana kroz primjenu istražnih sredstava i metoda, maksimalno jačati u smislu zakonitog, a posebno efikasnog primjenjivanja, skladno odredbama Zakona o krivičnom postupku i pravilima kriminalistike, kako bi društvena zajednica imala puno povjerenje u njih. Time bi se ostvarila njihova potpunija i plodotvornija ustavna i zakonska funkcija, dok bi moralni principi pravde bili bar djelimično zadovoljeni.

LITERATURA:

1. Bošković, M. (2004). *Organizovani kriminalitet i korupcija*. Banja Luka: Visoka škola unutrašnjih poslova.
2. Bošković, M. (2003). *Transnacionalni organizovani kriminalitet*. Beograd: Policijska akademija.
3. Ignjatović, Đ. (1998). *Organizovani kriminalitet, drugi deo*. Beograd: Policijska akademija.
4. Ignjatović, Đ. (1998). *Organizovani kriminalitet*. Beograd: Policijska akademija.
5. Govedarica, M. (2010). „Funkcionisanje jedinca za posebne istrage MUP RS u kontekstu posebnih istražnih radnji, lišenja slobode i zastupanja optužnice“. Zbornik radova, *Savremene tendencije krivične represije kao instrument suzbijanja kriminaliteta*. Bijeljina: Srpsko udruženje za krivičnopravnu teoriju i praksu.
6. Matijević, M. (2010). „Posebnim istražnim radnjama ka efikasnijoj istrazi“. Zbornik radova, *Savremene tendencije krivične represije kao instrument suzbijanja kriminaliteta*. Bijeljina: Srpsko udruženje za krivičnopravnu teoriju i praksu.

7. Matijević, M. (2005). „Stanje i tendencije organizovanog kriminaliteta u Republici Srpskoj – Bosni i Hercegovini, sa posebnim osvrtom na saradnju policije i tužilaštva“. Zbornik radova. Beograd: Policijska akademija.
8. Pavišić, B. (2008). „Novi Hrvatski zakon o kaznenom postupku“, *Hrvatski ljetopis za kazneno pravo i praksu*, vol. 15, broj 2/2008, Zagreb, str. 489-60.
9. Simović-Nišević, M. (2010). *Otkrivanje i dokazivanje krivičnih djela organizovanog kriminaliteta u Bosni i Hercegovini*. Sarajevo: Privredna štampa.
10. Simović, M. (2009). *Krivično procesno pravo*. *Knjiga 1 i 2*. Banja Luka, Bihać: Pravni fakultet.
11. Šikman, M. (2011). *Organizovani kriminalitet*. Banja Luka: Visoka škola unutašnjih poslova.
12. Škulić, M. (2002). *Organizovani kriminalitet*. Beograd: Dosije.

Drugi izvori:
13. Modul, Centar za edukaciju sudija i tužilaca Republike Srpske, Federacije BiH.
14. Ministarstvo sigurnosti Bosne i Hercegovine, Informacija o stanju sigurnosti u Bosni i Hercegovini, januar–juni 2010. godine, Sarajevo, 2010.
15. Vijeće ministara Bosne i Hercegovine, Strategija Bosne i Hercegovine za borbu protiv organizovanog kriminaliteta (period 2009–2012. godine), Sarajevo, 2009.
16. Vijeće ministara Bosne i Hercegovine, Strategija za borbu protiv korupcije (2009–2014), Sarajevo, 2009.
17. Zakon o krivičnom postupku BD BIH (“Sl. glasnik BD”, br. 10/03,48/04, 06/05, 12/07,14/07, 21/07).
18. Zakon o krivičnom postupku BiH (“Sl. glasnik, BiH”, br. 03/03, 32/03, 36/03, 26/04, 63/04, 12/05, 48/05, 46/05, 76/06, 29/07, 32/07, 53/07, 76/07, 15/08, 58/08, 12/09, 16/09, 93/09).
19. Zakon o krivičnom postupku FBiH (“Sl.novine FBiH”, br. 35/03, 37/03, 56/03, 78/04, 28/05, 55/06, 27/07, 53/07, 09/09, 12/10).
20. Zakon o krivičnom postupku RS („Sl. Glasnik RS”, br. 50/03, 111/04, 115/04, 29/07, 68/07, 119/08).
21. www.msb.gov.ba
22. www.mupvladars.net
23. www.tuzilastvobih.gov.ba
24. www.wikipedia.com

IN / EFFICIENCY OF CURRENT CRIMINAL JURISDICTION IN FIGHTING AGAINST CRIME WITH A SPECIAL FOCUS ON INVESTIGATION

Abstract: It's about ten years since the establishment of a new criminal procedural law in the Republic of Srpska - Bosnia and Herzegovina. By adopting the Law on Criminal Procedure of the Republic of Srpska - Bosnia and Herzegovina from 2003, it was expected significantly enhanced efficiency in combating crime, especially of the most serious form, ie. organized and transnational crime, which endangering the most important social values.

Changes of the "old" Law on criminal procedure were in the sphere of establishing a "new" concept of the investigation (combining police and prosecutorial investigation activities), with the abolition of traditional police criminalistic processing, and "consignation" of the investigation to the jurisdiction of the prosecution. From the police bodies was revoked the authorities, that they possessed for decades (police detention, work with the suspect without the presence of counsel, the filing of criminal charges, etc.). By the new LCP were introduced a very powerful operative methods and funds, "special investigations" in obtaining evidence in the most complex forms of criminal activity.

Some analyzes from the previous period shows that there were some changes in the realization and understanding of the competence of the authorities and the ways of performing tasks. Mutual relations and cooperation between police, prosecutors, judges, lawyers and other entities in the previous and the main criminal proceedings is significantly altered. Evaluation of the results of the new legislation is very different. Some believe that was improved the efficiency of all entities, the other think that this model is totally inefficient and ineffective, and there are those who give a partial value to the current model, legal certainty and efficiency of the measures and actions.

This paper will analyze the development of crime, ranging from reporting, disclosure of unknown perpetrator, clarifying the offense, taking action of proving - investigation and a criminal prosecution, adjudication. Paper also will present certain comparative data and give possible conclusions about the quality, efficiency of the competent authorities at various stages of previous and the main criminal proceedings.

Keywords: Crime, criminal procedural law, investigations, efficiency, detecting, clarification, judgment, dark field of the crime, cooperation and professionalism.

Prethodno saopštenje – UDK 351.74/.76(4-672 EU)

UNUTRAŠNJA BEZBEDNOST EU I POLICIJSKA SARADNJA U POSTLISABONSKOJ ERI

Prof. dr Snežana Nikodinovska-Stefanovska
Fakultet bezbednosti – Skopje, Republika Makedonija
snikodinovska@fb.uklo.edu.mk
Ass. mr Marjan Đurovski
Fakultet bezbednosti – Skopje, Republika Makedonija
mgjurovski@fb.uklo.edu.mk

Apstrakt: Stupanjem na snagu decembra 2009, godine, Ugovor iz Lisabona (LU) postepeno je uveo veliki broj promena koje su otvorile brojna pitanja povezana sa aktivnostima Evropske unije (EU) na polju unutrašnje bezbednosti. Između ostalog, LU ukida trostubnu strukturu Unije uvedenu ugovorom iz Mastrihta i daje pravni status EU. Lisabonski ugovor postavlja razvoj prostora slobode bezbednosti i pravde kao drugi cilj EU, nakon promoviranja mira i blagostanja njenih građana. Prostor slobode, bezbednosti i pravde sačinjen je od različitih i kompleksnih političkih oblasti, uključujući, između ostalih, pitanja vezana za policijsku i pravosudnu saradnju, imigraciju, azil, granice i evropsko državljanstvo. Ugovorom iz Lisabona oblast slobode, bezbednosti i pravde spada u podeljene nadležnosti EU, što znači da Unija deli nadležnosti sa državama članicama gde se primenjuje „redovni zakonodavni postupak".

Ugovor iz Lisabona i Štokholmski program podstakli su usvajanje velikog broja strateških dokumenata za dalji razvoj prostora slobode, bezbednosti i pravde. Strategija unutrašnje bezbednosti je jedan od nekoliko dokumenata koji određuju pravac razvoja unutrašnje bezbednosti EU.

Kreiranje i sprovođenje politike u oblasti pravde i unutrašnjih poslova je u direktnoj vezi sa jačanjem zakona, garantovanjem slobode i prava građana, kao i obezbeđivanje stabilnosti demokratskih institucija. Definiranje pristupa Republike Makedonije integraciji u oblasti pravde i unutrašnjih poslova određeno je sa nekoliko ključnih determinanti. Treba obezbediti sistem stabilnih institucija koje funkcionišu i garantuju podršku drugih sektora integracije. Isto tako, potrebno je približavanje standardima i pravilima neophodnim za uspostavljanje bliže saradnje relevantnih institucija u Republici Makedoniji sa institucijama EU i državama članicama.

U radu se analiziraju implikacije Ugovora iz Lisabona na prostor slobode, bezbednosti i pravde i posebno policijske saradnje, kao i značenje Strategije unutrašnje bezbednosti za stvaranje evropskog bezbednosnog modela. Dalje u radu biće prikazane aktivnosti Republike Makedonije u oblasti harmonizacije nacionalnog zakonodavstva sa zakonodavstvom EU u oblasti pravde i unutrašnjih poslova.

Kjučne reči: Lisabonski ugovor, prostor slobode, beznednosti i pravde, policijska saradnja, strategija unutrašnje bezbednosti

UVOD

Uloga Evropske unije (EU) u domenu unutrašnje bezbednosti datira još od sredine 1970-tih stvaranjem Grupe TREVI, neformalnog foruma za saradnju

policijskih i pravosudnih organa EZ, kao odgovora na terorističke izazove tog vremena. Međutim, tek Ugovor o Evropskoj uniji iz 1992 godine, koji je stupio na snagu 1993. godine, poznatiji kao Ugovor iz Mastrihta, formalno institucionalizira saradnju u oblasti pravosuđa i unutrašnjih poslova između država članica kao trećeg stuba EU. Cilj saradnje u ovim oblastima, koje su identifikovane kao oblasti zajedničkog interesa država članica EU, bio je da obezbedi slobodno kretanje ljudi, istovremeno obezbeđujuči sigurnost građana Unije. Naime, Ugovor o Evropskoj uniji sistematizovao je i proširio domet aktivnosti tadašnje Evropske zajednice u dve glavne nove poitičke oblasti: vanjska politika i unutrašnji poslovi – tzv. drugi[1] i treći stub[2] Unije. Budući da većina evropskih vlada u to vreme nije bila spremna deliti nacionalni i izvršni suverenitet u ovim osetljivim oblastima sa centralnim evropskim institucijama, bila je usvojena specifična procedura za donošenje odluka u ovim novim oblastima zajedničke evropske aktivnosti. Ove procedure uključuju jednoglasno odlučivanje/konsenzus; limitiranu ulogu Evropske komisije (EK) i Evropskog parlamenta (EP) u proceduri donošenja odluka, i nikakvu ulogu Evropskog suda pravde (ESP).

Amsterdamski ugovor iz 1997. godine, koji je stupio na snagu 1999. godine, revidira Ugovor iz Mastrihta, kako u formalnopravnom smislu tako i u pravcu konsolidacije triju stubova na osnovu kojih deluje EU. Vlade država članica EU su se saglasile da kreiraju oblast slobode, bezbednosti i pravde[3] do 2004. godine. Posebno značajne promene izvršene su u trećem stubu. Prvo, napušten je rigidni međudržavni tretman zajedničkih politika i oblika saradnje u ovim oblastima, koji je bio zavisan od volje država i njihove spremnosti za saradnju. Saradnja se ne razvija samo na inicijativu država članica, a pravilo jednoglasnosti ustupa mesto pravilu većinskog odlučivanja za određene zajedničke politike i procedure odlučivanja. Ovaj ugovor delimično transferira političke oblasti iz međuvladinog trećeg stuba u prvi komunitarni stub. Naime, jedan deo nadležnosti iz trećeg stuba, kao što su režim vanjskih i untrašnjih granica EU, vizni režim, azil, imigracije i sudska saradnja u građanskim stvarima, prebačen je u prvi supranacionalni stub EU – stub Zajednice, gde su se odluke donosile kvalifikovanom većinom (tzv. tradicionalni "metod zajednice"). Najosetljivije oblasti pravosudne i policijske saradnje u krivičnim stvarima ostaju u trećem stubu EU, sada primenovanom u policijsku i pravosudnu saradnju u krivičnim stvarima, gde se primenjuje takozvani međuvladin metod odlučivanja (intergovernmental metod), što znači da su se odluke donosile jednoglasno, tj. saglasnošću svih država članica.

Poslednji ugovor EU tzv. Ugovor iz Lisabona[4] (2009) daje mogućnost za jačanje uloge EU u domenu unutrašnje bezbednosti. Naime, ovaj ugovor uvodi niz novina, odnosno dopunjuje i menja Ugovor o Evropskoj uniji i Ugovor o osnivanju Evropske zajednice pa je otuda često nazivan reformskim ugovorom.

Ugovorom iz Lisabona izmenjen je Ugovor o osnivanju EZ i preimenovan

---

[1] Zajednička spoljna i bezbednosna politika – Common Foreign and security policy (CFSP).

[2] Pravda i unutrašnji poslovi – Justice and Home Affaairs (JHA).

[3] Area of Freedom, Security and Justice (AFSJ).

[4] Puni naziv ugovora je: Treaty of Lisbon amending the Treaty on European Union and the Treaty establishin the European Community (Official Journal of the European Union, C 306, 2007). http://eur- lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2008:115:0201:0328:EN:PF

u Ugovor o funkcionisanju EU (UFEU), a Ugovor o EU koji je, isto tako, pretrpeo više promena, zadržava svoj naziv. I posle Lisabona ostaju dva osnivačka ugovora. Međutim, pre Lisabona svaki se odnosio na različiti entitet – Uniju i Zajednicu i različiti pravni sistem – pravo unije (Union law) i pravo zajednice (Community law). Nakon Lisabona, i pored dva ugovora, postoji samo jedan entitet –Unija, jedini sistem i jedinstveni set institucija, gde je razlika između stubova (skoro) ukinuta. Ovo obeležava kraj apsurdnog dualizma između Unije i Zajednice, uspostavljenog Mastrihtskim kompromisom. Kao što je već pomenuto, i pored činjenice da i dalje postoje dva osnivačka ugovora, oni se sada odnose na jedan jedini entitet. Tako su osnovna pravila Unije podeljena između dva odvojena teksta: EU i UFEU. Iako je naglašeno da oba ugovora imaju jednako pravno značenje, oni se faktički razlikuju u sadržini i formalnim pravnim režimima. Prvi ugovor sadrži principe i osnovna pravila za Uniju; ustanovljava/postavlja njene ciljeve, vrednosti, kompetencije, institucionalnu strukturu, odnose sa državama članica i evropskim građanima i procedure za amandmane, pristupanje i napuštanje Unije. Drugi ugovor postavlja pravila po kojima će institucije delovati, način na koji se uređuje domače tržište, kao i odredbe za reguliranje implementacije zajedničkih politika (Micossi, 2009).

Ugovor iz Lisabona daje, prvi put, pravni subjektivitet EU, ukida „trostubnu strukturu“ EU, proširuje glasanje kvalifikovanom većinom na veliki broj pitanja unutrašnje bezbednosti, jača kompetencije EU u oblasti krivičnog i krivičnog procesnog prava, daje mogućnost za etabliranje Evropskog javnog tužioca i mogućnost za definiranje uslova pod kojim policija može da deluje na teritoriji druge države članice. Sve ove novine pružaju mogućnost za jačanje uloge EU u domenu unutrašnje bezbednosti. Međutim, prostor slobode, bezbednosti i pravde spada u podeljene nadležnosti EU, što znači da u ovoj oblasti Unija deli nadležnosti sa državama članicama. LU u članu 4 st. 2 ističe da će Unija poštovati osnovne funkcije države, uključujuči zaštitu teriorijalnog integriteta države, održavanje reda i mira i zaštitu nacionalne bezbednosti. Posebno se naglašava da nacionalna bezbednost ostaje u jedinstvenoj nadležnosti svake države članice.

Kakve su implikacije LU na oblast slobode bezbednosti i pravde, osobito na policijsku saradnju?

LISABONSKI UGOVOR I PROSTOR SLOBODE, BEZBEDNOSTI I PRAVDE

Jedna od najznačajniih novina LU je svakako ukidanje trostubne strukture EU, što je omogučilo razvitak politika i akcija u oblasti slobode, bezbednosti i pravde (SBP). Naime, Mastrihtska struktura EU zasnovane na tri stuba podrazumevala je primenu različitih pravnih režima za pitanja/aspekte SBP iz prvog stuba – vize, azil, migracije i druge politike povezane sa kretanjem ljudi i za politike iz trećeg stuba – policijsku i sudsku saradnju u krivičnim stvarima, što je predstavljalo izvor stalnih komplikacija (Balzacq&Carrera, 2005). Naime, odredbe koje se odnose na saradnju u oblasti pravde i unutrašnjih poslova (ex 3. stub), Lisabonski ugovor postavlja u Naslov V – Oblast slobode, bezbednosti i pravde, Ugovora o funkcionisanju Evropske unije. Ovaj naslov je podeljen na pet poglavlja sa ukupno 23 člana (čl. 67–89). Poglavlja sadržana u ovom naslovu jesu: Opšte odredbe; Politika o

pograničnoj kontroli, azilu i imigracijama; pravosudna saradnja u građanskim stvarima; Pravosudna saradnja u krivičnim stvarima i Policijska saradnja .

Ugovorom iz Lisabona je predviđeno da Unija čini prostor slobode, bezbednosti i pravde na kojem se poštuju osnovna prava i različitost pravnih sistema i tradicija država članica.[5] Takođe je predviđeno da EU radi na osiguranju visokog nivoa bezbednosti preventivnim delovanjem protiv kriminala, rasizma, ksenofobije i protiv njih se bori saradnjom i merama koje su usaglašene između nadležnih policijskih, pravosudnih i drugih nadležnih organa, kao i međusobnim priznanjem sudskih odluka u krivičnoj oblasti i, ukoliko je neophodno, približavanjem krivičnih zakonodavstva.[6]

Što se tiče policijske saradnje, Lisabon predviđa da Unija razvija policijsku saradnju kojom su obuhvaćeni svi nadležni organi država članica, uključujuči policijske, carinske i druge nadležne službe specijalizovane za oblast prevencije, otkrivanja i istragu krivičnih dela.[7]

Ugovorom iz Lisabona sva pitanja koja se odnose na pravdu i unutrašnje poslove (Justuce and home Affairs-JHA)[8] potpadaju pod tzv. Community method, koji je sada generalno pravilo u jedinstvenoj oblasti slobode, bezbednosti i pravde. Ugovor o funkcionisanju EU predviđa da postupak saodlučivanja postaje redovni zakonodavni postupak (*ordinery legislative procedure),* što podrazumeva podelu ovlaščenja za odlučivanje između EP i Saveta. Pre Lisabona, potreba jednoglasnosti u Savetu je otežavala proces legislacije, ali obuhvatanje ove materije pravilom glasanja kvalifikovanom većinom otvara prostor za izlaz iz ove situacije. Tako, sada Evropski parlament ima paralelnu legislativnu ulogu preko procedure saodlučivanja poznatu kao redovni zakonodavni postupak u skoro svim slučajevima. To znači da je EP kolegislator zajedno i na istoj osnovi sa Savetom.

U oblasti policijske saradnje između država članica EU većina odluka se donosi u okviru redovnog zakonodavnog postupka. Tako EP i Savet mogu utvrditi mere koje se odnose na: skupljanje, čuvanje, obradu i razmenu relevantnih informacija; podršku pri obukama osoblja, i saradnju u razmeni eksperta, opreme i istraživanja u otkrivanju kriminala; zajedničke istražne tehnike u otkrivanje ozbiljnih formi organiziranog kriminala.[9] Međutim postoje i odluke koje se donose u okviru posebnog zakonodavnog postupka. Poštujuči različite pravne sisteme i tradicije, LU uvodi nekoliko posebnih aranžmana i crvene linije. Naime, Savet može, u saglasnošću sa posebnim zakonodavnim postupkom, da utvrdi mere za operativnu saradnju policijskih, carinskih i drugih organa nadležnih za sprovođenje zakona (law enforcement), specijalizovane za oblast sprečavanja i otkrivanja krivičnih dela, kao i vođenje istrage o njima. U tom slučaju Savet,

[5] Čl.67, st.1 Ugovora o funkcionisanju Evropske unije (UFEU).
[6] Čl.67 st. 3 UFEU.
[7] Čl.87 st. 1 UFEU.
[8] Naziv Pravda i unutrašnji poslovi ('Justice and Home Affairs' – JHA) ne postoji u ugovorima. Međutim, ovaj naziv je poznatiji i prepoznatljiviji, a, isto tako, predstavlja izbor Komisije za naziv njena dva generalna direktorata (GD) u ovoj oblasti: pravda (Justice), koja sadrži osnovna prava i državljanstvo i unutrašnji poslovi (Home Affairs), koji uključuje migraciju, bezbednost a posebno terorizam i organizovani kriminal i civilnu zaštitu. Ova dva GD zamenjuju GD za pravdu, slobodu i bezbednost (poznat pod francuskim akronimom JLS).
[9] Čl.87 st.2 UFEU.

nakon konsultovanja Evropskog parlamenta, odlučuje jednoglasno.[10] Međutim, ako jednoglasnost nije postignuta, LU predviđa mogućnost pokretanja mehanizma *bliže saradnje* (enhanced cooperation) i u oblasti policijske saradnje. To znači da grupa od najmanje devet država članica može zatražiti da se o predlogu mera za operativnu saradnju izjasni Evropski savet. U tom slučaju postupak u Savetu se suspenduje. Posle diskusije, i u slučaju da se o tome postigne konsenzus, Evropski savet, u roku od četiri meseca, vrača predlog Savetu na usvajanje. Međutim, ako nije postignut konsenzus u istom roku, a najmanje devet država članica žele da uspostave bližu saradnju na osnovu predlog mera, one o tome obaveštavaju EP, Savet i EK. U tom slučaju pristupanje bližoj saradnji smatra se odobrenim i mogu se primenjivati odredbe o bližoj saradnji.[11]

U posebnom zakonodavnom postupku Savet odlučuje o još jednom važnom pitanju u oblasti policijske saradnje, a to je mogućnost intervencije nadležnih organa država članica na teritoriji druge drave članice. Naime, Savet u posebnom zakonodavnom postupku utvrđuje uslove i ograničenja pod kojima nadležni organi država članica mogu intervenisati na teritoriji druge države članice uz saglasnost i u dogovoru sa nadležnim organima te države.[12] Ovo je u saglasnosti sa mogućnostima ponuđenim državama članicama EU da upotrebe 'emergency brakes' i/ili da upotrebe mehanizam "bliže saradnje" (Guild & Carrera, 2011).

Monopol zakonske inicijative koji je Komisija imala u okviru prvog stuba EU, LU proširuje na postupak donošenja svih zakonskih akata (Radivojević, 2009). To znači da Lisabonskim ugovorom Komisija ima ekskluzivno pravo na legislativnu inicijativu, osim u policijskoj i sudskoj saradnji u krivičnim stvarima. Naime, sada pravo zakonske inicijative imaju paralelno Komisija i države članice, ali ne više na ravnopravnoj osnovi. Za razliku od Komisije, države to pravo ne mogu koristiti pojedinačno, već je potrebno da predlog zakonskog akta podnese grupa sastavljena od najmanje jedne četvrtine ukupnog broja država-članica.[13]

Što se tiče Evropskog suda pravde (ESP), LU donekle menja njegovu nadležnost. Naime, ESP dugo nije imao nadležnosti u oblasti policijske i pravosudne saradnje. Međutim, ovaj sud ni sada nema opštu nadležnost da tumači i kontroliše zakonitost akata usvojenih u oblast SBP. Naime, i nakon završetka tranzicionog[14] perioda od pet godina, Sud neće biti nadležan da kontroliše zakonitost ili proporcionalnost operacija/akcija izvršenih od strane policije ili drugih organa koji izvršavaju zakon u zemljama članicama EU. Sud isto tako neće odlučivati o pitanjima koja su u nadležnosti država u odnosu na održavanje javnog reda i mira kao i obezbeđenja/zaštite unutrašnje bezbednosti.[15]

---

[10] Ibid., st. 3 t. 1 UFEU.
[11] Ibid.,t. 3 UFEU.
[12] Čl.89 UFEU.
[13] Čl. 76 UFEU.
[14] Čl. 10 Protokola 36 (Protocol (No 36) on Transitional Provisions) **"**According to this provision, as a transitional measure, the powers of the Commission and the Court of Justice in relation to acts dealing with 'police cooperation and judicial cooperation in criminal matters" will continue to be 'as they were' in the EU Third Pillar for a period of five years after the entry into force of the Treaty of Lisbon."
[15] Čl.276 UFEU. Vidi više: http://www.publications.parliament.uk/pa/ld200708/ldselect/ldeucom/62/62.pdf

Pored jačanja uloge EP, Lisabonski ugovor predviđa i veću uključenost nacionalnih parlamenata u procesu donošenja odluka u EU. Naime, predviđeno je da se nacionalnim parlamentima moraju slati svi nacrti Komisije, inicijative drugih država članica, inicijative Evropske centralne banke, kao i nacrti Evropskog parlamenta. Nacionalnim parlamentima je data veća uloga u monitoriranje aplikacije principa subsidijrnosti u vezi s policijskom i pravosudnom saradnjom u krivičnim stvarima. Nacionalni parlamenti imaju veće nadležnosti u kontroli Evropola i Evropravde i nove nadležnosti u pogledu zaštite građanskih sloboda i osnovnih prava. EP je, takođe, potpuno uključen u definiranje strukture i funkcionisanje Evropola i Evropravde, kao i u polja delovanja i zadatke ovih agencija. Takođe EP, zajedno sa nacionalnim parlamentima, ima povećanu ulogu u detaljno ispitivanje/istraživanje aktivnosti Evropola i Evropravde.

LU predviđa jednu značajnu institucionalnu novinu, a to je mogućnost kreiranja Evropskog javnog tužioca (European Public Prosecutor). Iako je predviđeno da se bavi pitanjima finansijskog kriminala, budući tužilac mogao bi imati uticaja na slučajeve povezane sa transacionalnim kriminalom, kao što je međunarodni terorizam ili trgovina drogom (Bacquias, 2008).

STRATEGIJA UNUTRAŠNJE BEZBEDNOSTI

Stupanje na snagu Lisabonskog ugovora i usvajanje Stokholmskog programa[16] predstavljalo je podsticaj za usvajanje više strateških dokumenata za dalji razvoj oblasti SBP. Strategija unutrašnje bezbednosti (SUB) jedan je od nekoliko dokumenta koji daje orijentaciju za dalji razvoj ove oblasti.

Osnovi za usvajanje jedne SUB postojali su neko vreme u dokumentima EU. Preporuke i ukazivanja na potrebu jedne strategije pojavljuju se još 2006. godine u diskusiji Saveta oko "arhitekture unutrašnje bezbednosti (Council document 7039/2/06), kao i u izveštaju za Haški program (Council document 15844/06).

Usvajanjem Stokholmskog programa decembra 2009. godine, Evropska unija je postavila sebi zadatak da usvoji strategiju unutrašnje bezbednosti sa ciljem da se „dalje poboljša bezbednost u EU, i ujedine napori u suzbijanju organizovanog kriminala, terorizma i drugih pretnji kako bi se zaštitili život i bezbednost evropskih građana". U Stokholmskom programu unutrašnja strategija nije predstavljena kao posebni strateški dokument, već kao zaokružena celina u čiji zahvat ulaze već usvojeni evropski dokumenti, kao što su Evropska strategija bezbednosti [17] i Strategija spoljne dimenzije prostora slobode, bezbednosti i pravde[18].

Finalni tekst Strategije unutrašnje bezbednosti bio je usvojen od Saveta za JHA 25 februara 2010. (Council document 6870/10), za vreme španskog predsedništva, sa namerom da kreira "evropski model bezbednosti".

---

[16] The Stockholm Programme – *An open and secure Europe serving and protecting the citizens:* Doc. 16484/09.

[17] European Secyrity strategy" A safer Europe in a better world", 12 December 2003, http//www.cosillium.europa.eu/uedocs/cmsUpload/78367.pdf

[18] A Strategy for the External Dimensions of JHA: Global Freedom, Security and Justice, Council of the European Union, 15446/05.

Ciljevi Strategije su da omogući zajedničko delovanje postojećih politika u borbi protiv transnacionalnih bezbednosnih izazova, rizika i pretnji i kreiranje jednog "integriranog (holističkog) pristupa" bezbednosti koji će se baviti uzrocima i posledicama "ne-bezbednosti". Integrisani pristup bezbednosti treba da postane prepoznatljiva karakteristika evropskog modela bezbednosti u odnosu na pristupe drugih bezbednosnih aktera u svetu. Ovaj pristup podrazumeva zajedničke akcije saradnje organa koji sprovode zakon (law enforcement bodies), pravosudnu saradnju, upravljanje granicama (border management) i civilnu zaštitu u saglasnosti sa zajedničkim evropskim vrednostima, kao što je zaštita ljudskih prava.

Startegija je trebala da skupi u jedan dokumenat sve mere koje su bile usvojene tokom godina i da obezbedi okvir za postavljanje strateških smernica. Dokumentat je baziran na tri osnovne središnje tačke: definiciju rizika i pretnji, vodeće principe bezbednosne politike i definiranje strateških smernica.

U prvom delu Strategija identifikuje glavne izazove za unutrešnju bezbednsot EU kao i odgovor tim izazovima. Strateg prepoznaje bezbednost kao ključni faktor za obezbeđenje visokog kvaliteta života građana u evropskom društvu. Iako ne postoje stvari kao što je "zero risk", Unija se obavezuje da kreira sigurnu okolinu u kojoj se građani EU osećaju zaštičeni (Nikodinovska-Stefanovska, 2010).

Dalje, Strategija identifikuje principe i smernice/uputstva za akciju u pravcu postizanja "evropskog bezbednosnog modela". Principi uključuju, između ostalog, poštovanje osnovnih prava, vladavinu prava, zaštitu građana, naročito najrannjivije grupe, transparentnost i odgovornost u politikama bezbednosti, solidarnost i poverenje među državama članicama.

Generalna dijagnoza pretnji i izazova bila je praćena strateškim smernicama za akciju. Naime, na osnovu postavljenih principa Strategija je predvidela brojne smernice za akciju, "da bi garantovala unutrašnju bezbednost EU". Ove smernice uključuju proaktivni (intelegence-led) pristup vođen prevencijom i anticipacijom, jačanje razmene informacija između agencija koje sprovode zakon preko upotebe baze podataka EU, unpređenje saradnje između bezbednosnih agencija EU kao što su EUROPOL, EUROJUST, FRONTEX , CEPOL, Koordinator za borbu protiv terorizma i SitCen i obezbeđivanje koordinacije između njih od strane Stalnog komiteta za unutrašnju bezbednost[19], tela koji deluje u okviru Saveta.

Iako na prvi pogled deluje da je unutrašnja strategija bezbednosti „još jedna u nizu" strategija EU, primetno je da je ona pisana u duhu novina koje su zaživele stupanjem na snagu Lisabonskog ugovora, u decembru 2009. godine. Lisabonski ugovor je omogućio integrisanje politika unutrašnje bezbednosti (ukidanjem stubova) i pridavanje većeg značaja nadnacionalnim telima EU. Strategijom je planirano da njena razrada i implementacija bude jedan od prioriteta rada Stalnog komiteta za unutrašnju bezbednost.

Posle usvajanja SUB, Evropska komisija je krajem 2010. predstavila dokument Savetu i EP naslovljenim „Evropska strategija unutrašnje bezbednosti u pokretu: pet koraka napred ka bezbednijoj Evropi",[20] kojim se nastavlja proces

[19] Standing Committee on Internal Security, COSI. Stvaranje COSI predviđeno je članom 71 Ugovora o EU, kao i Odlukom Saveta (2010/131/EU).

[20] Commission Communication The EU Internal Security Strategy in Action: Five steps towards a more secure Europe (COM(2010)673) of 22 November 2010

primene Stokholmskog programa i Strategije unutrašnje bezbednosti. Predviđeno je sprovođenje više od četrdeset mera sa ciljem suzbijanja glavnih bezbednosnih pretnji u Evropi za vreme od 2011. do 2014. godine. Ovim akcionim planom za sprovođenje Strategije unutrašnje bezbednosti izrađuje se „krovni" mehanizam četvorogodišnjih mera za suzbijanje teških krivičnih dela, organizovanog i visokotehnološkog kriminala, te terorizma i, najzad, upravljanja spoljnim granicama i vanrednim situacijama.

Za sprovođenje akcionog plana odgovorne su institucije EU, te države članice i različite agencije EU. Posebno je naglašena važna uloga Stalnog komiteta za unutrašnju bezbednost.

REPUBLIKA MAKEDONIJA I EU INTEGRACIJE – oblast slobode, bezbednosti i pravde

Period nakon osamostaljivanja RM postavilo je nove izazove u oblasti vladavine prava i održavanja unutrašnje stabilnosti zemlje. Proces demokratizacije i proces tranzicije, praćeni ekonomskom krizom, komplikovani uticajem regionalne nestabilnosti, ratova i konflikata na širi društveni plan karakteriše i transformacija društvenih vrednosti i normi. Ovakvi procesi rezultiraju pojavom novih vidova kriminaliteta, povećanim nasiljem, prisutnošću organizovanog i transnacionalnog kriminala, kao i većeg boja povratnika među izvršiocima. Interetničke tenzije predstavljale su dopunjujuči otežavajuči faktor u procesu unutrašnje demokratizacije i garantovanje principa vladavine prava[21].

Neposredni kontekst Republike Makedonije (RM) – njen geopolitički položaj, novija istorija konflikta u regionu, situacija sa granicama, postkonfliktna stanja – daje dopunjujuće značenje svim pitanjima iz oblasti pravde i unutrašnjih poslova, postavljajući komplikovane/složene zahteve.

Kreiranje i sprovođenje politike u oblasti PVR je neposredno povezano s jačanjem vladavine prava, garantovanjem sloboda i prava građana i obezbeđivanjem stabilnosti demokratskih institucija. Formuliranje pristupa RM integracijama u oblasti PVR određeno je/ zavisi od nekoliko ključnih determinanti:

- potreba obezbeđivanja sistema stabilnih institucija koje funkcionišu u oblasti PVR i garantuju podršku drugih sektora integracije;
- potreba približavanja standarda i pravila neophodnih za uspostavljanje bliže saradnje relevantnih institucija RM sa institucijama EU i država članica;
- potreba formuliranja i implementacije adekvatnih politika u oblasti kretanja ljudi;
- potreba donošenja adekvatnih i efikasnih mera u borbi protiv organizovanog kriminala i korupcije;
- potreba jačanja regionalne saradnje.

U izveštaju Evropske komisije (EK) za 2011. godinu o napretku Republike Makedonije (RM) u Poglavlju 24, u delu: slobode, bezbednost i pravda, konstatovan je napredak u više oblasti.

[21] www.sep.gov.mk

Izmenom Zakona o strancima obezbeđen je pravni okvir za ustanovljavanje nacionalne baze podataka o strancima, obuhvatajući podatke o azilu, migracijama i vizama. Baza je funkcionalno povezana sa svim relevantnim institucijama. Razmena informacija i koordinacija ilegalne migracije sa zemljama iz regiona je ojačana. Što se tiće azila, u ovoj oblasti je postignut ograničeni napredak.

Građani RM mogu da putuju slobodno u EU. Vizna liberalizacija za građane koji putuju u šengen zonu je izvršena 19. 12. 2009. godine. Pravila bezviznog režima poštuju se od strane većeg dela putnika. Međutim, i pored bezviznog režima, povećan je broj neosnovanih traženja azila u nekoliko članica EU. Nadležne vlasti uvele su grupu mera protiv ove pojave, uključujući javne kampanje sa posebnim fokusom na ranjive grupe, kao i veću kontrolu na samim granicama. Ojačana je međusobna kontrola granica između RM i Bugarske otvaranjem Zajedničkog kontakt centra za policijsku i carinsku saradnju. Pored toga, potpisani su dokumenti za saradnju i zajedničke granične kontrole sa Bugarskom, Srbijom i Kosovom. RM je formirala dve mobilne jedinice na centralnom nivou da bi povećala efikasnost borbe protiv ilegalne migracije i prekograničnog kriminala i operativnu upotrebu analize rizika[22].

Komisija konstatuje da je postignut napredak u oblasti policijske saradnje i borbi protiv organizovanog kriminala (OK). Naime, formirano je međunarodno odeljenje za koordinaciju sprovođenja zakona koje je odgovorno za razmenu policijskih obaveštajnih informacija u okviru MUP-a. Isto tako, u MUP-u je formirano posebno odeljenje za OK. Sve službe koje se bave OK sada spadaju u okvir Centra za suzbijanje OK, koji uklučuje nacionalnu bazu za obaveštajne podatke i nacionalni centar za koordinaciju koji je odgovoran za strateško planiranje i skupljanje obaveštajnih informacija.

I pored napretka u oblasti policijske saradnje i borbe protiv OK, napori relevantnih organa za izvršavanje zakona, kao što su MUP, Carinska uprava i Finansijska policija, u borbi protiv OK traba da ojaćaju. U isto vreme, Komisija ukazuje da su potrebni značajni napori da bi se obezbedilo potpuno sprovođenje reformi policije u praksi, kao i da se obezbedi uspostavljanje nacionalne baze obaveštajnih podataka. Ukazano je na napredak policije u odnosu na borbu protiv terorizma. U 2011. godini Uprava za sprečavanje pranja novca i finasiranje terorizma prijavila je pet sumnjivih transakcija povezanih sa finansiranjem terorizma.

Komisija je konstatovala značajan napredak u oblasti spoljnih granica i saradnji u Šengen zoni, kao i u carinskoj saradnji.

Iz svega ovoga Komisija zaključuje da je RM na dobrom putu u ispunjavanju standarda EU u oblasti slobode, bezbednosti i pravde.

LITERATURA

1. Bacquias, J., (2008). Freedom, security and justice: the new Lisbon (Treaty) agenda, *Policy Brief.*
2. Griler, S., Zeller, J. (eds.), (2008).The Lisbon Treaty, EU Constitutionalism without a Constitutional Treaty? SpringerWienNewYork.

[22] www.sep.gov.mk

3. Guild, E.& Carrera, S. (2011). Towards an Internal (In)security Strategy for the EU? *CEPS Paper in Liberty and Security in Europe..*
4. Micossi, S. (2009). Democracy in the European Union u S., Micossi, &, G., L., Tosato (eds.), *The European Union in the 21st century, perspectives from the Lisbon Treaty,*(pp.214-236). Centre for European Policy Studies, Brussels.
5. Nikodinovska-Stefanovska, S. (2010).The EU Internal security Strategy, *Suzbijanje kriminala i evropske integracije (zbornik radova)*, Beograd, 321–328.
6. Radivojević, Z. (2009). Institucionalne novine u Lisabonskom ugovoru, *Pravni život*, Beograd, br. 14, 37–60.
7. Treaty of Lisbon amending the Treaty on European Union and the Treaty establishin the European Community (Official Journal of the European Union, C 306, 2007). http://eur- lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2008:115:0201:0328:EN:PF
8. 'Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union", Official Journal no C 115, 9 May 2008.
9. Стратегија на Република Македонија во ЕУ, Секретаријат за ЕУ интеграции на Владата на РМ, Скопје, 2006.

RESUME

The Maastricht Treaty included a third pillar that dealt with Justice and Home Affairs (JHA) cooperation. Like the second pillar, Common Foreign and Security Policy (CFSP), it was intergovernmental cooperation. Decisions normally required unanimity. The role of the Commission was very limited and the European Court of Justice (ECJ) was largely excluded.

The Amsterdam Treaty started moving some of JHA to the first pillar, thus introducing the Community method, with majority voting and increased roles for the Commission and the ECJ. The treaty introduced the concept of an Area of Freedom, Security and Justice (AFSJ). In its original form, the AFSJ comprised the fields of borders, immigration, asylum and judicial cooperation in civil matters in a legally binding form (previously called the EU's "first pillar"), and policing, terrorism and judicial cooperation in criminal matters in the more intergovernmental venue of the EU (formerly known as the "third pillar").

The entry into force of the Lisbon Treaty on 1 December 2009 has consecrated the standing of the area of freedom, security and justice (AFSJ) as the European Union's (EU) second objective after the promotion of peace and the well-being of its citizens. The Lisbon Treaty has simultaneously introduced a number of changes. The Lisbon Treaty formally abolished the old pillar structure in Justice and Home Affairs policies and brought (to varying degrees and subject to several exceptions) the different policy fields of the AFSJ into one fairly homogeneous legal and institutional framework. The AFSJ is now an area of shared competence between the EU and the Member States, where the 'ordinary legislative procedure' applies.

Since the entry into force of the Treaty of Amsterdam the EU has – as part of the general Treaty objective of the 'area of freedom, security

and justice' (AFSJ) – an explicit mandate to provide EU citizens with a 'high level of security', primarily through police and judicial cooperation measures. The EU's internal security mandate is, however, different from that of the states themselves as the EU's role is limited to that of a provider of 'added value' with respect to internal security functions that Member States already fulfill at the national level, with the security competences of the Member States remaining predominant and being explicitly protected in the Treaties. The principle of subsidiarity is very much at the core of the AFSJ security concept as action at the EU level can only be justified if internal security issues – because of their cross-border nature– can potentially be more effectively handled through common action at the EU level. Although to some extent original and innovative because of its extension of the notion of 'internal security' to an 'area' encompassing the territories of 27 Member States, the EU's security mandate is therefore limited in its substantive reach. The gradual extension of this substantive reach remains dependent on the political consensus among the Member States, and it will remain so even under the Lisbon Treaty, that explicitly protects the Member States' national internal security functions.

An Internal Security Strategy for the EU:" Towards a European Security Model" is a Spanish initiative that aims to bring together in a sole document all the measures that have been adopted over the years and provide them with a framework to set down strategic guidelines. The resulting document is comprehensive and contemplates the need to work in a coordinated way outside the boundaries of the EU. It is also based on three fundamental axes: the definition of risks and threats, the guiding principles of the security policy and the defined strategic guidelines.

The strategy lays out a European security model, which integrates among others action on law enforcement and judicial cooperation, border management and civil protection, with due respect for shared European values, such as fundamental rights. Also, the Internal Security Strategy takes into account the External Security Strategy developed by the EU.

Internal Security Strategy carries a simple message on the shared threats and shared response. According to the Strategy security is one of the major priorities in conditions of technological advances and lack of internal borders. The aim is to cover all threats facing the lives and safety of citizens, including natural and man-made disasters.

What distinguishes the concept of an Internal Security Strategy from what has been in place since 1993 under the Maastricht and Amsterdam Treaties is that it moves way beyond the idea that justice and home affairs simply covers the policy areas of policing, immigration and asylum and judicial cooperation. The concept of internal security must be understood as a wide and comprehensive concept which straddles multiple sectors.

Prethodno saopštenje – UDK 343.85: 351.74/.75

SAVREMENI KONCEPT POLICIJSKOG RADA U ZAJEDNICI („COMMUNITY POLICING“) U FUNKCIJI SUZBIJANJA KRIMINALA

Mr Boban Simić, predavač
Kriminalističko-policijska akademija, Beograd (boban.simic@kpa.edu.rs)
Prof. dr Željko Nikač
Kriminalističko-policijska akademija, Beograd (zeljko.nikac@kpa.edu.rs)
Mr Marija Blagojević, naučni saradnik
Kriminalističko-policijska akademija, Beograd (marija.blagojevic@kpa.edu.rs)

Apstrakt: Politika preventivnog rada na bezbednosnom sektoru deo je sveukupne politike zemlje u borbi protiv kriminala. Praksa je pokazala da, ukoliko se društvena zajednica ne uključi u intenzivnu preventivnu borbu protiv kriminala, šanse za prevenciju od strane nadležnih službi jeu znatno manje. Iz tog razloga neophodno je da se u područjima koja beleže visoku stopu kriminala izgradi model lokalne zajednice koja će se ponašati kao snažan odbrambeni mehanizam. Ostvarenje tog cilja je od velikog značaja za prevenciju kriminala u društvu, a samim tim i na lokalnom području (sektoru). Jedan od veoma aktuelnih i instruktivnih modela rada policije na međunarodnom planu je koncept „community policing” (policija u zajednici), koji zaslužuje punu pažnju u smislu njegove implementacije i na naše uslove, naročito uz sve specifičnosti, kada su u pitanju svrsishodnost, opravdanost i očekivani efekti njegove primene kod nas.

Ključne reči: prevencija, kriminal, bezbebednosni sektor, „community policing”.

UVOD

Pod kriminalitetom se podrazumevaju sve protivpravne delatnosti za koje su propisane neke društvene sankcije. U savremenom društvu kriminalitet je opšta društvena pojava. Ona postoji danas u svim zemljama i svim društvenim zajednicama, bez obzira na njihovo društveno-ekonomsko uređenje i njihov politički sistem.

Osnovne karakteristike savremenog kriminaliteta jesu: *masovnost, stalni apsolutni i relativni porast, organizovanost, porast recidivizma i profesionalizma, međunarodni karakter i dr*. Činjenica da kriminalitet predstavlja veoma opasno društveno zlo uslovila je neophodnost da svako organizovano društvo na ovu pojavu reaguje na sasvim određen način. Kompleksnosti kriminaliteta mora se suprotstaviti kompleksnost državne i društvene prevencije i represije.

Bez obzira na činjenicu koliko je jedno društvo dobro organizovano, ono ne može uspešno da se suprotstavi kriminalitetu samo ukoliko je ta obaveza poverena isključivo za to specijalizovanim organima. U demokratskim društvima ne postoje stvarni razlozi za nesklad između interesa koji se nalaze u osnovi delovanja državnih organa i interesa građana, odnosno opštedruštvenih interesa. Zajednička

zainteresovanost državnih organa i građana da se suprotstavljaju kriminalitetu određuje mesto, položaj, zadatke i njihovu koordinaciju u suzbijanju i sprečavanju kriminaliteta.

Ulogu policije u celom sistemu treba posmatrati u svetlu toga da je suprotstavljanje kriminalitetu aktivnost koja zahteva određen stepen organizovanosti i stručnosti uz primenu određenih metoda i sredstava, koja građani i drugi subjekti društva ne poseduju, pa je samim tim i njihov doprinos u tom domenu moguć jedino uz saradnju sa policijom. Pod uticajem demokratskih procesa u pojedinim državama postoje tendencije da se građani samostalno organizuju u lokalnoj zajednici radi preventivnog delovanja. Za sada aktivnost javnosti, odnosno građana i njihovih udruženja nije dovoljna u sprečavanju i suzbijanju inkriminisanih ponašanja. S druge strane, organi unutrašnjih poslova se angažuju po službenoj dužnosti, i to kao specijalizovani državni organi uz nedovoljno učešće i podršku javnosti. Jedan od bitnih uslova preventivnog funkcionisanja organa unutrašnjih poslova jeste zakonski usklađeno postupanje tih organa sa aktivnošću drugih subjekata, pre svega građana. Svest građana o potrebi suprotstavljanja kriminalitetu postaje društvena potreba i opredeljenje u demokratskom društvu u kome građani mogu samoinicijativno i sopstvenim zalaganjem da doprinesu sprečavanju kriminaliteta. Demokratski procesi u društvu treba da omoguće građanima da aktivno učestvuju u procesu šireg društvenog suprotstavljanja kriminalitetu. Uslov je da se to učešće zasniva na pravnim i etičkim normama, kao i na pozitivnim stavovima i reakcijama javnog mnjenja koje imaju poseban značaj kada je u pitanju podrška nekom šire postanjem preventivnom programu ili akciji.

Od razvoja preventivnog delovanja policije u najvećoj meri zavisi i njena efikasnost u budućnosti.[1] Za pouzdano predviđanje i prevenciju potrebno je obezbediti koncentraciju informacija (podataka i saznanja) i njihovu obradu, distribuciju korisnicima i zaštitu na jednom mestu. To je celishodno sa gledišta policije u odnosu na druge organe u domenu dolaska do informacija.

Samo dobro organizovan preventivni rad policije omogućava planski osmišljeno, racionalno i efikasno izvršavanje preventivno-represivnih (mešovitih) zadataka policije. To dalje od policije zahteva da neprekidno bude pripravna i osposobljena za zaštitu brojnih pravnih dobara, a naročito za sprečavanje i suzbijanje krivičnih dela i prekršaja i preduzimanje mera radi progona njihovih izvršilaca.

PREVENTIVNO POSTUPANJE POLICIJE NA BEZBEDNOSNOM SEKTORU

Rad na bezbednosnom sektoru, kao osnovni način policijskog postupanja, uključuje, pored redovnog represivnog, i pojedine vidove preventivnog postupanja. Preventivna aktivnost policajaca se prvenstveno sastoji u sprečavanju povratnika da nastave sa kriminalnim ili prekršajnim ponašanjem. Među tim aktivnostima je i nadzor nad objektima i područjima na kojima se češće ispoljavaju kriminalne ili socijalnopatološke pojave i ponašanja. S ciljem preventivnog postupanja policije na sektoru, od velikog značaja je prikupljanje

[1] Šire: Krstić, O., (2007), Prevencija kriminaliteta, Fakultet za bezbednost i zaštitu, Banja Luka.

informacija o pojavama koje ukazuju na mogućnost narušavanja javnog reda i mira u većem obimu, ugrožavanja bezbednosti građana i njihove imovine, javnih dobara i slično. U preventivne aktivnosti u vezi sa narušavanjem javnog reda i mira spada i saradnja sa organizatorima javnih skupova, kao i aktivnosti koje se preduzimaju radi blagovremenog otkrivanja i sprečavanja delatnosti ili stanja koja ugrožavaju ličnu bezbednost određenih ličnosti, odnosno objekata, pogotovo onih od posebnog značaja. Tu spadaju i poslovi policijske pomoći, koji se pružaju državnim organima sa javnim ovlašćenjima u cilju sprovođenja njihovih izvršnih odluka. Pored ovih nosećih poslova na bezbednosnom sektoru i druge aktivnosti organa unutrašnjih poslova, kao što su bezbednost saobraćaja, izdavanje odobrenja za nabavku, držanje i nošenje oružja i drugi upravni poslovi imaju određene preventivne efekte.

Kriminalističko-preventivna delatnost, a samim tim i suzbijanje kriminala odvija se na području policijske stanice. Kao mikrorejon, područje policijske stanice ima svoje pozorničke i patrolne rejone. U zavisnosti od potreba, a uz poštovanje geografske celine, pozornički i patrolni rejoni mogu biti grupisani po sektorima. Sektori se formiraju, pre svega, radi jedinstvene koordinacije pri obavljanju pozorničke i patrolne delatnosti, odnosno preventivne delatnosti u celini. Cilj sektorskog rada jeste u angažovanju većeg broja policajaca u takvom mikropodručju u odnosu na ukupnu problematiku, a na principu međusobne saradnje i koordinacije.

Teritorija policijske stanice podeljena je na pozorničke rejone, koji ne moraju da budu teritorijalno podudarni sa administrativnim podelama. Pozornički rejon je epicentar kriminalističko-preventivne delatnosti i funkcionisanja organa unutrašnjih poslova u celini, posebno u urbanim sredinama. Realizacija kriminalističko-preventivne delatnosti pokazala se kao vrlo uspešna i na mikrorejonima (luke i pristaništa, sajmovi, železničke stanice, autobuske stanice, stanice metroa, magistralni putevi i raskrsnice, hoteli itd.), kao posebnim punktovima pozorničkog rejona. Tako je pozornički rejon postao simbol policijske organizacije i kriminalističko-preventivne delatnosti. Istovremeno, to je veza policije sa javnošću preko koje se reflektuje ne samo tehnička moć i oprema, nego i organizatorska funkcija policije (očuvanje javnog reda i mira, zaštita građana i njihove imovine od svih oblika kriminalne aktivnosti, saradnja sa stanovništvom), a samim tim i celokupna bezbednosna aktivnost.

Kriminalističko-preventivni poslovi na pozorničkom rejonu obično se dele na:

- opšte i
- posebne.

Obavljanje poslova i kriminalističko-preventivna delatnost u celini na pozorničkom rejonu je kontinuiran, neprekidan posao. Nema prevencije bez kontinuirane delatnosti, a takođe ni drugih poslova i zadataka vezanih za suzbijanje kriminala kao što su opservacija, legitimisanje i stalno prikupljanje obaveštenja o krivičnim delima i njihovim izvršiocima.

Posebnu grupu poslova čine mere i radnje koje se preduzimaju prema proceni bezbednosne situacije ili su oni pak nastali kao odraz konkretnih policijskih situacija.

Delatnost uniformisanih pripadnika policije u lokalnoj zajednici (sektoru), koja se uglavnom ogleda u vršenju pozorničke i patrolne službe, treba

uskladiti sa radom drugih službi organa unutrašnjih poslova, odnosno potrebno je obezbediti čvrstu akcionu povezanost tog dela policije sa drugim operativnim radnicima policije na sektoru. Ta saradnja podrazumeva jedinstveno delovanje sektorskih policajaca i operativnih linija, zajedničko organizovanje poslova i pojedinih operativnih akcija, stalno i blagovremeno međusobno obaveštavanje, povezivanje i saradnju prilikom preduzimanja pojedinih operativno-taktičkih mera i radnji. Naročito kada je reč o akcijama tipa racije, zasede i potere, te drugim akcijama u kojima se angažuje veći broj policajaca i više policijskih sredstava. Poseban vid saradnje na sektoru trebalo bi da bude između radnika policije koji deluju na sektoru, s jedne, i građana i drugih subjekata, s druge strane. U okviru pozorničke i patrolne delatnosti obavljaju se poslovi suzbijanja i sprečavanja kriminaliteta. To su:

- *poslovi koj se odnose na otkrivanje krivičnih dela i učinilaca,*
- *pronalaženje i hvatanje učinilaca krivičnih dela,*
- *pojačan nadzor i lokalna kontrola određenih kategorija delinkvenata, što ima isključivo preventivni značaj,*
- *prikupljanje svih obaveštenja koja imaju značaj za bezbednost i zaštitu lica i imovine.*

Pripadnici pozorničke i patrolne službe su u situaciji da, s obzirom na zadatke koje obavljaju, dolaze do saznanja kako o planiranim tako i o izvršenim krivičnim delima. Obavljanje te službe na sektoru pruža značajne mogućnosti za preduzimanje pojedinih preventivnih mera. Te mere rezultat su prethodnih saznanja ili ličnih zapažanja uniformisanih policajaca koja se odnose i na opasne pojave ili pretkrivična stanja koja prete da se pretvore u kriminalna ispoljavanja.

Uniformisani radnici policije bi, po pravilu, trebalo da uočavaju takve pojave i da se po njihovom predlogu preduzimaju preventivne mere u odnosu na određena lica čije je držanje kriminogeno, ranije osuđivana lica, uslovno otpuštena, te na nosioce određenih socijalno-patoloških pojava (alkoholičari, narkomani, kockari, skitnice, prostitutke i sl.). Radi prevencije se preduzimaju dnevni i noćni patrolni obilasci, zasede, racije, nadziru se ulice, trgovi, rečna i morska pristaništa, javni lokali i drugi objekti od značaja na sektoru. Te mere mogu imati i represivan cilj, kada se preduzimaju radi otkrivanja dela i učinioca, pri čemu se njihovim vršenjem, ako je uspešno, ostvaruju i značajni preventivni rezultati.

Kako su pozornička i patrolna delatnost među najfrekventnijim delatnostima koje vrše organi unutrašnjih poslova, to je značajniji organizacioni i funkcionalni okvir u kome se danas stvaraju uslovi za njihovo vršenje. One su sektorski način obavljanja poslova, što podrazumeva saradnju službe unutrašnjih poslova sa građanima, mesnim zajednicama, radnim organizacijama i drugim subjektima.

Takav način rada trebalo bi da doprinese boljem usmeravanju službe na aktivnost, potpunijem „*pokrivanju terena*" i racionalnijem korišćenju raspoloživih snaga, te boljoj orijentaciji na ostvarivanje preventivnog učinka prilikom vršenja pozorničke i patrolne delatnosti.

Sektorski način rada organa unutrašnjih poslova, koji je usko vezan za obavljanje pozorničke i patrolne delatnosti, treba da se zasniva na izučavanju ukupnog kriminogenog i opšteg stanja na području pojedinih mesnih zajednica, kao i prikupljanju, obradi i sređivanju podataka koji su od značaja za podelu područja na sektore. Pozornički i patrolni obilasci usmereni su na mesta gde se najčešće vrše

krivična dela i prekršaji, ili se ispoljavaju socijalno-patološke pojave, te u odnosu na lica prema kojima je preduzeta mera pojačanog nadzora, odnosno kriminalistička kontrola. Trebalo bi imati u vidu da je pozornik na sektoru obavezan da deluje preventivno u odnosu na jedan broj delikata čija je pojava objektivno uslovljena (na primer, mnogobrojna krivična dela i prekršaji u oblasti saobraćaja, koji su, po svojoj prirodi, najčešće i nehatni, ali po obimu i posledicama koje ostavljaju, veoma opasni).

Planiranje konkretnih zadataka na pozorničkom i patrolnom rejonu u zavisnosti je od veličine i gustine naseljenosti određenog područja, koncentracije imovinskih dobara na njemu, vršenja krivičnih dela i prekršaja, stepena njegove ugroženosti i izloženosti kriminalnom napadu, postojanja pojedinih područja i lokacija sa kriminogenim predispozicijama, gde su takvi rizici češći (autobuske i železničke stanice, sajmovi, pijace, noćni klubovi, kockarnice, i slično). Međutim, trebalo bi imati u vidu da se situacija, odnosno opasnosti kriminalnog ispoljavanja na određenom području menjaju, odnosno one se prenose sa onih mesta i rejona gde su prisustvo pozornika i patrola veći na manje kontrolisana područja. To znači da planiranje i intenziviranje pozorničke i patrolne službe u pogledu vremena, mesta i učestalosti, te opasnosti od kriminalnih pojava treba da bude u stalnom menjanju i prilagođavanju, bez obzira na to što postoje na duže vreme pozornički i patrolni rejoni na određenim područjima. Sve je izraženija potreba da se pozornička i patrolna delatnost brže menjaju i prilagođavaju savremenim zahtevima. Odnosno, danas se sve više teži tome da se uloga uniformisanih policajaca u pozorničkoj i patrolnoj delatnosti programski poboljša i dovede na nivo njihovog operativnijeg delovanja prema kriminalitetu i njegovim nosiocima.

Pored adekvatne stručne osposobljenosti, neophodno je da policajac na pozorničkom i patrolnom rejonu bude motivisan za preventivni rad, odnosno, neophodno je da za takav rad ima dovoljno profesionalnog i stručnog znanja i opredeljenja. To istovremeno od policajca pozornika, te operativnih radnika uopšte, zahteva vanredno poznavanje društvenih prilika, prilagođavanje društvenoj sredini, odnosno ostvarivanje pravilnog odnosa sa građanima i njihovim asocijacijama. Činjenica je da sve te zahteve teško može sam da ispuni uniformisani radnik koji je zadužen za svoj pozornički rejon, zbog čega su mu potrebni dodatna edukacija i usmeravanje.

Poželjno je i da pozorničku i patrolnu dužnost na istim pozorničkim i patrolnim rejonima duže obavljaju isti uniformisani radnici. To se opravdava potrebom da pozornici upoznaju prilike, ljude i objekte na određenom području, te da izgrade određeni odnos sa građanima. Policijska delatnost koju obavlja pozornička i patrolna služba danas nije funkcionalna ako se osloni samo na sadržinu tradicionalnog programa, jer prisustvo policajca na pozorničkom rejonu i efekti koje ostvaruje svojom pojavom na eventualne delinkvente nisu dovoljni da bi uspešno preventivno delovao kao što se to obično misli. Danas u eri profesionalizacije i specijalizacije kriminalaca i zloupotrebe naučnih i tehničkih dostignuća ne možemo se više oslanjati na pretpostavku da patrolna i pozornička služba izazivaju kolebanje kod kriminalaca koji nameravaju da izvrše krivično delo, čak i kada imaju utisak da su mesta krivičnog dela dobro „*pokrivena*”. Sa stanovišta kriminalističke preventive, veoma je važno da pozornik stekne ugled i poverenje građana u svom rejonu i onda kada deluje represivno. Zvaničan, suviše krut, pa i

agresivan način obavljanja pozorničke i patrolne delatnosti, inače karakterističan za klasičan i danas uveliko prevaziđen način obavljanja te službe, često otuđuje i udaljava uniformisanog radnika od građana, umanjuje njegovu operativnost i izoluje ga.

Takođe, odnos javnosti i policije sa stanovišta mogućih konfliktnih situacija ispoljava se najčešće u odnosima između pripadnika policije – uniformisanih radnika i građana. Ti konflikti u slučaju netaktičnog postupanja policajca, odnosno agresivnosti građana, u onim najekstremnijim slučajevima, završavaju se napadom na uniformisanog radnika ili upotrebom sredstava prinude, prema čemu je česta opasnost od ugrožavanja života, a neretko i slučajevi sa smrtnim ishodom na jednoj ili drugoj strani. Trebalo bi, naime, imati u vidu činjenicu da je u ličnosti građanina koji se sukobljava sa policajcem najčešće opasni kriminalac koji u tom sukobu ni sam ne želi kompromis. Opšta situacija doprinela je tome da je agresivnost kriminalaca veoma obimna i praćena nasiljem. Neretko te konfliktne situacije, koje su najčešće na ulici, pospešuju neobavešteni, pa i nedobronamerni građani, koji svojim ponašanjem stvaraju još veće tenzije, pa samim tim i žešća reagovanja na obe strane. Te pojave imaju suprotno dejstvo od preventivnog, veoma su kriminogene i štete ugledu policije.

Primerena i pravovremena informacija do koje policajac dolazi u pozorničkom i patrolnom rejonu osnovni je uslov za pravilno i blagovremeno suprotstavljanje kriminalitetu, bilo da se krivično delo nalazi u pripremnoj fazi ili su posledice već nastupile. Trebalo bi poći od realne pretpostavke da za gotovo svako krivično delo ili prekršaj javnog reda i mira koji su izvršeni ili koji se istražuju ima u pozorničkom i patrolnom rejonu, odnosno sektoru, dovoljno informacija da bi se delo rasvetlilo ili delikt predupredio. Što neposredniji kontakt građanin – policajac, zasnovan na uzajamnom poverenju, trebalo bi takođe da uključi što više pozornika u život i rad u mesnoj zajednici.

Uslov za uspešnu kriminalističkopreventivnu delatnost na pozorničkom rejonu svakako je poznavanje prilika i okolnosti. Poznavanje karakteristika mikrorejona u suštoj je suprotnosti sa čestim izmenama policajaca. Nažalost, ova činjenica u našoj praksi se previđa, pa je to jedan od razloga gubljenja kontinuiteta sa javnošću, što je u svakom slučaju velika manjkavost.

Planiranju preventivnih poslova na pozorničkom rejonu mora se pristupiti krajnje odgovorno, bez potcenjivanja pojedinih poslova i zadataka, uz stalno isticanje njihovog značaja kako bi postali sastavni deo rutinske delatnosti svakog policajca.

Opšti deo plana u skladu je sa bezbednosnim stanjem na samom pozorničkom rejonu, a prema trajanju može biti stalan, povremen i sezonski. U opštem delu plana neophodno je istaći zaštitne objekte od posebnog značaja, kao i načine njihove zaštite, preventivne mere u odnosu na pojedina krivična dela, način koordinacije sa patrolnom službom, osnovne subjekte kojima je neophodna elementarna zaštita, kontrolu recidivista, koordinaciju rada sa ostalim službama, posebno inspekcijsko-kontrolnog nadzora. Opšti deo plana obično se odnosi na stalne poslove vezane za godišnje planove kriminalističkopreventivne delatnosti na pozorničkom rejonu.

Poseban deo plana podrazumeva razradu konkretnih aktivnosti, mera i radnji na pozorničkom rejonu. Obično, vremenski gledano, reč je o tromesečnim

i mesečnim aktivnostima, zasnovanim na prethodnom iskustvu i bezbednosnom stanju pozorničkog rejona. To ne znači da poseban deo plana mora da se razlikuje od opšteg dela. Naprotiv, ovde se polazi od opšteg ka pojedinačnom. Neretko, poseban deo plana mora obuhvatiti i poslove u posebnim policijskim situacijama, kao što je na primer koordinacija sa jedinicama teritorijalne odbrane i civilne zaštite.

Neposredni izvršioci planiranih mera i radnji moraju biti upoznati sa zadacima koji im predstoje pri obavljanju kriminalističkopreventivne delatnosti na pozorničkom rejonu. Dominantan način upoznavanja u našoj praksi je grupno upoznavanje usmenim putem.[2] Pored ovog načina, postoji:

- *pojedinačno upoznavanje,*
- *upoznavanje kroz pisane forme i*
- *upoznavanje dostupnim sredstvima veze.*

Sasvim je logično da izvršilac nekog posla bude informisan o problematici koja ga očekuje. Bez toga nema ni povratne informacije o obavljenom poslu, obavezama izveštavanja o učinjenom i neučinjenom. Otuda upoznavanje sa predstojećim situacijama može biti: uopšteno i pojedinačno.

Uopšteno, odnosno kompleksno upoznavanje podrazumeva osnovne policijske situacije kao elementarna saznanja za pojedinačnu, individualnu razradu realizacije na pozorničkom rejonu.

Pojedinačno, odnosno konkretno upoznavanje čini osnov rangovanja policijskih situacija na terenu i iznalaženje najadekvatnijih rešenja za svaku policijsku situaciju konkretno. U zavisnosti od situacije, upoznavanje je moguće obaviti u policijskoj stanici i na pozorničkom rejonu.

Upoznavanje podrazumeva povratnu informaciju, a to je izveštavanje. Izveštavanje najčešće podrazumeva aktivnost policajca, preventivne mere i radnje koje je preduzimao, njegovo mišljenje u odnosu na primenjene metode sprečavanja i suzbijanja krivičnih dela i njihovih izvršilaca. Pravilo je da se izveštavanje obavlja posle završene službe. Međutim, ima i takvih policijskih situacija koje zahtevaju izveštavanje sa pozorničkog rejona, obično radio-vezom.

Obaveza policajca jeste da obavesti građane o stanju kriminaliteta i bezbednosnoj situaciji u sektoru i obratno. To će mu omogućiti da se informiše o ispoljavaju raznih socijalnopatoloških pojava i devijacija, te da stekne uvid u pojedina kriminogena stanja koja su pred neposrednim kriminalnim ispoljavanjem.

SARADNJA IZMEĐU POLICIJE I GRAĐANA NA BEZBEDNOSNOM SEKTORU

Savremena kriminalno-policijska praksa i moderna kriminologija upućuju na jednu važnu činjenicu. Borba protiv kriminala, naročito na preventivnom planu nema velikih šansi za uspeh ako se u tu borbu zajedno i ravnopravno sa policijom ne uključi lokalna društvena zajednica, tj. sami građani. Zato je u okviru velikog broja metoda i tehnika prevencije naglašen značaj organizovanog delovanja građana. Ako se preventivno delovanje na kriminal svede isključivo na tradicionalne metode

[2] Vidi: Bošković, M.,(2000), Organizovani kriminalitet, Policijska akademija, Beograd.

policije, koje se najčešće sastoje od brze intervencije na već ispoljeni kriminal, ne može se očekivati da se stopa kriminala bitno snizi. Za taj zadatak potreban je nov pristup – ***partnerstvo policije i zajednice.***[3]

Partnerstvo policije i lokalne zajednice danas predstavlja aktuelno stremljenje u prevenciji kriminaliteta u teoriji i praksi, a dosadašnji rezultati tih nastojanja idu u prilog činjenici da taj obrazac može postati dominantan model prevencije u XXI veku. Zato je neophodno da se tim pitanjima posveti posebna pažnja. Prema tome, ovde nije reč o nekoj posebnoj preventivnoj metodi ili tehnici, već se prvenstveno radi na organizacionom modelu koji bi garantovao veći uspeh od svih postojećih tehnika prevencije.[4]

Pod pojmom „*partnerstvo*" podrazumeva se ravnopravnost učesnika koji sarađuju. To znači da je neophodno da se prevaziđe odnos dominacije i podređenosti koji tradicionalno policiji daje superiornu ulogu, dok zajednica predstavlja dopunski deo. Naprotiv, partnerstvo podrazumeva jednako pravo na zalaganje i akciju kako policije tako i društvene zajednice. Sam pojam "zajednice" najpre se razume u smislu„lokalne zajednice", tj. socijalnog organizma koji izgrađuju stanovnici jednog gradskog, odnosno urbanizovanog područja, najčešće susedstva.[5]

Pretpostavke na kojima treba da se zasniva saradnja policije i zajednice jesu:

- ***šire definisanje policijskog delovanja,***
- ***preuređenje policijskih prioriteta,***
- ***obraćanje pažnje na pitanja kvaliteta života i socijalne dezorganizacije određenih gradskih područja – susedstva, promena modela odlučivanja u pravcu zajedničkog odlučivanja policije i zajednice,***
- ***smanjenje uticaja birokratskih mehanizama kojima je rad policije neretko definisan,***
- ***orijentacija na rešavanje problema i prevenciju, a ne na reakciju kada se desi incident,***
- ***priznavanje činjenice da lokalna zajednica igra ključnu ulogu u rešavanju problema susedstva,***
- ***reorganizacija policijskih službi kako bi se ohrabrili i nagradili novi modeli ponašanja policajaca.***

Prvi zadatak koji se mora ispuniti, a koji predstavlja pretpostavku uspešne saradnje između policije i zajednice, jeste ukidanje svih barijera u komunikaciji između partnera. Ovde se misli prvenstveno na psihološke, organizacione, funkcionalne i druge barijere koje postoje na obe strane. Policija u svom tradicionalnom ruhu, nema „naviku»da građanstvo vidi kao partnera u rešavanju određenih pitanja. Neophodno je prevazilaženje shvatanja da su jedino policijske službe stručno osposobljene i nadležne za pitanja kriminala, te se u tom smislu uloga lokalne zajednice vidi kao sekundarna. To je neophodno, jer takav stav

[3] Šire: Nikač, Ž. (2007), Policija u zajednici, KPA, Beograd.
[4] Šire: Riechers,L., Roberg.,R, Community Policing: A Critical Review of Underlying Assumtions, U: Willard M. Oliver, Community Policing, Clasical Readings
[5] Vidi: Cordner, G.W. (1995), "Community policing: elements and effects", *Police Forum*, Vol. 5 No. 3.

policije izaziva nepoverenje građana prema policiji, naročito u svetlu činjenice da delovanje policije na sprečavanje pojave kriminala i nije naročito uspešno. To znači da se model „*hladnih*» odnosa između lokalne zajednice i policije mora neutralisati da bi se ostvarila intenzivna saradnja – partnerstvo između ta dva učesnika.[6]

Policija mora da prihvati činjenicu da je sama lokalna zajednica mnogo bolje upućena u kriminal koji se dešava u njenoj sredini, i da se na njenu ulogu u sprečavanju kriminala mora ozbiljno računati. To je pravac koji vodi ka izgradnji mostova saradnje između lokalne zajednice i policije. U tom smislu policija mora da ostvari:

- ***zajednički rad policije i građana i identifikaciju lokalnih problema,***
- ***edukaciju građana o uzrocima kriminala i socijalnoj dezorganizaciji,***
- ***zajedničku izgradnju akcionog plana za preventivno delovanje,***
- ***zajednički rad u identifikaciji i mobilizaciji snaga neophodnih za preventivnu borbu protiv kriminala.***

Cilj tih mera jeste da lokalna zajednica postane samostalan i snažan organizam koji se uspešno brani od kriminala. To je ključni zadatak partnerstva. U takvoj situaciji se otvara mogućnost da policija svojim delovanjem reaguje u kritičnim situacijama, kada sama zajednica već obavi značajan deo preventivnog zadatka. Ostvarivanje tog modela neće biti uspešno sa onim lokalnim zajednicama koje u osnovi i nisu „zajednice”. tj. sa onim susedstvima gde ne postoje gotovo nikakve socijalne veze među pojedincima. Istraživanja pokazuju da je upravo u tim lokalnim okvirima stopa kriminaliteta najveća. Zato je u takvim situacijama najpreči zadatak policije da se izgradi sama lokalna zajednica. To se postiže jačanjem socijalnih veza među stanovnicima, a koriste se sva sredstva, uključujući i metod „*od vrata do vrata*”. Pripadnici jedne lokalne zajednice obaveštavaju se o svim problemima koji ih okružuju i pozivaju na zajedništvo. Time se stvara pretpostavka da jedno socijalno dezorganizovano područje dobije svoj socijalni oblik. Na taj način se stvaraju pretpostavke za preventivnu borbu protiv kriminala koju će voditi sami građani.

Oblici saradnje između policije i građana mogu biti različiti. Samo partnerstvo može da varira po veličini i tipu, ili pak po broju posrednih službi, etničkoj strukturi, broju članova, kriterijumu za članstvo, modelu odlučivanja, pristupima i orijentaciji na prevenciju. U osnovi, partnerstvo se uvek mora definisati u zavisnosti od specifičnosti lokalne zajednice u okviru koje se samo partnerstvo ostvaruje.

ZAKLJUČAK

Preventivno postupanje ne treba vezati samo za ovlašćenja iz zakona, jer se zakonska rešenja odnose uglavnom na represivne mere, dok se preventiva razrađuje minimalno i uopšteno. Upravo ta zakonska neutemeljenost može na neki način da demotiviše operativne radnike na njihovu primenu. Efekti preventivnog postupanja nisu neposredni i vidljivi kao kod represije.

---

[6] Vidi: Palmiotto,M,. Community Policing, A Policing Strategy for the 21 st Century, Maryland, 2000, str. 174–175.

Rezultati se, po pravilu, javljaju naknadno, s obzirom na to da ne postoji vremenska identičnost postupanja i pozitivnih preventivnih efekata. Ti rezultati su zato lošije vrednovani i obično se ne pripisuju konkretnom policijskom službeniku, jer je sa duže vremenske distance teško utvrditi njegov stvarni doprinos. Sve to dovodi do toga da sistem vrednovanja operativnog rada ide na štetu preventivnog rada, pa su rezultati represije jedino merilo rada.

Kočnicu u svakodnevnom samoinicijativnom angažovanju radnika organa unutrašnjih poslova u prevenciji, čine i dalje prisutni stavovi o organima unutrašnjih poslova kao represivnim organima čija aktivnost uvek treba da donosi neposredne rezultate.

Praksa je pokazala da, ukoliko se društvena zajednica ne uključi u intenzivnu preventivnu borbu protiv kriminala, šanse za prevenciju od strane nadležnih službi su znatno manje. Zato je neophodno da se u područjima koja beleže visoku stopu kriminaliteta izgradi model lokalne zajednice koja će se ponašati kao snažan odbrambeni mehanizam. Ostvarenje tog cilja je od velikog značaja po perspektivnu prevenciju kriminaliteta u društvu, a samim tim i na lokalnom području (sektoru). Jedan od veoma aktuelnih i instruktivnih modela rada policije na međunarodnom planu **community policing** koji zaslužuje punu pažnju u smislu njegove implementacije i na naše uslove, naročito uz sve specifičnosti kada su u pitanju svrsishodnost, opravdanost i očekivani efekti njegove primene kod nas. Po ovom modelu policija i građani ostvaruju dvosmernu i neposrednu komunikaciju, pri čemu se policija angažuje u rešavanju svih važnijih problema građana na lokalnom području, pre svega onih čije realizovanje ima i određene kriminalnopreventivne efekte.

Primenu pojedinih modela ***community policinga***, na naše prilike za sada prate samo načelne rasprave i stavovi, te određeni praktični pokušaji koji tek treba sebe da opravdaju. Njihova neposredna primena, međutim, nije nimalo jednostavna, jer ona zahteva kako izmene u okviru državnih organa, pre svega policije, tako i određene promene u društvu (zakonske, socijalne, promene običaja, moralnih stavova i sl.).

LITERATURA:

1. Aronowitz, A. (1998), *Crime Prevention: A Community Policing Approach in Netherlands*, The Hague.
2. Cordner, G.W. (1995), "Community policing: elements and effects", *Police Forum*, Vol. 5 No. 3, pp. 1-8.
3. Goldstein, H. (1979), "Improving policing: a problem-oriented approach", *Crime & Delinquency*,Vol. 25, pp. 236-258.
4. Goldstein, H. (1990), *Problem-Oriented Policing*, McGraw-Hill Publishing Company, New York, NY.
5. Kelling, G.L. and Stewart, J.K. (1989), "Neighbourhoods and police: the maintenance of civil authority", *Perspectives on Policing*, National Institute of Justice, Washington, DC.
6. Nikač, Ž. (2007), Policija u zajednici, KPA, Beograd.
7. Projekat „Teorijski i praktični aspekti implementacije policije u zajednici", autor:

Simonović B., MUP RS, VŠUP, IRJ, Beograd. 2005.
8. Riechers, L.M. and Roberg, R.R. (1990), “Community policing: a critical review of underlying assumptions”, *Journal of Police Science and Administration*, Vol. 17 No. 2, pp. 105-14.
9. Simonović, B. (2001), Uloga policije u prevenciji kriminala na nivou lokalne zajednice, Bezbednost, broj 1, Beograd.
10. „Strateški program razvoja policije u zajednici“, MUP RS, Direkcija policije, UP u sedištu, Bgd., 2007.god. Autori: UP/1 – Gačević G., Vasilijević A. i Milenić Ž.
11. Trojanovicz R., Bucqueroux B., Community policing,: How to Get Started, Anderson Publishing Company, Cincinati 1990.
12. Wilson J. & Kelling G. (1982), Broken Windows, Atlantic Monthly, 3, 29-38.
13. Wolfer, L., Baker,T. & Zezza, R. (1999), Problem Solving Policing Eliminating Hot Spots, FBI Law Enforcement Bulletin, 11, 9-14.

Summary: Policy of prevention work in the security sector is part of the overall policy of the country in the fight against crime. Commitment to oppose the crime prevention depends on the willingness of the community (society) to access and remove the root social causes of crime as opposed to traditional practice that conflicts with the consequence Although the social and criminal-political opposition to the need for crime prevention because of the high demands of a growing volume of crime and to that the most dangerous social, we are still far from a scientifically-designed concept of crime prevention in general social level, to be successful and functionally reflected in a narrow local area.

Practice has shown that if the community does not engage in an intensive preventive crime fighting chance for the prevention of the relevant services are considerably less. It is therefore necessary that the areas marked by high crime rate to build a model community that will act as a powerful defense mechanism. Achieving this goal is very important perspective on crime prevention in society and therefore the local area (sector). One of the most current and instructive model of policing to *community policing* international level that deserves full attention in terms of its implementation and to our particular requirements with all the specifics in terms of appropriateness, feasibility and expected effects of its application here. In this model the police and citizens exercise and two-way direct communication with the police are engaged in solving all major problems of citizens in the local area, especially those whose implementation has certain criminal and preventive effects.

Applications of this model here is not easy because it requires not only changes in the state organs, primarily the police, but also some changes in society. Today, with the right question is whether to continue with the main changes of the sectoral models that our law enforcement with varying success applied for thirty years, and applied some of the foreign models or a combination thereof.

Stručni rad - UDK 343.13: 340.237(497.7)

THE SPECIAL INVESTIGATIVE MEASURES IN THE NEW MACEDONIAN LAW ON CRIMINAL PROCEDURE

Katerina Krstevska PhD, Assistant Professor
Faculty of Security - Skopje, University "St. Kliment Ohridski" - Bitola
Idrizovo b.b., 1000 Skopje, Republic of Macedonia (work)
Ljupco Todorovski MA, Director
Bureau of Public Security, Ministry of Internal Affairs
Dimce Mircev b.b., 1000 Skopje, Republic of Macedonia (work)

Mobile phone: +389 (0)70 276 385
E-mail: katerina.krstevska@gmail.com

Abstract: Special investigative measures (SIM) entered the Macedonian criminal legislation in 2004 when the Law on Criminal Procedure (LCP) was changed and amended. This LCP's novella followed after the change of the Constitution in 2003, when the Amendment XIX replaced the Article 17. Namely, the Constitution guarantees the freedom and inviolability of the correspondence and other forms of communication, and stipulates that only a court decision, under conditions and in procedure prescribed by law, may authorize non-application of the principle of inviolability of correspondence and other forms of communication, if this in necessary for preventing or detecting criminal acts, for conducting a criminal procedure or if it is required in the interests of security and defense of the Republic.

By defining the purpose and types of the SIM, criminal acts for which SIM may be ordered, persons against whom SIM may be ordered, organs authorized for their ordering and implementing, their use as evidence in the criminal procedure, their duration etc., Macedonian legislator in the new LCP tried to encompass this sensitive area of human rights and fundamental freedoms, bearing in mind the European standards.

Key words: Special investigative measures; Law on Criminal Procedure; Republic of Macedonia

INTRODUCTION

The Amendment XIX to the Constitution of the Republic Macedonia,[1] raised the opportunity for changing and amending the Law on Criminal Procedure dated 1997 (LCP),[2] in the section dedicated to the conduction of the pre-trial procedure.

[1] See: Constitution of the Republic of Macedonia ("Official Gazette of the Republic of Macedonia" No. 52/1991), and its Amendments ("Official Gazette of the Republic of Macedonia" No. 01/1992, 31/1998, 91/2001, 84/2003, 107/2005, 03/2009, 13/2009, 49/2011).

[2] Law on Criminal Procedure ("Official Gazette of the Republic of Macedonia" No. 15/1997, 44/2002, 74/2004, 15/2005 - consolidated text, 83/2008, 67/2009, 51/2011).

It should be pointed out that the Assembly on November 17, 2010, adopted the new LCP ("Official

This Amendment, adopted by the Assembly on December 12, 2003, by replacing the Article 17 guarantees the freedom and inviolability of the correspondence and other forms of communication, and stipulates that only a court decision, under conditions and in procedure prescribed by law, may authorize non-application of the principle of inviolability of correspondence and other forms of communication, if this is necessary for preventing or detecting criminal acts, for conducting a criminal procedure or if it is required in the interests of security and defense of the Republic.[3]

Similar goal is defined in the Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR). By ratifying this Convention in 1997,[4] Republic of Macedonia undertook the obligation to fully abide the provisions that everyone has the right to respect for his/her private and family life, his/her home and his/her correspondence, and at the same time there shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.[5]

Ten months after the adoption of the Amendment XIX (October 14, 2004), the Assembly adopted the Law on Changing and Amending the LCP, by which for the first time in the Macedonian legal system a Special investigative measures (SIM) were prescribed.

INTRODUCING SPECIAL INVESTIGATIVE MEASURES IN THE MACEDONIAN LEGISLATION

One of the most commonly used explanations for the necessity to prescribe SIM, given by the Macedonian relevant authorities, is to respond to the new

---

Gazette of the Republic of Macedonia" No. 150/2010). According to the Article 568, this Law is enforced on the 8th day from the day of its announcement in the "Official Gazette of the Republic of Macedonia", and will begin to apply after expiration of 2 years from the date of its entry into force. However, the provisions concerning the execution of the electronic delivery will begin to apply after the expiry of 1 year from the date of its entry into force.

[3] Until the amendments in 2003, the Article 17 of the Constitution stated:
"The freedom and confidentiality of correspondence and other forms of communication is guaranteed. Only a court decision may authorize non-application of the principle of the inviolability of the confidentiality of correspondence, in cases where it is indispensable to conduct the criminal procedure or required in the interests of the defense of the Republic."

[4] See: Law on Ratification of the Convention for the Protection of Human Rights and Fundamental Freedoms and the First Protocol, Protocol No. 4, Protocol No. 6, Protocol No. 7 and Protocol No. 11 to the said Convention ("Official Gazette of the Republic of Macedonia" No. 11/1997); Protocol No. 12 ("Official Gazette of the Republic of Macedonia" No. 30/2004); Protocol No. 13 ("Official Gazette of the Republic of Macedonia" No. 30/2004); Protocol No. 14 ("Official Gazette of the Republic of Macedonia" No. 30/2005); Protocol No. 14 bis to the said Convention ("Official Gazette of the Republic of Macedonia" No. 41/2010).

[5] Analysis of the Article 8 of the ECHR, as well as numerous judgments of the European Court of Human Rights concerning this Article, see in: Kilkell, U. (2001). *The right to respect for private and family life - A guide to the implementation of Article 8 of the European Convention on Human Rights (Human rights handbooks, No. 1).* Strasbourg.

challenges in the fight against organized crime and its forms, by introducing a new procedural solutions,[6] particularly by introducing SIM.

In essence, the current LCP regarding the SIM has undergone three changes until 2011. The first changes and amendments were the ones mentioned above - in October 2004 in the scope of the pre-trial procedure beside "1. Criminal report and authorities of the organs in the pre-trial procedure", a new title was added "2. Special investigative measures" and five new Articles 142-b, 142-c, 142-d, 142-e and 142-f. The second changes and amendments were in July 2008 when the Article 142-b was changed, and the third changes were in April 2011 when the Articles 142-b and 142-d were changed. It emerges that for the SIM, the following years are significant:

- 2003 - when the Amendment XIX to the Constitution was adopted,
- 2004 - when SIM were introduced in LCP,
- 2008 - when SIM's provisions were changed regarding the type of the criminal acts and under which criteria SIM may be ordered,
- 2011 - when the provisions concerning the 3rd measure were specified.[7]

Also, it should be pointed out that the new LCP dated 2010 dedicates to the SIM Articles 252 to 271 of the Chapter XIX, under the Section D "Procedural measures and actions for securing persons and evidence" (together with Chapter XVI "Measures for securing the presence of persons and uninterrupted conduction of the criminal procedure", Chapter XVII "Measures for finding and securing persons and objects" and Chapter XVIII "Means of evidence").

PURPOSE AND TYPES OF SPECIAL INVESTIGATIVE MEASURES IN THE NEW LAW ON CRIMINAL PROCEDURE

The new LCP in Article 252 defines the ***purpose*** that should be achieved by using SIM, i.e. when it is likely to provide data and evidence necessary for successful conduction of the criminal procedure, which otherwise cannot be obtained. If these conditions are fulfilled, then the following ***types*** of measures may be undertaken:

---

[6] See: Government of the Republic of Macedonia: *Draft-Law on Changing the Law on Criminal Procedure* (submitted to the Assembly in March, 2011). p. 3.
Similar explanation was given in 2004, see: Government of the Republic of Macedonia: *Draft-Law on Changing and Amending the Law on Criminal Procedure* (submitted to the Assembly in February, 2004). p. 1-13. Namely, SIM's prescription determines a clear and precise legal framework and adequate procedural safeguards against their abuse, which complies with the European requirements for incorporating a modern investigative measures in the area of criminal justice and human rights, and in order to obtain data and evidence necessary for conducting the criminal procedure and facilitating the prosecution of the perpetrators of criminal acts, especially the acts of organized crime, corruption, money laundering, illegal trafficking of human beings, arms and drugs and other serious forms of crime.
However: Матовски, Н., & Лажетиќ - Бужаровска, Г., & Калајџиев, Г. (2011*). Казнено процесно право - второ изменето и дополнето издание.* Скопје. p. 268, note that although SIM are promoted in the public as strictly targeted towards the most serious threats of organized crime, terrorism etc., an opportunity is created for SIM widely to be used.

[7] Analysis of the SIM in the current LCP, see in: Матовски, Н. (2005). *Новелата на Законот за кривичната постапка на Република Македонија од 2004 година.* Скопје. p. 24-28.

1) Monitoring and recording of the telephone and other electronic communications within a procedure stipulated in a separate law;[8]
2) Monitoring and recording in home, closed or fenced space that belongs to that home or commercial space marked as private or in a vehicle and entrance to those premises in order to create conditions for monitoring of communications;[9]
3) Secret monitoring and recording of persons and objects with technical devices outside the home or commercial space marked as private;[10]
4) Secret insight and search of computer system;[11]
5) Automatic or other way of searching and comparing personal data;[12]

---

[8] The Assembly in 2006 adopted a special law that regulates this subject - Law on Monitoring Communications ("Official Gazette of the Republic of Macedonia" No. 121/2006, 110/2008, 4/2009 - consolidated text).

[9] Both measures from Article 252 paragraph 1 items 1 and 2 of the new LCP represent one measure in the current LCP (Article 142-b paragraph 1 item 1 - Monitoring of communications and entrance in home and other premises or in means of transport in order to create conditions for monitoring of communications, under conditions and procedure prescribed by law).
The new LCP (Article 268) restricts the use of the 2nd measure - it may only be directed towards the suspect and may be implemented only at the suspect's home. But, it shall be allowed in the homes of others, only if it is based on a reasonable doubt that the suspect resides there. If during the recording there are indications that statements will be intercepted, which belong to the basic sphere of private and family life, then the recording will be stopped, and the documentation on such statements will be destroyed immediately.

[10] In essence, this measure in the current LCP has undergone one change. Thus, in 2004 was named as "Secret surveillance, monitoring and visual-audio recording of persons and objects with technical devices", and in 2011 was changed into "Secret surveillance, monitoring and recording of persons and objects with technical devices, outside of home and other premises".
According to: Ruskovska, V., & Ilievski, J., & Heras, D. L. M. (2010). *Special Investigative Measures - Domestic and International Practice.* Skopje. p. 29, a major problem is the question whether the recording must be both visual and audio or can it be only visual or only audio recording? It must be emphasized that in the time period when the application of SIM began, MOI had pretty much outdated equipment at its disposal. In many cases, if there was a picture there was no sound or vice versa. The defense would use this as an argument during the closing statements or in the appeal procedure. Acting upon a Request for an extraordinary review of a final judgment, the Supreme Court took a stand in regard to those claims of the defense that "this investigative measure is not directed towards providing a mandatory simultaneous audio and visual recording, but it is permitted to conduct separate visual, or audio recording, depending on the circumstances of the specific case". Even more so, since it is not always possible to carry out a synchronized audio and video recording and in certain cases this is not even needed having in mind the type of evidence that needs to be obtained, i.e. the nature of the fact that needs to be verified on the basis of the obtained evidence.
In order to eliminate all dilemmas what is meant under "recording", the new LCP in Article 21 defines "the recording shall mean visual-audio or visual or audio recording".

[11] This measure in the current LCP has longer term - "Insight and searching in computer system, seizure of computer system or part of it or the base for storing computer data".

[12] The 5th measure of the new LCP is defined in Article 265, and it includes an automatic or other way of searching and comparing collections of personal data of persons and other data which are directly related to them and their comparison with certain characteristics of the person for whom there is a reasonable assumption that is connected to the criminal act, in order to exclude the persons who are not suspected or to identify the persons who possess characteristics that are required for the investigation. This entails an obligation for the legal entities and natural persons that process personal data, to allow an uninterrupted enforcement of the order for the application of the measure, by making the required personal data available and by submitting them to the competent authorities.
All personal data collected by using this measure must be deleted or destroyed if the criminal procedure has

6) Insight in realized telephone or other electronic communications;[13]
7) Simulated purchase of objects;
8) Simulated giving and receiving a bribe;[14]
9) Controlled delivery and transport of persons and objects;[15]
10) Use of undercover agents for monitoring and collecting information or data;[16]
11) Opening simulated bank account,[17] and
12) Simulated registration of legal entities or using existing legal entities for data collection.[18]

It is important that in a case when there is no information available about the identity of the perpetrator of the criminal act, the above mentioned SIM may be also ordered towards the object of the criminal act.[19] In addition, the new LCP stipulates an obligation to the persons to keep as an official secret the data that they have somehow found out, that are related or have resulted by the SIM's application (Article 264).

---

not been initiated within 15 months after the completion of the measure. The deletion or destruction of the personal data is performed under the supervision of the Judge of the pre-trial procedure, Public Prosecutor and Representative of the Directorate for Personal Data Protection, after which the Public Prosecutor shall prepare a minutes.

[13] The 6th measure, as well as the 5th measure, is new SIM, i.e. the current LCP does not prescribe them.

[14] The 4th measure of the current LCP "Apparent (simulated) purchase of objects, as well as apparent (simulated) giving a bribe and apparent (simulated) receiving a bribe", in the new LCP is divided in two separate measures "Simulated purchase of objects" and "Simulated giving and receiving a bribe".

[15] This measure remains the same, with a note that in the new LCP is 9th measure, and in the current LCP is 5th measure.

[16] This measure remains the same, with a note that in the new LCP is 10th measure, and in the current LCP is 6th measure.

Namely, officials of the Judicial Police may be engaged as undercover agents. In exceptional cases, other persons may also be engaged, who with the Public Prosecutor's approval conduct an investigation under a hidden or changed identity. For the needs of the investigators with the hidden identity, a personal and other documents and paperwork may be prepared, changed and used, and the competent state organs and other legal entities are obliged to enable the preparation of these documents, while their employees are obliged to keep all data and information regarding the preparation of these documents as classified information. In this way, the persons shall have the right with their changed identity to participate in the legal circulation.

What is meant under the Judicial Police is defined in Article 21 of the new LCP - "Judicial Police are the police officers of the Ministry of Internal Affairs (MOI) and the members of the Financial Police (FP) and by the law authorized persons of the Customs Administration (CA) working on detection of criminal acts", i.e. the duties of the Judicial Police are performed by: police officers in the organizational units within MOI, FP and CA, which according to their legally prescribed scope of work, undertake measures and activities for detection of criminal acts, capturing and reporting of the perpetrators, securing the evidence for the criminal acts and other measures that provide an uninterrupted conduction of criminal procedure; members of the Judicial Police at the Investigative Centres of the Public Prosecution Office (PPO) and the officials assigned to the Public Prosecutor pursuant to Article 50.

[17] The term of the 7th measure in the current LCP "Opening apparent (simulated) bank account, where founds that originate from committed criminal act can be deposited", in the new LCP is shortened to "Opening a simulated bank account".

[18] The 12th measure in the new LCP is 8th measure in the current LCP, named as "Registration of apparent (simulated) legal entities or usage of the existing legal entities for data collection".

[19] The same provision is prescribed in the current LCP. See: Article 142-b paragraph 3 of the current LCP.

The new LCP distinguishes ***three categories of criminal acts*** for which SIM may be ordered (Article 253),[20] i.e. when there are grounds for suspicion for the following criminal acts:

- *First* category - criminal acts for which at least 4 years of imprisonment is prescribed, which have been prepared, are being committed or have been committed by organized group, gang or other criminal association, or
- *Second* category - strictly listed criminal acts from the Criminal Code (CC),[21] or
- *Third* category - criminal acts against the State (Chapter XXVIII), criminal acts against the humanity and the international law (Chapter XXXIV) of the CC.

Encouraging and *assisting* SIM is specifically regulated in the new LCP. Hence, according to the Article 254 by undertaking SIM, committing a criminal act must not be encouraged, and at the same time against the person who undertakes SIM, a criminal prosecution shall not be initiated for the actions that represent assistance to a criminal act, that have been performed in order to secure data and evidence for successful conduction of the criminal procedure.[22]

---

[20] Compare to: Article 142-b paragraphs 1 and 2 of the current LCP.

[21] It refers to the following criminal acts of the CC: Murder (Article 123); Kidnapping (Article 141); Mediation in prostitution (Article 191 paragraphs 1, 3 and 4); Showing pornographic materials to a minor (Article 193); Production and distribution of child pornography (Article 193-a); Luring to an intercourse or other sexual act of a minor who has not turned 14 years of age (Article 193-b); Unauthorized production and release for trade of narcotic drugs, psychotropic substances and precursors (Article 215 paragraphs 1 and 3); Damage and unauthorized intrusion into a computer system (Article 251 paragraphs 4 and 6); Extortion (Article 258); Blackmail (Article 259 paragraph 2); Appropriation of goods under temporary protection or cultural heritage or natural rarities (Article 265); Taking out i.e. exporting abroad of goods under temporary protection or cultural heritage or natural rarities (Article 266 paragraph 1); Alienation of cultural heritage of particular importance that is in a state ownership (Article 266-a); Money laundering and other criminal proceeds (Article 273 paragraphs 1, 2 and 3 and paragraphs 5, 6, 8 and 12); Smuggling (Article 278 paragraphs 3 and 5); Customs fraud (Article 278-a); Misuse of official position and authority (Article 353); Embezzlement in the service (Article 354); Fraud in the service (Article 355); Making personal use in the service (Article 356); Receiving a bribe (Article 357 paragraphs 1, 4, 5 and 6); Giving a bribe (Article 358 paragraphs 1 and 4); Unlawful mediation (Article 359 paragraph 6); Unlawful influence on witnesses (Article 368-a paragraph 3); Criminal association (Article 394 paragraph 3); Terrorist organization (Article 394-a paragraphs 1, 2 and 3); Terrorism (Article 394-b) and Financing terrorism (Article 394-c).
It should be stressed that the CC since the adoption of the new LCP (2010) has undergone four changes and amendments ("Official Gazette of the Republic of Macedonia" No. 37/1996, 80/1999, 04/2002, 43/2003, 19/2004, 81/2005, 60/2006, 73/2006, 07/2008, 139/2008, 114/2009, 51/2011 - two changes and amendments, 135/2011, 185/2011), because of which some of the titles of the above mentioned criminal acts have been changed; a new provisions have been added in the current criminal acts and this entails re-numeration of other paragraphs; new criminal acts have been prescribed that should be covered by SIM etc. All of this implies the necessity for correction of the new LCP.
The comparison of the new LCP's Article 253 paragraph 2 and the current LCP's Article 142-b paragraph 2 shows that the new LCP expands the scope of criminal acts to which SIM may be applied from 17 to 28. Otherwise, the initial text of the Article 142-b of the current LCP in 2008 was amended with a new provision i.e. paragraph 2 which entered the strictly listed criminal acts to which SIM may be applied, with a condition - in order to secure data and evidence for successful conduction of the criminal procedure, which otherwise cannot be obtained or their provision may lead to a greater difficulties.

[22] The current LCP also has provisions with the same content, with a note that the Article 142-b paragraph 4 (encouraging) and 5 (assisting), does not refer to all SIM, but only to the measures of the items 4, 6, 7 and 8.

Although SIM are in the scope of the Section D "Procedural measures and actions for securing persons and evidence", the new LCP in Article 259 highlights that the data, reports, documents, and objects obtained by using these measures, under conditions and in a manner stipulated by the Law itself, may be used as evidence in the criminal procedure.[23] However, the statements obtained by using SIM from the persons who are relived from the duty to testify are excluded, i.e. they cannot be used as evidence. On the other hand, if the undercover agents were used for monitoring and collecting information or data (10th measure), then they may be examined as protected witnesses under the conditions determined in Articles 226 to 232 of the new LCP, with a note that their identity is an official secret.[24]

ORDERING AND IMPLEMENTING SPECIAL INVESTIGATIVE MEASURES ACCORDING TO THE NEW LAW ON CRIMINAL PROCEDURE

According to the new LCP, the ***written order*** for implementing SIM may be issued by:

- Judge of the pre-trial procedure - for the measures from the Article 252 paragraph 1 items 1, 2, 3, 4 and 5 upon an elaborated request of the Public Prosecutor, and
- Public Prosecutor - for the measures from the Article 252 paragraph 1 items 6, 7, 8, 9, 10, 11 and 12.[25]

---

[23] The current LCP has provision with a similar content. Thus: Article 142-c paragraph 1 of the current LCP.
If during the implementation of the SIM, it is not acted in accordance with the provisions of the new LCP, then the court decision may not be based on the obtained data. Thus: Article 259 paragraph 5 of the new LCP. Compare to: Article 142-e paragraph 4 of the current LCP.

[24] The current LCP has provisions with a similar content. Thus: Article 142-c paragraph 2 and 3 of the current LCP.
In order to protect the life, physical integrity or freedom of the investigators with a hidden identity, as well as of those closely related to them, their identity shall remain a secret even after the completion of the procedure. Thus: Article 270 of the new LCP.
The new LCP does not contain a provision as the current LCP (Article 142-e paragraph 5), according to which the PPO and the Investigative Judge in appropriate manner, with a copy of the records without personal data, will prevent the unauthorized persons, as well as the suspect and his/her attorney to establish the identity of the persons who have undertaken SIM.

[25] Compare to: Article 142-d of the current LCP. Thus, if it is a pre-trial procedure, then the SIM will be determined by order issued by the Public Prosecutor or Investigative Judge, and if it is an investigation then only by order issued by the Investigative Judge.
The Investigative Judge in the pre-investigative procedure decides with a written elaborated order for implementation of SIM from Article 142-b paragraph 1 items 2 to 8 of the current LCP, and the proposal given by the Public Prosecutor, should also be elaborated and in writing. If disagreements arise between the Public Prosecutor and the Investigative Judge, then the Council from Article 22 paragraph 6 of the current LCP shall decide.
When the Public Prosecutor decides about the implementation of SIM in the pre-investigative procedure, once again the order should be in writing and should be elaborated, but the proposal shall be given by MOI. This situation refers to SIM from the Article 142-b paragraph 1 items 4 to 8, with an additional condition - there should be no information available about the identity of the perpetrator of the criminal act.

This order may *refer to a person*, who: first - has committed a criminal act under Article 253, second - undertakes an action for committing a criminal act under Article 253, or third - is preparing to commit a criminal act under Article 253 when such preparation is punishable according to the CC's provisions. Furthermore, the order may also refer to a person who receives or forwards consignments from the suspect or if the suspect uses his/her communication device.[26]

The order, which may refer to one or more SIM, must contain the following *elements*: a. legal term of the criminal act; b. person or objects upon which the measures will be implemented; c. technical devices that are going to be used; d. scope and location of the implementation of the measures; d. information and evidence on which the grounds for suspicion are based and explanation of the reasons due to which the data and the evidence cannot be obtained otherwise; f. organ that has to implement the order; and f. duration of the measure. If it is about the 1st and the 2nd measure (Article 252 paragraph 1 items 1 and 2), then the order for monitoring and recording of the communications should also include the type of the telecommunication system, the telephone number or other data to identify the telecommunication plug.[27]

Since the Judge of the pre-trial procedure and the Public Prosecutor are organs authorized for ordering SIM, authorized organs for SIM's ***implementation*** are the Public Prosecutor or the Judicial Police under his/her control.[28] If the Judicial Police implements the measure, then it must prepare two types of *reports* that are going to be submitted to the Public Prosecutor. In the first case - during the SIM's implementation, the report will be prepared upon the request of the Public Prosecutor, and in the second case - after the SIM's implementation, a separate report will be prepared containing: time of commencement and completion of the measure; number and identity of the persons encompassed by the measure and brief description of the course and the results of the implementation of the measure. As an annex to the separate report, the complete documentation of the technical recording will be submitted, which afterwards the Public Prosecutor will forward it to the Judge of the pre-trial procedure.[29]

It is important to indicate that the order may also be ***extended*** to another criminal act. Thus, if during the SIM's implementation, data is received about a criminal act that is not included in the order, then the measure will be prolonged only in case of a criminal act under Article 253 and the data collected in this regard may be used as evidence in the criminal procedure.

Furthermore, the new LCP imposes an obligation to the Public Prosecutor of the Republic of Macedonia once a year to submit a *report to the Assembly* about the

---

[26] If during the implementation of the measure, communications of persons who are not subject of the order are monitored and recorded, the Public Prosecutor is obliged to set them aside and to inform the Judge of the pre-trial procedure. Upon the proposal of the Public Prosecutor, the Judge of the pre-trial procedure may order from the overall documentation on the implementation of the measure, only the parts that are related to the criminal act for which the order was issued to be set aside. Thus: Article 255 paragraph 3 of the new LCP.

[27] The elements of the order for SIM's implementation are more preciously defined in the new LCP, compared to the current LCP (Article 142-e paragraph 2: a. data regarding the person against whom the SIM are applied when the perpetrator is known; b. grounds for suspicion for the committed criminal act; c. facts from which SIM's implementation derives; d. manner, scope and duration of the SIM).

[28] The order, according to the current LCP, is implemented by MOI, CA and FP (Article 142-e paragraph 1).

[29] Compare to: Article 142-f of the current LCP.

SIM that are requested in the previous calendar year, in which it will specify: number of the procedures in which SIM are ordered according to the Article 252; criminal acts that served as a ground according to the division set in the Article 253; whether the procedure is connected with a prosecution of organized crime; number of monitored objects and number of monitored persons for each procedure per accused and non-accused persons; SIM's duration; whether the monitoring produced a results that are relevant to the procedure or there is a probability that they might be relevant to the procedure; if the monitoring did not produced a relevant results, the reasons thereof shall have to be differentiated, due to technical reasons and other reasons; and costs arising from SIM's implementation.

DURATION AND TERMINATION OF SPECIAL INVESTIGATIVE MEASURES ACCORDING TO THE NEW LAW ON CRIMINAL PROCEDURE

The SIM may ***last*** no longer than 4 months upon the Article 260 paragraph 1 of the new LCP. However, there are possibilities their duration to be prolonged. Hence, the basic 4 months may be prolonged for:

- Another 4 months (4+4, or total 8 months) - if it refers to the measures under the Article 252 paragraph 1 items 1, 2, 3 and 4. This extension will be approved by the Judge of the pre-trial procedure, upon an elaborated written request of the Public Prosecutor,
- Another 6 months (4+4+6, or total 14 months) - if it refers to the measures under the Article 252 paragraph 1 items 1, 2, 3 and 4, with an additional condition - criminal acts for which at least 4 years of imprisonment is prescribed, for which there is a reasonable doubt that they have been committed by an organized group, gang or other criminal association. Also in this case, the deadline will be prolonged by the Judge of the pre-trial procedure, upon an elaborated written request of the Public Prosecutor, based on the assessment of the usefulness of the data obtained by the implementation of the measure and with reasonable expectation that the measure may continue to result with data of interest to the procedure,
- Until the purpose, for which the measure was determined, is accomplished, that is, until the completion of the investigation at the latest - if it refers to the measures of the Article 252 paragraph 1 items 9, 10, 11 and 12.[30]

[30] The Article 301 of the new LCP determines when the investigative procedure completes. Thus, the first case is when the Public Prosecutor estimates that the situation has been sufficiently clarified to file an indictment or to terminate the investigative procedure.
The investigative procedure should be completed within 6 months starting from the day of the issuance of the order for its conduction. However, if it is not completed within this deadline, then the Public Prosecutor is obliged to inform the higher Public Prosecutor thereof, who in complex cases may extend this deadline for another 6 months (6+6, or total 12 months). The deadline of 12 months may be extended for another 3 months (6+6+3, or total 15 months), and if it is a case of acts of organized crime, then the deadline of 15 months may be extended for another 6 months (6+6+3+6, or total 21 months). In the last two cases (15 and 21 months), the deadline is extended by the Public Prosecutor of the Republic of Macedonia.

If the Judge of the pre-trial procedure does not approve the extension of the duration of the measure, the Public Prosecutor has a right to appeal to the Court Council from the Article 25 paragraph 5, that shall rule within 24 hours.

The organ, that issued or extended the order for SIM's implementation, is obliged immediately to order ***termination*** of the measures, as soon as the objectives for which they have been determined are accomplished, or the reasons due to which they have been approved cease to exist. If the Public Prosecutor abandons the criminal prosecution or if the collected information by the SIM is not significant for the conduction of the procedure, they will be destroyed under the supervision of the Judge, for which the Public Prosecutor will prepare minutes.[31]

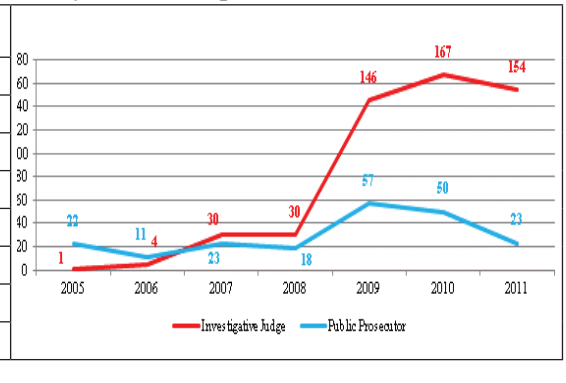
SPECIAL INVESTIGATIVE MEASURES IN THE PERIOD 2005 TO 2011

As to the SIM's implementation so far, or implementation based on the current LCP (2005 to 2011), according to the data available to MOI, it can be noted that SIM were applied under 532 orders issued by the Investigative Judge and 204 orders issued by the Public Prosecutor.

An average of 105 orders was issued per year, out of which 76 orders were issued by the Investigative Judge, and 29 orders by the Public Prosecutor. Seen from the graphic presentation, the issuance of the orders has an increasing trend until 2010 when 217 orders were issued, and in 2011 this number drops to 177 orders. Further, the Investigative Judge issued most of the orders in 2010 (167), while the Public Prosecutor issued most of the orders in 2009 (57).

Organ that issued orders for SIM's implementation

Year	Investigative Judge	Public Prosecutor	Total
2005	**1**	**22**	23
2006	**4**	**11**	15
2007	**30**	**23**	53
2008	**30**	**18**	48
2009	**146**	**57**	203
2010	**167**	**50**	217
2011	**154**	**23**	177
Total	532	204	736



SIM, under the current LCP, last much shorter. Hence, SIM of the Article 142-b paragraph 1 items 2 to 8 may last up to 4 months, with a possibility for extention for another 3 months at the most (4+3, or total 7 months), if there are justified reasons and upon a proposal of the Public Prosecutor when the order is issued by the Investigative Judge, or upon a proposal of MOI, when the order is issued by the Public Prosecutor. The Council from the Article 22 paragraph 6 shall decide if there is a disagreement between the Public Prosecutor and the Investigative Judge.

[31] The new LCP prescribes a possibility for notification of the concerned person about SIM's termination. This is done upon his/her request, after which the Public Prosecutor will submit the written order to him/her if that is not harmful to the procedure. The person may also refer this request to the Court.

If in the first two years of SIM's implementation, the Public Prosecutor was the one who dominated in the issuance of the orders, the situation is changing in the following years. Thus, in 2005 and 2006 he/she participated with a high 96% and 73%, the participation in the total number of issued orders in the coming years is consistently reduced to only 13% (43% in 2007; 38% in 2008; 28% in 2009; 23% in 2010; 13% in 2011).

CONCLUSION

Given that the SIM's implementation enters an especially sensitive sphere of human rights and freedoms, their usage should be restricted only to the conditions prescribed by law, i.e. when it is likely to provide data and evidence necessary for successful conduction of the criminal procedure, which otherwise cannot be obtained. This implies that all efforts must be made in order the data and the evidence to be ensured through other "less sensitive" procedural measures and actions, and the usage of SIM to be the ultimate tool for fighting a crime. Concerning the Table's data, a positive note can be made that the number of the issued orders for SIM's implementation is in decline, which implies that the relevant authorities are trying to comply with these remarks.

All of this is closely related to the consistent respect of the Article 8 of the ECHR, that guarantees the right to respect for private and family life, and Article 17 of the Macedonian Constitution, i.e. the SIM should not to be only prescribed by law, but they must be implemented under the law; there should be no "less sensitive" measure to achieve the same purpose; they should be applied towards serious criminal acts; as well as to be limited by time and to fall under a judicial control.

REFERENCES

1. Constitution of the Republic of Macedonia ("Official Gazette of the Republic of Macedonia" No. 52/1991), and its Amendments ("Official Gazette of the Republic of Macedonia" No. 01/1992, 31/1998, 91/2001, 84/2003, 107/2005, 03/2009, 13/2009, 49/2011).
2. Criminal Code ("Official Gazette of the Republic of Macedonia" No. 37/1996, 80/1999, 04/2002, 43/2003, 19/2004, 81/2005, 60/2006, 73/2006, 07/2008, 139/2008, 114/2009, 51/2011 - two changes and amendments, 135/2011, 185/2011).
3. Government of the Republic of Macedonia: *Draft-Law on Changing the Law on Criminal Procedure* (submitted to the Assembly in March, 2011).
4. Government of the Republic of Macedonia: *Draft-Law on Changing and Amending the Law on Criminal Procedure* (submitted to the Assembly in February, 2004).
5. Kilkell, U. (2001). *The right to respect for private and family life - A guide to the implementation of Article 8 of the European Convention on Human Rights (Human rights handbooks, No. 1)*. Strasbourg.

6. Law on Criminal Procedure ("Official Gazette of the Republic of Macedonia" No. 150/2010) - new LCP.
7. Law on Criminal Procedure ("Official Gazette of the Republic of Macedonia" No. 15/1997, 44/2002, 74/2004, 15/2005 - consolidated text, 83/2008, 67/2009, 51/2011) - current LCP.
8. Law on Monitoring Communications ("Official Gazette of the Republic of Macedonia" No. 121/2006, 110/2008, 4/2009 - consolidated text).
9. Law on Ratification of the Convention for the Protection of Human Rights and Fundamental Freedoms and the First Protocol, Protocol No. 4, Protocol No. 6, Protocol No. 7 and Protocol No. 11 to the said Convention ("Official Gazette of the Republic of Macedonia" No. 11/1997); Protocol No. 12 ("Official Gazette of the Republic of Macedonia" No. 30/2004); Protocol No. 13 ("Official Gazette of the Republic of Macedonia" No. 30/2004); Protocol No. 14 ("Official Gazette of the Republic of Macedonia" No. 30/2005); Protocol No. 14 bis to the said Convention ("Official Gazette of the Republic of Macedonia" No. 41/2010).
10. Матовски, Н., & Лажетиќ - Бужаровска, Г., & Калајџиев, Г. (2011*). Казнено процесно право - второ изменето и дополнето издание.* Скопје.
11. Матовски, Н. (2005). *Новелата на Законот за кривичната постапка на Република Македонија од 2004 година.* Скопје.
12. Ruskovska, V., & Ilievski, J., & Heras, D. L. M. (2010). *Special Investigative Measures - Domestic and International Practice.* Skopje.

SUMMARY

Ten months after the adoption of the Amendment XIX of the Macedonian Constitution (October 14, 2004), the Assembly adopted the Law on Changing and Amending the Law on Criminal Procedure (LCP), by which for the first time in the Macedonian legal system a Special investigative measures (SIM) were prescribed. It emerges that several years are significant for this measures: 2003 (Amendment XIX to the Constitution was adopted); 2004 (SIM were introduced in LCP); 2008 (SIM's provisions were changed regarding the type of the criminal acts and under which criteria SIM may be ordered); and 2011 (provisions concerning the one of the measures were specified). Also, an important year for SIM is 2010 when the new LCP was adopted, in which the Macedonian legislator is trying to encompass this sensitive area of human rights and fundamental freedoms, bearing in mind the European standards, especially the Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms.

According to the new LCP, SIM should be used when it is likely to provide data and evidence necessary for successful conduction of the criminal procedure, which otherwise cannot be obtained. If these conditions are fulfilled, then 12 types of measures may be ordered towards 3categories of criminal acts. Since organs authorized to order SIM are the Judge of the pre-trial procedure (for the measures from the Article 252 paragraph 1 items 1, 2, 3, 4 and 5) and the Public Prosecutor (for the measures from the Article 252 paragraph 1

items 6, 7, 8, 9, 10, 11 and 12), it follows that organs authorized for SIM's implementation are the Public Prosecutor or the Judicial Police under his/her control. Concerning the SIM's duration under the new LCP, they may last no longer than 4 months, but there are possibilities their duration to be prolonged.

As to the SIM's implementation based on the current LCP (2005 to 2011), they were applied under 532 orders issued by the Investigative Judge and 204 orders issued by the Public Prosecutor. A positive note can be made that the number of the issued orders for SIM's implementation is in decline, which implies that the relevant authorities are trying to comply with the requests that there should be no "less sensitive" measure to achieve the same purpose; to be applied towards serious criminal acts; to be limited by time and to fall under a judicial control. Finally, it must be pointed out that the data, reports, documents and objects obtained by using these measures may be used as evidence in the criminal procedure only if the measures were implemented under conditions and in a manner stipulated by the Law itself.

Stručni rad - UDK 343.85: 343.431

SPECIFIČNOSTI OTKRIVANJA I DOKAZIVANJA KRIVIČNOG DELA TRGOVINE LJUDIMA

Mr Dragan Milidragović
Dejan Drobnjak
Policijska uprava u Novom Sadu
Mr Nenad Milić
Kriminalističko-policijska akademija u Beogradu

Apstrakt: Trgovina ljudima je jedna od najvećih i najprofitabilnijih globalnih kriminalnih aktivnosti, zajedno sa trgovinom narkoticima, oružjem i pranjem novca. Više od pola miliona ljudi, najčešće žena i dece, svake godine postaju žrtve trgovine ljudima. Trgovina ljudima je visoko profitabilna, a istovremeno i nisko rizična kriminalna aktivnost, naročito kod seksualne eksploatacije, koja uništava kvalitet života, a kod najtežih oblika i sam život žrtava. To je moderno ropstvo čije su žrtve najčešće žene i devojke.

Postupanje policijskih službenika u slučajevima otkrivanja i dokazivanja krivičnog dela trgovine ljudima, uz nužne elemente pripreme, planiranja i realizacije, odlikuje i niz specifičnosti. One su diktirane kako osobenostima i kompleksnošću samog krivičnog dela, tako i teškom situacijom i stanjem žrtava, specifičnostima vezanim za njihov uzrast, psihofizičke karakteristike, etničke i kulturološke osobenosti, vrste eksploatacije, intezitet povreda i preživele traume.

U uvodnom delu rada ukazano je na problem trgovine ljudima i na rasprostranjenost ove kriminalne delatnosti u svetu i na našim prostorima. Takođe, u ovom delu ukazano je na odredbe Krivičnog zakonika kojima je normirano ovo krivično delo. U prvom delu rada obrađeni su načini izvršenja krivičnog dela trgovine ljudima i načini na koje policija saznaje za izvršenje ovog krivičnog dela, uz primere iz policijske prakse i statističke podatke o broju otkrivenih krivičnih dela trgovine ljudima na prostoru Republike Srbije. Poseban deo rada odnosi se na specifičnost metoda u otkrivanju i dokazivanju krivičnog dela trgovine ljudima. U poslednjem delu rada ukazano je na probleme koji utiču na postupak dokazivanja ovog krivičnog dela, a u zaključnim razmatranjima dati su predlozi za otklanjanje problema u otkrivanju i dokazivanju ovog krivičnog dela i unapređenje efikasnosti policije u njegovom otkrivanju.

Ključne reči: trgovina ljudima, načini saznanja, načini izvršenja, otkrivanje i dokazivanje krivičnog dela.

UVOD

Trgovina ljudima danas se s pravom svrstava u red najvećih, najozbiljnijih i najteže rešivih izazova i pretnji bezbednosti pojedinca, društva, države i međunarodne zajednice. Posebno zabrinjava rastući trend trgovine ljudima, koji se najčešće obrazlaže visokom profitabilnošću i neznatnim rizikom po izvršioce krivičnih dela. Trgovina ljudima i krijumčarenje migranata posle ilegalne trgovine narkoticima i

oružjem je najisplativiji oblik „krimi biznisa“, koji samo u Evropi godišnje donese „profit“ od nekoliko milijardi dolara. U naučnim i stručnim krugovima sve češće se tvrdi da je ovaj oblik kriminala profitabilniji od krijumčarenja oružja i droge, jer je „žena trajnija roba i može se prodavati i više puta u toku eksploatacije“. Uz to, pažnja službi bezbednosti je tradicionalno više usmerena ka trgovini drogom i oružjem nego prema krijumčarenju i trgovini ljudima (Mijalković, 2010: 28)[1].

Efekti globalizacije, masovno siromaštvo, slabo imovinsko stanje, niska i neredovna primanja, loši uslovi života, kriminalizacija društva, korupcija, organizovani kriminalitet, dezorganizacija političke elite i nemogućnost donošenja racionalnih ekonomskih i političkih odluka, socijalno raslojavanje i ekspanzija bede najvećeg dela stanovništva, raspad vrednosnog sistema, povećanje stope kriminaliteta, rat u neposrednom okruženju, hiper inflacija, ekspanzija terorizma na Kosovu, NATO agresija, stalna politička previranja, privlačnost boljeg života, propusti u obrazovanju i vaspitanju, slabljenje socijalne kontrole i dr., uslovi su koji su doprineli nastanku i razvoju trgovine ljudima na području Republike Srbije[2].

Međunarodne organizacije raspolažu različitim podacima o broju ljudi koji godišnje postanu žrtve trgovine ljudima i o zaradi koja se ostvari od ove kriminalne aktivnosti. Prema podacima Ujedinjenih nacija, 700.000 žena, dece i muškaraca svake godine postanu žrtve trgovine ljudima. US State Department procenjuje da 900.000 žena, dece i muškaraca godišnje postanu žrtve trgovine ljudima (20.000 žrtava na teritoriji SAD). Zarada ostvarena od trgovine ljudima procenjuje se na 7–60 milijardi američkih dolara godišnje, a po nekim procenama i do 507 milijardi američkih dolara godišnje. Milijarde dolara stečene trgovinom ljudima služe da se dalje finansira organizovani kriminal, terorizam i korupcija[3].

U stručnoj literaturi, domaćim i međunarodnim dokumentima i propisima postoji mnoštvo definicija trgovine ljudima. Član 3 Protokola za prevenciju, suzbijanje i kažnjavanje trgovine ljudskim bićima, posebno ženama i decom[4], sadrži obavezujuću definiciju trgovine ljudima za države potpisnice Konvencije. Prema ovoj definiciji, trgovina ljudima se definiše kao: „vrbovanje, prevoženje, prebacivanje, skrivanje i primanje lica, putem pretnje silom ili upotrebom sile ili drugih oblika prisile, otmice, prevare, obmane, zloupotrebe ovlašćenja ili teškog položaja, davanja ili primanja novca ili drugih koristi da bi se dobio pristanak lica koje ima kontrolu nad drugim licem, u cilju eksploatacije. Eksploatacija obuhvata, kao minimum, eksploataciju prostitucije drugih lica ili druge oblike seksualne eksploatacije, prinudni rad ili službu, ropstvo ili odnos sličan ropstvu, servitut ili uklanjanje organa.

U zakonodavstvu Republike Srbije, krivično delo trgovine ljudima inkriminisano je u članu 388 Krivičnog zakonika[5]. Pored krivičnog dela trgovine

---

[1] Navedeno prema: Ghrib, A. (2002). *Trafficking in Unaccompanied minors-France, Trafficking in Unaccompanied minors in the Europen Union*, IOM-IHESI (Brussels-Paris), p. 31; Maizhevich, H. (2001). *Trafficking in Women in EU Policy*, (izdavač i mesto nepoznati), p.19.

[2] O ovim i drugim uslovima koji doprinose nastanku i razvoju trgovine ljudima, videti više (Mijalković, 2010: 70–77).

[3] O broju žrtava trgovine ljudima i profitu koji se ostvaruje od trgovine ljudima, videti više htpp/www.astra.org.rs, sajt dostupan 15.02.2012.

[4] Ovaj Protokol dopunjava Konvenciju Ujedinjenih nacija protiv transnacionalnog organizovanog kriminala. „Službeni list SRJ”, Međunarodni ugovori, broj 6/2001.

[5] „Službeni glasnik RS” broj 85/2005, 88/05-ispr., 107/05-ispr i 72/09 i 111/2009.

ljudima iz člana 388 Krivičnog zakonika, u članu 389 KZ inkriminisano je krivično delo trgovina maloletnim licima radi usvojenja i u članu 390 Krivičnog zakonika, krivično delo zasnivanje ropskog odnosa i prevoza lica u ropskom odnosu.[6]

U ovom radu obrađeni su načini saznanja za izvršeno krivično delo trgovine ljudima i metodi koji se koriste za dokazivanje krivičnog dela trgovine ljudima. Takođe, u radu je ukazano na probleme u dokazivanju krivičnog dela trgovine ljudima. U zaključnim razmatranjima dati su predlozi za efikasnije postupanje policije u otkrivanju krivičnog dela trgovine ljudima.

OTKRIVANJE KRIVIČNOG DELA TRGOVINE LJUDIMA

Postupanje policijskih službenika u slučajevima otkrivanja krivičnog dela trgovine ljudima, uz nužne elemente pripreme, planiranja i realizacije u krivičnim stvarima treba da odlikuje i prisustvo brojnih specifičnosti. One su diktirane osobenostima i kompleksnošću zločina, ali i teškom situacijom i stanjem žrtava, specifičnostima vezanim za njihov uzrast, psihofizičke karakteristike, etničke i kulturološke osobenosti, vrstu eksploatacije i intezitet povreda i preživele traume (Žarković, Elez, 2010: 67).

Izvršenje krivičnog dela trgovina ljudima odvija se u tri faze:

- **faza regrutacije** (vrbovanja). U ovoj fazi izvršilac krivičnog dela nastoji da ostvari direktni ili indirektni kontakt sa žrtvom. U zavisnosti od ličnosti žrtve (stepena obrazovanja, fizičke konstitucije, konkretnih namera prema žrtvi), izvršilac upotrebljava silu ili pretnju radi napada na život i telo žrtve, ili žrtvi bliskog lica, ili dovodi u zabludu ili održava u zabludi žrtvu, zloupotrebljava poverenje i odnos zavisnosti, teške prilike, dolazi do ličnih dokumenata i putnih isprava žrtve, pa na taj način priprema žrtvu za naredne faze u izvršenju krivičnog dela[7].
- **faza tranzita** podrazumeva da izvršilac krivičnog dela prevozi, prebacuje, predaje, prodaje, kupuje, posreduje u prodaji, sakriva ili drži žrtvu krivičnog dela.
- **faza eksploatacije** se ispoljava u više oblika: radna eksploatacija; prinuda na vršenje krivičnih dela; seksualna eksploatacija; prinudno prosjačenje; ropstvo i njemu slični odnosi; trgovina organima; prinudno korišćenje u oružanim sukobima.

Do podataka o izvršenom krivičnom delu trgovine ljudima pripadnici policije dolaze na različite načine, primenom različitih metoda i sredstava. Najčešći u praksi načini saznanja za izvršeno krivično delo trgovine ljudima jesu: prijave oštećenog lica ili žrtve, prijava građana i operativni rad policije.

---

[6] Videti član 388, 389. i 390. Krivičnog zakonika.

[7] U cilju sprečavanja i otkrivanja krivičnog dela trgovine ljudima, policijski službenici bi trebalo da posvete pažnju: nadzoru i proveri oglasa kojima se u sredstvima informisanja ili putem interneta nudi zaposlenje u zemlji ili inostranstvu za: konobarice, plesačice, radnice u domaćinstvu, dadilje, kućne pomoćnice, kozmetičarke, građevinske radnike ili radnike u poljoprivredi, razne sezonske poslove itd. U postupku vrbovanja i regrutacije, tj, uspostavljanja kontakta sa potencijalnim žrtvama, moguće su i zloupotrebe poznanstva, navodno iskrenih ljubavnih i prijateljskih, ali i porodičnih veza (Žarković, Elez, 2010: 60).

Prijave oštećenog lica – žrtve krivičnog dela: saznaje se za izvršeno krivično delo najčešće u poslednjoj fazi, fazi eksploatacije, a ređe u fazi regrutacije i tranzita. Još u fazi regrutacije izvršilac krivičnog dela ostvaruje kontakt sa žrtvom, neposredno putem oglasa za primamljive poslove u inostranstvu (poslovi foto-modela, manekenki, atraktivne ponude sa velikim zaradama) na koje se žrtve same javljaju i sa njima izvršilac nastoji da upostavi odnos poverenja. Nakon uspostavljenog poverenja, žrtvama se obećava bezbrižna budućnost, pomoć prilikom zaposlenja, brak, i samim tim žrtva se dovodi i održava u zabludi. Najčešće žrtve trgovine ljudima jesu mlade devojke i žene, naivne i lakoverne osobe, siromašne i nezaposlene osobe, deca, fizički i drugi radnici.

Do prijave u fazi regrutacije retko se dolazi, jer žrtva još uvek nije svesna šta joj se može dogoditi. Opreznije žrtve pokušavaju da se informišu o poslu koji im se obećava, raspituju se, kontaktiraju osobe za koje znaju da su se nalazile na takvim ili sličnim poslovima, kontaktiraju nevladine organizacije, prave fotokopije svojih dokumenata i sl. U fazi tranzita, žrtvi krivičnog dela ostaje malo prostora za komunikaciju sa spoljnim svetom, uglavnom se prevozi zajedno sa izvršiocem krivičnog dela, ili sa saizvršiocima, neretko se žrtvi oduzimaju lična dokumenta, putne isprave, mobilni telefoni, pa je iz navedenih razloga broj prijava u ovoj fazi mali. U mestu smeštaja, žrtve se nalaze pod stalnim nadzorom izvršioca ili saizvršioca, obično su to razrađeni mehanizmi, gde se izvršioci osećaju sigurno, a žrtvi ne ostavljaju mogućnosti za komunikaciju. Najveći broj prijava izvršenja krivičnog dela trgovine ljudima od strane žrtve je u fazi eksploatacije. U ovoj fazi žrtva se nalazi pod konstantnim pritiskom da donese imovinsku korist za izvršioca (trafikera) te se prisiljava na prostituciju, prinudni rad, na vršenje krivičnih dela i sl.

U slučajevima interne trgovine ljudima, žrtva se poverava porodici, prijateljima, a u manjem broju slučajeva kontaktira nevladine organizacije, poziva SOS telefone i policiju. Žrtva se na prijavu odlučuje tek nakon što shvati da je to jedini preostali način da se prekine izvršenje krivičnog dela[8]. U slučaju transnacionalne trgovine ljudima, žrtva se ne nalazi u svojoj zemlji, uglavnom ne poznaje jezik, institucije i slično, što otežava mogućnost da žrtva prijavi izvršenje krivičnog dela. U ovakvim slučajevima, veliki broj žrtava pokušava bekstvo od izvršioca krivičnog dela, ali mali broj u tome uspe. Izvršioci imaju razrađene mehanizme kontrole rada žrtava, te je mali broj onih žrtava koje uspevaju da pobegnu. Značajnu ulogu u prijavljivanju krivičnog dela u inostranstvu imaju i ambasade i konzulati kojima se žrtva obraća. Žrtva može dati najveći broj informacija o izvršiocu krivičnog dela

[8] U Novom Sadu u aprilu 2011. godine, pripadnici Odeljenja pogranične policije za strance, suzbijanje ilegalnih migracija i trgovine ljudima, zaprimili su krivičnu prijavu oštećenih-žrtava U. S. i J. D. za izvršenje krivičnog dela trgovine ljudima. Po zaprimanju krivičnih prijava i prikupljenih drugih dokaza, osumnjičenom R. B iz Novog Sada određeno je zadržavanje do 48 sati. Po isteku zadržavanja R. B. je sa krivičnom prijavom priveden kod dežurnog istražnog sudije Višeg suda u Novom Sadu zbog postojanja osnovane sumnje da je izvršio krivično delo trgovine ljudima. Osumnjičeni je u periodu od decembra 2010. godine do aprila 2011. godine iskoristio težak materijalni položaj U. S. i J. D., te ih eksploatisao da se za njegov račun bave prostitucijom. Kada su U. S. i J. D. htele da prekinu da se bave prostitucijom, osumnjičeni im je pretio i nasilnički se ponašao prema njima i uz upotrebu fizičke sile primoravao ih na prostituciju, pronalazivši klijente. Nakon saslušanja, istražni sudija Višeg suda osumnjičenom R. B odredio je pritvor do 30 dana. Postupak pred Višim sudom u Novom Sadu je toku.

trgovine ljudima, to su informacije „iz prve ruke“, koje mogu da budu značajne i za kasnije dokazivanje krivičnog dela. Žrtva može dati podatke o licima koja su je vrbovala, licima koja su vršila prevoz, prevoznim sredstvima koja su korišćena, zatim o mestima gde je bila smeštena i samom licu koje vrši eksploataciju. Na taj način može se doći do korisnih saznanja o izvršiocima, ulozi u organizovanoj kriminalnoj grupi, što može olakšati rad državnih organa, pre svega policije, u prikupljanu dokaza.

Žrtva nekada nije ni svesna da se nad njom vrši krivično delo trgovine ljudima. Neretko čak i pristaje da se eksploatiše (npr. da se bavi prostitucijom za račun izvršioca te na taj način i sama ostvaruje imovinsku korist – zaradu), čak i kada bude prepoznata kao žrtva od strane nadležnih institucija, odbija saradnju. Pristanak žrtve na eksploataciju ili na uspostavljanje ropskog ili njemu sličnog odnosa ne utiče na postojanje krivičnog dela[9] i ne umanjuje odgovornost pred zakonom onih lica koja su izvršioci krivičnog dela trgovine ljudima.

Do podataka o izvršenom krivičnom delu trgovine ljudima putem **prijava građana** može se doći u sve tri faze izvršenja krivičnog dela. Najčešće izvršenje krivičnog dela prijavljuju lica bliska žrtvi, porodica, rođaci, prijatelji, a u manjem broju slučajeva i ostali građani[10]. U fazi regrutacije – vrbovanja, lica bliska žrtvi ili potencijalnoj žrtvi iskazuju veći stepen opreznosti od same žrtve, u pogledu poslova koje nose veliku zaradu, primamljivih oglasa za rad u inostranstvu, ili poslova modela i manekenki. U ovoj fazi prijave se podnose u slučaju sumnji u posao koji se nudi potencijalnoj žrtvi.

U fazi tranzita, prijave ova lica podnose u trenutku kada prestane komunikacija sa žrtvom ili kada ih žrtva obavesti šta joj se dešava. U ovoj fazi, prijave u malom broju podnose i građani koji nisu bliski žrtvi, najčešće kada shvate da se radi o potencijalnoj žrtvi krivičnog dela. Takvih prijava nema u velikom broju, iz razloga što u najvećem broju slučajeva, čak i kada građani dođu u kontakt sa žrtvom, ne shvate da se radi o žrtvi krivičnog dela trgovine ljudima.

U fazi eksploatacije, prijave najčešće podnose građani koji su svedoci eksploatacije (komšije, slučajni prolaznici), ali i lica bliska žrtvi u slučajevima kada žrtva uspe da kontaktira s njima i saopšti u kakvoj se situaciji nalazi. Građani se obraćaju i prijavljuju izvršenje krivičnog dela trgovine ljudima, državnim organima (policiji, javnom tužilaštvu, centrima za socijalni rad, ambasadama ili konzulatima) i nevladinim organizacijama (Astra, Beosuport, Atina, Centar za prava deteta,

---

[9] Vidi član 388 stav 10 Krivičnog zakonika.

[10] Prijavom građana policijski službenici u Novom Sadu došli su do podataka da su tri lica iz Selenče izvršila krivično delo trgovine ljudima. Po prikupljenim dokazima u decembru 2009. godine, podneta je krivična prijava protiv tri lica iz Selenče, zbog postojanja osnovane sumnje da su izvršila krivično delo trgovina ljudima iz člana 388 KZ, na štetu četiri osobe, od kojih su dve maloletne. Osumnjičeni su u periodu od godinu dana pronašli oštećene, te ih vrbovali za poljske radove, stupali u seksualne odnose sa njima, nakon čega su počeli da ih seksualno eksploatišu, pronalazeći mušterije kojima su oštećene pružale seksualne usluge. Oštećene devojke lošeg su imovinskog stanja, a neke od njih imale su i poremećene porodične prilike (deca razvedenih roditelja ili bez roditeljskog staranja), te su bile pogodne za vrbovanje. a Jedan od osumnjičenih je pretvorio svoju porodičnu kuću u Selenči u mesto okupljanja ljudi zainteresovanih za korišćenje seksualnih usluga, Žrtve su zadržavale samo deo zarađenog novca, dok je ostatak pripadao osumnjičenim licima. U Višem sudu u Novom Sadu u toku je krivični postupak za navedeno delo.

Antitrafiking centar, Save the children i dr.) kao i međunarodnim organizacijama (UNICEF, UNHCR, OEBS, IOM, Crveni krst). Između svih navedenih organizacija postoji povezanost u borbi protiv trgovine ljudima. U Republici Srbiji, koordinaciju rada organizacija koje učestvuju u suprotstavljnju trgovini ljudima obavlja Služba za koordinaciju zaštite žrtava trgovine ljudima.

Operativnim radom policija dolazi do podatka da se priprema izvršenje krivičnog dela ili je izvršeno krivično delo trgovine ljudima. Jedan od zadataka Ministartva unutrašnjih poslova Republike Srbije jeste sprečavanje, otkrivanje i rasvetljavanje krivičnih dela, prekršaja i drugih delikata, zatim drugi vidovi borbe protiv kriminala i otklanjanje njegovih organizovanih i drugih oblika, kao i otkrivanje i hvatanje izvršilaca krivičnih dela i prekršaja i drugih lica za kojima se traga i njihovo privođenje nadležnim organima[11]. Prepoznavanje situacije i pratećih okolnosti krivičnog dela trgovine ljudima od strane policijskih službenika i preduzimanje adekvatnih mera na sprečavanju i suzbijanju krivičnog dela, podrazumeva ne samo poznavanje normativnog osnova i okvira postupanja i opštih kriminalističkih principa i pravila, već i potpuno razumevanje brojnih osobenosti krivičnog dela trgovina ljudima[12].

Pripadnici policije treba da prepoznaju situaciju u kojoj okolnosti izvršenja krivičnog dela nisu očigledne, ilegalan prelazak državne granice, nedozvoljen boravak u stranoj zemlji, prostituciju, prosjačenje, posedovanje opojnih droga i njihovu zloupotrebu, korišćenje falsifikovanih isprava, prevare i slično. Policijski službenici ne treba da očekuju da sve žrtve trgovine ljudima imaju ista obeležja, i da će se žrtve same izbaviti i doći u policiju i zatražiti pomoć. Pojedine žrtve to neće uraditi zato što još uvek nisu svesne da su žrtve trgovine ljudima, bez obzira što se eksploatacija nad njima vrši, dok su druge fizički sprečene od izvršioca krivičnog dela da zatraže pomoć. Jedan broj žrtava to ne čini iz straha za sopstveni život, ili život bliskih lica, ali i usled nepoverenja u policiju.

Policija pored prijava žrtve i drugih subjekata, samoinicijativno preduzima i niz drugih mera i radnji kako bi došla do podataka da se priprema izvršenje krivičnog dela trgovine ljudima, ili da je već izvršeno krivično delo trgovine ljudima[13]. Koristeći prijateljske i poznaničke veze, informatore i saradnike,

---

[11] Vidi član 10 Zakona o policiji (Službeni glasnik Republike Srbije", br. 101/2005, 63/2009-odluka US i 92/2011).

[12] Operativnim radom policijski službenici Policijske uprave u Novom Sadu došli su do podataka da jedno lice iz Novog Sada primorava dve maloletne osobe da se njega bave prostitucijom. Proveravajući dobijene podatke, policijski službenici su prikupili potrebne dokaze o izvršiocu i krivičnom delu i u januaru 2010. godine podneli krivičnu prijavu protiv jednog lica iz Novog Sada, zbog postojanja osnovane sumnje da je izvršilo krivično delo trgovine ljudima iz člana 388 KZ, na štetu dve maloletne osobe. Osumnjičeni je vrbovao maloletne oštećene, koje se nalaze pod starateljstvom Centra za socijalni rad, pa koristeći njihov uzrast, i odsutnost roditeljskog staranja, primoravao ih da se za njega bave prostitucijom na tzv. „Kaćkoj petlji" u Novom Sadu – ulična prostitucija. U slučajevima kada bi oštećene odbile da se bave prostitucijom, osumnjičeni je primenjivao silu i tako ih primoravao na prostituciju. Eksploatacija je trajala oko pet godina, gde su gotovo svakodnevno oštećene morale da budu sa više „mušterija". Zaređeni novac oštećene su davale osumnjičenom, koji je na taj način sticao protivpravnu imovinsku korist. Pred Višim sudom u Novom Sadu, postupak je okončan i izvršilac je je pravosnažno osuđen na 6 godina zatvora.

[13] U aprilu 2009. godine ministar unutrašnih poslova Republike Srbije doneo je Obaveznu instrukciju o postupanju sa krijumčarenim licima. U instrukciji je data lista indikatora za prepoznavanje stvarne

ovlašćena službena lica dolaze do značajnih podataka koji mogu biti od ključne važnosti za otkrivanje krivičnog dela trgovina ljudima. Do početnog podatka može se doći i na relativno lak način, dostupan neograničenom broju ljudi, preko oglasa, reklama, internet stranica, na kojima se nude zaposlenja sa visokim zaradama uz malo rada. U cilju efikasnijeg postupanja svih subjekata u otkrivanju i dokazivanju krivičnog dela trgovine ljudima, državni organi i nevladine organizacije ustupaju sve informacije policiji kojoj je na raspolaganju najširi spektar ovlašćenja predviđenih za otkrivanje ovog krivičnog dela[14].

OBEZBEĐENJE DOKAZA ZA IZVRŠENO KRIVIČNO DELO TRGOVINE LJUDIMA

U zavisnosti od načina saznanja i raspoloživih informacija o krivičnom delu trgovine ljudima, policija preduzima mere i radnje, prvenstveno na sprečavanju izvršenja krivičnog dela trgovine ljudima, a ako je izvršeno krivično delo, na prikupljanju neophodnih dokaza za pokretanje krivičnog postupka.

Od specifičnosti krivičnog dela zavisiće, mere i radnje (metodi) koje će policija koristiti za prikupljanje dokaza o krivičnom delu i izvršiocu. U praksi dokazi za izvršeno krivično delo trgovine ljudima obezbeđuju se najčešće kombinacijim ličnih i materijalnih dokaza, kao što su: saslušanje svedoka-oštećenog, pretresanje stana, privremeno oduzimanje predmeta, saslušanje osumnjičenog, uviđaj, veštačenje, nadzor i snimanje telefonskih i drugih razgovora ili komunikacija, kao i druge mere i radnje čije preduzimanje zavisi od specifičnosti krivičnog dela.

Saslušanje svedoka-oštećenog (žrtve). Iskustvo je pokazalo da su razgovori sa žrtvama zločina trgovine ljudima među najsloženijim i najstresnijim službenim razgovorima. Upravo stoga, ali i zbog važnosti iskaza žrtve u postupku rasvetljavanja i dokazivanja kriminalne aktivnosti trgovaca, veoma pažljivo treba pristupiti izboru službenih lica koja će kontaktirati sa žrtvom i razgovarati sa njom. Prednost treba dati službenim licima koja su već učestvovala u kriminalističkim obradama ove vrste i koja su u mogućnosti da pravilno informišu žrtvu o položaju, pravima i obavezama u krivičnom postupku (Žarković, Elez, 2010: 68)[15].

---

ili potencijalne žrtve trgovine ljudima i trgovine decom radi usvojenja među krijumčarenim licima. U prilogu instrukciji navedena su pitanja koja pripadnici policije treba da postavljaju ukoliko dođu u kontakt sa potencijalnim žrtvama trgovine ljudima.

[14] U 2010. godini policijski službenici MUP Republike Srbije zbog izvršenih krivičnih dela trgovine ljudima podneli su 47 (51) krivičnih prijava protiv 99 (94) lica. Krivična dela izvršena su nad 76 (85) oštećenih lica (žrtava trgovine ljudima), 37 (34) žrtava trgovine ljudima seksualno je eksploatisano, 8 (9) radno, 5 (2) je eksploatisano zbog vršenja krivičnih dela, 10 (4) radi prosjačenja i 4 (5) radi prinudne udaje. Od 99 (94) izvršilaca krivičnih dela, 76 (73) su muškarci, 23 (21) žene, a od 76 (85) žrtava, 9 (15) žrtava je starosne dobi ispod 14 godina, 23 (33) žrtve su starosne dobi od 14 do 18 godina i 44 (37) žrtve starosne dobi preko 18 godina. Od ukupno 47 (51) podnetih krivičnih prijava, najviše, 15 (14) krivičnih prijava podnela je Policijska uprava u Novom Sadu, zatim PU za grad Beograd 8 (10). U zagradi su dati podaci za 2009. godinu. O rezultatima MUP-a u otkrivanju krivičnog dela trgovine ljudima i drugim statističkim pokazateljima videti više www.mup.gov.rs dostupan 15.02.2012. godine.

[15] Ukoliko je žrtva maloletno lice ili dete, ovlašćeno službeno lice mora biti obučeno i za ovakav vid razgovora. U praksi je uočena negativna pojava da se žrtva o već iznetim detaljima više puta ispituje:

Praksa je pokazala da se slučajevi krivičnog dela trgovine ljudima zasnivaju uglavnom na ličnim dokazima, pre svih, na iskazima oštećenih lica i svedoka. Vođenje razgovora sa žrtvom o detaljima krivičnog dela, moguće je tek po isteku perioda u kome će žrtva sagledati svoju poziciju, osetiti sigurnost i zainteresovanost da sarađuje, i saglasno tome pristati na razgovor. Bilo kakav pritisak na žrtvu, njeno omalovažavanja i prebacivanje zbog nekritičkog razmišljanja i lakovernosti kojom je doprinela tome da postane žrtva, neminovno dovodi do sekundarne viktimizacije, dodatne traumatizacije, ali i do stvaranja ili produbljivanja nepoverenja prema policijskim službenicima. Obaveza policijskog službenika je da u komunikaciji sa žrtvom bude profesionalan, otvoren i pošten, da pokazuje iskreno saosećanje i da vrši stalnu procenu rizika – za žrtvu i njene bližnje (rizik je i činjenica samog postojanja kriminalne organizacije koja ima izrazitu reputaciju nasilja i osvete), da uvažava hitne potrebe žrtve, da je obavesti o raspoloživoj pomoći i načinima njenog ostvarivanja (uključivanje u rad centara za socijalni rad, Službe za koordinaciju zaštite žrtava trgovine ljudima, smeštaj u sigurne kuće i dr.). S obzirom na to da je dovođenje u situaciju žrtve i njeno traumatično iskustvo i surova eksploatacija, gotovo po pravilu, vezano za raznovrsne, manje ili više perfidne i okrtune prevare, policijskog službenika ne treba da čude nagle i snažne promene raspoloženja, manjkavosti prostorne i vremenske orijentacije, kao i problemi i greške pri percepciji, pamćenju i prisećanju događaja, da ga pogađaju i obeshrabruju agresija, neprijateljstvo, sumnjičavost i nepoverenje, nepotputnost, nejasnoća, pa i kontradiktornost izjava. Samo puno razumevanje i uvažavanje situacije, dostojanstva, ličnih prilika, osećanja, dilema, pa i želja žrtve (npr. u izboru službenog lica sa kojim želi da razgovara jer zna jezik žrtve, istog je pola, pripada istoj nacionalnoj i etičkoj grupi i sl.), uz stvaranje optimalnih uslova za razgovor, mogu dati pozitivne rezultate (Žarković, Elez, 2010: 67,68)[16].

Pretresanje stana i drugih prostorija vrši se u stanu i drugim prostorijama u kojima se mogu pronaći žrtve krivičnog dela (stan u kome je vršena eksploatacija) ili predmeti koje je osumnjičeni koristio za izvršenje krivičnog dela (mobilni telefoni, nosači podataka, računari, falsifikovana dokumenta, oružje, opojne droge). Jedna od teškoća prilikom pronalska stana i drugih prostorija u kojima se vrši seksualna eksploatacije jeste stalno premeštanje žrtava u druge objekte. Čak i pri najmanjoj opasnosti od otkrivanja osumnjičeni lako nalazi novo mesto gde će smestiti žrtvu krivičnog dela i nastaviti njenu eksploataciju.

Kod radne eksploatacije nešto je lakši posao za policiju, jer osumnjičeni pored žrtve mora promeniti lokaciju i predmete koje koristi žrtva u radu (uglavnom razne mašine). U slučajevima prinudnog prosjačenja često se menjaju mesta u okviru jednog grada, ali i sam grad, pa i država. Nisu retki slučajevi da se prinudno prosjačenje domaćih državljana u vreme letnje sezone vrši u Republici Crnoj Gori i Republici Hrvatskoj.

O izvršenom pretresu stana i drugih prostorija sačinjava se zapisnik o pretresu stana i drugih prostorija, gde se navodi zatečeno stanje i pronađeni predmeti. Zapisnik predstavlja dokaz u krivičnom postupku. Pretresu prisustvuju dva punoletna svedoka, koja imaju veliku ulogu u slučaju pronalaska žrtve krivičnog

---

u policiji, javnom tužilaštvu, pred istražnim sudijom i tokom glavnog pretresa pred sudskim većem.

[16] O specifičnostima razgovora sa žrtvom trgovine ljudima videti više (Žarković, Elez, 2010).

dela ili drugih predmet. Oni će se u krivičnom postuku pojaviti kao svedoci. Nisu retki slučajevi u kojima odbrana okrivljenog na glavnom pretresu pokušava da ospori Zapisnik o pretresu stana i drugih prostorija i svedoci koji su bili prisutni u toku pretresa, ključni su za prezentovanje pravog stanja stvari u toku vršenja pretresa.

Privremeno oduzimanje predmeta može biti preduzeto u toku vršenja pretresa stana i drugih prostorija, ili prilikom pretresa lica, ili pregleda lica i vozila. Oduzeće se predmeti koji mogu poslužiti kao dokaz u krivičnom postupku. O oduzimanju predmeta sačinjava se potvrda o privremeno oduzetim predmetima koja se u krivičnom postupku može koristiti kao dokaz. Kod krivičnog dela trgovine ljudima, u najvećem broju slučajeva oduzimaju se mobilni telefoni iz kojih se veštačenjem mogu dobiti informacije o komunikaciji okrivljenog sa žrtvom (vrbovanje, ponude za posao, pretnje i sl.). Osim mobilnih telefona, koji predstavljaju značajan izvor podataka, oduzimaju se i nosači podataka (CD, DVD, razne memorije, memorijske kartice, hard diskovi i dr.) na kojima se mogu pronaći fotografije i video zapisi žrtava. U slučajevima seksualne eksploatacije, prinudne prostitucije, nisu retkost da okrivljeni na računarima, CD, DVD, mobilnim telefonima i sl., sakupljaju kolekcije fotografija (uglavnom nagih žrtvi) koje prikazuju potencijalnim mušterijama, radi kupovine žrtava, kao i radi dalje prodaje i eksploatacije ili korišćenja seksualnih usluga. U stanovima osumnjičenih pronalaze se i falsifikovana dokumenta pripremljena za žrtve, opojne droge koje se neretko daju žrtvama radi lakše kontrole, oružje kojim se vrši zastraživanje žrtava i drugi predmeti.

Saslušanje osumnjičenog u pretkrivičnom postupku predstavlja dokaz u krivičnom postupku samo u slučaju ako je prilikom saslušanja bio prisutan branilac osumnjičenog i uz ispunjenje ostalih uslova predviđenih Zakonikom o krivičnom postupku. U slučajevima priznanja osumnjičenog, policijski službenici dužni su da nastave sa prikupljanjem drugih dokaza, jer se često dešava da osumnjičeni više puta menja svoj iskaz, kako u istrazi, tako i na glavnom pretresu. Priznanje na glavnom pretresu sud može ceniti kao olakšavajuću okolnost u toku donošenja presude i odlučivanja o kazni. U slučajevima trgovine ljudima, praksa pokazuje da nije veliki broj lica koja priznaju izvršenje krivičnog dela.

Uviđaj se preduzima kada je za utvrđivanje ili razjašnjavanje kakve važne činjenice u postupku potrebno neposredno opažanje[17]. Kod krivičnog dela trgovine ljudima uviđaj se najčešće vrši u stanu i drugim prostorijama u kojima su pretresom pronađeni predmeti krivičnog dela ili su pronađene žrtve krivičnog dela. O izvršenom uviđaju sačinjava se zapisnik o uviđaju, koji se u krivičnom postupku koristiti kao dokaz. U toku uviđaja neophodno je obezbediti i fiksirati tragove krivičnog dela; preporučuje se fotografisanje ili snimanje stana i drugih prostorija, a po potrebi, prilikom vršenja uviđaja angažovaće se i veštaci.

[17] U pretkrivičnom postupku, za krivična dela za koja je propisana kazna zatvora do deset godina, policija može sama obaviti uviđaj i odrediti veštačenja koja ne trpe odlaganje, osim obdukcije i ekshumacije leša, ako istražni sudija nije u mogućnosti da odmah iziđe na lice mesta. Ako istražni sudija stigne na lice mesta u toku uviđaja, on može preuzeti ove radnje (član 238 st.3. Zakonika o krivičnom postupku, "Službeni list" br. 70/2001 i 68/02 i "Službeni glasnik RS", br. 58/04, 85/05-dr. zakon, 49/07,20/09-dr. zakon, 72/09 i 76/10)

Veštačenje se određuje kada za utvrđivanje ili ocenu neke važne činjenice treba pribaviti nalaz i mišljenje od lica koje raspolaže potrebnim stručnim znanjem. U slučajevima trgovine ljudima obično se radi o psihološkim, psihijatrijskim veštačenjima žrtve, ali nisu retka ni grafološka veštačenja, ili veštačenja opojnih supstanci[18].

Nadzor i snimanje telefonskih i drugih razgovora ili komunikacija preduzima se u skladu sa posebnim odredbama za krivična dela organizovanog kriminala, korupcije i druga izuzetno teška krivična dela u koja spada i krivično delo trgovine ljudima[19]. Ovu meru inicira policija, koja raspolaže podacima da neko lice vrši krivično delo trgovine ljudima, nakon prikupljenih podatka o brojevima mobilnih telefona koji se koriste za izvršenje krivičnog dela. Na osnovu naredbe istražnog sudije otpočinje se sa nadzorom komunikacija. U toku nadzora komunikacija mogu se prikupiti značajni podaci o izvršiocu krivičnog dela, saizvršiocima, oštećenim licima, ali i dokazi koji se u kasnijem krivičnom postupku, uz druge dokaze mogu koristiti. Na ovaj način mogu se dokazati uloge više izvršilaca u kriminalnoj grupi ili organizovanoj kriminalnoj grupi, mogu se utvrditi uloge izvršilaca, zaduženih za vrbovanje, falsifikovanje dokumenata, smeštaj žrtve, prevoz, prihvat, prodaju, kao identifikacija organizatora kriminalne grupe[20].

PROBLEMI DOKAZIVANJA KRIVIČNOG DELA TRGOVINE LJUDIMA

Suđenja u Republici Srbiji organizovana su tako da sva zainteresovana lica koja čekaju (stranka, druga pozvana lica, javnost i sl.) stoje ispred sudnice dok ih sud ne prozove. Žrtva trgovine ljudima, takođe, čeka u istom prostoru zajedno za okrivljenim ili njemu bliskim licima, pa joj se može lako pretiti, a strah i pritisak sa kojim se tada suočava utiču na njeno davanje iskaza. Sam mehanizam procesa trgovine ljudima i dugotrajno zlostavljanje i ponižavanje utiču na to da žrtva često nema samopouzdanja i da se plaši okrivljenog jer je i tokom procesa trgovine bila svedok demonstracije njegove moći, te ove pretnje shvata zaista ozbiljno. Svako pojavljivanje žrtve u svojstvu oštećene pred sudom za nju je preloman i strašan korak za koji je potrebna velika hrabrost. Svedočenje žrtve zahteva ozbiljnu podršku u vidu njene zaštite i u pravcu pripreme za svedočenje i sprovođenje samog postupka svedočenja. To treba učiniti na način koji neće dovesti do ponovne viktimizacije žrtve, što u našoj praksi često nije slučaj (Banić, 2010: 81)[21].

---

[18] O psihološkim traumama žrtve trgovine ljudima, videti više (Slavković, 2010).

[19] Vidi glavu XXIX Zakonika o krivičnom postupku koja sadrži posebne odredbe o postupku za krivična dela organizovang kriminala, korupcije i druga izuzetno teška krivična dela.

[20] Pored nadzora komunikacija za otkrivanje krivičnog dela trgovine ljudima koriste se i telefonski listinzi. O kriminalističkom značaju telefonskih listinga za otkrivanje i rasvetljavanje krivičnih dela, videti više, (Milidragović, 2010).

[21] Zakonik o krivičnom postupku iz 2006 godine ("Službeni glasnik" broj 46/06), sadržao je neka zakonska pravila čiji cilj je bio da se pomogne oštećenoj strani za vreme davanja iskaza, kao što su postavljanje punomoćnika oštećenog za vreme saslušanja, saslušanje uz pomoć psihologa, socijalnog radnika ili drugog stručnog lica, saslušanje u drugoj prostoriji, u zgradi ili van zgrade suda, upotrebom tehničkih sredstava uz postavljanje pitanja oštećenom posredstvom organa koji vodi postupak,

Jedna od osnovnih pretpostavki za održavanje glavnog pretresa je prisustvo stranaka, pa se, ukoliko okrivljeni (koji se nalazi na slobodi) ne dođe na glavni pretres, suđenje ne može održati, već se odlaže. Međutim, u postupcima ove vrste to se često zloupotrebljava. Okrivljeni vrlo dobro znaju da je pritisak i stres koji žrtva trpi sve veći što se suđenje više puta odlaže, a da istovremeno njena odlučnost da da potpun iskaz slabi, te je jedna od strategija trgovaca ljudima, upravo odlaganje suđenja. Sudovi u Republici Srbiji su prilično tolerantni na nedolaske okrivljenih na suđenja ukoliko dostave iole smisleno opravdanje, iako imaju mogućnost da preduzmu kako mere obezbeđenja prisustva okrivljenog, tako i da provere istinitosti razloga koje okrivljeni navode za nedolaženje na glavni pretres (provera lekarskih uverenja, veštačenjem zdravstvenog stanja okrivljenih i sl.). Situacija je još komplikovanija ukoliko postoji više okrivljenih, jer se oni često dogovaraju na koji način će odložiti suđenje, pa tako na svaki glavni pretres ne dolazi bar jedan od njih i time smanjuju sumnju suda u izigravanje sudskog postupka. Sve ovo uslovljava da žrtve više puta dolaze u sud da svedoče, ponovo se suočavajući sa stresom i strahom koji taj dolazak povlači, a dodatno se komplikuje ukoliko žrtva živi u drugom gradu ili u drugoj zemlji (Banić, 2010: 83)[22]. U cilju rešenja ovih problema potrebno je zakonom predvideti drugačiji način saslušanja žrtava trgovine ljudima i drugih posebno osetljivih svedoka, a radi efikasnijeg sprovođenja krivičnog postupka sudovi treba više da koriste mere za obezbeđenje prisustva okrivljnog tokom suđenja.

ZAKLJUČAK

Trgovina ljudima je jedna od delatnosti organizovanog kriminala koja kriminalnim grupama i pojedincima donosi velike zarade. Ujedinjene nacije smatraju da je trgovina ljudima prema ostvarenom profitu treća po veličini kriminalna delatnost u svetu, odmah iza trgovine oružjem i narkoticima

Republika Srbija danas je prepoznata kao zemlja porekla, tranzita i krajnje destinacije žrtava trgovine ljudima. U cilju efikasnije delatnosti policije u otkrivanju krivičnog dela trgovine ljudima odnosno prepoznavanja indicija koju ukazuju na izvršenje krivičnog dela trgovine ljudima, neophodna je dodatna edukacija pripadnika policije, pre svega granične policije, policije opšte nadležnosti, saobraćajne policije i kriminalističke policije.

Policija opšte nadležnosti, granična policija, kriminalistička i saobraćajna policija, najbrojniji su deo policije i svakodnevno u svom radu dolaze o kontakt sa izvršiocima krivičnih dela i prekršaja, među kojima su i izvršioci krivičnog dela trgovine ljudima. Edukacijom ovog sastava policije o brojnim osobenostima

psihologa, pedagoga, socijalnog radnika ili drugog stručnog lica. Aktuelni Zakonik o krivičnom postupku ne sadrži ove odredbe. Radi izbegavanja ponovne viktimizacije žrtve i svedočenja žrtve bez stresa i pritiska od strane prisutnih u sudnici, izmenama aktuelnog ZKP-a, neophodno je predvideti rešenje kao u ZKP iz 2006. godine.

[22] Zakon o maloletnim učiniocima krivičnih dela i krivičnopravnoj zaštiti maloletnih lica ("Službeni glasnik", broj 85/05), obavezuje sud da prilikom saslušanja maloletnih oštećenih vodi o računa o njihovom uzrastu, svojstvima ličnosti, obrazovanju, prilikama u kojima žive, posebno nastojeći da se izbegnu moguće štetne posledice po njihovu ličnost i razvoj, a da se saslušanje obavi uz pomoć psihologa, pedagoga ili drugog stručnog lica.

krivičnog dela trgovine ljudima, načinima izvršenja i indicijama od značaja za otkrivanje krivičnog dela trgovine ljudima, postigli bi se bolji rezultati u otkrivanju ovog krivičnog dela, kao i u obezbeđenju dokaza za krivični postupak.

Kada je krivični postupak u pitanju, izmenama Zakonika o krivičnom postupku neophodno je predvideti odredbe o saslušanju posebno osetljivih svedoka odnosno mogućnosti postavljanja punomoćnika za vreme saslušanja, saslušanje uz pomoć psihologa, socijalnog radnika ili drugog stručnog lica, saslušanje u drugoj prostoriji, u zgradi ili van zgrade suda, upotrebom tehničkih sredstava uz postavljanje pitanja oštećenom posredstvom organa koji vodi postupak, psihologa, pedagoga, socijalnog radnika ili drugog stručnog lica, na ovaj način bi se sprečilo zastrašivanje svedoka u sudnicama i čekaonicima ispred sudnica.

Izbegavanje pojavljivanja okrivljenih na glavnom pretresu pod raznim izgovorima i opravdanjima branilaca, a sve radi oduglovačenja krivičnog postupka i mogućnosti uticaja na žrtvu radi promene iskaza, sudovi treba da rešavaju merama za obezbeđenje prisustva okrivljenog u krivičnom postupku.

LITERATURA

1. Banić, M. (2010). *Zaštita trgovine ljudima u krivičnom postupku,* Suzbijanje trgovine ljudima – dobre prakse – priručnik za institucije, Astra, Beograd, str. 80–86.
2. Bošković, M.(2003). *Transnacionalni organizovani kriminalitet*, Beograd, Policijska akademija.
3. Vasiljević, T., Grubač, M.(2003). *Komentar Zakonika o krivičnom postupku*, Beograd, Službeni glasnik.
4. Mijalković, S. (2010). Suprotstavljanje trgovini ljudima i krijumčarenju migranata, Beograd, Službeni glasnik.
5. Milidragović, D**.** (2010). *Pravni osnov nadzora komunikacija putem telefonskog listinga*, Zbornik radova: „Pravo i forenzika u kriminalistici“, Beograd, Kriminalističko-policijska akademija, str. 217–227.
6. Simonović, B.(2004). *Kriminalistika*, Kragujevac, Pravni fakultet.
7. Slavković, B. (2010). *Trgovina ljudima – iskustvo kompleksne traume, neophodnost zaštite preživelih od retraumatizacije od strane institucija, profesionalaca i procedura*, Suzbijanje trgovine ljudima – dobre prakse – priručnik za institucije, Astra, Beograd, str. 26–37.
8. Žarković, M., Elez, S., (2010). *Osnovni elementi postupanja policijskih službenika u suprotstavljanju trgovini ljudima,* Suzbijanje trgovine ljudima – dobre prakse – priručnik za institucije, Astra, Beograd, str. 58–73.
9. Konvencija Ujedinjenih nacija protiv transnacionalnog organizovanog kriminala sa Protokolom za prevenciju, suzbijanje i kažnjavanje trgovine ljudskim bićima,naročito ženama i decom i Protokolom protiv krijumčarenja emigranata kopnom, morem i vazduhom, Službeni list SRJ”, Međunarodni ugovori, broj 6/2001.
10. Zakon o potvrđivanju konvencije Saveta Evrope o borbi protiv trgovine ljudima (“Sl. glasnik RS – Međunarodni ugovori”, br. 19/2009).
11. Krivični zakonik Republike Srbije (“Službeni glasnik RS”, 85/2005, 88/2005 –

ispr., 107/2005 – ispr., 72/2009 i 111/2009).
12. Zakonik o krivičnom postupku ("Službeni list", br. 70/2001 i 68/2002 i "Sl. glasnik RS", br. 58/2004, 85/2005, 115/2005, 85/2005 – dr. zakon, 49/2007, 20/2009 – dr. zakon, 72/2009 i 76/2010).
13. Zakon o policiji (Službeni glasnik Republike Srbije", br. 101/200563/2009 – odluka US i 92/2011).
14. Zakon o maloletnim učiniocima krivičnih dela i krivičnopravnoj zaštiti maloletnih lica ("Službeni glasnik", broj 85/05).
15. Zakonik o krivičnom postupku ("Službeni glasnik Republike Srbije", broj 46/06).
16. Internet prezentacija NVO ASTRA www.astra.org.rs dostupna 15.02.2012.
17. Internet prezentacija MUP Republike Srbije, www.mup.gov.rs dostupna 15.02.2012.
18. Strategija borbe protiv trgovine ljudima u Republici Srbiji www.mup.gov.rs dostupna 15.02.2012.

SPECIFICS OF DETECTION AND PROOF OF CRIMINAL ACTS OF TRAFFICKING

Abstract*:* trafficking is one of the largest and the most profitable global criminal activity, along with drug trafficking, weapons and money laundering.More than half a million people, mostly women and children, each year become victims of trafficking. Human trafficking is highly profitable and at the same time low-risk criminal activity, especially concerning sexual exploitation, which destroys victims' quality of life, and in the most serious cases also victims' life. That is modern slavery whose victims are mostly women and girls.

Conduct of police officers in cases of detection and proving the criminal act of human trafficking, with the essential elements of preparation, planning and implementation is defined by different characteristics. Those are defined by both the characteristics and complexity of the criminal act and also by the difficult situation and condition of victims, specifics related to their age, mental and physical characteristics, ethnic and cultural characteristics, exploitation type, intensity of injury and traumas.

In the introduction, it is pointed to the problem of human trafficking and the spread of criminal activities in the world and our region. In this section it is also pointed to the provisions of the Criminal Law, which defines that criminal act.In the first part are defined modes of committing of trafficking and the ways in which the police find out for committing of this crime, along with examples of police practices and statistics on the number of detected criminal acts of trafficking in the Republic of Serbia. A special section of this article refers to the specific method of detecting and proving the criminal act of human trafficking. In the last part is pointed to problems that affect the process of proving this criminal act, and in concluding remarks are given suggestions for solving detecting and proving problems and improving police efficiency and effectiveness in its detection.

Key words*:* human trafficking, ways of learning, methods of execution, detecting and proving criminal acts.

Stručni rad – UDK 316.334.3:316.7(4) „ 2001-2010”

MOVEMENT OF CRIME IN THE REPUBLIC OF MACEDONIA IN THE PERIOD 2001 - 2010, AND THE IMPORTANCE OF THE EUROPEAN INTEGRATION IN FIGHT AGAINST CRIME

M.A. Stevco Jolakoski,
Head of Department of Road Transport and Infrastructure in the Ministry of Transport and Communications

Abstrakt: In recent years the fight, or discovery and clarification of cases of crime in the Republic of Macedonia was one of the main priorities in its actions. Whether it was the detection of organized criminal activities of individuals or OF groups of national and international level, along with the intensification of international cooperation, the objectives of the actions always remained the same: rigorous, effective and indiscriminating repression of all forms of crime.

The purpose of this paper is to provide analysis of the crime in the Republic of Macedonia in the period 2001 - 2010, and to emphasize the importance of European integration in the fight against crime.

Of course in cleaning up of these cases more than useful was also the international cooperation, which has a special treatment in the activities of the Macedonian police as one of the strategic benchmarks in functioning of the Ministry of Interior. Having regard that not only the world trends, but also the constant transformation of transnational criminal activities in the field of organized crime, require from all greater unity, organization, coordination and cooperation in the interests of citizens and states.

In the Republic of Macedonia, in the period 2001-2005, criminal acts have been continually in increase which is the most evident in 2003 and the increase is 23%. This negative trend of increase in criminal acts, after a long period, was interrupted in 2006 when it decreased slightly by 2.7%, and then in 2007 again a larger increase of 19% was reported, while the remaining years the number of criminal acts oscillates with slight tendency to increase or decrease. As to the crimes committed by juveniles, their share in the total crime ranges in average from 14.7% to 21.7% per year, and it should be pointed out that despite the fact that in 2010 the number of criminal acts is the biggest, participation of the juveniles in doing criminal acts is in the lowest level, that is 14.7%.

Given the importance of this issue and the fact that the world pays great attention to this topic, this paper will offer guidance on transfer of the best world practices concerning cooperation in combating crime and the importance of the European integration and the joint coordination and cooperation aimed at reducing crime.

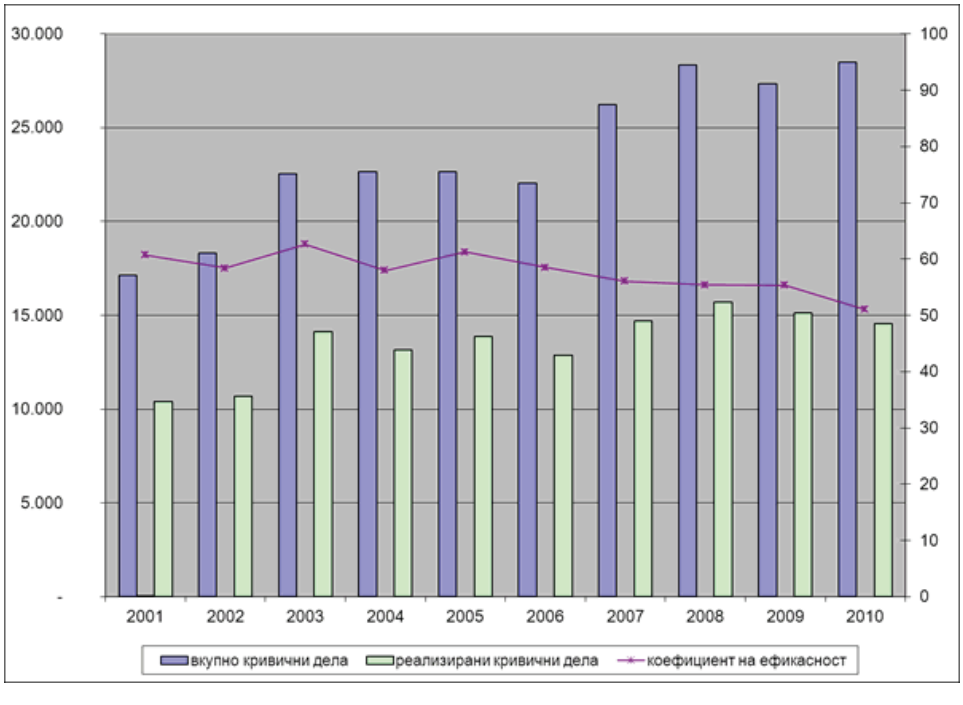
Keywords: crime, European integration, cooperation

MOVEMENT OF CRIME IN THE REPUBLIC OF MACEDONIA IN THE PERIOD 2001 - 2010

In the period 2001-2005, the crimes have been in a steady rise which is most evident in 2003 and it is 23%. This negative trend of increase in crime, after a long time, was interrupted in 2006 when it decreased slightly by 2.7%, and in 2007 again a larger increase of 19% was reported, while in the other years the number of crimes oscillates with tendency of slight increase or decrease. As regards crimes committed by juveniles, their share in the total crime ranges on the average from 14.7% to 21.7% per year, and it should be noted that despite the fact that in 2010 the number of crimes is greatest, participation of the juveniles in committing crimes is in the lowest level and it is 14.7.[1]

	2001	**2002**	**2003**	**2004**	**2005**	**2006**	**2007**	**2008**	**2009**	**2010**
Total Criminal Acts	17.139	18.308	22.547	22.663	22.634	22.024	26.224	28.327	27.330	28.489
Realized Criminal Acts	10.410	10.696	14.123	13.148	13.870	12.881	14.700	15.690	15.128	14.540
Coefficient of Efficiency	60,7	58,40	62,63	58,00	61,27	58,48	56,05	55,38	55,35	51,03
Criminal Acts Perpetrated by juveniles	2255	2116	2393	2624	2.399	2.360	2.242	2.326	2.382	2.136

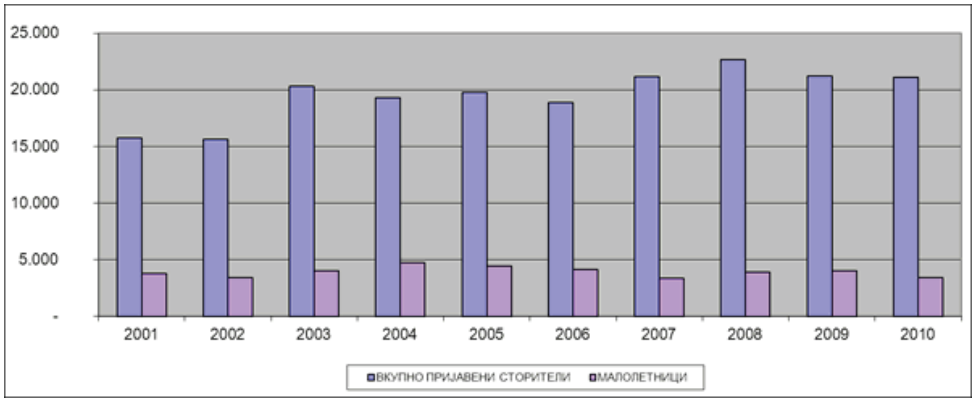
Source: www.moi.gov.mk



[1] www.moi.gov.mk

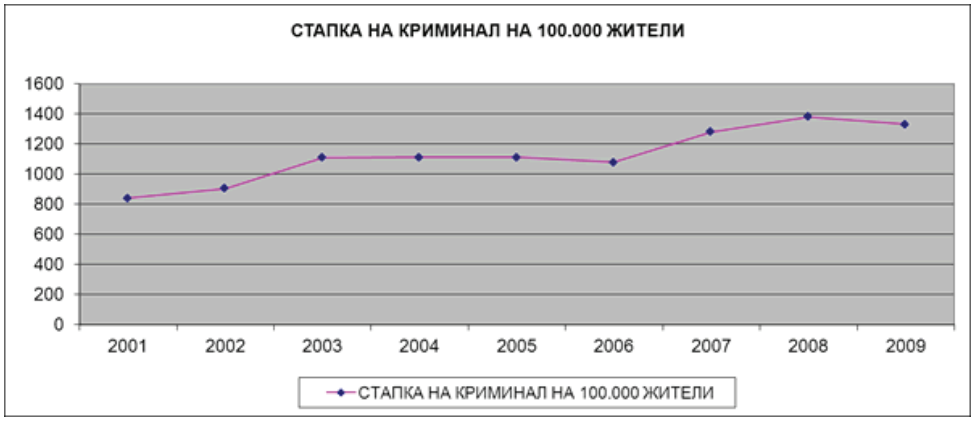
PERPETRATORS OF CRIMINAL ACTS IN THE PERIOD 2001-2010

	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010
TOTAL NUMBER OF PERPETRATORS	15.760	15.651	20.313	19.277	19.755	18.858	21.167	22.690	21.226	21.093
JUVENILES	3.791	3.423	4.032	4.746	4.447	4.143	3.377	3.888	4.015	3.415
ADULTS	11.969	12.228	16.281	14.531	15.308	14.715	17.790	18.802	17.211	17.678



Criminal rate

	2001	2002	2003	2004	2005	2006	2007	2008	2009
CRIME RATE AT 100.000 POPULATION	840,7	904,70	1110,70	1113,50	1113,60	1078,60	1282,20	1382,70	1331,40
TOTAL NUMBER OF CRIMINAL ACTS	17.139	18.308	22.547	22.663	22.634	22.024	26.224	28.327	27.330
NUMBER OF POPULATION	2.038.651	2.023.654	2.029.892	2.035.196	2.032.544	2.041.941	2.045.177	2.048.619	2.052.722



TYPICAL CRIMINAL ACTS IN THE AREA OF ORGANISED CRIME IN THE PERIOD 2001-2010

In the area of organized crime, this ten-year period is characterized by a significant number of detected corruption offenses, the trend of which has changed with a decrease only in 2006. Also, after the incrimination of trafficking and smuggling migrants, by the amendments to the Criminal Code in 2002 and 2004, significant planning measures have been taken for detection of these acts, which resulted in their greater representation in the total number of criminal acts in this area.[2]

	2001		2002		2003		2004		2005		2006		2007		2008		2009		2010	
	REG. CR. ACTS	REP. CR. ACTS	REG. CR. ACTS	REP. CR. ACTS	REG. CR. ACTS	REP. CR. ACTS	REG. CR. ACTS	REP. CR. ACTS	REG. CR. ACTS	REP. CR. ACTS	REG. CR. ACTS	REP. CR. ACTS.	REG. CR. ACTS	REP. CR. ACTS.	REG. CR. ACTS	REP. CR. ACTS	REG. CR. ACTS	REP. CR. ACTS	REG. CR. ACTS	REP. CR. ACTS
MONEY FORGERY ART.268	145	153	177	236	144	139	122	133	195	175	172	152	167	144	120	96	134	119	217	181
ACCEPTING BRIBES ART.357	20	20	13	13	4	5	15	15	14	16	6	7	23	66	12	18	16	77	13	16
GIVING BRIBES ART.358	7	7	8	8	9	11	16	17	6	7	4	5	17	19	14	15	26	28	9	9
MONEY LAUNDRY ART.273	-	-	-	-	-	-	-	-	40	87	20	63	10	28	4	15	12	40	6	50
CRIMINAL AFFILIATION ART.394	-	-	-	-	-	-	-	-	-	-	-	-	-	-	10	76	10	96	10	97
TRAFICKING ART.418-A	-	-	18	33	42	78	19	42	12	40	3	4	3	4	1	4	1	1	-	-
SMUGGLING OF MIGRANTS ART.418-B	-	-	-	-	-	-	21	28	35	61	23	54	32	64	36	96	26	53	27	58
Organizing of a group to carry out trafficking deeds and smuggling migrants Art.418 c	-	-	-	-	-	-	3	4	2	23	3	21	6	27	11	64	5	17	6	31
TRADE WITH JUVENILE ART.418-D	-	-	-	-	-	-	-	-	-	-	-	-	-	-	9	21	7	15	3	10

Source: www.moi.gov.mk

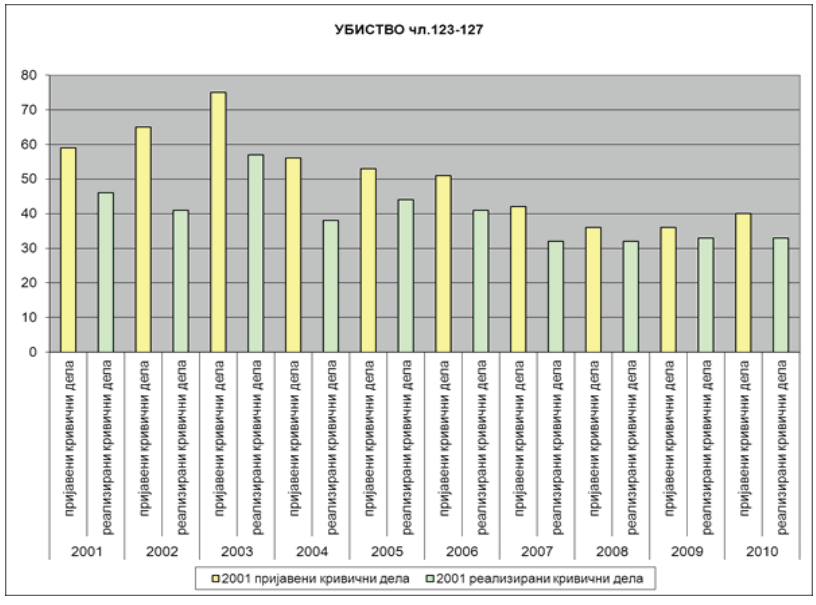
[2] www.moi.gov.mk

CRIMINAL ACTS AGAINST LIFE AND BODY

As far as 2003, murders as most severe forms of criminal acts against life and body have a steady rise and from 2004 on they are constantly decreasing. Besides reducing the number of committed criminal acts it is important that in this period a constant high efficiency of the police has been noted in the realization of these deeds, which in 2009 reached even 92%. In the period until 2004 the efficiency of the police ranged from 63% to 78%.

	2001		2002		2003		2004		2005		2006		2007		2008		2009		2010	
	REP. CR. ACTS	REAL. CR. ACTS	REP. CR. ACTS	REAL. CR. ACTS	REP. CR. ACTS	REAL. CR. ACTS	REP. CR. ACTS	REAL. CR. ACTS	REP. CR. ACTS	REAL. CR. ACTS	REP. CR. ACTS	REAL. CR. ACTS	REP. CR. ACTS	REAL. CR. ACTS	REP. CR. ACTS	REAL. CR. ACTS	REP. CR. ACTS	REAL. CR. ACTS	REP. CR. ACTS	REAL. CR. ACTS
MURDER ART.123-127	59	46	65	41	75	57	56	38	53	44	51	41	42	32	36	32	36	33	40	33
Attempted Murder	34	31	70	54	69	56	64	56	64	56	49	43	59	54	43	36	47	44	39	37
Serious Body Injury Art.131	188	185	203	192	231	225	267	263	384	378	441	435	349	346	213	211	228	220	248	241
Endangering with Dangerous Tool while Fighting or Quarreling Art.133	84	82	103	101	133	130	125	123	169	169	122	120	142	140	138	138	152	152	157	153

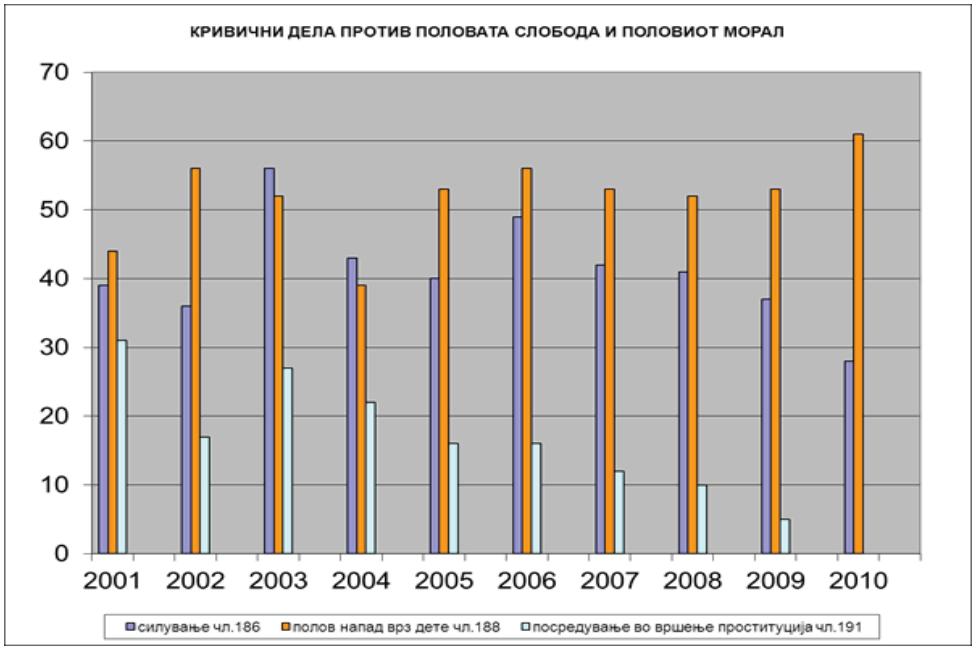
Source: www.moi.gov.mk



	2001		2002		2003		2004		2005		2006		2007		2008		2009		2010	
	REP. CR. ACTS	REAL. CR. ACTS	REP. CR. ACTS	REAL. CR. ACTS	REP. CR. ACTS	REAL. CR. ACTS	REP. CR. ACTS	REAL. CR. ACTS	REP. CR. ACTS	REAL. CR. ACTS	REP. CR. ACTS	REAL. CR. ACTS.	REP. CR. ACTS	REAL. CR. ACTS	REP. CR. ACTS	REAL. CR. ACTS	REP. CR. ACTS	REAL. CR. ACTS	REP. CR. ACTS	REAL. CR. ACTS
Illegal Deprive of Freedom Art.140	13	10	12	11	17	17	17	15	18	18	20	18	46	44	40	38	30	29	26	25
KIDNAPPING Art.141	6	4	20	6	18	12	29	22	24	20	24	17	30	24	14	13	16	13	17	13

Source: www.moi.gov.mk

	2001	**2002**	**2003**	**2004**	**2005**	**2006**	**2007**	**2008**	**2009**	**2010**
Rape Art.186 39	39	36	56	43	40	49	42	41	37	28
Sexual Abuse of Helpless Person Art.187	7	6	7	12	7	5	21	6	12	6
Sexual Attack on Child Art.188	44	56	52	39	53	56	53	52	53	61
Sexual Abuse with Breach of Duty Art.189	3	2	1	3	7	3	0	2	3	0
Mediating for soliciting Art.191	31	17	27	22	16	16	12	10	5	0
Incest Art.194	2	1	1	2	3	2	1	3	7	3

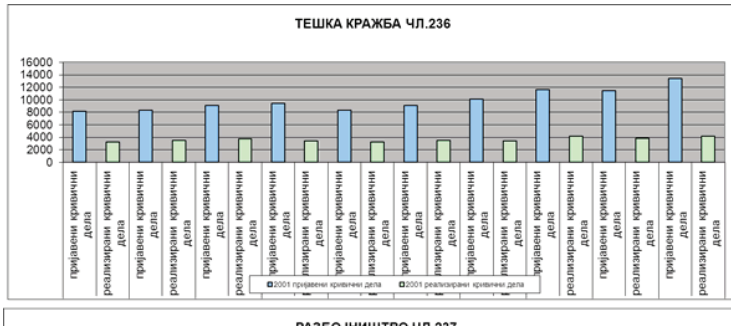


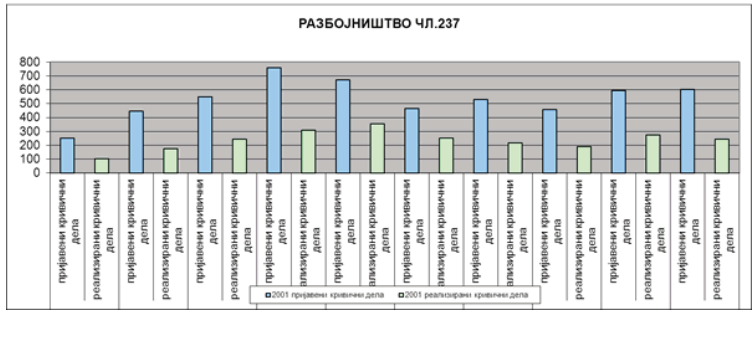
CRIMINAL ACTS AGAINST PROPERTY

Core of the general crime consists of crimes against property, and the most among them are serious thefts, thefts and robberies. In the period from 2001 to 2010, except 2005, the number of serious thefts is increasing steadily, while property offenses accompanied with violence or robberies until 2004 appear to be in an increase which reaches its maximum in 2004 with 758 robberies registered. In 2005 this negative trend was interrupted resulting in a decrease of 12% which continues in 2006, and in the coming years the situation is variable and is characterized by a slight decrease or increase of these deeds.

	2001		2002		2003		2004		2005		2006		2007		2008		2009		2010	
	REP. CR. ACTS	REAL. CR. ACTS	REP. CR. ACTS	REAL. CR. ACTS	REP. CR. ACTS	REAL. CR. ACTS	REP. CR. ACTS	REAL. CR. ACTS	REP. CR. ACTS	REAL. CR. ACTS	REP. CR. ACTS	REAL. CR. ACTS	REP. CR. ACTS	REAL. CR. ACTS	REP. CR. ACTS	REAL. CR. ACTS	REP. CR. ACTS	REAL. CR. ACTS	REP. CR. ACTS	REAL. CR. ACTS
THEFT ART.235	2542	1232	2983	1423	3624	1800	4003	1802	4513	2020	4669	2019	5530	2047	6046	2190	5137	1872	4896	1459
SERIOUS THEFT ART.236	8193	3267	8370	3542	9128	3777	9439	3453	8329	3244	9055	3534	10148	3429	11629	4192	11501	3853	13399	4204
ROBBERY ART.237	253	102	447	174	548	242	758	307	670	355	466	253	529	215	458	191	597	274	604	244
FRAUD ART.247	313	278	345	287	534	487	745	694	646	619	407	376	733	698	572	523	665	569	647	595
EXTORTION ART.258	11	11	25	22	30	18	31	21	43	35	20	15	29	27	32	26	35	32	28	21

Source: www.moi.gov.mk





MORE DISTINCTIVE CRIMINAL ACTS IN THE AREA OF ECONOMIC CRIME IN THE PERIOD 2001-2010

In the area of economic crime the most common crime is "abuse of official position and authority," which is mostly registered in 2003. It should be noted that since 2008 the number of detected offenses against computer crime and fraud in obtaining credit has increased.

	2001		2002		2003		2004		2005		2006		2007		2008		2009		2010	
	REG. CR. ACTS	REP. CR. ACTS	REG. CR. ACTS	REP. CR. ACTS	REG. CR. ACTS	REP. CR. ACTS.	REG. CR. ACTS	REP. CR. ACTS	REG. CR. ACTS	REP. CR. ACTS	REG. CR. ACTS	REP. CR. ACTS	REG. CR. ACTS	REP. CR. ACTS	REG. CR. ACTS	REP. CR. ACTS	REG. CR. ACTS	REP. CR. ACTS	REG. CR. ACTS	REP. CR. ACTS
ABUSE OF OFFICIAL POSITION AND AUTHORITY ART.353	168	200	178	221	854	1130	504	631	275	346	291	360	477	742	367	567	290	466	246	432
TAX EVASION ART.279	111	125	84	91	109	134	96	125	114	178	35	68	40	65	67	107	54	89	50	107
DAMAGE AND UNAUTHORIZED ENTRY IN A COMPUTER SYSTEM ART.251	-	-	2	2	1	3	7	7	2	1	2	4	7	11	20	30	63	73	36	43
FRAUD IN GETTING CREDIT OR OTHER CONVENIENCE ART.249	3	3	2	3	3	3	1	1	28	31	10	10	25	39	88	168	67	136	74	121

Source: www.moi.gov.mk

COOPERATION IN CRIMINAL CASES IN EU MEMBER COUNTRIES

By the Treaty of Amsterdam EU member countries introduced creation of the area of justice, freedom and security[3] in the Treaty on European Union, and thus offering the citizens of the Union a greater degree of safety. This objective should be achieved mainly in three ways: (1) through closer cooperation between the police, customs and other competent authorities of the EU member countries and by involvement of Europol, the European Police Office, (2) through closer cooperation between police authorities, (3) through harmonization of criminal law of the EU member countries. Last two areas are merged under the term "Cooperation in criminal cases" (meaning: cooperation in preventing and combating criminal acts).

The need for cooperation in these areas is justified by the progress in the European integration and serves as a measure for supporting the central concept in the realization of the European Community or the internal market. The opening of internal borders as a consequence of free movement of persons makes the necessary compensation for the gaps in the control and security caused by falling away of the border controls. Partial contribution to it can be made by contractually envisaged forms of cooperation in preventing and combating criminal offenses. Moreover, in the cooperation the supporting idea, freedom, as a fundamental goal of the European integration would lose its meaning if it could not be enjoyed in a legal space in which a citizen could count on its security and the rule of law in a country. [4]

JUDICIAL COOPERATION

Judicial cooperation in preventing and prosecuting criminal acts consists of two elements. First, cross-border prosecution of criminal acts should be facilitated through cooperation between the authorities for criminal prosecution. At the same time attention is paid, in particular, to recognition of decisions (for example, decisions about confiscation), facilitating extradition and, in general, to gradual harmonization of the law of criminal procedure. In this regard, introduction of the European arrest warrant is of essential importance. It will shorten the current procedure of delivery for 32 types of felonies. Cooperation of the judicial authorities is supported, inter alia, through the European Judicial Network and through the institution of "Eurojustice", created by a decision of 2002, which in severe criminal acts of cross-border context, coordinates and assists the investigation and prosecution. Second, after the entry into force of the Treaty of Amsterdam, the harmonization of substantive criminal law is treated in Articles 29 and 31 e in the third pillar. Now the Treaty explicitly mentions the establishment of regulations concerning the minimum elements for criminal acts and penalties for certain cross-border and serious offences. Meanwhile, these powers are used repeatedly by different framework decisions, first of all in the area of organized crime, terrorism and trafficking.[5]

---

[3] Article 29 of the Treaty of the European Union

[4] Werner Vajdenfeld Wolfgang Vesels, Rulebook in European integration

[5] Peter Graf Christian Miller Graf, Friedman Kajner "Europe from A to Z" pager.393

POLICE COOPERATION

In the framework of police cooperation in preventing and prosecuting the crime Europol is of utmost importance. The tasks of Europol are, in particular, combating illegal drug trafficking, illegal trade in radioactive and nuclear substances, smuggling emigrants, illegal trade in motor vehicles, trafficking, including sexual violence against children and the production and dissemination of child pornography, terrorism and forgery or money laundering. In this regard, the Service has a range of powers, in particular, exchange of information, development of crime analysis, providing experts and technical assistance in the investigation of the member countries and, finally, cooperation with third countries. In general, it appears that Europol mainly has function in the support and coordination, as well as limited operational functions that were supposed to be intensified in accordance with the provisions of the projected constitutional treaty. In addition, the Agency offers numerous other instruments to enhance the cooperation of national authorities or police authorities for criminal prosecution. Examples are the possibility of establishing joint investigating groups, offered by the framework decision of 2002 establishing the European Police Academy and the forms of police cooperation arising from the Convention implementing the Schengen agreement (among them the power to cross-border monitoring[6] and cross border pursuit[7], which means prosecution across state borders). In addition, the Schengen Information System is available to all police services, which in addition to the file with persons against whom a prohibition on entry has been pronounced, contains also file on investigations. By putting into operation of the upgraded Schengen Information System the information exchange should be improved, which is the core of police cooperation.

PERSPECTIVES AND CONCLUSION

Further development can be encouraged, especially from the challenges of fighting crime. In this regard, the adoption of additional legal acts is less necessary and the implementation of existing instruments is more necessary in all member countries. In short and medium term, the European Commission in its Green Paper on criminal procedure, sees the focus of the legislative activity primarily in the full realization of the principle of mutual recognition and in an appropriate creation of process guarantees for comprehensive providing of the basic rights associated with judiciary. In this regard there are specific initiatives of the Commission, for example, a proposal for a framework decision on European warrant to collect evidence that will greatly simplify the application for collecting evidence in other member countries.

Regarding the Treaty of Lisbon there is essentially a new impetus for integration according to the material areas. In particular, the opportunity should be given to form European Public Prosecutor, which as European prosecution authority could investigate and act before national courts. Thus, for the first time the

[6] Article 40 of the Convention implementing the Schengen Agreement
[7] Article 41 of the Convention implementing the Schengen Agreement

European officials would be entrusted essential state responsibilities that previously were reserved for their national sovereignty. Later the possibility of harmonization of the substantive criminal law and criminal procedure law would be extended.

On the basis of the above stated it could be concluded that the fight against crime requires cooperation between the states. Republic of Macedonia and the other countries from the Western Balkans that began the path to be full members of the European Union with all forces should aim to be soon part of the European family. European integrations, among other positive things they have, undoubtedly contribute to a better and more efficient fight against crime, because of the way the fight is carried out within the member countries and ideas that are planned for that fight to develop in the future. As before, so in the future, the Republic of Macedonia is firmly working towards becoming a full member of the European Union, and by that time it will greatly cooperate with all European institutions aiming at successful fight against crime.

REFERENCES:

1. www.moi.gov.mk
2. www.sep.gov.mk
3. Treaty on European Union from Amsterdam
4. Werner Vajdenfeld Wolfgang Vesels, Handbook of European integration
5. Christian Miller Peter Graf, Friedman Kajner “Europe from A to Z.”
6. Convention implementing the Schengen Agree

Prethodno saopštenje – UDK 351.74/.75:004.738.5(497.7)

ADEKVATNI KADAR U PODSISTEMU PRIVATNE BEZBEDNOSTI – FAKTOR USPEŠNOG SUZBIJANJA KRIMINALA U R. MAKEDONIJI

Mr Borče Petrevski
MUP R. Makedonije, borcepetrevski@zahoo.com
Mr Aleksandra Dimitrovska
dipl. psiholog, mr Fakulteta bezbednosti, sandrapsiho@zahoo.com

Apstrakt: Agencije za obezbeđenje osoba i imovine (AOOI) i detektivi, kao segmenti podsistema privatne bezbednosti u R. Makedoniji, imaju važan udeo u uspešnoj borbi sa kriminalitetom u jednoj savremenoj državi, osobito u delu njegove prevencije. Efektivni rad u svakoj instituciji, sektoru ili bilo kojoj organizaciji, pored adekvatno postavljene zakonske regulative o regulisanju konkretne delatnosti i tržišni rad, prije svega ovisi od adekvatne pripreme kadra koji neposredno deluje u okviru tog segmenta.

U R. Makedoniji, kao zemlji u tranziciji, postoje određena ograničenja u razvoju ovog dela ukupnog bezbednosnog sistema, kako s finansijskog, tako i sa stručnog aspekata.

Sa ciljem da se utvrdi stupanj razvijenosti podsistema privatne bezbednosti u R. Makedoniji, tačnije stanje, način funkcionisanja, stupanj implementacije EU standarda, način obuke i menadžiranje kadra, kao i način kontrole ovog društvenog segmenta, u 2010. godini sprovođeno je istraživanje na uzorku od: 20 menadžera AOOI, 309 radnika obezbeđenja, 2 predsednika komore za obezbeđenje, 2 predstavnika MUP-a, 123 korisnika usluge i 253 građanina R. Makedonije.

Rezultati pokazuju nedovoljan stupanj razvoja ovog bezbednosnog podsistema, osobito u poštovanju standarda i nivou obučenosti kadra. U radu će biti razrađeno stanje, kao i dati predlozi u pravcu unapređenja podsistema privatne bezbednosti.

Ključne reči: privatna bezbednost, kadar, edukacija, standardizacija, bezbednost

UVOD

Privatni bezbednosni podsistem (PBP) kao deo ukupnog bezbednosnog sistema (BS) ima važan udeo u sveukupnoj bezbednosti R. Makedonije (RM) kao zemlje u tranziciji, koji proces povlači postepenu decentralizaciju pojedinih nadležnosti iz javne ka privatnoj bezbednosti. Pod privatnom bezbednosti (PB) podrazumeva se "planska, organizovana i zakonski zasnovana, samostalna ili zajednička delatnost i funkcija pojedinaca, preduzeća, privatnih i/ili profesionalnih agencija, usmerena ka sopstvenoj zaštiti ili zaštiti drugih, kao i zaštiti relevantnih osoba, prostora, objekata, poslovanja ili delatnosti, a koje nisu pokrivene ekskluzivnom zaštitom državnih organa."[1] Dakle, dok se državni bezbednosni sistem

[1] Stajić, Lj. (2008). *Osnovi sistema bezbednosti*. Pravni fakultet, Novi Sad.

(DBS) sve više fokusira na ukupne bezbednosne situacije u zemlji i asimetrične pretnje međunarodnog karaktera, ovlaščenja temelji na osnovu prava i obaveza države da krivično goni i kazni počinioce nezakonitog ponašanja, prioritetno štiti društvene interese i deluje preventivno i represivno, PBP-u ostaju interna i lokalna stanja i problema, ovlašćenja zasnova na pravu pojedinca na ličnu zaštitu, koje prenosi u skladu sa ugovorom sa AOOI ili detektiva, štiti privatni interes ili interes klijenta, oni prvenstveno preduzimaju preventivne mere usmerene da spreče različite oblike ugrožavanja ljudi i imovine.[2] Naime, u nadležnosti AOOI, subjekat PBP u RM jesu: obezbeđivanje ljudi, objekata i imovine, stražarsko-portirska služba (obezbeđivanje i kontrola pristupa), zaštita objekata uz pomoć tehničkih sredstava, zaštita podataka koji su poslovna tajna, itd. Pri tome, prekoračenja ovlašćenja, a naročito mogućnost primene sredstava prinude od strane AOOI, može izazvati ozbiljne poremećaje i negativne posledice u smislu kršenja ljudskih prava i sloboda, koja zahtevaju čvrstu kontrolu nadzora aktivnosti i strogo zakonsko definisanje forme, način, intenziteta i uslova njihove primene.

U tom smislu, uočljiva je važnost relevantnosti osoblja u okviru PBP i ukupnog BS, utvrđeno u uslovima trenutnog stupnja razvoja RM kao jedne od zemalja u tranziciji i niskih ekonomskih mogućnosti, gde su standardi u svim društvenim segmentima na niskom nivou.

Zakonska regulativa i subjekti PBP u RM

Zakonske norme koje pokrivaju PBP u RM, smeštene su u: Ustavu RM, Krivičnom zakoniku, Zakonu o krivičnom postupku, Zakonu o unutrašnjim poslovima, Zakonu o policiji, Zakonu o obezbeđenju osoba i imovine (ZOOI), Zakonu o detektivskoj delatnosti, Zakonu o oružju, Zakonu o zaštiti i spasavanju, Zakonu o požarnikarstvu, Statutu Komore RM o obezbeđenju osoba i imovine, kao i drugoj podzakonskoj regulativi u oblasti obezbeđenja i vršenja detektivske delatnosti.

Subjekti PBP-a u RM jesu:AOOI (kao pravna lica registrovana za pružanje usluga ili za vlastite potrebe), Komora RM za obezbeđenje osoba i imovine, detektivi i Ministarstvo unutrašnjih poslova (MUP).

1. *AOOI* se registrira za redovni rad upisom u Centralnom registru i shodno ZOOI[3]. Pored opštih, nužno je ispunjavanje i posebnih uslova: najmanje 10 osoba zaposlenih u redovni radni odnos, sa dobijenom licencom za vršenje poslova obezbeđenja osoba i imovine[4] i legitimacijom za

---

[2] Спасески Ј., Аслимоски П., Герасимоски С., *Приватна безбедност*. Коста Абраш – Охрид, 2008, стр.32.

[3] Zakon o obezbeđenju osobe i imovine, Sl. novine R. Makedonija br. 80/99, Izmene i dopune Zakona, Sl. novine br. 66/07, Ispravke zakona, Sl. novine br. 84/07, Prečišćen tekst Zakona, septembar 2010. g.

[4] Potrebni uslovi za dobijanje licence jesu: da je osoba državljanin RM, da ima prebivalište u RM, pravosnažnom presudom da joj nije izrečena mjera bezbednosti – zabrana obavljanja profesije, delatnosti ili dužnosti, da ima završeno najmanje srednje obrazovanje, dve godine pre dobijanja licence da nije obavljala poslove u oblasti bezbednosti i odbrane kao ovlašćena službena osoba i položila je stručni ispit (koji se sastoji od teoretskog i praktičnog dela); polaže se pred Komisijom imenovanom od ministra unutrašnjih poslova, sastavljenom od osoba zaposlenih u MUP-u i angažovanih od strane Komore.

obezbeđenje[5] (izdata od Komore), kao i dozvola za rad pravnog lice – AOOI (izdata od MUP-a RM). Osnivač AOOI može biti domaće (pravno ili fizičko) lice. U RM postoji oko 180 registrovanih AOOI, od kojih aktivno rade oko 50, izdato je oko 16.100 licenci i oko 5.100 službenih legitimacija.

2. *Komora* RM za obezbeđenje osoba i imovine formirana je u junu 2000. g., čija delatnost je usmerena uspešnijem organizovanju obezbeđenja osoba i imovine, unapređenju stručnosti, profesionalnosti i poslovnosti u delatnosti, kao i zaštiti same profesije, pri čemu je uslov za formiranje udruživanje najmanje 10 pravnih subjekata.[6] U periodu 2006–2010. g. funkcionirala je i Komora za obezbeđenje osoba i imovine „Detektiv Skoplje" i izdavala je licence za obezbeđivanje bez dobijenog odobrenja iz MUP-a.[7] U okviru svojih nadležnosti, Komora organizira polaganje stručnog ispita budućih radnika obezbeđenja, izdaje licence i legitimacije, vodi evidencije pravnih osoba koje obavljaju delatnost – obezbeđenje osoba i imovine, vodi evidenciju radnika koji imaju licence i legitimacije, i vrši druge poslova. Isto tako, Komora vodi posebnu brigu o obezbeđivanju uslova ispravnog, uspešnog i nezavisnog vršenja poslova obezbeđenja, zaštiti predmeta rada, javnih i službenih ovlašćenja. U dosadašnjem radu, na planu inplementacije zakonske odredbe, Komora svoju aktivnost ostvaruje organizovanjem međunarodnih konferencija i radionica, izdavanjem linence i legitimacije za rad, izdavanjem stručne literature i novina, održavanjem godišnih sastanaka itd., i u 2011. god. aktivno je uključena u izradu novog ZOOI, čije predlog izmena koprespondira sa zaključcima i predlozima ovog istrazivanja, a deo njih su i predlozi ovog rada.

3. *Detektivsku delatnost* u RM može obavljati samo detektiv koji poseduje licencu za obavljanje delatnosti detektiva, izdatu od strane MUP-a RM.[8] Prema raspoloživim podacima, ova vrsta aktivnosti u našoj zemlji praktično je implementirana u 2011. g., i do sada je registrovano samo 5 privatnih detektiva[9]. Razlozi za to su vrlo strogi uslovi za dobijanje dozvola izraženi kroz: visok iznos na osiguranje od odgovornosti za štetu ka klijentu ili trećem licu prouzrokovanu u vršenju detektivskog rada, teški i naporan trening i relativno visoke cene usluge. Ovo ima za posledicu nelegalno obavljanje detektivske delatnosti od pojedinih AOOI ili drugih osoba sa

---

[5] Za dobijanje legitimacije, pored potvrde o nepostojanju zabrane poslovanja, potrebno je i lekarsko uverenje o opštom zdravstenom stanju.

[6] Statut Komore Republike Makedonije o obezbeđenju osobe i imovine, od 15.03.2011 g.

[7] U julu 2010 g. predsednik Komore i 15 članova Ispitne komisije osuđeni su za nezakonito izdavanje licence o obezbeđenju, a Komora je prestala da funkcioniše, zbog kojih razloga rezultati dobijeni iz intervjua sa njenim predsednikom nisu prikazani u radu .

[8] Pored opštih uslova za uspostavljivanje radnog odnosa, detektiv mora pored već navođenih uslova za dobijanje licence za obezbeđenje, da ima i: završeno visoko obrazovanje, da uživa ugled za obavljanje detektivskog rada, tj. svojim dosadašnjim načinom života, ponašanja i rada da garantuje da će savesno i pošteno obavljati detektivsku delatnost, kao i da je položio stručni ispit.

[9] Zakon o detektivskoj delatnosti, Sl. novine R. Makedonija br. 80/99, Izmene i dopune Zakona, Sl. novine br. 66/07, Dopune Zakona, Sl. novine br. 86/08, Izmene i dopune Zakona, Sl. novine br. 51/11.

iskustvom (bivši zaposleni u bezbednosnim ili policijskim institucijama) motivisani određenom finansijskom nadoknadom, protivuslugama, itd.

4. Kontrolu i nadzor nad PBP obavlja *MUP*. Pri tome, upravnopravni nadzor[10] je u nadležnosti Odseka za oružje, eksplozivne i opasne materije[11], „kao sastavne jedinice Odeljenja za upravne poslove pri SUP Skoplje, dok su slučajevi prekoračenja ovlašćenja u nadležnosti lokalnih policijskih stanica (PS)[12]. Do sada u RM zbog nepravilnosti u radu nije zatvorena nijedna AOOI i nijedna licenca nije oduzeta.

Opis nadležnosti AOOI-a i ovlašćenja radnika obezbeđenja

Delatnostima obezbeđenja osobe i imovine, uslovima propisanim zakonom, bave se pravne osobe registrovane za tu delatnost tj. AOOI, i to u obliku pružanja usluga, i pravne osobe koje to obavljaju za vlastite potrebe. Ove delatnosti mogu se obavljati kao: *fizičko* bezbeđivanje osoba za njihovu osobnu zaštitu i obezbeđivanje imovine od pristupa nepozvanih osoba, uništavanja, oštećenja, nezakonitog oduzimanja i drugih oblika štetnog delovanja[13]; i *tehničko* obezbeđivanje osoba i imovine tehičkim sredstvima i ureda po propisanim standardima.

Pri obavljanju ove delatnosti, radnici obezbeđenja imaju slična ovlašćenja[14] kao i policijski sluzbenici, ali u odnosu na njih u ZOOI-u broj ovlašćenja je manji, ogranicena su samo na prostor koji se obezbeđuje (osoba, imovina, novac i dr. dragocenosti); ali i nisu detaljno precizirana i razrađena u podzakonskim aktima,

---

[10] Ta kontrola se sastoji od uvida u dokumentaciju AOOI-provere njihovih registracija, provere licence i legitimacije, kontrole posedovanja i skladištenja vatrenog oružja i opasnih materija, eksploziva itd.

[11] Redovne obaveze ovog Odseka jesu: izlazak na mesto događaja u slučaju nastalog požara, kontrola objekata i skladišta koja raspolažu oružjem i eksplozivnim materijama, izdavanje saglasnosti za benzinske pumpe, rezervoare, gasne uređaje itd., kao i kontrola nad poslovanjem AOOI.

[12] Koji u svakom pojedinačnom slučaju odlučuju po svojoj proceni, na osnovu prethodno dostavljenog izveštaja AOOI o primeni sredstava prinude. Ukoliko se od strane rukovodnih službenih osoba u PS proceni da je primena bila neopravdana, podnosi se odgovarajuća prekršajna ili krivična prijava. Istovremeno, o primeni i rezultatima postupanja nadležne PS, pismeno se obaveštava Komesarijat za javni red i mir (JRM) u SUP Skoplje, koji dalje obaveštava Sektor policije u Birou za javnu bezbednost (BJB).

[13] To podrazumeva zaštitu od: 1. direktnog napada koji ugrožava život radnika obezbeđenja ili osobe koja se štiti, za što se smatra svaki fizički napad na način ili sredstvom (oružjem, opasnim oruđem ili drugim sličnim predmetom kojim se može ugroziti život) koje predstavlja neposrednu opasnost po život, kao i 2. direktan čin napada kojim se ugrožava imovina koja se štiti, što uključuje bilo kakvu radnju usmerenu ka nezakonitom oduzimanju imovine, oštećenju ili uništenju objekata, kao i propadanju i uništenju uređaja u objektu, čime se prouzrokuje materijalna šteta (sabotaže, diverzije).

[14] 1) utvrđivanje identiteta osobe koje ulaze ili izlaze iz imovine koja se obezbeđuje, 2) upozoravanje osoba da se udalje sa imovine koja se obezbeđuje, pod uslovom da se neovlašćeno zadržavaju u njoj, 3) ne dozvoljava ulaz nepozvane osobe u imovinu koja se obezbeđuje; 4) prijavljivanje i isporuka policiji osobe zatečene u vršenju krivičnog dela koje se goni po službenoj dužnosti, 5) nedozvoljavanje ulaza/izlaza vozila ili osoba sa prtljagom kada je potrebno da se pregleda vozilo ili prtljag, a vozač to onemogućava, 6) nedozvoljavanje neovlašćenog snimanja ili unošenja sredstava i opreme za tu svrhu; 7) obavljanje kontrole i mera zaštite i izveštavanje o nastalom požaru, eksploziji ili drugim katastrofama; 8) obavljanje bezbednosno-tehničke zaštite pravnog lica; 9) obavljanje lično-tehničke zaštite osoba, 10) obavljanje obezbeđivanja transporta novca i drugih dragocenosti ili poverljivih dokumenata pravnog lica; 11) primena fizičke snage i vatrenog oružja, samo kada je to neophodno za postizanje zadataka, sve do dolaska policije: 12) korišćenje posebno obučenog psa pri odbijanju neposrednog napada na radnika obezbeđenja ili na osobu ili imovinu koja se štiti.

zbog čega je njihova primena u praksi ostavljena AOOI i njihovoj slobodnoj proceni, što dovodi do većeg broja dilema i praktičnih problema. Zakonski obavezna obuka radnika AOOI-ja traje kraće i na nižem je nivou kvaliteta u odnosu na one u MUP-u, s obzirom na kraće vreme postojanja PBP-a, finansijske mogućnosti države i domen aktivnosti razvijenih do sad u ovom podsistemu, što povećava potrebu dopunske obuke pre i u toku poslovanja. Ali, s druge strane, ova delatnost ima više rizika i nepredviđenih situacija, što zahteva posebne predispozicije kod radnika, njihovu obučenost i kompetentnost, sa aspekta prirode posla koja pretpostavlja široku paletu situacija u kojima radnik treba brzo doneti adekvatnu odluku i adekvatno odreagovati, uzimajući u obzir i ovlašćenja koja su mu propisana u ZOOI-ju. U tom pravcu, kao i kod policijskih službenika, greške u procenama treba svesti na minimum, zbog razloga što su štetne kako za pojedinaca, tako i za kolege, građane i imovinu koja se štiti, s obzirom na to što su između ostalog, radnici AOOI-a ovlašćeni i za primenu fizičke snage, vatrenog oružja[15] i upotrebu dresiranog psa.

Sve ovo je pokazatelj potrebe adekvatnosti sistema i programa obuke, ispitivanja, ocenjivanja, selekcije i kontrole kadra, sa ciljem uspešnog sprovođenja njegove delatnosti, i pored toga što ovisi o više globalnih faktora, kako ekonomskog stanja države, stupnja razvijenosti PBP-a u RM, odnosa MUP-a, sudskih organa i Komore sa AOOI-jem, kao i zakonske regulative kojem se preciziraju okviri ove delatnosti.

Obuka, sistem izdavanja licenci i selekcija

Saglasno sadašnjem sistemu, obuka za dobijanje licence za obezbeđivanje sprovodi se po propisanom programu[16], koji se sastoji od 40 časova (34 teoretske i 6 časova praktične) nastave, koju obavljaju policijski sluzbenici MUP-a – instruktori, imenovani rešenjem ministra unutrašnjih poslova. Ispitivanje pri polaganju stručnog ispita sprovodi petočlana Komisija, išto tako imenovana rešenjem ministra, sastavljena od tri člana iz MUP-a i dva člana na predlog Komore. Uslovi za izbor ovih osoba su da imaju najmanje završeno visoko obrazovanje i odgovarajuće stručno iskustvo iz oblasti obezbeđenja.

Proveru osposobljenosti za rukovanje vatrenim oružjem, kao deo stručnog ispita, obavlja Komisija MUP-a sastavljena od policijskih službenika u uniformi. Program i način polaganja stručnog ispita, kao i osposobljavanje fizičkih osoba i obrazac licence za rad propisuje ministar unutrašnjih poslova.

Pri tome, s obzirom na to da su radnici iz ove oblasti ovlašćeni da koriste sredstava prinude, logična je potreba prethodne procene psihološke podobnosti kadra, koja je zakonski propisana u formi obaveznog lekarskog pregleda, ali praktično se sprovodi samo strogo formalno, tako da ukupna odgovornost za selekciju kadra preostaje AOOI-jima, od kojih samo jedam deo smatra potrebnim angažovati i stručno lice (psihologa) za selekciju kadra.

S druge strane, sama delatnost pretpostavlja niz različitih situacija koje traže adekvatne reakcije, kao i potrebu posebnih vrsta obezbeđenja (npr. transport novca, patrolno obezbeđenje, bodigard itd.) koje zahtevaju posebne doobuke

[15] Zakon o oružju (Neoficijelni prečišćen tekst) od 06.10.2010 g.

[16] Pravilnik o programu i načinu polaganja stručnog ispita i osposobljavanju fizičkih osoba za obavljanja poslova obezbeđenja osoba i imovine, Sl. novine br. 46/08.

i specijalizacije, koje nisu uključene u program i ostavljene su za obuku samim AOOI-jima.

Saglasno specifičnosti ove delatnosti, postavlja se pitanje *u kojoj meri je ova obuka dovoljna za uspešno sprovođenje radnih zadataka u praksi; koliki je procenat psihološki nepodobnih osoba koje su stekle licencu i rade u ovom bezbednosnog segmentu; koliko ovaj sistem obuke može odgovoriti specifičnim tipovima obezbeđenja i doobuke; u kojoj meri sistem kontrole je adekvatan i može odgovoriti uspešnoj detekciji nepravilnosti koje se dešavaju u ovom sektoru; ukratko, koliki je stepen adekvatnosti kadra angažovanog u ovom segmentu i koliki su rizik i posledice eventualnih nepravilnosti pri realizaciji radnih angažmanima?*

METODOLOGIJA

Uzorak: Uzorak se sastoji od šest grupa ispitanika: 309 radnika obezbeđenja, 20 menadžera AOOI-ja, dvojice predsednika komore obezbeđenja, dvojice predstavnika MUP-a zaduženih za kontrolu, 123 korisnika usluga i 253 građanina RM. Istraživanje je sprovođeno u periodu mart–juni 2010. godine.

Cilj: Utvrđivanje adekvatnosti kadra angažovanog u PBP u RM i davanje predloga strategije za njegovo unapređivanje i osposobljavanje prema standardima CoESS-a.

Hipoteza: Potrebno je unapređivanje kvaliteta i kompetentnosti kadra u PBP u RM, sa aspekta selekcije, obuke i sprovodenja zadataka, za šta su neophodne su promene u zakonskoj regulativi, praktičnoj implementaciji i adekvatnoj kontroli.

Instrumenti i metodi. Intervju i upitnik sa 65 pitanja.

Statistika i analiza. Deskriptivne statističke metode: frekvencije i procenti.

REZULTATI I DISKUSIJA

1. Sa ciljem ***opisa kadra*** koji radi u AOOI-ju, na osnovu uzorka obuhvaćenog istraživanjem, možemo zaključiti da su pripadnici:

- *muškarci* (95% radnika i menadžera i predstavnika Komore i MUP-a)
- najzastupljena *uzrasna kategorija* kod radnika je 21–30 godina (44,66%), a код menadžera su jednako zastupljene sve tri kategorije 31–40, 41–50 i iznad 50 godina (po 30%), tj. sa uzrastom proporcionalno raste i pozicija u AOOI
- najveći dio radnika su sa srednjem (87,06%), a menadžera sa visokim (60%) ili višom (15%) školom, tj. sa *stupnjem obrazovanja* raste i pozicija u AOOI
- najveći deo radnika (49,84%) i menadžera (55%) je sa *radnim* stažom od 3 do 10 godina, ali pri tom, za razliku od ostalih, kod radnika dominira iskustvo do 3 godine (41,10%), a kod menadžera iznad 10 godina (35%), što znači da je jedan od uslova za menadžiranje u ovoj delatnosti praktično iskustvo iz oblasti
- iako je kod radnika veliki broj osoba bez *prethodnog radnog iskustva* u drugim institucijama (45,63%), a kod menadžera iskustva u MUP-u i ARM (45%), i kod radnika (54,37%) i kod menadžera (75%) preovladuju oni sa prethodnim iskustvom u odnosu na one bez iskustva. To znači da iskustvo

u državnim bezbednosnim i ostalim institucijama, menadžere stavlja u funkciju sticanja i realizacije pozicija u PBP, ali se one izjašnjavaju da iskustvo u državnim bezbednosnim institucijama kod njihovog kadra nije prednost pri zapošljavanju, niti pri uživanju beneficija ili statusa. Obrazloženje za to je da je za njih jednostavnije obučavanje radnika ispočetka po standardima AOOI, nego preobuka bivših radnika MUP-a i ARM, koji imaju veće zahteve u pogledu uslova i plata, a da pri tom nisu dovoljno obučeni i adaptirani. Tome u prilog je postojanje iskustva iz *dopunskih kurseva van obuke* za licencu, tj. 67,64% radnika ih nema, a 75% menadžera ih je prošlo.

2. U odnosu na ***stupana poznavanja i adekvatne primene postojećih zakonskih ovlašćenja*** (i pored toga što postoji nekoliko ovlašćenja koja su saglasna standardu, i kod nas ih radnici primenjuju nezavisno od toga što su u zakonu izostavljeni, kao: naređivanje, zadržavanje, upotreba drugih sredstava prinude itd.), radnici pokazuju nedovoljno poznavanje, razgraničenje, dileme ili prekoračenja najviše u odnosu na "teška" ovlašćenja, a shodno tome možemo i zaključiti da nedostaje adekvatna obuka. U prilog tome su u sledeći rezultati:

- 89,64% radnika pokazuje praktičnu primenu detaljnog nasuprot površnog pretraživanja pri sprovođenju *pregleda osobe, stvari, vozila i prtljaga*, što u suštini predstavlja pretres, a za šta prema ZOOI-a radnici u AOOI nisu ovlašćeni, tj. pretres isključivo vrše ovlašćena lica iz MUP-a.
- i pored toga što u ZOOI-u nije precizirano u kojim situacijama su radnici ovlašćeni primeniti *fizičku snagu i vatreno oružje* (osobito termin „kad je to neophodno potrebno" i „ukoliko se na drugi način ne može odbiti neposredan napad"), samo 23,95% jasno pravi razliku kad i šta primeniti, sa čime su saglasni i menadžeri. Nasuprot tome, 85,44% radnika izjašnjava se da nisu bili u dilemi šta upotrebiti, dok 75% menadžera to negira. To može značiti da radnici nisu svesni postojanja dileme iz razloga što se nisu suocili sa takvom situacijom, a osobito zbog toga što veći broj AOOI-a ne dozvoljava nošenje i korišćenja oružja, ili radnici prikrivaju dilemu oko ovoga, na što ukazuje suprotni stav menadžera. U prilog tome je i predlog o njihovom dopreciziranju u ZOOI ili podzakonskim aktima, kao i povećana obuka i tom delu. Kao glavni razlog tome menadžeri navode neadekvatne procene, koje pre svega ovise od dispozicija ličnosti, ali i iz iskustva i adekvatne obuke radnika.
- Postojanje *prekoračenja ovlašćenja radnika* AOOI-a potvrđuje i Komora, nasuprot službenim licima iz MUP-a za kontrolu i nadzor koja to negiraju, ili menadžerim kod kojih postoji podvojen stav (50%), ali za ovo je važan razlog i nekoordinacija službenih lica MUP-a sa lokalnim PS, zaduženim za otkrivanje krivičnih dela, među kojima i prekoračenja ovlašćenja, gde se radnici tretiraju kao obični građani.

3. ***Obuka*** kao jedan od ključnih faktora za kvalitetno obavljanje ove vrste usluga u većem broju nedostaje kod AOOI u RM, što i pored ekonomskog i finansijskog stanja države i AOOI, ovisi i od neadekvatne postavljenosti sistema obuke za licenciranje i kontrolu MUP-a, u AOOI-u. To potvrđuju sledeći rezultati:

- Prema 82.52 % radnika i 100% menadžera, u AOOI-u su *zaposljeni i neadekvatni kadrovi.* Dok radnici kao *najvažniji razlog* za to ističu:

neprofesionalno ponašanje (44,01%) i fizičku nespremnost (43.37%); menadžeri – zapošljavanje osoba iz kriminalnih sredina (70%) i neprofesionalno ponašanje (55%), psihološku nesposobnost osoba u AOOI (25%), kao i zapošljavanje osoba bez licence (25%). Ovo može implicirati negativne reperkusije po bezbednosti, pa u tom smislu, sve je više izdržan stav o potrebi strogo selektivnim pristupom izdavanja licenca pru zapošljavanju u AOOI i dodeljivanje konkretnih obaveza na poslu.

- 68,93 % radnika i 95% menadžera veruje da postojeći *kriterijumi za izdavanje licenci* za obezbeđivanje dozvoljavaju i nekompetentnim osobama da dobiju pravo obavljanja delatnosti, a 100% svih ispitanika smatra da bi trebalo uspostaviti standarde o tome ko bi mogao biti uključen u obuku kao instructor.
- 91.26 % radnika veruje da je *obuka efiktivna ili delimično efektivna*, nasuprot 90% menadžera, prema kojima je obuka delimično neefektivna i 95% njih smatra da njen kvalitet treba da bude bolji. Kao najvažniji faktori za efektivnu obuku navode se: potreba praktičnog rada kroz primere (76,70 % radnika i 75% menadžera), kao i potreba veće kompetencije osoba koje izvode obuku (21.68% radnika ei 55% menadžera)
- U pogledu ocenjivanja *efikasnostiz provere znanja*, kod obe grupe ispitanika kao najvažniji faktor je naveđen neadekvatni kriterijum ocenjivanja, što znači dobijanje licence bez potrebnog nivoa znanja (47.25 % radnika i 45% menadžera). Naglašava se i potreba većeg uključivanja pitanja vezanih za rešavanje praktičnih problema i simulacije realnih situacija, kao dela testa, kao i višeg stupnja kompetentnosti članova Komisije za ispitivanje.
- Što se tiče predloga o uvođenju *seminara i debate* kao stalne prakse u radu AOOI-ja, s čime se slažu sve grupe ispitanika, menadžeri ukazuju na to da: oni ne treba da budu samo forma i "parada", da ih treba organizovati u kontinuitetu; teme da proizlaze iz AOOI-a, da su zastupljeniji slučajevi i problemi iz prakse, propisan obavezni transfer znanja i aktuelnih informacija do najnižeg nivoa radnika u AOOI; više literature, organizovanje obuke i u drugim gradovima u RM; povećanje učešća naših predstavnika na međunarodnim seminarima u cilju korišćenja iskustava država iz našeg regiona, povećanje učešća eksperata iz nauke i MUP-a na seminarima, kako bi kao gosti razmenili mišljenja o problemima sa pravnog, praktičnog i naučnog aspekata. Prema njima, za sve ovo presudni značaj ima Komora, koja je u osnovi organizator i nosilac ove vrste aktivnosti u domenu PBP.

4. ***Odnos Komore prema AOOI-a*** ima presudan uticaj na kvalitet rada i nivo razvoja PBP u RM, saglasno njenoj ulozi – unapređenje profesionalnosti, stručnosti i poslovnosti rada AOOI-na. Njenim efikasnom funkcionisanjem omogućava se zaštita prava i realizacija potreba AOOI-ja nasuprot DBS, što je ključni preduslov za unapređenje njihovog poslovanja, a što uključuje adekvatnost osoblja u AOOI-ju. I pored toga što Komora ne odlučuje o sistemu obuke i proceni kompetentnosti osoblja, u njenom domenu je borba za promjene u ZOOI-u i odnosu sa MUP-om u cilju približavanja ovog segmenta standardima EU. U tom pravcu, iako generalno postoji zadovoljstvo kod 70% menadžera, pre svega zbog: korektnosti u ponašanju,

blagovremenosti u izveštavanju, pružanju potrebnih informacija, dostave druge dokumentacije, itd., postoje i primjedbe u odnosu na: potrebu za bržim promenama u ZOOI i donošenje podzakonskih akata saglasno trenutnim problemima, pomoć oko nelojalne konkurencije između AOOI-a kao jedne od glavnih prepreka za razvoj ove delatnosti, ravnopravni tretman, osobito kod zahteva manjih AOOI-a, itd. Sve ovo ima veliki značaj za AOOI mogućnosti izgradnje adekvatnog bezbednosnog osoblja u ovom segmentu.

5. ***Kontrola nad poslovanjem AOOI-a***, kao filter nepravilnosti u poslovanju, koje su jedna od glavnih prepreka u razvoju PBP-a, na posredan nacin utiče na uspešnost AOOI-a u izgradnji adekvatnog kadra u ovom društvenom segmentu. Rezultati pokazuju neefektivnost postojećeg sistema kontrole AOOI-a i potrebu aktivnijeg angažmana MUP-a kao jedan od preduslova za razvoj ovog podsistema i to:

- *retko* se obavlja – nekoliko puta godišnje, samo u slučajevima dojave ili anonimnih prijava da neka AOOI radi nezakonski, ali pri toga izostaje detektiranje AOOI-a koji nisu registrovani ili radnici nemaju službene legitimacije, a koji postoje u određenoj meri i niko ih ne prijavljuje. Nepravilni rad potvrđuju radnici koji se izjašnjavaju da pojedine AOOI obavljaju nelegalne aktivnosti, i to: neovlašćeno primenjuju sredstava za prisluškivanje i snimanje u poslovanju (46,28%), nelegalno prate osoba i vozila (64,40%), bave se "reketom" (59,87%) i nelegalno rade (71,84%). Ovo potvrđuje i 60,87% građana, koji su odgovorili da postoje i AOOI koji u celini ne rade ispravno, a kao razlozi za to su sledeći: nedovoljno obučen kadar i neuspostavljenost standarda u PBP. Ovo je još jedan pokazatelj o postojanju nelojalne konkurencije kao faktora o smanjenja kvaliteta, a time i cena usluga, što podrazumeva pogrešan pravac razvoja PBP-a.
- obavlja se kao sporedni rad ili sa drugačijim ciljevima, tj. 95% menadžera i 46,61% radnika izjašnjavaju se da se kontrola vrši selektivno i samo formalno.
- sve grupe ispitanika navode potrebu uvođenja kriterijuma i standarda za osobe ovlašćene u MUP-u za kontrolu rada AOOI, a kao kriterijume predlažu: inspektori da poseduju posebnu licencu za obavljanje kontrole, adekvatno stručno teoretsko i praktično znanje iz oblasti, detaljno poznavanje AOLI-a i drugih zakona i podzakonskih akata vezanih za delatnost, da budu poštene osobe i istovremeno da ne rade i druge zadatke u MUP-u.

6. Postojeća z***akonska regulativa*** kao okvir nadležnosti i prostor u kome država propisuje uslove kretanja i promjene u ovom segmntu, može se reći da je pored finansijskog stanja, jedini materijalni pokazatelj stupnja razvoja svesti i približavanja standardima i normama u PBP onima iz EU. To određuje meru u kojoj se omogućava adekvatnim subjektima u PBP da obavljaju adekvatne angažmane, između ostalog i za unapređenje kadrova, ali sa druge strane, i pored prilagođivanja AOOI-a CoESS-u (Europska konfederacija PB), problemi još uvek ostaju na praktičnom nivou i u finansijskom aspektu. U tom pravcu, i pored toga što je 95% menadžera odgovorilo u prilog ukupnom usaglašavanju propisa, sa ciljem lakšeg prilagođavanja standardima pre ulaska RM u EU i povećanja kvaliteta poslovanja,

u RM još uvek ne postoje institucionalni preduslovi za to. Sa ovakvom adaptacijom slažu se i Komora i MUP, s tim što i pored toga što RM zasad nema obavezu da primenjuje direktive CoESS-a, fakat da smo pridruženi clan CoESS-a upućuje na to da standarde treba primenjivati, ali sa komentarom za eventualno delimično usaglašavanje, pre svega zbog slabog ekonomskog stanja države.

Kao što smo već rekli, zakonska regulativa pokriva sve dosadašnje domene PBP-a, kako ovlašćenja, obuke i kontrole, tako i da pored prepreka u ovim domenima iz praktičnog aspekta, koje smo već spomenuli, njih treba i zakonski pokriti, što ukazuje na potrebu adekvatnih promena AOOI-a. Takve promene u ovom momentu su u fazi parlamentarne procedure, i pored toga što, ne može se reći da bi takvim izmenama svi propusti bili anulirani.

1. Pored ZOOI-a kao pravnog okvira, glavni preduslov sa ekonomskog aspekata je nivo razvoja privrede u državi, što direktno utiče na ***način menađiranja AOOI-a*** i kadrove u njima, kao uslov nihovog efektivnog poslovanja. Kao što smo već napomenuli, nelojalna konkurencija je jedan od glavnih negativnih faktora kvaliteta u poslovanju u ovom segmentu, pa time adekvatnost menadžerskog kadra, osobito njegova kompetentnost, obučenost i finansijska potpora mogu smanjiti negativnosti povezane sa stupnjem razvoja jedne države u tranziciji kao što je RM.

Nasuprot zadovoljstvu radnika svojim poslom (96,44%), kao i poslovanjem menadžera (72,49%), koje proizlazi iz: redovnosti mesečnih prihoda, dobrih radnih uslova, postojane nadgradnje i razvoja u AOOI, discipline i saradnje među kolegama; 23,30% njih izrazilo je delimično ili ukupno nezadovoljstvo menadžiranjem, i to zbog: neadekvatnosti menadžerskog kadra, prijema nekompetentnih i neobučenih osoba, niske plate, nemanje mogucnosti za napredak u karijeri, favorizovanja nekvalitetnog kadra, omogućavanja privilegija pojedinim radnicima, neadekvatnih uslova u prostorijama za rad, neprofesionalizma u radu, nedovoljne informisanosti, neadekvatnih materijalno-tehničkih sredstava za rad, nebrige o zaposlenima itd. U tom pravcu, najveći dio radnika (58,90%), kao i 60% menadžera izjavili su da niske plate, naspram odgovornog posla, uzimaju kao prioritetni faktor koji negativno utiče na uspeh menadžiranja. Prema radnicima, na drugom mestu je nedovoljno obučeni kadar koji zapošljavaju menadžeri, a prema menadžerima je to politička orijentacija menadžera od koje ovisi obim rada AOOI-a, ali zato nedovoljno obučeni kadar ističu kao treći faktor, što je pokazatelj značaja gorenavedenih preduslova i neadekvatnosti kadrova u AOOI u RM. Kao što sme već rekli, glavni faktor koji negativno utiče na menadžiranje jeste slaba ekonomska razvijenost u državi, nedostatak bezbednosne kulture stanovništva, kao i nelojalna konkurencija, a smanjenjem kvaliteta usluga i cena, smanjuju se i plate radnika.

To znači da i pored toga menadžeri pokušavaju izvući maksimum koji je moguć u ovom području u okvirima ovog tipa usluga i za period od deset godina dovesti do određenog nivoa razvoja ovih usluga, a u narednom periodu očekuje se i uža selekcija i eventualna specijalizacija pojedinih AOOI-a za određene tipove obezbeđenja.

I pored nedostataka šireg aspekta, korisnici usluga ocenjuju da su zadovoljni (44,72%) ili vrlo zadovoljni (50,41%) načinom na koji dobijaju usluge AOOI-a, i to u nekoliko aspekata, kao što su: profesionalizam (52,03%), čuvanje poslovne

tajne (60,98%), stručnost u postupanju (54,47%), odnosi sa klijentima (55,28%) i sl. Nivo visokog zadovoljstva najverovatnije je rezultat toga što su generalno ciljevi ove delatnosti postavljeni vrlo nisko – zaštita imovine od krađa (izuzev kod pojedinih klijenata), čime se opravdava niski nivo cena koje klijenti mogu platiti. Ukratko, uslugu koju nude AOOI, menadžeri ispunjavaju i više nego što su plaćeni. Iz tih razloga, nema puno prostora za negativne reakcije klijenata, što ne ukazuje na tako visok stupanj razvoja ove delatnosti. Negativni komentari u osnovi odnose se na nedovoljnu obučenost kadra koji se bavi ovom delatnošću.

U tom pravcu je i stav građana (75,89%) da ipak postoji potreba za AOOI i pored postojanja policije; ili o postojanju pozitivnog (47,83%) tj. delimičnog uticaja (36,36%) AOOI-a po bezbednost uopšte; a u građanima AOOI pružaju veću sigurnost (71,15%).

LITERATURA

1. Бакрески, О.(2008) *Контрола на безбедносниот сектор,* Аутопринт, Скопје
2. Бошковић, М., Кекови,ћ З.,(2003) *Обезбеђење лица, имовине и пословања предузећа* (студија), ВШУП, Београд
3. Даничић, М., Стајић, Љ., (2008) *Приватна безбједност,* Комесграфика, Бања Лука
4. Драшковић, Д., (1984) О*снови методологије истражувања безбедносних појава*, Скопје
5. Герасимоски, С., (2009) *Позитивни и негативни искуства на развојот на приватната безбедност во светот и воопшто во Република Македонија*, Varstvoslovje, Fakultet za varnostne vede
6. Матијевић, М., (2004) *Неке карактеристике приватне детективске дјелатности,* Дефендологија, Бања Лука
7. Skakavac, Z. i dr.(2008) *Privatna bezbednost – stanje i perspektive*, Zbornik radova, Fakultet za pravne i poslovne studije, Novi Sad
8. Спасески, Ј., Аслимоски, П., Герасимоски, С., (2008) *Приватна безбедност.* Коста Абраш – Охрид
9. Stajić, Lj. (2008). *Osnovi sistema bezbednosti*. Pravni fakultet, Novi Sad
10. Тумановски, Д. и др., (2001) *Обезбедување на лица и имот,*2-ри Август С,Скопје

REZIME

U R.Makedoniji, kao zemlji u tranziciji, PBP se počeo razvijati u posljednjih desetak godina, pa do sada ima oko 180 registrovanih AOOI, od kojih aktivno radi oko 50, izdato je oko 16.100 licenci i oko 5.100 službenih legitimacija, a registrovano je samo 5 detektiva. Stupanj kompetentnosti kadra u velikoj meri ovisi od psiholoških predispozicija, stupnja obučenosti, finansijskog stanja pojedinaca i AOOI i sistema kontrole, a njegova nekompetentnost ima štetene posledice po bezbednost i zdravlje kako pojedinaca, saradnika i klijenata, tako i šire zajednice. Iz rezultata možemo zaključiti da, što se tiče strukture kadra u AOOI u R. Makedoniji, može se reći da se radi o muškoj profesiji, gde su radnici koji nju direktno vršeu sa srednjem obrazovanjem, a kod menadžera preduslov je prethodno iskustvo u državnim bezbednosnim i ostalim institucijama. I pored toga što postoje zakonska ovlašćenja koja se primenjuju, kod radnika je prisutno nedovoljno poznavanje, razgraničenje, dileme i prekoračenja najviše u pogledu „teških" ovlašćenja. Ukratko, može se reći da u AOOI u RM postoji i deo neadekvatnog kadra, postojeća obuka i kontrola ne odgovaraju potrebama savremenog koncepta privatne bezbednosti, a nelojalna konkurencija i finansijska ograničenja glavni su faktori koji negativno utiču na kvalitet poslovanja. U tom pravcu, predlaže se: 1. Da obuka bude sveobuhvatnija, fokusiranija na praktične probleme, na upotrebu vatrenog oružja, praktičnu primenu ZOOI-ja, način ponašanja, komunikacije i odnose sa ljudima, kao i da bude koncentriranija na delatnost kojoj je namenjena. 2. Uvođenje efektivne kontinuirane dopunske obuke u formi *seminara i debate*, kao stalna praksa u radu AOOI-ja, koja će proizaći iz potrebe AOOI-ja, uključiće više praktične obuke i iskustva stranih instruktora i stručnih osoba iz nauke, MUP-a itd., u čemu presudni značaj ima Komora; 3. Uspostavljanje adekvatnih standarda, kao preduslova za instruktore, članove Komisije za ispitivanje i ovlašćene osobe iz MUP-a za kontrolu nad AOOI i stroži selektivni pristup pri izdavanju licence, kao i pri proveri znanja, tako i sa aspekta psiholoških predispozicija, što podrazumeva i uključivanje adekvatnih psiholoških testova u ovoj proceduri za utvrđivanje podobnosti kandidata za ovu delatnost; 5. Aktivniji odnos Komore i MUP-a oko nelojalne konkurencije između AOOI-ja, kao jedne od glavnih prepreka u razvoju ove delatnosti.

Na kraju, može se reći da i pored niskog nivoa razvoja PBP-a u RM, on ipaki ima pozitivan doprinos bezbednosti u našoj zemlji i pre svega uspešno dopunjava policiju u obavljanju pozorničke delatnosti.

Stručni rad - UDK 351.74/.76: [343.326: 004]

POLICE STRATEGY IN PREVENTIVE ERADICATION OF MODERN ORGANIZED CRIME

Teaching Assistant MA Tatjana Gerginova
Faculty of Security - Skopje
tanjagerginova@gmail.com

Abstract: Within this paper I will speak about the preventive action of the police in preventing and combating organized crime and other forms of crime, such as economic crime, property crime, etc. I will determine the strategy of the police action in establishing adequate and effective means and methods for prevention and fight against organized crime today. It is necessary the police to investigate the specific mechanisms, tactics and technique of execution of certain types of organized crime. For research on each type of organized crime is required the police to undertake the following activities: determining the typical practices and concealment of certain crime; determining the specifics in terms of occurrence and the masquerade of typical traces; study of individual characteristics of the personality of organized delinquent and personality of the victim of organized crime, and study the specifics about the source of criminal information, analysis of all factors (social, economic, legal and political) on internal and international level, witch condition growth of the modern organized crime, selections of areas and forms of action in order to take measures for immediate action, harmonization of legislation with international legal standards on combating organized crime, deepening cooperation and expansion of legal instruments for this purpose and establishing effective and international cooperation activities for prevention, early detection and eradication of organized crime at the regional and international level.

Key words: prevention, suppression, strategy and police action.

INTRODUCTION

The Realization and development of common European security, means shaping a security environment that is based on cooperative relations and mutually coordinated activities in the field of security, maintaining stability, preventing and resolving crises expressed mostly through targeted leading role of NATO in creating security policy. Member states of the Partnership for Peace (PfP) and Euro-Atlantic Partnership Council (EAPC), through process and mechanisms led by NATO continuous act of expanding the zone of democracy and stability in Europe.

Southeast Europe, despite the progress in the security state remains a region where there are still threats to security, rooted in political extremism, extreme nationalism, religious and racial intolerance, which together with the existence of weak state institutions and lack of rule of law in some countries and regions, and transnational threats, are the basis for a high degree of risks and dangers for the Republic of Macedonia, the region and Europe. Special threat and a source of instability is the presence of large amounts of illegal arms, of which is not immune Macedonia.

Achieving a sense of security in the modern world is a fundamental task of the state in a new security environment in which state institutions should respond adequately to the changing nature of internal and external threats, risks and challenges. Today's world is characterized by rapid and dynamic changes that carry new and often unpredictable risks and hazards to the security of the state. The trend of globalization of the world, despite the advantages brought risks and threats, mostly caused by the deepening gap between rich and poor, and internationalization of certain hazards, the most extreme of which are international terrorism, organized crime, illegal migration and trafficking in drugs, weapons, people and strategic materials. As a special threat and a source of instability is the presence of vast quantities of illegal weapons to the security of the Republic of Macedonia.[1] The aim is to point out the internal threats that can get momentum or reinforcement from the outside and vice versa, where the external threats with his internationalism (smuggling, corruption, organized crime etc.). Acquire domestic features and become internal threats. The strategic orientation and objective of the Republic of Macedonia and its consistent commitment is future as part of the European family and a member of NATO and the EU.[2] From a security perspective, actually Macedonia is one of the crossroads of major routes of terrorism, illegal migration, trafficking in drugs, weapons and people from Asia and Africa to Western Europe. Despite all efforts to protect the border and eliminating these threats, the Republic of Macedonia is aware that alone can not solve transnational threats without the assistance and cooperation with its neighbors and the international community.

THE TERM PREVENTION AND POLICE WORK

In order to be achieved internal security, the state must constantly build and enhance the security system, to promote and develop national security strategy and above all to promote the system for crisis management. In this regard it is necessary to act preemptively which means taking measures and actions by the state authorities to prevent the risks and dangers for internal stability and functioning of the state and its order established by the Constitution and prevention of risks and dangers for the goods and the environment, health and life, property and other goods from a larger scale. In the struggle to combat forms of organized crime is crucial the preventive police action, and multidisciplinary approach which means involving citizens, NGOs, media etc..

Prevention in the most general sense means action, measures and procedures that are directed to prevent evil. The word "prevention" means totality of a planed (set in a single system) and organized measures and procedures that

[1] Integration into NATO is one of the vital interests of the Republic of Macedonia, which in NATO sees one of the key pillars of the modern, and Euro-Atlantic security architecture. Republic of Macedonia supports the processes of transformation and expansion of the alliance, and it participates in building peace and stability in the region, Europe and worldwide, as well as prevention and building instruments for early warning of tensions and crises in order – timely,efficient and peaceful resolution of crises.

[2] For the Security Policy of the Republic of Macedonia, more in the paper of Mr. Tatyana Gerginova titled as"Security Strategy of the Republic of Macedonia", published in the Yearbook of the Faculty of Security in 2010.

seek to prevent the action or to remove the influence of etiological factors that lead to criminality.[3]

Within a modern democratic society, one of the basic functions of the policeis preventing and detecting crimes and their perpetrators. Police should prevent deviant or asocial and unlawful conduct of individuals or social groups that are sanctioned as crimes. In general, crime is one of the most acute problems in all modern countries, which confirms the fact that it is in constant growth. Because of its social danger and harm, police is trying to prevent (preventive and repressive) with constantly finding adequate and effective methods and means. The aspiration is that the repressive measures move into the area of preventive measures in terms of warning of its occurrence. Preventive activity is a result of social action, as well developed safety culture.[4] Today, police are equal subject of prevention along with other state bodies and institutions, NGOs, courts, public prosecution, inspections, educational institutions and other bodies. In fact, the police should be the initiator, organizer mobilizator of the prevention activities. Therefore the repressive action of the police is conditioned by adequate organization, technical and personnel equipment and means of removing the causes of disruption and elimination of their carriers force the legal permitted manner.

Under the Law on Internal Affairs,[5] the role of police in the prevention of committing crimes and misdemeanors is detection and apprehension of the perpetrators and taking other measures stipulated by law to prosecute perpetrators of such crimes. Under the Law on Police,[6] the role of police in the prevention of committing crimes and misdemeanors is detection and apprehension of the perpetrators and taking other measures stipulated by law to prosecute perpetrators of those crimes.

The suppression of crime marks the application of adequate strength, reaction to something that already exists, so this term reflects more to the repressive action, apart from preventing that reflects preventive action.[7]

So, suppression means planned systematic action on removing the causes of crime and is aimed at preventing the penetration of crime in new areas and its maintenance within certain limits of a certain level, while prevention is aimed at preventing criminal before it happens. Today, the policy of prevention and suppression of crime is a policy of prevention and repression. Repressive component of the fight against crime have been determined and linked with the activity of state bodies in the criminal justice area, comprising: stipulation of offenses and penalties; detection of crimes and their perpetrators, prosecution, trial and imposition of criminal sanctions, enforcement of the pronounced criminal

---

[3] For the term prevention see more in the paper "The repression aimed at preventing organizitaniot Transnational Crime" prof. Dr. Ljupco Arnaudovski , published in the draft program Tempus and Cards "Higher level of training for the fight against organized crime", Skopje, 2002, p.79th

[4] About preventive and repressive suppression of modern organized crime, see more at "Systems analysis of the legal framework and cooperation between the competent institutions ity in the fight against organized crime" - Research team consisted of Mr. Todor Vitlarov, Dr. Gordan Kalajdziev e Dr. Miodrag Labovic, Dr. Turpen Stojanovski, Skopje, June 2005, p. 18 to 20.

[5] Law on Internal Affairs, Official Gazette of the Republic of Macedonia, No., 92/2009, Article 2.

[6] Law on Police,Official Gazette of the Republic of Macedonia, no. 114/2006, Article 5.

[7] S.Kostich., Basic Criminal operative - 1 Deo; VSUP, Beograd, 1982, p. 196th.

sanction etc.. However, the repressive component transform and evolve, gaining preventive elements. It is a criminal justice prevention, whose primary sense is the state authorities to work quickly and efficiently, and the basic principle that prevention consists in the endeavor to discover as many crimes, to catch their perpetrators and to them to apply appropriate measures. In fact, it is prevention through repression, by detecting and sanctioning certain criminalized behaviors.

In order to prevent committing crimes and misdemeanors, police officers undertake planned and organized measures to establish the causes which condition the criminal and antisocial behavior of individuals or social groups. Police officers perceive and manifestacionite phenomenological forms of criminal behavior through their continuous monitoring and analyzing them in order to appropriately and effectively targeting preventive activity. General preventive activity of police officers covering quality material documenting criminal and antisocial behaviors of individuals and social groups, cooperation and coordinated activities with other institutions or entities that receive educational, social, humanitarian, custodial and other similar purposes, for taking common preventive activities. Exercise of general prevention includes creating civic advisory groups on the territory of a particular police station of general jurisdiction, involving representatives of local governments or associations of citizens, in order to identify reasons for locally occurring security problems and building the appropriate recommendations for preventive planning activities of the police station and appropriate public presentation of practical experiences regarding successful implementation of preventive activities for organizing and performing.

SPECIFIC TYPES OF PREVENTIVE ACTION OF THE POLICE

Direct preventive action by police officers is determined depending on the subject of protection and can be: prevention in blood offenses and violent offenses; prevention in the property crime; prevention in the field of economic crime; prevention in the field of juvenile delinquency; prevention in the field of traffic safety on roads and prevention in the field of organized crime.

The preventive action by police officers is directed towards:

- Collecting data and information about events, situations and behaviors that contribute to the performance of certain offenses;
- Further, strengthened and continuous covering points, places, areas and certain environments where have been performed certain offenses or may be expected their occurrence. The task is accomplished by determining the mobile preventive patrols at critical points and in critical time in the composition and number corresponding to the specific needs.
- Trough patrol activity, police officials follow the movement of known perpetrators of offenses, with main goal to prevent and detect attempts to re-execution of criminal acts.
- Police officers plan measures and activities (if necessary by applying appropriate technical means, such as photographic cameras and camcorders) for observation points, places, premises and public buildings, which are made criminal offenses with elements of violence or expected

breach of public order and peace, doing other crimes and misdemeanors to prevent and identify their perpetrators.

- Police officers shall initiate through the appropriate specialized institutions and state authorities taking measures to overcome causal factors and conditions that enable to carry out criminal acts or reducing their influence and strengthen cooperation with the organs of local government and NGOs to combat antisocial appearances and behaviors a reflection of the security situation in the area.
- Police officers need to take and organize activities that will stimulate the launching of the safety culture of the citizens and taking appropriate measures for their own technical and other permitted protection. For this purpose we organize additional classes to raise traffic culture, indicating that citizens are potential victims especially for property offenses, advising on the application of protective devices, as well as introducing measures to prevent attacks on life and personal security of citizens.

In order to prevent property crime[8] police officers take preventive measures and activities that protect life and personal security of citizens, which identify threats that can jeopardize the same. In order to prevent property crime, police officers are giving advice through the media in order to indicate the citizens to protect their property, they follow the measures for external security of facilities from theft and functioning of the guard service, and for established states are initiated actions to remedy deficiencies (application of modern safety and alarm devices for protection of the building and property from theft). According to the needs of a particular situation, police officers may establish special units that intervene in critical time-critical places where usually perform property offenses or are expected to be committed property offenses.

Preventive actions to prevent economic crime[9] include: research on its emergent forms and determining preventive measures that should be applied for its suppression: analysis of results of measures and their compliance with future activities that need to be taken for proper handling with specific forms of this type of crime, further establishing closer cooperation with the financial police and customs officers to combat economic crime and initiating change and adoption of regulations governing the issues in this area, based on experiences gained and results from analysis of criminal behaviors and modalities of their implementation.

Police officers undertake preventive actions aimed directly at preventing juvenile delinquency[10], and this is realized by ensuring the presence of a number of police officers in areas where this phenomenon is expressed, as well as monitoring the behavior of known minors who have committed criminal acts. This is realized by the police officers responsible for juvenile delinquency. To prevent juvenile delinquency, police officers are enforcing preventive actions based on specific

[8] Rules on how to perform police work, "Official Gazette of the Republic of Macedonia" no. 149/2007, Article 97.

[9] Rules on how to perform police work, "Official Gazette of the Republic of Macedonia" no. 149/2007, Article 98.

[10] Rules on how to perform police work, "Official Gazette of the Republic of Macedonia" no. 149/2007, Article 99.

assessments of the emergent forms of criminal behavior in which participants are minors. Police officers take notice and encourage cooperation with the custody order taking measures to eliminate the causes of delinquent behavior of juveniles, a group of representatives of the authorities for custody and police officers on juvenile delinquency, which will exchange data and information about opportunities and ways to prevent juvenile delinquency, police officers identify leaders of the juvenile criminal groups and separate them from the group to further social and educational care.

Police officers take preventive action against perpetrators of blood and other offenses with elements of violent behavior, by taking the following preventive measures and activities that protect life and personal security of citizens, "police officers directly study the etymology of bullying behavior (exploring causes that produce its occurrence and origin, to explore the conditions that preceded such as interpersonal relationships, threats, threat to social security for children because of family problems, indulge in alcoholism, psychopathic manifestations and the like) police officers initiate and mobilize all entities and institutions for resolving issues relating to the protection of life and personal security of citizens, public understanding of the areas, sites and facilities where the frequency performance of certain offenses for the violent behavior in order to initiate appropriate preventive treatment of citizens, police officers initiate and cooperate with other authorities and institutions to take appropriate measures within their competence to solve specific problems that lead to violence and suggest possibilities for their solution (information on social services, maintenance of organized and scheduled meetings with civic associations in schools, etc..). Preventive actions of police officers in the field of blood offenses include taking immediate appropriate measures of physical disabling the attack against the life of citizens and exercising control over the circumstances that affect a particular case. This is realized so that police officers exercise constant control of possession and carrying weapons, cool weapons and other dangerous weapons, implement operational control over vulnerable areas, planned provision of places are held public meetings, entertaining and other public events, as well as other public spaces or rooms, direct physical control over persons known as the perpetrators of offenses of this kind or that there are grounds to suspect that may occur as such). "

Police officers undertake preventive activities in the field of organized crime[11], establishing his emergent forms in areas that are present, defining and identifying indicators which individually or collectively identify the crime of this kind, and their executors, collect data and information for the existence of organized crime and their joint processing in cooperation with other competent authorities; explore emergent forms of organized crime and its bearers, and the grounds for their detention (ethnic solidarity, the same language, customs, social and familial closeness, internal organizational structure criminal groups or organizations, etc..). Police officers undertake measures and activities to determine the types of activities that often manifest an organized criminal activity, such as trafficking

[11] For the measures and activities undertaken by police officers in the field of organized crime see more in Article 101 of the Rules on how to perform police work, "Official Gazette of the Republic of Macedonia" no. 149/2007.

and smuggling of narcotic drugs, weapons, gold and expensive cars, pimping, prostitution, trafficking in human beings or parts of human body, illegal gaming, extortion of protection money that is not required (racket), illegal employment mediation, cross-border smuggling of people and goods, counterfeiting labels of goods, fraud insurance and venture capital, evasion customs duties and taxes, forgery of money and organized carrying heavy or armed robbery, police officers take preventive measures and activities for understanding of preparation and planning of organized crime, the manner of execution of work and further use of funds derived from organized crime, as well as the internal and external protection of the organizers of organized crime and the perpetrators. Police officers exercise regular communication with other competent authorities in order to promptly assess the possible development of the situation and common occurrence in taking measures for detecting, documenting and combating organized crime; transmission of acquired experience, knowledge and experience in the application of funds and methods, the establishment of practical cooperation with foreign authorities and informing the public.

NEED FOR PREVENTIVE AND COORDINATED ACTION WITH OTHER POLICE AUTHORITIES TO MONITOR, RESEARCH AND PREVENTION OF MODERN ORGANIZED CRIME

In modern society, as a consequence of scientific and technological development, computerization, internationalization, modern organized crime gets a new phenomenological features that seem dangerous because of the consequences and causes complex and difficult to detect. The notion of phenomenology of crime basically means knowledge about the scope, dynamics, internal structure and the type of offenses and the structure of offenders according to their social and criminological characteristics. Exploration of the phenomenology of crime occurs as a complex scientific and practical, empirical research problem, because in fact crime is a hidden phenomenon, its players seem to remain undetected or take measures to conceal the crime, to remove or destroy the traces. By taking these actions the perpetrators, essentially change those facts by which can not be recognized the crime and thereby alter the picture of it. Organized crime is manifested through legal and illegal forms of action, hiding in legal forms of action of the organs and institutions, taking special precautions, and upon its internal organization and principles of operation creates great difficulties to penetrate into it and inside to learn about its features.

For eradication and prevention of organized crime, each country must build its own strategy to combat organized crime and care for its accomplishment, to distribute the tasks of all public authorities (police, courts, customs, financial police, inspection and other control authorities) and to coordinate and unite their work. Their future activities should focus on assessment and review of internal organization and work, interconnection and coordination, harmonization of regulations and procedures, primarily those in the Member States of the European Union, could successfully cope with these complex, international and domestic more and more improved methods of action of the perpetrators of the risks and

threats in the Republic of Macedonia. Ministry of Interior in particular need to promote and develop procedures and mechanisms to combat terrorism, illegal migration, trafficking in drugs, weapons, people and strategic materials with those in developed countries. It should also improve coordination and develop common operating procedures armed forces, especially in the fight against terrorism and border security. To improve the security situation in the country, it is necessary the Ministry of Interior to build new instruments and to improve alignment and coordination of existing measures and instruments to prevent corruption, the most difficult forms of crime such as blackmail, murder, racketeering, etc., and destruction of property of citizens.

The fight against terrorism, organized crime, illegal migration, trafficking in drugs, weapons, people and strategic materials is particularly complex task that should take a number of specific measures and activities, including the carrier should be the organization of effective border police coordination mechanisms and procedures for interstate exchange of information, cooperation and assistance, especially those mechanisms and procedures established in the Member States of the European Union and NATO.

It is necessary constantly maintaining and improving the efficiency and objectivity of the means and methods for collecting data and information that are important for the country's security, quality and continuous expert analysis of the security environment of the country, because the active participation of the police in its creation and preventing certain risks and hazards to the security of the country. It is inevitable and continuous education of experts, with their competence can contribute to more effective achievement of internal and external security of the state. It is important to continuously promote the work of the bodies responsible for control of crossing the state border, the main goal to effectively control the border and border zones outside designated legally defined border crossings, and to prevent all kinds of illicit trade and to build capacity and unique procedures in connection with realization of cooperation and mutual assistance with neighboring countries, the entire region and the international community.

Geopolitical and geo-strategic environment of our country, imposes the need to define a security policy, whose implementation will successfully protect all vital values (sovereignty, independence, territorial integrity of the country's legal order, human rights and freedoms), which is one of important conditions for survival of the country. For that purpose, in our country is normative and is pointed unique system of integrated security (defense and security), which provides effective opposition to all modern forms of organized crime, and all external and internal stakeholders endangerment.

For achieving this goal, police and other authorities in our country, each within its scope of work, take appropriate measures to prevent and protect from various types of crime (property crime, economic crime, organized crime, blood offenses, juvenile delinquency, etc.)

- Identifying the forms of property crime, economic crime, organized crime;
- Timely and realistic assessment of the intention of the perpetrators of property crime, economic crime, organized crime, and that their goals and plans;

- Establishment of a strategy to be applied to prevent activities associated with preparing and organizing the perpetrators of property crime, economic crime, organized crime and exposing them to domestic and international public;
- Effectively disabling the connection between internal and external perpetrators of property crime, economic crime, organized crime,
- Vigorous fight against all forms of organized crime.

CONCLUSION

Organized crime is one of the most acute problems in all modern countries, and it is constantly growing, so there are still difficulties in connection with locating and determining the most important theoretical and practical problems related to its discovery, proof and prevention. Today we see constantly identifying new phenomenological features and new qualifications through which seek to express its danger and difficulty. Because of its social danger and harm (this crime is the most difficult by the dangers which brings by itself and consequences for humans, social groups, the normal functioning of legal state and its authorities and institutions, all material and spiritual goods and values) all countries endeavor to suppress (preventively or repressively) with constantly finding adequate and effective methods and means. This can be achieved by establishing appropriate cooperation of police, judicial authorities and control of crossing the state border. Today it is necessary continuous education, training of all Criminal and other police forces, for discovering the secret use of modern forensic and technical resources, tactical ways and scientific methods in basic aim of building crime strategy perspective and long-term management and suppression of organized crime.

In the modern world, organized crime is an international phenomenon, so it is necessary to connect the regional police forces of all countries with the main goal, joint criminal coping and suppression of organized crime. It is a criminal act in operational, investigative and judicial activities.

It is necessary the police to investigate the specific mechanisms and the way of exploring different types of organized crime, detecting features of the organization in all phases of criminal conduct, defining the most effective criminal-technical means, tactical ways and scientific methods to combat the appropriate types of organized crime. Tactics and technique of implementing operational and investigative activities will be aimed at clarifying the individual type of organized crime and understanding of tactics and techniques that use organized delinquent as professional criminals from the largest scale or range.

For each type of organized crime is necessary to undertake the following: determining the typical practices and concealment of certain crime; down to specifics in terms of occurrence and the masquerade of typical traces, the study of individual personality characteristics of organized delinquent and personality of the victim of organized crime and studying the specifics about the application of the source of crime information.

REFERENCES

1. Angeleski M. "In the fight against organized crime is required organized scientific and professional approach," Yearbook of Faculty of Security, Skopje, 2002;
2. Boshkovich, M. "Organized Transnational Crime", Police Academy, Belgrade, 2003, p. 24th;
3. Code of Police Ethics, "Official Gazette of the Republic of Macedonia" no. 72/2007;
4. Defense management, Democratic and Civilian Control, Including Integration of Security Sector, pp. 2-3;
5. Hugh, P., "Concept for global security," Tabernakul, Skopje, 2009;
6. Kotovchevski M., National Security of the Republic of Macedonia, Vol I and II, Skopje, 2000;
7. Law on Police, "Official Gazette of the Republic of Macedonia" no. 114/2006;
8. Law on Internal Affairs, "Official Gazette of the Republic of Macedonia", No, 92/2009;
9. Masleša R., "Theory and security system", "Magistrat", Sarajevo, 2001,p.3;
10. National conception of security and defense published in the Official Gazette of the Republic of Macedonia, no. 40 of 23 June 2003;
11. Rules on how to perform police work, "Official Gazette of the Republic of Macedonia" no. 149/2007.
12. Systems analysis of the legal framework and cooperation between the competent institutions in the fight against organized crime - the research team consisted of Mr. Todor Vitlarov, Dr. Gordan Kalajdziev Dr. Miodrag Labovic, Dr. Turpen Stojanovski, Skopje, June 2005.
13. Wolfers A., National Security as an Ambiguous Symbol, Discord and Collaboration, John Hopkins University Press, Baltimore, 1962nd.

Prethodno saopštenje - UDK 351.74/.75: 343.85

STRATEGIC ASPECTS OF PREVENTING ILLICIT TRAFFICKING IN SMALL ARMS AND LIGHT WEAPONS

Ivan Ristov
Faculty of Security – Skopje
E-mail: ivan.ristov1@gmail.com

Abstract: Crime prevention metaphorically can be compare with solving a jigsaw puzzle. To solve a jigsaw puzzle is not merely "to make a picture." Either a child or a contemporary artist could do that by scattering selected pieces, as abstract shapes, upon some neutral ground. But, such a picture would not be a solution. To achieve that all the pieces must be used, their plain sides must be turned down, and they must be interlocked without forcing until no holes remain.[1]

Strategic aspect of prevention of illicit trafficking in SALW is one of the trickiest jigsaw puzzles to solve. We need all the fragments of the problem that we can collect using strategic (criminal) intelligence interlocked all together producing a solution.

According to the lows of economic science, market demands (doesn't matter legal or illegal) and the offers, depends directly on a number of factors: Offered price of the product , profits by its sale, the costs of input, technology, the amount of income of consumers, market size and other relevant factors. In the case of illicit trafficking in SALW these relevant factors we should seek in all places where operates terrorist organization, run international and internal wars, revolutions of paramilitary organizations with state authorities… Using strategic intelligence we must collect all this pieces of information to predict the behavior of all relevant parts of the puzzle and later build solid crime prevention.

Key words: Crime prevention, Illicit trafficking, SALW, Strategic intelligence, Terrorism

INTRODUCTION

We can't be 100% certain about how much trafficking in small arms and light weapons (SALW) worth on the world financial market, but according some data till 2002 is ranged between 2 and 10 billion US dollars per year, from which 10 to 20% of the profit fall under illicit trafficking[2]. According to other available information, it is assumed that in year 2000, legal trade in arms ranges somewhere around 5 billion dollars and illicit trafficking around 1 billion dollars worldwide.[3]

[1] uhn, Thomas S., The structure of scientific revolutions, 3rd edition, The University of Chicago press, page: 52

[2] Nicholas Marsh, "Two Sides of the Same Coin? The Legal and Illegal Trade in Small Arms," *Brown Journal of World Affairs* 9 (Spring 2002): Page: 200–217.

[3] Council of Europe, Organized crime situation report 2004, Focus on the threat of cybercrime, Strasbourg 23 December 2004, Page: 32.

But we should emphasize that in this figure is included only SALW. Over 1100 companies from 98 countries produced this types of weapons worldwide from which only USA and Russia produce over 70%.[4] It is assumed that by 2001 on the world market are located over 500 million pieces SALW in circulation[5], from which 20% or 100 million pieces of rifles that can be bought in many cases for a price less than 100 dollars per piece[6]. This type of weapon is easily portable, has a long shelf life and in most cases is transferred (recycle) from a zone of conflict to another, contributing to instability in a certain area and causing the greatest number of victims or about 90% in military conflicts.[7] When we talk about the so-called heavy weaponry whose monitoring since its production to the actual user is relatively easier, we should note that in the world generally small group of countries manufacture this kind of weapons, from which largest percentage or nearly 80% of all financial transaction[8] are done by the five permanent members of the Security Council of UN led by the USA[9]. Remain 20% shares Germany, Israel, Ukraine, Italy, Brazil, Spain and smaller percentage of several other countries. In order to see what's the size of this market we will only mention that in 2009 is achieved an agreement for sale this type of weapons (which includes tanks, helicopters, fighter jets etc.) with developing nations[10] in value of about 45.1 billion of which around 17.4 billion dollars or 38.5% from the U.S. and 4.10 billion dollars or 15.8% from Russia, and achieved 17 billion dollars total real seal of weapons in 2009.[11]

From the used data we can pull a conclusion that illicit trafficking in firearms is a very serious type of crime where is involved a lot of money. Thus its self indicates of existing serious criminal organizations which success depends of this illegal activity. In this type of crime, perpetrators, criminal undergrounds from several countries, mostly associated with former employees of national security structures. That's why it must seriously approaches to crime prevention, especially proactive actions by the law enforcement agencies, using criminal (strategic) intelligence units.

ILLICIT TRAFFICKING IN SMALL ARMS AND LIGHT WEAPONS IN BALKAN ESSPECIALY IN MACEDONIA

In European continent, smuggling and illegal trafficking in weapons, ammunition and explosives is mostly expressed in the Balkan, the Czech Republic and countries of former USSR. During the Cold War in countries that were part of

[4] Ibid.
[5] Council of Europe, Organised crime situation report 2001, Strasbourg, December 2002, page 35
[6] William Hartung and Rachel Stohl, "Hired Guns," *Foreign Policy* (May/June 2004): 28–29
[7] Council of Europe, Organised crime situation report 2001, Strasbourg, December 2002, page 35.
[8] Government-to-government, foreign military sales (FMS) transaction.
[9] Richard F. Grimmett, *Conventional Arms Transfers to Developing Nations, 1994–2001* (Washington: Congressional Research Service, 2002), Page: 1–14.
[10] As used in this report, the developing nation category includes all countries except the United States, Russia, European nations, Canada, Japan, Australia, and New Zealand. A listing of countries located in the regions defined for the purpose of this analysis—Asia, Near East, Latin America, and Africa—is provided at the end of the report.
[11] Richard F. Grimmett, *Conventional Arms Transfers to Developing Nations, 2002–2009* (Washington: Congressional Research Service, 2010), Page: 2.

the USSR were stockpiled huge amounts of weapons when after the collapse of this federation and the withdrawal of troops from the now independent states managed to find its way to the war that began in the former Yugoslavia and in other conflict zones around the world. Russian and Italian criminal organizations then only saw a huge opportunity for profit through illegal transfer of vast quantities of weapons in the former Yugoslavia. It is assumed that in the period from October 1992 to March 1994 in cooperation Belgian, Russian[12] and Italian criminal organizations managed to bring nearly over 13,000 tons of arms and ammunition to Croatia and Bosnia and Herzegovina.[13]

In 1997, in the Republic of Albania happened "collude to stage" stealing from military facilities in this country of 700,000 pieces of various types of weapons, which were later used directly in armed conflicts in Kosovo, southern Serbia and in the Republic of Macedonia[14].

After the conflict in former Yugoslavia and signing the Dayton agreement, by 1998 repeatedly had been cut up channels of illicit trafficking in firearms from the former crises areas to Austria and Germany[15]. In 2000 it was notice an increase activity of smuggling weapons from Bulgaria in southern Serbia, Kosovo and Macedonia.[16] We can conclude from the data that in some parts of South-Eastern Europe large amounts of disposable weapons led to a social condition called "gun culture", directly referring to the 2001 conflict in Macedonia.[17]

Macedonia has a specific position in the Balkan. Regardless, whether you travel from north to south or from west to east, mountain ranges in Macedonia offer the most accessible route. Situated in the heart of the Balkans, Macedonia connects Belgrade to Solun(Thessaloniki) on the Aegean Sea and Istanbul to Durres on the Mediterranean. For these reasons, Bismarck once famously mentioned that whoever controls Macedonia controls the entire Balkan Peninsula. Today, networks of organized crime exploit the advantages observed by Bismarck[18]. With its geostrategic position Republic of Macedonia is a land transit and final destination in the smuggling of weapons. The war conflict in 2001 only confirmed that since Macedonia independence in 1991 until the beginning of the conflict enormous amounts of weapons, ammunition and explosives are smuggled through illegal channels in R. Macedonia. Smuggling and illegal trafficking in weapons in

---

[12] In the period 1999 - 2000, Russian criminal groups in cooperation with Belgian criminal groups managed to bring over 200 tons of weapons to Sierra Leone.

[13] Council of Europe, Organized crime situation report 2004, Focus on the threat of cybercrime, Strasbourg 23 December 2004, page: 33

[14] Миодраг, Л., Николовски М., Организиран криминал и корупција, нови теоретски димензии, практични консеквенции и методика на истражување, Скопје, 2010 година, страна 457.

[15] Council of Europe, Committee of experts on criminal law and criminological aspects of organized crime, Report on the Organised crime situation in Council of Europe member state year 1998, Strasbourg 17 December 1999, page 37.

[16] Council of Europe, Organised crime situation report year 2000, Strasbourg, December 2001, page 61

[17] Council of Europe, Organized crime situation report 2004, Focus on the threat of cybercrime, Strasbourg 23 December 2004, page 33.

[18] Роберт Хислоп, Затишје пред бура? Влијанието на прекуграничните мрежи, корупцијата и криумчарењето врз стабилноста на Македонија и врз безбедноста во регионот, Документ подготвен за презентација на Годишниот собир на Американското здружение за политички науки за 2001 година, Сан Франциско, Калифорнија, страна 4.

Macedonia in most cases are run by Albanian organized crime groups which also were the key element in maintaining and organizing paramilitary forces in 2001.[19] By 2001 Albanian nationalism as retrograde social phenomenon aimed toward secession a part of the territory of Macedonia and merging with Albania, managed to produce the creation of illegal forms of association on that basis[20] with Albanian organized crime as a reference point for all criminal activity today. Considering the irreconcilability and orthodoxy of the holders of Albanian nationalism it is crystal clear that for a longer period of time smuggling and illegal arms trading will burden the security situation in the Republic of Macedonia. These criminal organizations did not stop with smuggling and illicit trafficking in weapons not even after the conflict. That this continues to happen to this day testify large quantities of weapons, ammunition and explosives seized by the Ministry of interior on several occasions in the period after 2001 until 2010. During this period, including the 2001 MOI seized a total of 1,523 pieces of revolvers and pistols, 680 rifles pieces, 4,117 pieces of remaining weapons, 161,922 rounds of ammunition and 262,91kg explosives and 217 pieces of explosive charge and 72 pieces of TNT explosives.[21]

PHENOMENOLOGICAL CHARACTEISTICCS OF ILLICIT TRAFFICKING IN SMALL ARMS AND LIGHT WEAPONS AND PROACTIVE CRIMINAL INTELLIGENCE ACTIONS OF LAW ENFORCEMENT AGENCIES

Criminal phenomenology allows us a detailed study of the morphology of the crimes, the modus operandi of the criminal acts, gives us a clearer picture of their perpetrators (individuals or criminal groups), tell us what is the scope and dynamics of criminality, with which is actually gained a clearer picture of decrease or increase of crime in terms of multiple time periods. Scientific results obtained by studying the phenomenological characteristics of such crimes can be used to obtain the existing crime policy towards actual reality, successful prevention and repression, as well as discovering new techniques and methods in proactive and reactive work in the fight against crime. Without these information law enforcement agencies will be like in the famous story from a Persian mystic about the elephant in the dark room, ie, of which side we would approach the problem that's how will see the problem, formally without its essence. Studying the phenomenological features of this type of crime in the world and especially in Europe and in the Balkan Peninsula we encountered a loop scheme that constantly is used by criminal organizations.

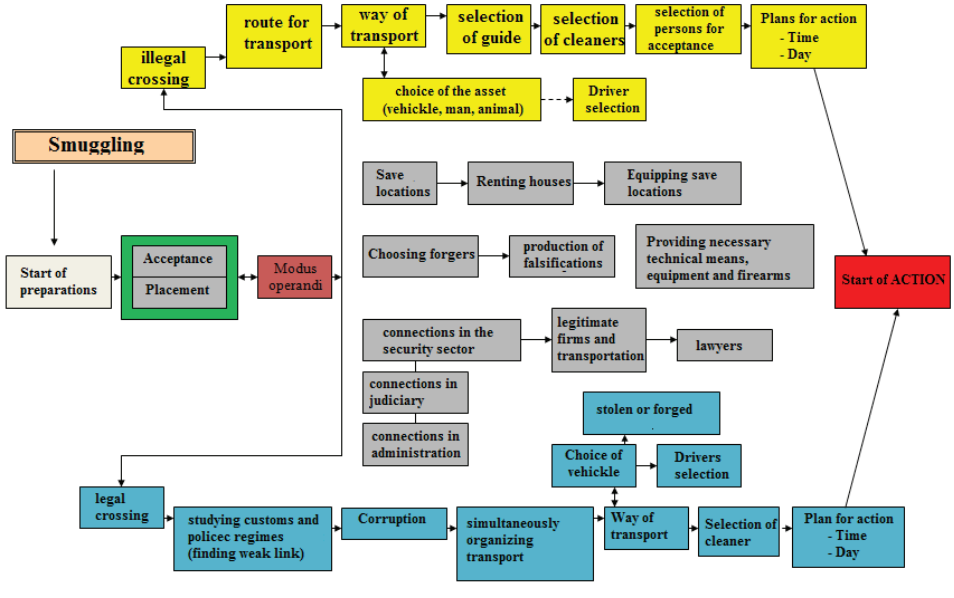
Smuggling and illicit trafficking in firearms is a serious criminal activity that requires serious preparations. If we break down this criminal activity in several mutually connected activities we notice that is need a serious material and human

[19] Ibid.

[20] Батковски, Т., Илегални здруженија (банди, организации и групи) создадени од позициите на албанскиот национализам во Македонија во периодот 1945 – 1987 година, Докторски труд, Факултет за Безбедност – Скопје, 1993 година.

[21] Source: Ministry of inferior, Republic of Macedonia. Available at: [http://www.moi.gov.mk/DesktopDefault.aspx?tabindex=0&tabid=397] 22.01.2012 година.

resources for its execution (primarily when this actions are carried out by criminal groups rather than individuals). Analyzing several cases of smuggling of weapons and illicit trafficking here and abroad we have tried to give a schematic representation of the overall activity that takes place within the group so the realization of the incriminated act will be successful.



[22]

From the schematic we can observe that the actions that are taken regards the acceptance and placement of weapons, choice of legal or illegal passage to transfer over state border, the decision on mode of transport, providing security locations (houses) if necessary, corruption individuals from the security structures if necessary and so on.

Using criminal intelligence law enforcement agencies constantly need to refill the databases with this type of data. Are there any indications that in some area operates a particular criminal organization which operates in illicit trafficking in firearms, what's the type of the organization, what is the modus operandi of the organization, whether the smuggling is commonly done through illegal crossings or through legal crossing points, what kind of transportation is used, links between criminals and the people from the police, national security, judiciary, custom, finding the save locations (houses) that are used as places for meetings and storage of the smuggled weapons in order to prevent passing from owner to another. Gathering more and more information the jigsaw puzzle will slowly start to get its looks. These data must continuously be well handled and analyzed in order to set new strategic goals and work plans for the law enforcement agencies.

[22] Schematic representation of the activity run by criminal groups, smuggling weapons, ammunition and explosives.

ETIOLOGICAL CHARACTERISTICS AND PREVENTION OF ILLICIT TRAFFICKING IN SMALL ARMS AND LIGHT WEAPONS IN THE REPUBLIC OF MACEDONIA

The study of etiological characteristics of specific type of crime is equally for proactive and preventive action of law enforcement agencies.

Crime causes can be defined as indirect and direct forces, factors, relationships and influences that produce a specific effect, but because of the establishment of causal relationships and determining the character of the cause of a phenomenon in criminology appears to be a very complex process, criminologists often avoid discussing of causes of crime and use the term "crime factors" which includes whole of reasons, causes and conditions that lead to the emergence and manifestation of a particular phenomenon. As for the smuggling and illicit trafficking in arms, criminal factors can be divided into three groups.

The first group of factors includes social-economic factor, the second group is composed of political-ideological factors and the third group micro group factors.[23] The first group social-economic factors are manifested in many different forms. For example poverty and unemployment can lead to engagement in illegal arms trafficking mainly for profit. However looking at the bigger picture and taking the previously mentioned economic laws of supply and demand we came to conclusion that even the social structure and social order can lead to increased illegal trade in weapons of a certain area.

The second group of factors or political-ideological is especially typical for the countries of the Balkan Peninsula in particular Republic of Macedonia.

As an independent country Macedonia these last 20 years hardly passed through its fragile democracy collided with a series of difficulties which barely managed somehow, with serious consequences of social functioning. After the independence Macedonia clashed with the appetites of the smaller ethnic communities hidden behind their demands for greater human rights, actually appearing territorial claims, especially Albanian ethnicity which engaged in the earliest social transformations. Albanians from Republic of Macedonia initially boycotted the referendum for independence and later conducted an illegal referendum called Ilirida acquisition of autonomy. We should mention that, as far as the Albanian nationalism and political action, the professor at the Faculty of Security – Skopje, Tome Batkovski, in his doctoral dissertation[24] managed to prove that Albanian nationalism as retrograde social phenomenon focused toward secession of a part of the territory of Republic of Macedonia and its merging with Albania - generates creating illegal forms of association on this basis and that these illegal associations are a product of Albanian nationalism, but it themselves, in turn, affect the closure of the Albanian ethnic group in Macedonia and its disintegration from the general political and cultural environment.

---

[23] Димовски Злате, Илегалната трговија со оружје и тероризмот во Република Македонија, Графотранс-Скопје, 2005 година, страна 43; Арнаудовски, Љ., Криминологија, Скопје, 2007 година, страна 590-681

[24] Батковски, Т., Илегални здруженија (банди, организации и групи) создадени од позициите на албанскиот национализам во Македонија во периодот 1945 – 1987 година, Докторски труд, Факултет за Безбедност – Скопје, 1993 година

These illegal organizations whose main political objective is a territorial pretensions and separation of parts of the Republic of Macedonia carried out illicit trafficking an smuggling in arms, as proof of this claim is the armed conflict in 2001 where come to light weapons that were build up illegally all previous years.

This group of factors also includes and the impact of religion on crime. We are witnessing a growing Islamist radicalism that appears on the territory of the Republic of Macedonia and the Balkans, the wahhabi movement among Muslim believers is pronounced, and it can certainly lead to future terrorist acts that preceded acquisition of illegal weapons, ammunition and / or explosive materials[25].

The third group of factors include the so-called micro group criminal factors which themselves incorporate the impact of family as a factor for criminality, school as a factor for criminality and the impact of peers, neighborhood and housing conditions. Again, the focus falls on how these factors affect the Albanian citizens in Republic of Macedonia as the main carriers of smuggling and illegal arms trafficking in the territory of the Republic of Macedonia. If in certain environments between the Albanian national group it is present Albanian nationalist indoctrination, it increases the possibility of appearance of holders of illegal activity from these areas, and by increasing the degree of conflict of Albanian national group and its subculture to common culture in Macedonia is increasing the opportunities to call Albanian nationalism and illegal associations on this basis.[26]

About indoctrination within the families we can't talk because we do not possess a sufficient number of quality data and science is not a field of speculation, but as far as the indoctrination that is done through the educational process, there are serious indications that in a good part of the Albanian schools in Republic of Macedonia is teaching from various unapproved books, that glorifies great Albania idea, by the Ministry of Education and Science which actually forms a gap in the understanding of history.

Etiological study is important primarily for the creation of a criminal policy and strategy for prevention of this type of crime. Data obtained and analyzed, have to represent the foundation that will be constructed on the fight against this type of crime. If its realized for instance that a particular area of possible ethnic or interreligious tensions and later conflicts (and for every conflict is a necessary weapon), it is necessary undertaking such policies which will result in calming the tensions and acceptance of joint solutions between hostile groups etc...

---

[25] Head of the IRCM, Reis-ul-Ulema Hadzi Sulejman Efendi Rexhepi in an exclusive interview with journalist Zarijeta Hajro Jajaga (07/07/2010) from the Albanian service of Radio Free Europe said: Wahhabis control four mosques in Skopje, and MOI is passive despite verbal support. Head also said that IRCM tried to hide the fact that in Macedonia act radical wahhabi with hope and belief that they will distance themselves but sadly it never happened. Source: [http://www.makdenes.org/content/article/2093516.html] 20.01.2012

[26] Батковски, Т., Илегални здруженија (банди, организации и групи) создадени од позициите на албанскиот национализам во Македонија во периодот 1945 – 1987 година, Докторски труд, Факултет за Безбедност – Скопје, 1993 година.

REFERENCE

1. Council of Europe, Committee of experts on criminal law and criminological aspects of organized crime, Report on the Organised crime situation in Council of Europe member state year 1998, Strasbourg 17 December 1999
2. Council of Europe, Organised crime situation report 2001, Strasbourg, December 2002
3. Council of Europe, Organized crime situation report 2004, Focus on the threat of cybercrime, Strasbourg 23 December 2004
4. Kuhn, Thomas S., The structure of scientific revolutions, 3rd edition, The University of Chicago press
5. Nicholas Marsh, "Two Sides of the Same Coin? The Legal and Illegal Trade in Small Arms," *Brown Journal of World Affairs* 9 (Spring 2002)
6. Protocol on Blinding Laser Weapons, 13 October 1995. (Protocol IV to the 1980 Convention).
7. Protocol on Explosive Remnants of War, 28 November 2003 (Protocol V to the 1980 Convention).
8. Protocol on Prohibitions or Restrictions on the Use of Incendiary Weapons,10 October 1980 (Protocol III to the 1980 Convention).
9. Protocol on Prohibitions or Restrictions on the Use of Mines, Booby-Traps and Other Devices as amended on 3 May 1996 (Protocol II as amended to the 1980 Convention).
10. Richard F. Grimmett, *Conventional Arms Transfers to Developing Nations, 1994–2001* (Washington: Congressional Research Service, 2002)
11. Richard F. Grimmett, *Conventional Arms Transfers to Developing Nations, 2002–2009* (Washington: Congressional Research Service, 2010)
12. South Eastern Europe Clearinghouse for the Control of Small Arms and Light Weapons (SEESAC), Cross border trafficking in South Eastern Europe - assessing trafficking activities in the Southern Adriatic region, 18.03.2003
13. Stockholm international peace research institute (SIPRI), Mark Bromley and Paul Holtom, IMPORT CONTROLS AND AN ARMS TRADE TREATY, July 2011 available at: [http://books.sipri.org/files/misc/SIPRIBP1107b.pdf]
14. United Nations, Protocol against the Illicit Manufacturing of and Trafficking in Firearms, Their parts and Components and Ammunition, supplementing the United Nations Convention against Transnational Organized Crime, General Assembly resolution 55/255 of 08.06.2001
15. United Nations. Convention against Transnational Organized Crime. 15.11.2000, available_at_[http://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-e.pdf] [23.01.2011];
16. William Hartung and Rachel Stohl, "Hired Guns," *Foreign Policy* (May/June 2004): 28–29
17. Арнаудовски, Љ., Криминологија, Скопје, 2007 година
18. Батковски, Т., Илегални здруженија (банди, организации и групи) создадени од позициите на албанскиот национализам во Македонија во периодот 1945 – 1987 година, Докторски труд, Факултет за Безбедност – Скопје, 1993 година.
19. Димовски Злате, Илегалната трговија со оружје и тероризмот во Република Македонија, Графотранс-Скопје, 2005 година

20. Миодраг, Л., Николовски М., Организиран криминал и корупција, нови теоретски димензии, практични консеквенции и методика на истражување, Скопје, 2010 година
21. Ристов Иван, КРИМИНАЛИСТИЧКА ОБАВЈЕШТАЈНОСТ КАО ДИО НОВЕ ТЕХНИКЕ И МЕТОДЕ БОРБЕ ПРОТИВ ТЕРОРИЗМА, Безбједност–Полиција–Грађани, годинаVII, број1-2/11, Бања Лука, 2011 година.
22. Роберт Хислоп, Затишје пред бура? Влијанието на прекуграничните мрежи, корупцијата и криумчарењето врз стабилноста на Македонија и врз безбедноста во регионот, Документ подготвен за презентација на Годишниот собир на Американското здружение за политички науки за 2001 година, Сан Франциско, Калифорнија

SUMARY

Whenever we mention the term of weapon first association that everyone occur to mind is a war or armed conflict, which is not far from the logic if it takes into the account that the largest percentage of smuggling and illegal and legal trade in arms worldwide appears as a result of the needs of someone armed conflict, whether internal or international. Therefore the international community, concerned about the danger that brings weapons before the Second World War began with the adoption of a convention governing the use and marketing of certain types of weapons. Till this date the documents adopted by the international community that targets problem with weapons for the purpose of our paper can be divided into two parts: Documents which generally regulate certain aspects of smuggling and illegal trafficking in arms, ammunition and explosives that are more related to armed conflicts and human rights (document under international humanitarian law) and documents that regulate more closely smuggling and illegal arms trafficking, ammunition and explosives. What is important for us in terms of smuggling and illegal trade in arms, ammunition and explosives are those international documents in which the international community defines and criminalize this activity. In 2000 was adopted a United Nations Convention against Transnational Organized Crime. But we are specifically interested in the protocol that supplements the United Nations Convention against Transnational Organized crime: United Nations Protocol against the Illicit Manufacturing of and Trafficking in Firearms, Their parts and Components and Ammunition. This protocol is the basic international instrument which sanctions this criminal activity. This document must be the base from where will come every strategic prevention that will be applied in the countries worldwide. All countries in the world must work together and exchange data that are collect by their law enforcement agencies using criminal intelligence.

Prethodno saopštenje - UDK 341.231.14(4)(497.7)

CRIMINAL LAW AND EUROPEAN STANDARDS WITH THE OVERVIEW OF THE CRIMINAL LAW AND THE CONSTITUTION OF REPUBLIC OF MACEDONIA

Assistant Professor PhD Marjan Arsovski
(arsovskim@yahoo.com)
Faculty forSecurity– Skopje

Abstract: European standards had its latest amendment with The Treaty of Lisbon entered into force on 1 December 2009.

Despite the fact that the Treaty amends the Treaty on European Union and the Treaty establishing the European Community it also incorporated the Charter of Fundamental Rights of the European Union as a integrated part. For that reason the EU must act and legislate consistently with the Charter and the EU's courts will strike down EU legislation which contravenes it.

Criminal law of different countries establishes as the body of rules that defines conduct that is not allowed because it is held to threaten, harm or endanger the safety and welfare of people, and sets out the punishment to be imposed on people who do not obey these laws. Criminal law also protect the basic human right established in the Charter of Fundamental Rights of the European Union and the Constitutions.

In this context the research paper aims to show the positive and negative aspects Criminal law regulation of basic human rights envisage in the Charter of Fundamental Rights of the European Union and the Constitution of Republic of Macedonia.

Keywords: Criminal law, European human rights, Constitution.

After the catastrophic events of the First and Second World War, in the minds of European nations has increased the desire for the establishment of a European Union (like USA), driven by the aspiration for a united Europe and to eliminate the possibility of another war on the European continent. However, considering heterogeneous set of languages and cultures in the integration of Europe could not begin with the cultural, military and political integration, and so in the beginning it only integrated economic policies of group of countries from Europe, starting in 1957 with the signing of the Treaty establishing the European Community. In the following decades, the legal architecture of the Community has undergone significant upgrades, except the protection of the basic human rights, which since the Treaty of Lisbon have had insignificant reforms through the introduction of a new chapter in the Basic Agreement, which is " Charter of Fundamental Rights of the European". In this context, this research paper aims to provide significant new findings that a new chapter introduced by the Lisbon Treaty would lead in the better protection of the human rights, thus increasing the EU as a "collective actor" in the international scene.

TREATY OF LISBON

Negotiations to modify the European Union began in 2001, resulting first in the Treatyestablishing a Constitution for Europe, which would have repealed the pre-existing European treaties and replaced them with a "constitution".[1] Although ratified by a majority of Member States, this was abandoned after being rejected by French and Dutch voters in 2005. After a "period of reflection", Member States agreed instead to maintain the pre-existiing treaties, but to amend them, salvaging a number of the reforms that had been envisaged in the constitution. An amending "reform" treaty was drawn up and signed in Lisbon in 2007. The Treaty of Lisbon or Lisbon Treaty is an Reform Treaty that amends the two treaties which form the constitutional basis of the European Union (EU).[2] The Lisbon Treaty was signed by the EU member states on 13 December 2007, and entered into force on 1 December 2009. It amends the Treaty on European Union (TEU; also known as the Maastricht Treaty) and the Treatyestablishing the EuropeanCommunity (TEC) also known as the Treaty of Rome which was renamed to the Treaty on the Functioning of the European Union (TFEU).The Treaty made the Charter of FundamentalRights (the Union's bill of rights,), legally binding and referencing it as an independent document rather than by incorporating it into the treaty itself.

THE CHARTER OF FUNDAMENTAL RIGHTS OF THE EUROPEAN UNION

The Treatyestablishing the EuropeanEconomicCommunity in 1957 did not include any reference to fundamental or human rights. The EEC Treaty was written a few years after the failure of the EuropeanDefenceCommunityTreaty and the EuropeanPoliticalCommunityTreaty. This latter treaty had included rights provisions and Craig and de Búrca argue that, in light of that failure, the drafters of the EEC Treaty wished to avoid any implicitly political elements.[2] In ruling as it did in Handelsgesellschaft the ECJ had, in effect, created a doctrine of unwritten rights which bound the Community institutions.[3] While the court's fundamental rights jurisprudence was approved by the institutions in 1977 and a statement to that effect was inserted into the treaties by the Maastricht Treaty, it was in 1999 that the European Council formally went about the process of initiating the drafting a codified catalogue of fundamental rights for the EU.[4]

The Charter of Fundamental Rights of the European Union enshrines certain political, social, and economic rights for European Union (EU) citizens and

[1] Treaty establishing a Constitution for Europe, Official Journal of the European Union C 310,16 December 2004.

[2] Consolidatedversion of theTreaty on EuropeanUnion, Official Journal of the EuropeanUnion C83,30.3.2010, p1-388

[3] Judgment of the European Court of Justice of 17 December 1970, Internationale*Handelsgesellschaft*, 1970 ECR 1125, Case 11/70.

[4] Joint Declaration by the European Parliament, Council and the Commission concerning the protection of fundamental rights and the ECHR (OJ C 103, 27/04/1977 P. 1-2)

residents, into EU law.[5] It was drafted by the European Convention and solemnly proclaimed on 7 December 2000 by the EuropeanParliament, the Council of Ministers and the European Commission. However its then legal status was uncertain and it did not have full legal effect[1] until the entry into force of the Treaty of Lisbon on 1 December 2009. Following the entry into force of the LisbonTreaty in 2009 the fundamental rights' charter has the same legal value as the European Union treaties. The Charter referred to in the Treaty is an amended version of the 2000 document which was solemnly declared by the same three institutions a day before the signing of the Lisbon Treaty itself. Under the Charter, the European Union (EU) must act and legislate consistently with the Charter and the EU's courts will strike down EU legislation which contravenes it. The Charter only applies to EU member states when they are implementing EU law and does not extend the competences of the EU beyond the competences given to it in the treaties.

The Charter contains some 54 articles divided into seven titles. The first six titles deal with substantive rights under the headings: dignity, freedoms, equality, solidarity, citizens' rights and justice, while the last title deals with the interpretation and application of the Charter. Much of Charter is based on the European Convention on HumanRights (ECHR), the case-law of the European Court of Justiceand pre-existing provisions of European Union law.

I. The first title **dignity**, guarantees:
   1. Human dignity
   2. Right to life
   3. Right to the integrity of the person
   4. Prohibition of torture and inhuman or degrading treatment or punishment
   5. Prohibition of slavery and forced labour.[6]

II. The second title **freedoms** (liberty) guarantees:
   1. Right to liberty and security
   2. Respect for private and family life
   3. Protection of personal data
   4. Right to marry and right to found a family
   5. Freedom of thought, conscience and religion
   6. Freedom of expression and information
   7. Freedom of assembly and of association
   8. Freedom of the arts and sciences
   9. Right to education
   10. Freedom to choose an occupation and right to engage in work
   11. Freedom to conduct a business
   12. Right to property
   13. Right to asylum
   14. Protection in the event of removal, expulsion or extradition

[5] Charter Of Fundamental Rights Of The European Union, Official Journal of the European Union C 83/391, 30.3.2010.

[6] Its provisions are mostly based on the ECHR, although Article 1 closely reflects Article 1 of the German Basic Law

III. The third title **equality** covers,
1. Equality before the law
2. Non-discrimination
3. Cultural, religious and linguistic diversity
4. The Union shall respect cultural, religious and linguistic diversity.
5. Equality between women and men
6. The rights of the child
7. The rights of the elderly
8. Integration of persons with disabilities

IV. The fourth title covers **solidarity (economic)**rights including the
1. Workers' right to information and consultation within the undertaking
2. Right of collective bargaining and action
3. Right of access to placement services
4. Everyone has the right of access to a free placement service.
5. Protection in the event of unjustified dismissal
6. Fair and just working conditions
7. Prohibition of child labour and protection of young people at work
8. Family and professional life
9. Social security and social assistance
10. Health care
11. Access to services of general economic interest
12. Environmental protection
13. Consumer protection

V. The fifth title covers the rights of the EU **citizens** (citizens' rights) such as the
1. Right to vote and to stand as a candidate at elections to the European Parliament
2. Right to vote and to stand as a candidate at municipal elections
3. Right to good administration
4. Right of access to documents
5. European Ombudsman
6. Right to petition
7. Freedom of movement and of residence
8. Diplomatic and consular protection

VI. The sixth title **justice** issues covers
1. Right to an effective remedy and to a fair trial
2. Presumption of innocence and right of defence
3. Principles of legality and proportionality of criminal offences and penalties
4. Right not to be tried or punished twice in criminal proceedings for the same criminal offence

VII. The seventh title concerns the interpretation and application of the Charter.

Article 51(1) of the Charter addresses the Charter to the EU's institutions, bodies established under EU law and, when implementing EU laws, the EU's member states. In addition both Article 6 of the amended Treaty of European Union and Article 51(2) of the Charter itself restrict the Charter from extending the competences of the EU. A consequence of this is that the EU will not be able to legislate to vindicate a right set out in the Charter unless the power to do such is set out in the Treaties proper. And individuals will not be able to take member states to court because they have failed to uphold the rights in the Charter unless the member state in question was implementing EU law. It is this last element of these that has been subject to the most debate.

The Charter is not the first outing for human jurisprudence in the EU. In interpreting the general principles of EU law described above, the European Court of Justice has already dealt the issue of whether those general principles applied to member states. Having ruled in Johnston v Royal Ulster Constabularythat a right to fair procedures was one of the general principles of EU law, in Kremzow v Austria the ECJ had to decide whether or not a member state were obliged to apply that principle in relation to a wrongful conviction for murder.[7]Kremzow's lawyers argued that his case came within the scope of EU law on the grounds that his wrongful conviction and sentence had breached his right to free movement within the EU. The ECJ responded by saying that since the laws under which Kremzow had been convicted were not enacted to secure compliance with EU law, his predicament fell outside the scope of EU law.

It may be noted, however, that the wording in Kremzow, referring to the "field of application of EU law", differs from the wording in the Charter which refers to the implementation of EU law. Although the amended explanatory memorandum issued alongside the Charter in 2007 describes the wording used in the Charter as reflecting ECJ precedent.

THE CONSTITUTION AND CRIMINAL CODE OF THE REPUBLIC OF MACEDONIA IN THE REALIZATION OF THE HUMAN RIGHTS

The Criminal Code of the Republic of Macedonia, i.e the first Macedonian codification of the criminal law, was adopted by the Parliament of the Republic of Macedonia on 23 July 1996 and came into force on November 1, 1996.[8] Its adoption marks the completion of the first phase of the reform of the Macedonian criminal law. This reform was primarily directed towards termination of the leftovers of the former socialist system and its criminal legislation, and moving toward securing an effective protection of the new democratic values, rule of law and human rights and freedoms against the criminal conducts. The reform took place several years after

[7] Judgment Of The Court (Fifth Chamber) of 29 May 1997 in Case C-299/95 (reference for a preliminary ruling from the ObersterGerichtshof): Friedrich Kremzow, WilfriedWeh, intervening v. RepublikÖsterreich (Article 164 of the EC Treaty - European Convention on Human Rights - Deprivation of liberty - Right to a fair trial - Effects of a judgment of the European Court of Human Rights). OJ C 212, 12.7.1997, p. 2–2.

[8] Criminal Code of the Republic of Macedonia,"OfficialGazette" no. 37/96: 80/99, 4/2002, 43/2003, 19/2004, 81/2005, 60/2006, 73/2006, 7/2008, 139/2008, 114/2009.

the proclamation of the Constitution of the independent and sovereign Republic of Macedonia in 1991.[9] Such delay created a broad area for development of the new forms of criminal activities in the privatization of the social capital, corruption, abuse of power, terrorism and acts of violence. This period was marked by striking tendency towards crime organizationand liaison between the criminal and the state-political structures.[10]

The Constitution, as the fundamental law of a state, contains the principles and provisions for human rights and freedoms, guarantees for their protection, as well as other provisions under the jurisdiction of the state authorities that directly refer to the criminal law. The Constitution proclaims the principles of the legality, the presumption of innocence, the prohibition of retrial for the same offense, the prohibition of extradition of national citizens and the right to asylum, the prohibition of death penalty, the guarantee of the right to exist and other fundamental rights, such as: prohibition of torture, right to a counsel, etc..

Constitution guarantied personal freedoms rights are grouped in four fields(divisions):

1. Personal freedoms and rights
   Right to life
   Right to protection of physical and moral integrity
   Right to prohibit discrimination
   Right to equality before the law
   Right to judicial pronouncement of sentence
   Right to freedom
   Right to privacy
   Freedom of movement and occurrence
   Freedom of thought and belief
   Freedom of religion
   Right to citizenship

2. Political freedoms and rights
   Freedom of public speech
   Freedom of political association
   Freedom of information
   The right of peaceful assembly
   suffrage
   Right of complaints and performing public functions

3. Economic freedoms and rights
   Right to property
   Right of inheritance
   Freedom to work and rights at work
   Right of trade unions and to strike
   Social freedoms and rights

[9] Constitutionof the Republic ofMacedonia, Official Gazetteno.52of 1991.
[10] Проф.д-р ВладоКамбовски.,Казненоправо-општдел, Скопје, 2006 год.,стр.150

4. Cultural freedoms and rights
Right to education
Freedom of scientific and artistic creativity
Freedom of expression of national affiliation.

At the same time, the Constitution is an organic law of the state itself, by which, what isparticularly important for the criminal law, the society determines the relationship between state and individual in the exercise of the power and sets limits on the state power of punishment. Emphasizing the undeniable fact of its ground bearing significance as a basic legal act, it leads us to a very simplified opinion about the central position of the Constitution in the legal system and, thus, its supremacy over the other branches of the law including the criminal law.

The protective function of the Criminal code is concentrated primarily on the human rights and freedoms. They are the core of the orientation of the basic instruments-sentence and other sanctions, through which the criminal code accomplishes its functions. On the other hand, the human rights and freedoms shall not and cannot be creation of the Constitution. They are natural and unconditional freedoms and rights, which must be observed by the Constitution itself. Thus, the constitutional principles and guarantees having criminal meaning are only an expression of the recognition and respect of their meta-juristic, meta-constitutional pre-existence and an useful reinforcement of their recognition, that may not be explicitly stated in the Constitution in order to exist. The guarantees of the human rights and freedoms, as well as the basic criminal code principles, may be found in some other acts, such as: the French Declaration of the right of the human from 1789.[11] The personal freedoms and rights protect and express the physical and spiritual integrity of the human and its legal position in the society. The oldest freedoms and rights were established in 16th and 17th century with the rise of the rationalism and the philosophy of John Locke. The first recognized personal liberties and rights are: the right to exist/life, liberty/freedom, property, happiness and freedom of conscience. The civil society, autonomous in relation to the state power, has been established on basis of these rights. These rights are pre-condition to exercise the other freedoms and rights. They are natural rights.[12] The exercise of these fundamental freedoms and rights of the human and citizen are included in the Article 50 of the Constitution of the Republic of Macedonia. The Constitution also provides for a legal protection for proceedings in front of the courts and proceedings in front of the Constitutional Court.[13] Thus, under the paragraph 1 of this Article of the Constitution, every citizen may request protection of the freedoms and rights set in the Constitution in front of the courts and the Constitutional Court of the Republic of Macedonia, in a procedure based on priority and urgency. With the same article, paragraph 2, the Constitution guarantees judicial protection of the legality of the individual acts performed by the state administration and other institutions executing public authorities.[14]

---

[11] Проф.д-р ВладоКамбовски.,Казненоправо-општдел, Скопје, 2006 год.,стр.27

[12] Проф.д-р ВладимирОртаковски.,Уставноправо(Прирачник – белешкиодпредавањата), Скопје, 2008 год.,стр 71

[13] СавоКлимовски, ВладимирМитков, ТатјанаКаракамишева и РенатаТренеска, Уставноправо и политичкисистем, Скопје, 2003.

[14] СветомирШкариќ, Споредбено и македонскоуставноправо, Матицамакедонска, Скопје 2004.

Courts protect the human rights and freedoms by addressing specific cases within their jurisdiction in proceedings prescribed by the laws (Law on Criminal Procedure, Law on Civil Procedure, Law on Administrative Disputes). (REF) The Constitutional Court protects the freedoms and rights, directly deciding upon specific complaints for protection of freedoms and rights, and indirectly, by assessing the constitutionality of the laws and constitutionality and legality of other regulations and general acts.[15]

The basic concept of the Macedonian Criminal code and the essence of its institutes is determined (as the leading philosophical ideas with legal and criminal-political content and features) by several principles that make the base ground for the contemporary Criminal law.

The principle of legality has the prime importance: no offense, no punishment or other sanction without a law. This principle is also integrated in the MCC (Macedonian Criminal Code): none can be sentenced or charged with other criminal sanction for an offense which, before it took place, was not prescribed in a law as a criminal offense and was not subject to a prescribed penalty by a law. Complementary to the legislators, other state bodies and courts, also the citizen is subject to the principle of legality. The citizen's liability to unconditional observance of the positive criminal norms is inherent part of the range of his/her rights and freedoms: there will be no freedoms and rights without fulfilling this liability, as otherwise the freedoms and rights of the individual can be abused because of the violation of the equal rights and freedoms other citizens.

The most of incriminations are based on prohibiting norms (prohibition of murder, prohibition of theft, tec.). The citizen meets such norms simply by failing to take prohibited action. Much less incriminations are based on imperative norms (failure to render aid, failure to report an offense, etc..). In such cases the individual is liable to adhere to the criminal code by taking activities for fulfillment of the norms set in the law. For the purpose of this action, the legal prohibitions must be simple, clear and understandable for everyone, and the law in which set has to be not only published, but widely distributed and explained, in order for citizens to be able to familiarize themselves with the legal provisions. On the other hand, this principle within its total meaning aims at guaranteeing the legal security of citizens. This means to protect the citizens from the supremacy the law maker to adopt laws that are not necessary and useful for the society or supremacy of the court and other state bodies in law enforcement. The content of the notion of legal security has two meanings: reliability/security and consistency of the legal order as such and legal security of the social life. Relationship of these two aspects grows from the unity of the normative and the real, and it opens the relation between the abstract and specific legal security which is reflected in the court's decision as res iudicata and the judicial precedent as an expression of the legal security. This dimension of the principle of legality - consistency and security/reliability in the judicial decisions is becoming more important given the shift of the modern criminal law toward the offender's personality and thus related extension of the judicial power in determining the sentence.

[15] http://www.ihr.org.mk/mk/praven-dijalog/praven-dijalog-br5/148-pravnata-zastita-na-covekovite-prava

On the other hand, the special role of the court and the court decision guaranteeing the legal safety is repeatedly emphasized by the strengthening of the court function as guarantor in protection of the human rights. It emphasizes the cooperative role of the court in ensuring legal safety and security. Further to this, the so-called judicial precedent or the case law as source of the criminal law becomes increasingly important. In the Macedonian system of criminal law, the court rulings do not constitute a source for criminal law.[16]

Pursuant to the above it can be concluded that the Constitution as the highest legal act which proclaims and defends the fundamental human rights is of particular importance for the criminal law, which in turn sets the relation between the state and the individual in exercising the power and limits the state's right to sanctioning.

REFERENCES:

1. Charter Of Fundamental Rights Of The European Union, Official Journal of the European Union C 83/391, 30.3.2010.
2. Consolidatedversion of theTreaty on EuropeanUnion, Official Journal of the EuropeanUnion C83,30.3.2010, p1-388
3. Constitutionof the Republic ofMacedonia, Official Gazetteno.52of 1991.
4. Criminal Code of the Republic of Macedonia,"OfficialGazette" no. 37/96: 80/99, 4/2002, 43/2003, 19/2004, 81/2005, 60/2006, 73/2006, 7/2008, 139/2008, 114/2009.
5. Joint Declaration by the European Parliament, Council and the Commission concerning the protection of fundamental rights and the ECHR (OJ C 103, 27/04/1977 P. 1-2)
6. Judgment Of The Court (Fifth Chamber) of 29 May 1997 in Case C-299/95 (reference for a preliminary ruling from the ObersterGerichtshof): Friedrich Kremzow, WilfriedWeh, intervening v. RepublikÖsterreich (Article 164 of the EC Treaty - European Convention on Human Rights - Deprivation of liberty - Right to a fair trial - Effects of a judgment of the European Court of Human Rights). OJ C 212, 12.7.1997, p. 2–2.
7. Judgment of the European Court of Justice of 17 December 1970, Internationale*Handelsgesellschaft*, 1970 ECR 1125, Case 11/70.
8. Treaty establishing a Constitution for Europe, Official Journal of the European Union C 310,16 December 2004.
9. Проф.д-р Владимир Ортаковски., Уставноправо (Прирачник белешкиодпредавањата), Скопје, 2008 год.,стр 71.
10. Проф.д-р ВладоКамбовски.,Казненоправо-општдел, Скопје, 2006 год.,стр.150
11. СавоКлимовски, ВладимирМитков, ТатјанаКаракамишева и РенатаТренеска, Уставноправо и политичкисистем, Скопје, 2003.
12. СветомирШкариќ, Споредбено и македонскоуставноправо, Матица македонска, Скопје 2004.

[16] Проф.д-р ВладоКамбовски.,Казненоправо-општдел, Скопје, 2006 год.,стр.159,164

CONCLUSION

The peoples of Europe create a Union based on common values, where problems are peaceful resolved and there common interest are protected.

With the adoption of the Charter of Fundamental Rights of the European Union, the Union contributes to the preservation and to the development of these common values while respecting the diversity of the cultures and traditions of the peoples of Europe.

The Charter reaffirms, with due regard for the powers and tasks of the Union and for the principle of subsidiarity, the rights as they result, in particular, from the constitutional traditions and international obligations common to the Member States, the European Convention for the Protection of Human Rights and Fundamental Freedoms, the Social Charters adopted by the Union and by the Council of Europe and the case-law of the Court of Justice of the European Union and of the European Court of Human Rights.

Enjoyment of these rights entails responsibilities and duties with regard to other persons, to the human community and to future generations.

However the idea that the purely economic end of the new EEC Treaty would be unlikely to have any implications for fundamental rights was soon to be tested.

To this end, it is necessary to strengthen the protection of fundamental rights in the light of changes in society, social progress and scientific and technological developments by making those rights more visible in a Charter.

In Republic of Macedonia, the court and the court decision have special role guaranteeing the legal safety emphasizing the court function as guarantor in protection of the human rights. It stresses the helpful role of the court in ensuring legal safety and security. Further to this, the judicial precedent becomes increasingly important.

From the above it can be concluded that the Constitution of the Republic of Macedonia as the highest legal act which proclaims and defends the fundamental human rights is of particular importance for the criminal law, which in turn sets the relation between the state and the individual in exercising the power and limits the state's right to sanctioning.

Prethodno saopštenje – UDK 341.231.14(4)

PRISONERS'HEALTH CARE: DEPRIVED OF THEIR LIBERTY NOT THEIR DIGNITY

Assistant Professor Marija Milenkovska
Faculty of Security – Skopje
e mail: marijamilenkovska@yahoo.com

Abstract: Everyone has right to enjoy the highest possible standard of health attainable, including the prisoners. Health policy in prisons shall be compatible with, national health policy. Within the Council of Europe number of acts are adopted that established standards regarding the quality of health care that should be provided to prisoners. At the same time, there is a developing jurisprudence of the European Court of Human rights upholding the obligation of the State to safeguard the health of the prisoners in its immediate jurisdiction. In this regard, the paper analyses the European standards regarding the health care in prison. Based on this analysis, the author argues that the State is obliged to protect the health and physical well-being of persons deprived of their liberty, by providing them with the requisite medical assistance even in times of economic difficulty. In addition, the author assesses the compatibility of Macedonian prisoners' health care system with the European standards.

Key words: Council of Europe, health care, prisoners.

INTRODUCTION

Article 1 of the European Convention on Human Rights and Fundamental Freedoms (ECHR) provides that the High Contracting Parties shall secure to everyone within their jurisdiction the rights and freedoms defined in this Convention. Therefore, the state has obligation not only to refrain from the activities and measures that arbitrary interference with the human rights and freedoms (negative obligations), but also to take certain activities and measures to protect the human rights and freedoms (positive obligations) within its jurisdiction (including the right to life and prohibition of torture). According to Akadji-Kombe such measures may be judicial (where the state is expected to lay down sanctions for individuals infringing the Convention, whether it issues legal rules for a kind of activity or for a category of persons), but they may also consist of practical measures (for example, of the measures which prison authorities are required to take in certain cases to prevent prisoner suicides).[1]In addition, he argues that the two kinds of measure – legal and practical – may even prove necessary at the same time (it is a question of circumstance).[2]

[1] Jean-François Akandji-Kombe, (2007) Positive Obligations under the European Convention on Human Rights, A guide to the implementation of the European Convention on Human Rights, Council of Europe, p.7.
[2] Ibid.

The duty of the State to protect the human rights and freedoms is particularly stringent where a person is in its immediate jurisdiction (prison, custody).The European Court of Human Rights (the ECtHR) - set up to ensure the observance of the engagements undertaken by the states in ECHR- observes that persons in custody are in a particularly vulnerable position and the authorities are under an obligation to account for their treatment.[3] [4]However, whether the State is obliged to provide (free of charge) prompt and adequate health care to prisoners? Unambiguously, yes. The prisoners regardless their legal status, as well as the nature of their offence[5]have right to enjoy the highest possible standard of health attainable. The Convention requires the State to protect the health and physical well-being of persons deprived of their liberty, for example by providing them with the requisite medical assistance.[6] A sharp deterioration in a person's state of health in detention facilities inevitably raises serious doubts as to the adequacy of medical treatment there.[7] The State responsibility under ECHR is greater where that individual dies. Thus, where a detainee dies as a result of a health problem, the State must offer a reasonable explanation as to the cause of death and the treatment administered to the person concerned prior to his or her death.[8]In this regard, the ECtHR has developed certain principles considering prisoners' health care [9] obligated for the state through extensive interpretation of the ECHR and the positive obligations it imposes. The ECtHR in its judgment stresses the importance of the relevant recommendations (Recommendation No. R (98) 7 concerning the ethical and organizational aspects of health care in prison; Recommendation Rec(2006)2 on the European Prison Rules) adopted by the Committee of Ministers of the Council of Europe.

At the same time, the European Commttiee for the Prevention of Torture and Inhuman or Degrading Treatment or Punishment (CPT) was established under the European Convention for the Prevention of Torture and Inhuman or Degrading Treatment or Punishment (1987). The CPT by means of visits examines the treatment of the persons deprived of their liberty with view to strengthening if necessary, the protection of such persons from torture or degrading treatment or punishment.[10]An inadequate level of health care can lead rapidly to situations falling within the scope of the term "inhuman and degrading treatment".[11] Thus, it is obvious that the prison

[3] Kats and others v Ukraine, no.29971/04, 18 March 2009, para. 104.

[4] All judgments of the ECtHR are available at: www.echr.coe.int/ECHR/EN/Header/Case-Law/Hudoc/Hudoc+database.

[5] For example in the case Dybeku v Albania (where the applicant complained of the inadequacy of his medical treatment) the Court considers that the fact that the applicant was found criminally responsible for an offence of homicide and sentenced to life imprisonment is not decisive for the question whether the authorities fulfilled their obligation under Article 3 of the ECHR.See: Dybeku v Albania, no. 41153/06, 2 June 2008, para.42.

[6] Kats and others v Ukraine, no. 29971/04, 18 March 2009, para.104.

[7] Makharadze and Sikharulidze v. Georgia, no. 35254/07, 22 November 2011, para.72.

[8] Ibid,

[9] The Coyle concludes that The ECtHR is producing an increasing body of case law confirming the obligation of states to safeguard the health of prisoners in their care. See: Andrew Coyle, (2007) Standards in Prison Health: prisoners as a patient in Lars Møller et al (Eds.), Health in prisons A WHO guide to the essentials in prison health, WHO, p.8.

[10] Article 1, European Convention for the Prevention of Torture and Inhuman or Degrading Treatment or Punishment (1987),

[11] CPT, 3rd General Report [CPT/Inf (93) 12], paragraph 30.

health care falls within the CPT's mandate and it developed ceriain standards regarding this issue. As *Murdoch* notes numerous human rights bodies (treaty based or otherwise) are involved in monitoring standards (considering prisoners' rights) through country visits and thematic investigation, and shortcomings in compliance can result in making the non-binding recommendation to the countries and to the adoption to additional statements of expectations.[12]The standards established by the CE (case law of the ECtHR, CPT's standards, conventions, recommendations) regarding prison health care as well as their implementation in the Republic of Macedonia is subject of analysis in addition of this paper.

RIGHT TO HEALTH CARE IN PRISON

Access to a doctor is the main characteristic of the right to health care in prison.[13]Prisoners should have access to a doctor, when necessary, at any time during the day and the night.[14] The access to doctor is the key consideration which have guided the CPT[15] during its visits to prison health care services.[16] At the same time, the medical treatment of sick prisoner should be adequate to his particular condition. Sick prisoners who require specialist treatment shall be transferred to specialised institutions or to civil hospitals, when such treatment is not available in prison.[17]The ECtHR observes the right to health or health care of the prisoners under the Article 2 (the obligation to protect the life of individuals in custody also implies an obligation for the authorities to provide them with the medical care necessary to safeguard their life)[18]and the Article 3 (the lack of appropriate medical care may amount to treatment contrary to prohibition of torture)[19]of the ECHR. However, as *Mowbray* concludes we can discern a considerable similarity in the development of positive obligations under Article 3 and those under Article 2 (including the duty to provide adequate medical care to detainees)[20]

The ECtHR considers three elements in relation to the compatibility of an applicant's health with his stay in detention: the medical condition of the prisoner, the adequacy of the medical assistance and care provided in detention, and the advisability

[12] Jim Murdoch, (2006), The Treatment of Prisoners European Standards, Council of Europe Publishing, p. 21.

13 European Prison Rules provides that prisoners shall have access to the health services available in the country without discrimination on the grounds of their legal situation. See paragraph 40.3.

[14] Recommendation No. R (98)7 of the Committee of Ministers concerning the ethical and organizational aspects of health care in prison, paragraph 4.

[15] CPT, 3rd General Report [CPT/Inf (93) 12], paragraph 32.

[16] In its reports the Committee points out that while in custody, prisoners should be able to have access to a doctor at any time, irrespective of their detention regime See CPT, 3rd General Report [CPT/Inf (93) 12], para. 4.

[17] Rec(2006)2 of the Committee of Ministers to member states on the European Prison Rules, para. 46.1.

[18] Makharadze and Sikharulidze v. Georgia, no. 35254/07, 22 November 2011, para. 71.

[19] Dybeku v Albania, no. 1153/06, 2 June 2008, para. 41.

[20] Alastair Mowbray, (2004) The Development of the Positive Obligations under European Convention on Human Rights by the European Court of Human Rights, Hart Publishing, Oxford, Portland, Oregon, p. 64-65.

of maintaining the detention measure in view of the state of health of an applicant.[21]In number of its judgments the ECtHR emphasizes the right of all prisoners to conditions of detention which are compatible with human dignity, so as to ensure that the manner and method of execution of the measures imposed do not subject them to distress or hardship of an intensity exceeding the unavoidable level of suffering inherent in detention; in addition, besides the health of prisoners, their well-being also has to be adequately secured, given the practical demands of imprisonment.[22]According the Coyle a number of countries experience great difficulty in providing health care of a reasonable standard to the population at large.[23]The ECtHR does not underestimate the significance of financial difficulties of the State. However it noted that in any event, a lack of resources cannot in principle justify detention conditions which are so poor as to reach the threshold of severity for Article 3 to apply.[24] In this context, the CPT has stated that even in times of grave economic difficulty nothing can relieve the state of its responsibility to provide the necessities of life to those whom it has deprived of liberty.[25] The ECHR could not be interpreted as laying down a general obligation to release a detainee on health grounds.[26]However, as Brems observes in a number of cases, the Court has found the very detention of a seriously ill person in itself to constitute a violation of Article 3.[27]Thus, in the case *Mouisel v France* the applicant who had been sentenced to fifteen years' imprisonment for armed robbery, false imprisonment and fraud claimed that his state of health (he was suffering from chronic lymphocytic leukemia) was incompatible with his continued imprisonment. The ECtHR said that continued detention undermined his dignity and entailed particularly acute hardship that caused suffering beyond that inevitably associated with a prison sentence and treatment for cancer and it concluded that France has violated the Article 3 of the ECHR.

The ECtHR particularly criticized the State failure to secure prisoner prompt access to doctor or to relevant medical tests which are indispensable for early and accurate diagnosis.[28]At the same time, the medical treatment of the prisoner by prison administration should be adequate to his particular condition. According to ECtHR the adequacy of medical assistance is always the most difficult element to determine.[29] Therefore, the ECtHR *must reserve, in general, sufficient flexibility, defining the required standard of health care, which must accommodate legitimate demands of imprisonment but remain compatible with the human dignity and the due discharge of its positive obligations by the State, on a case-by-case basis*.[30]Based on the jurisprudence of the ECtHR it could be established that the Court is not willing to

[21] Dybeku v Albania, no. 1153/06, 2 June 2008, para. 42
[22] Mouisel v France 67263/01, 21 May 2003,, no. para.40
[23] Andrew Coyle, (2009), A Human Rights Approach to Prison Management, Handbook for Prison Staff, 2nd Edition, International Centre for Prison Studies, p. 48.
[24] Dybeku v Albania, no. 1153/06, 2 June 2008, para. 50.
[25] Andrew Coyle, op.cit., p. 48.
[26] Dzieciak v Poland, no.77766/01, 9 March 2009, para. 91.
[27] Eva Brems,(2007), Indirect protection of social rights by the European Court for Human Rights in Exploring Social Rights: between theory and practice edited by Barak Erez Daphne and Gross M. Aeyal, Hart Publishing, Oxford, p. 143.
[28] See for example, Makharadze and Sikharulidze v. Georgia, no. 35254/07, 22 November 2011, para. 77.
[29] Ibid, 77.
[30] Ibid.

accept following omissions (having regarded all circumstances of the particular case) in medical treatment of prisoner: the lack of cooperation and coordination between the various state authorities;[31]the failure to take into account his health in the automatic extension of his detention;[32] the failure to transport him to hospital for scheduled operations[33] or for special treatment required; omission in supervision; failure to develop special hygiene or exercise regime particularly important in treatment of certain disease;[34] treatment as an ordinary rather than an emergency case;[35] the lack of supervision of daily taking of medication (particularly in case of mental illness);[36] the failure to take into account his mental state in disciplinary punishment (detention in punishment cell).[37]

ORGANIZATION OF PRISON HEALTH CARE

Health care in prison shall be integrated into, and compatible with, national health policy.[38]All necessary medical, surgical, physiatrist and dental service including those available in the community in conditions comparable to those enjoyed by the general public should be provided to the prisoners. As CPT stated: "*a prison health care service should be able to provide medical treatment and nursing care, as well as appropriate diets, physiotherapy, rehabilitation or any other necessary special facility, in conditions comparable to those enjoyed by patients in the outside community*."[39]At the same time, the prison health system should include services of the preventive and social medicine (supervision of the quantity, quality, preparation and serving of food, supervision of hygiene, suicide prevention, prevention of transmitted diseases, prevention of violence, limitation of the disruption of family and social ties), as it should guarantee effective supervision of the pharmacy and of the medicaments, including of their preparation, distribution and consummation.[40]

The State is obligated to provide that prison health system is appropriate equipped in terms of human resources (doctors, nurses, technical staff),[41]premises, equipment, medicaments, installations. Prison health care system shoul be organised

[31] Dzieciak v Poland, no.77766/01, 9 March 2009, para. 101.
[32] Ibid.
[33] Ibid.
[34] Longvinenko v Ukraine, no.3448/07, 14 January 2011, para. 74
[35] Dzieciak v Poland, no.77766/01, 9 March 2009, para. 101.
[36] Renolde v France no.5608/05 16 October 2008, para. 101.
[37] Ibid, paras. 106-109.
[38] Recommendation Rec(2006)2 of the Committee of Ministers on the European Prison Rules, para. 40.2.; Recommendation No. R (98)7of the Committee of Ministers concerning the ethical and organizational aspects of health care in prison, para. 10.
[39] CPT, 3rd General Report [CPT/Inf (93) 12], para. 38.
[40] Thus in the case Renolde v France (suicide of prisoner) the Court has serious doubts as to the advisability of leaving it to a prisoner suffering from known psychotic disorders to administer his own daily medication without any supervision.
[41] European prison rules provides: Every prison shall have the services of at least one qualified general medical practitioner; Arrangements shall be made to ensure at all times that a qualified medical practitioner is available without delay in cases of urgency; Where prisons do not have a full-time medical practitioner, a part-time medical practitioner shall visit regularly; Every prison shall have personnel suitably trained in health care (paras.40.1-40.4).

in manner that enables coordination and cooperation (for example: consultation) with the local public and private health institutions as well as possibility of timely transfer the sick prisoner, when necessary, to specialized institutions or civil hospital. Also, there should be coordination and communication within the prison health system, and effective mechanism for supervision and control of the quality of the medical services need to be established. The role of the ministry responsible for health should be strengthened in the domain of quality assessment ofhygiene, health care and organisation of health services in custody, in accordance with national legislation.[42]A clear division of responsibilities and authority should be established between the ministry responsible for health or other competent ministries, which should co-operate in implementing an integrated health policy in prison.[43]

The national authorities must ensure that every prisoner is examined by doctor as soon as possible after his admission in prison. The CPT in its reports reiterates the importance of medical screening of prisoners on admission above all because such screening is indispensable, in particular in the interests of preventing the spread of transmissible diseases, suicide prevention and the timely recording of any injuries.[44]

In organization of the prison healthcare particular attention should be paid (special appropriate equipped facility for accommodation and treatment within the prison, reinforced monitoring, isolation where is absolutely necessary and based on medical reasons only, specialist treatments, transfer in hospital, socio-therapeutic programs, etc.) to certain categories of particular vulnerable groups: mentally ill prisoner;[45]persons identified as suicide risk; drug, alcohol or medicaments addicts; prisoners infected with HIV/AIDS or other transmissible diseases; women, pregnant women, mother and children; adolescents; persons unsuited to continued detention.[46] [47]

PRISON HEALTH CARE PERSONNEL: TRAINING, DUTIES AND RESPONSABILITIES

European prison rules provides that the medical practitioner shall have the care of the physical and mental health of the prisoners and shall see, under the conditions and with a frequency consistent with health care standards in the community, all sick prisoners, all who report illness or injury and any prisoner to

[42] Recommendation No. R (98)7of the Committee of Ministers concerning the ethical and organizational aspects of health care in prison, para. 12.
[43] Ibid.
[44] CPT, (2008), Report to the Government of the RM, CPT/Inf (2008) 5, p .44.
[45] CPT argues that a mentally ill prisoner should be kept and cared for in a hospital facility which is adequately equipped and possesses appropriately trained staff which could be a civil mental hospital or a specially equipped psychiatric facility within the prison system. See CPT, 3rd General Report [CPT/Inf (93) 12], para.43.
[46] In CPT's opinion typical examples of this kind of prisoner are those who are the subject of a short-term fatal prognosis, who are suffering from a serious disease which cannot be properly treated in prison conditions, who are severely handicapped or of advanced age. See CPT, 3rd General Report [CPT/Inf (93) 12], para.70.
[47] See more in Recommendation No. R (98)7of the Committee of Ministers concerning the ethical and organizational aspects of health care in prison, paras. 36-71; CPT, 3rd General Report [CPT/Inf (93) 12], paras. 41-44; 52-70.

whom attention is specially directed.[48] Medical practitioner *inter alia* is obliged to diagnose any physical and mental illness of the prisoners and to take all measures necessary to its treatment; to identify any psychological or other stress brought on by the fact of deprivation of liberty; to identify, to treat and to prevent the spreading of transmissible diseases; to deal with withdrawal symptoms resulting from use of drugs, medication or alcohol.[49] At the same time, the medical personnel should inform the prisoners (as the prison staff) about the risks to their health and about the health care in prison and should develop appropriate health education programme and should provide training to prisoners and employees. Medical practitioners should not disregard their duties (to inspect and to advise the competent authorities) regarding the food and clothing of the prisoners and hygiene and material conditions in which they live (lighting, ventilation, sanitation, heating, overcrowding). Also, the doctor and other medical staff should pay particular attention to persons held in solitary confinement. Medical practitioner shall report to the director whenever it is considered that a prisoner's physical or mental health is being put seriously at risk by continued imprisonment or by any condition of imprisonment, including conditions of solitary confinement.[50]

Prison health care personnel has important role in recording torture or ill-treatment. As *Restellini* observes a doctor working in prisons may be called upon to perform two, somehow opposing roles: firstly that of care giver to the detainee as patient, and secondly that of independent medical expert asked to provide medical evidence concerning the patient to a court or other judicial process. [51]Medical practitioners in prison are obliged to record any sight of torture or ill-treatment and to report them to competent authorities.

Medical personnel engaged in prison should be provided with appropriate knowledge (versed in both general medical and psychiatric disorders)[52] and professional capacity[53] for the work it does (including knowledge about the relevant -national and international- prison regulation). According CPT prison doctors and nurses should possess specialist knowledge enabling them to deal with the particular forms of prison pathology and adapt their treatment methods to the conditions imposed by detention.[54]The doctor (medical personnel) should be regularly trained. In this regard, Recommendation R (98) provides that their training should comprise the acquisition of initial theoretical knowledge, an understanding of the prison environment and its effects onmedical practice in prison, an assessment of

---

[48] Recommendation Rec(2006)2 of the Committee of Ministers on the European Prison Rules, para.

[49] See for example, Recommendation Rec(2006)2 of the Committee of Ministers on the European Prison Rules, para. 42.3;

[50] Ibid, para. 43.3;

[51] Jean-Pierre Restellini, Prison-specific ethical and clinical problems in Lars Møller, HeinoStöver, Ralf Jürgens, Alex Gatherer and Haik Nikogosia, op.cit., p. 34.

[52] See paragraph 34 of the Recommendation No. R (98)7of the Committee of Ministers concerning the ethical and organizational aspects of health care in prison.

[53] CPT even suggests that the specific features of the provision of health care in a prison environment may justify the introduction of a recognized professional specialty, both for doctors and for nurses, on the basis of postgraduate training and regular in-service training; See CPT, 3rd General Report [CPT/Inf (93) 12], para. 77.

[54] See CPT, 3rd General Report [CPT/Inf (93) 12], para. 75.

their skills, and a traineeship under the supervision of a more senior colleague.[55] Prisoners' health care decisions could be governed only by medical criteria (complete professional independence), and any physical examination or medical intervention could be undertaken only by prisoner's consent. Medical confidentiality should be guaranteed and respected.[56]

MACEDONIAN PRISONERS' HEALTH CARE SYSTEM

The Republic of Macedonia (RM), as a member state of the Council of Europe, is obliged to completely implement and adhere to Strasburg standards concerning the treatment and the protection of convicts. The new Law on Execution of Sanctions (2006), represents a step forward in respect of the treatment of prisoners, including the ones in the field of health care. The Law is trying to balance between the goals of the sanctions and the protection of society and the victim on the one hand, and the dignity of the convicts and the need of enabling their successful reintegration in the society on the other hand. The convicts during imprisonment, are guaranteed protection of their psycho-physical and moral integrity and the right to personal safety.[57] At the same time, the Law prohibits any form of torture, inhumane or degrading treatment and establishes a mechanism of control over the operation of the penitentiaries and the correctional institutions, i.e. over the execution of the punishment.

The convicts, in accordance with the positive legal regulations of RM, are entitled to health care according to general regulations on expense of the Budget of the RM. The Law on Execution of Sanctions considers organizing of health care departments inside the penitentiaries and the correctional (education-correctional) institutions, and imposes obligatory hiring of a medical doctor in these institutions, who is going to care for the inmates' health. In addition to that, the legal regulations of RM allocate medical screening for each convict during entry into the correctional institution, registering and keeping their medical records (issuing a personal card of the convicted person), as well as a possibility for a sick person to be examined by a specialist at his/her own expense. The Law on Execution of Sanctions guarantees special treatment appropriate to their condition, to the convicts who are diagnosed with physical and mental disorders or certain addictions,[58]the convicts who are suspected of an infectious disease, or who have manifestations of a physical or a mental impairment that can interfere with them fitting in the surroundings, [59]as well as the convicts who would succumb to a mental illness and would show a severe mental disorder determined by a psychiatrist during the course of the

[55] Recommendation No. R (98)7of the Committee of Ministers concerning the ethical and organizational aspects of health care in prison, para. 34.
[56] Ibid, para. 13.
[57] Law on Execution of Sanctions, Official Gazette of the RM no. 2/2006; 57/2010.
[58] According to the article 126 of the Law on Execution of Sanctions, they undergo medical treatment in the institution when it is needed based on the findings of a physician and are referred to an appropriate health care facility.
[59] According to the article 127 of the Law on Execution of Sanctions, after the findings and a referral by a physician, they would be placed in separate rooms in the institution.

imprisonment.[60] Special treatment is provided to female inmates who are pregnant or have just given birth. It should be noted here that the law stipulates the possibility for imposing solitary confinement as a form of disciplinary action, in a manner which would protect the convict's health. In that direction, the action will either not be executed or will be terminated if it endangers the convict's health. In this case the disciplinary action will be replaced by a milder sentence (Article 182)

Pursuant to the Law on Execution of Sanctions, a series of bylaws have been adopted in order to more accurately regulate the way the prison sentence is carried, i.e. higher efficiency and professionalism of the staff / officials involved in the implementation of the treatment of the inmates in the prison and the correctional institution; Also, in collaboration with the OSCE Spillover Monitor Mission, a Programme for treatment of certain vulnerable categories of inmates was prepared (inmates who are addicted to drugs and psychotropic substances, inmates who are alcohol abusers, sexual delinquents, violent inmates, and inmates convicted of violent crimes, juveniles and young adults, female inmates, lifelong convicts).[61] What is important for the purpose of this paper is the fact that there was a Manual of the Instrument for assessment of the risk and the needs of the inmates. The Government of RM on April 27, 2010 adopted the Strategy for re-socialization and social adaptation of inmates who are doing time (2010-2012)[62] directed mainly towards improvement of material conditions and personnel staffing in the prisons, as well as the system of re-socialization and social adaptation of inmates, which according to CPT is a positive development in this area.[63]

Nonetheless, despite the positive changes that RM has undertaken in order to harmonize the Macedonian penitentiary system with the European one, the system of health care for the prisoners in RM is not in accordance with the European standards in the part of legislative, as well as their application and implementation in practice. Despite the serious criticism by relevant domestic and international institutions which our country has been facing for a longer period, there is a general impression that it does nothing or very little in order to overcome the flaws in the system of health protection of the prisoners. As the CPT concluded in its 2012 report: "*the findings of the 2010 visit demonstrate that, with the exception of Štip Prison, little progress has been made in the prisons visited to improve the provision of health care to prisoners. There remain a number of important structural deficiencies in this area.*" [64]Therefore, we shouldn't be surprised by the fact that the majority of complaints recently lodged by convicted persons with the Ombudsman are related to health protection.

The Republic of Macedonia has not fully implemented in practice the European and national standards for medical protection of prisoners. Prison

[60] According to the article 127 of the Law the correctional institution would refer them to the appropriate medical facility for treatment and shelter until there is no need of further treatment and shelter, which is regulated by general guidelines.

[61] Directorate for execution of sanctions, (2011), Annual report about the conditions and the work of penitentiaries and correctional institutions for 2010, Skopje, pp.10-11.

[62] Ibid, p. 9.

[63] CPT, (2012), *Report to the Government of the Republic of Macedonia on the visit to Republic of Macedonia carried out by CPT from 21 September to 1 October 2010*, CPT/Inf (2012) 4, p. 20.

[64] Ibid, p. 38.

health protection is not fully harmonized with standard health protection in the community (CPT). Despite the legal obligation of each institution (penitentiaries and correctional institutions) to hire a doctor who will take care of the health of persons deprived from liberty, the Annual Repport of the Directorate for execution of sanctions about the conditions and the work of penitentiaries and education-correctional institutions in Macedonia in 2010 revealed that in Gevgelija, Strumica, Ohrid and Kumanovo there were not any persons employed in the sector for health protection. At the same time, in institutions with medical staff their number is considerably smaller than it should be (the situation is particularly bad in Idrizovo penitentiary). Moreover, even in the institutions which employ medical personnel there isn't constant medical care, especially psychiatric one. The attempts to overcome the lack of medical personnel by delegating medical responsibilities to other prison personnel without sufficient knowledge, or to prisoners (which includes distribution of medications as well) are contrary to European standards. Although, CPT considers that sometimes prisoners themselves are allowed to act as medical orderlies (as a last resort), it is very clear that prisoners should never carry out triage functions, distribute medication, be present during consultations, have access to medical records or deliver care to other prisoners.[65]

Apart from lack of personnel, prisons in the RM are facing insufficient training among existing personnel for working in institutions of this type and lack of communication and control within the prison health system. The personnel in the health sector in existing penitentiaries and the correctional institutions in the RM also demonstrate unsatisfactory level of knowledge of legal regulations and professional knowledge[66], as well as indifference as far as patient care is concerned[67]. In trhis regard, the CPT considered that: "*it should also benoted that they are not employed directly by the Ministry of Health and have no links to a hospital in the community, which results in them being isolated from the mainstream of health care practice*."[68] In 2011 the Directorate for execution of sanctions carried out tests for assessing the knowledge of the whole personnel in penitentiaries and the correctional institutions, with the aim to determine the level of knowledge about the legal, safe and professional performance of their work duties. The test results revealed that the majority of employees in the health care sector (52,2%) possessed a low level of knowledge, 39,1% of them possessed intermediate level of knowledge, and there were only 8,7% with advanced level of knowledge,[69] which implies the need for additional training for this category of prison personnel[70] (see Graph 1).

---

[65] Ibid, p 39.

[66] Directorate for execution of sanctions, (2011), Analysis of the results of the tests for assessing the knowledge of the employees in penitentiaries and the education-correctional institutions, Skopje.

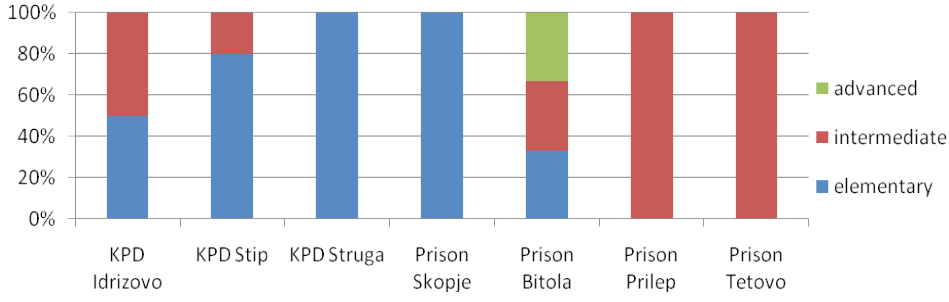
[67] CPT/Inf (2012) 4, p. 40.

[68] Ibid, 40.

[69] Directorate for execution of sanctions (2011), Analysis of the results of the tests for assessing the knowledge of the employees in penitentiaries and the education-correctional institutions, Skopje, p. 21.

[70] In 2010 the Ministry of Justice adopted a Programme for elementary and continuous training and assessment of the knowledge and capabilities of the personnel of penitentiaries and the correctional institutions with the aim to enhance the professionalism of prison personnel in carrying out their duties, and started with the trainings. In future, it should be worked on its consistent implementation in practice.

Graph no.1. Level of knowledge of employees in health care sector



Another serious problem regarding the convicts' health protection in the Republic of Macedonia is also the poor conditions in prison cells and the areas where health services and provided, as well as the lack of medications. Although in recent years there has been certain progress (renovations have been done, some equipment has been procured- as was the case with the dental office in Skopje prison, and the gynecological and dental office in Idrizovo penitentiary) the Republic of Macedonia is still far from meeting the standards typical for all democratic European countries.

CPT also notes that the legal obligation for medical screening of newly arrived convicts is not fully implemented, particularly in Idrizovo penitentiary and the prison in Skopje.[71] This is a serious defect in detecting possible physical and psychological illnesses (including infectious diseases) among convicts and eliminating risks derived from them, both for the life of other convicts housed in the institution and for their own lives (particularly from self-harm.) The presence of a prison officer while checking up the prisoners, is also against European standards in this segment (the right to medical confidentiality should be respected.

On the basis of the analysis of the official documents/materials of the European Commission, CPT and the Ombudsman of the Republic of Macedonia, what concerns us most are the cases of failure to provide medical care for the prisoners; delays in providing medical care which are not acceptable; rejection of doctors' recommendations for hospitalization or specialist care outside the prison facility; non-professional action (delay) by the authorities in processing requests for transfers in psychiatric institutions; flaws in the established system for protection from self-harm and failure to obey legal guarantees regarding the protection of the health of convicts in imposing and executing solitary confinement as a form of disciplinary action. Such behavior of state authorities is not in compliance with European standards in this segment. The state could be held liable with regards to ECHR for failure to provide or delay of competent authorities in pointing out to the need and adequate medical protection of persons deprived of freedom. The state's responsibility is even higher if a person under its immediate authority (a convict) with health problems dies, as was the case with the nineteen-year-old convict (heroin addict) who died in the prison in Gevgelija in August in 2010. Therefore, is very reasonable that the CPT demand requires the State to answer the following questions*:* "*was the person provided with Naloxone (an antidote toopiate intoxication) at Gevgelija Hospital before being transferred to Skopje given that he wasknown to be a drug addict*

[71] CPT, (2012), *Report to the Government of the Republic of Macedonia on the visit to Republic of Macedonia carried out by CPT from 21 September to 1 October 2010*, CPT/Inf (2012) 4, p. 40.

and on methadone maintenance?; why was it necessary to transfer thepatient to Skopje (a journey of three to four hours); why was the person not medically screenedduring the two days he was held in Gevgelija Prison;h ow did the person obtain the wound on hisforehead?"[72]

A particularly acute problem in Macedonian prisons is the treatment of drug addicts (lack of psychological and social support and education along with methadone therapy or the lack of methadone detoxication in general) and the persons with a specific infectious disease (lack of education about prevention). According to European standards (and Macedonian regulations also) the prison medical personnel have responsibilities regarding social and preventive medicine, as well. However, the CPT in its last report to the Macedonian Government concluded that health care services in the prisons visited have still not taken on the above-mentioned responsibilities.[73]

CONCLUSION

The prisoners are deprived of their liberty not their dignity. Hence, the State must take all necessary steps to comply with its obligation to respect the prisoners' human dignity, including providing them with the highest possible standard of health attainable. The prisoners shall have right to access to health services (including those available in the community) when necessary regardless their legal status, the nature of their offence as well as detention regime. The Council of Europe in order to find shared solutions to serious challenges facing European society concerning prison health care (overcrowding, high incidence of psychiatric symptoms among prisoners, suicides, spreading of transmissible diseases, lack of appropriate trained medical personnel, drug addicts, persons unsuited to continued detention) has established certain standards regarding the prisoners' right to health, the role of health personnel and the organization of the prison health care system. As the ECtHR notes "*the health of a detainee is now among the factors to be taken into account in determining how a custodial sentence is to be served, particularly as regards its length"*(*Mouisel v France*).

Despite the positive changes that Republic of Macedonia has undertaken in order to harmonize the Macedonian penitentiary system with the European one, the Macedonian prisoners' health care system is not in accordance (fully) with the European standards. Therefore, the RM should take steps towards: fully implementation of the legal obligation of each institution (penitentiaries and correctional institutions) to hire a doctor who will take care of the health of persons deprived from liberty as well as the legal obligation for medical screening of every prisoner upon its admission; improvement the material conditions in prison, including in the areas where health services are provided; appropriate equipped of prison health system in terms of human resources, premises, equipment, medicaments, installations; providing preventive health care; providing appropriate training and support to prison health staff, particular on the issue of transmissible diseases and drug addiction (in this context, the possibility should be considered to act on the suggestions by the CPT and thus involve Ministry of Health);strengthening the system for protection of self-harm as well as the supervision mechanism over the work of prison staff.

[72] Ibid, p. 44.
[73] Ibid, p. 42.

Winston Churchill said: "*The mood and temper of the public with regard to the treatment of crime and criminals is one of the unfailing tests of the civilisation of a country.*" We should ask ourselves what Macedonian prisons speak about us.

REFERENCES

1. Akandji-Kombe J.F., (2007) Positive *Obligations under the European Convention on Human Rights, A guide to the implementation of the European Convention on Human Rights*, Council of Europe.
2. Barak E. D., Gross M. A., (Eds.), (2007), *Exploring Social Rights: between theory and practice*, Oxford, Hart Publishing.
3. Coyle A, (2009), *A Human Rights Approach to Prison Management, Handbook for Prison Staff,* 2nd Edition, London, International Centre for Prison Studies.
4. CPT, (1993), 3rd General Report [CPT/Inf (93) 12].
5. CPT, (2012), *Report to the Government of the Republic of Macedonia on the visit to Republic of Macedonia carried out by CPT from 21 September to 1 October 2010*, CPT/Inf (2012) 4.
6. CPT, (2008), *Report to the Government of the Republic of Macedonia" on the visit to Republic of Macedonia" carried out by CPT from 39 June to 3 July 2008*, CPT/Inf (2008) 31.
7. CPT, (2008), *Report to the Government of the Republic of Macedonia on the visit to Republic of Macedonia carried out by CPT from 14 to 18 October 2007*, CPT/Inf (2008) 22.
8. CPT, (2008), *Report to the Government of the Republic of Macedonia on the visit to Republic of Macedonia carried out by CPT from 15 to 26 May 2006*, CPT/Inf (2008) 5.
9. Directorate for execution of sanctions, (2011), Annual report about the conditions and the work of penitentiaries and correctional institutions for 2010, Skopje.
10. Directorate for execution of sanctions (2011), Analysis of the results of the tests for assessing the knowledge of the employees in penitentiaries and the education-correctional institutions, Skopje
11. Dybeku v Albania, no. 1153/06, 2 June 2008
12. Dzieciak v Poland, no.77766/01, 9 March 2009
13. Kats and others v Ukraine, no. 29971/04, 18 March 2009,
14. European Convention for Protection of Human Rights and Fundamental Freedoms, (1950).
15. European Convention for the Prevention of Torture and Inhuman or Degrading Treatment or Punishment (1987).
16. Law on Execution of Sanctions, Official Gazette of the RM no. 2/2006; 57/2010
17. Longvinenko v Ukraine, no.3448/07, 14 January 2011
18. Makharadze and Sikharulidze v. Georgia, no. 35254/07, 22 November 2011
19. Møller L., Stöver H., Jürgens, R., Gatherer A., Nikogosian H., (Eds.), *Health in prisons A WHO guide to the essentials in prison health*, Copenhagen, WHO.
20. Mouisel v France 67263/01, 21 May 2003
21. Mowvray A, (2004) *The Development of the Positive Obligations under European Convention on Human Rights by the European Court of Human Rights*, Oxford, Portland, Oregon, Hart Publishing.

22. Murdoch J., (2006), *The Treatment of Prisoners European Standards*, Council of Europe Publishing.
23. Ombudsman of the RM 2008 Annual Report.
24. Ombudsman of the RM 2009 Annual Report.
25. Ombudsman of the RM 2007 Annual Report.
26. Recommendation No. R (98) 7of the Committee of Ministers to member states concerning the ethical and organizational aspects of health care in prison,
27. Rec(2006)2 of the Committee of Ministers to member states on the European Prison Rules
28. Renolde v France, no.5608/05 16 October 2008.

RESUME

The Council of Europe has established certain standards in the penitentiary field that guarantee dignified treatment of prisoners corresponding to the necessity of enabling their successful reintegration in the society. In this regard, the papers analyses the European standards (jurisprudence of the European Court of Human Rights, conventions, CPT's standards, relevant recommendations adopted by the Committee of Ministers) regarding prison health care and its implementation in the Republic of Macedonia, as member state of the Council of Europe. The first part of the paper provides detailed analysis of the European standards regarding health care in prison. The author considers the prison health care through (divided to) three main elements: the right to health in prison, organization of the prison health care and prison health care personnel: training, duties and responsibilities. In the second part of the paper the author assesses the compatibility of Macedonian prisoners' health care system with the European standards mainly through analysis of the legal framework in the country as well as through analysis of the reports of the European Commttee for the Prevention of Torture and Inhuman or Degrading Treatment or Punishment, the European Commission and the Ombudsman of the Republic of Macedonia.

Based on the analysis of the standards established within the Council of Europe, the author in the concluding remarks argues that the State is obliged to protect the health and physical well-being of persons deprived of their liberty, by providing them with the requisite medical assistance even in times of economic difficulty. The prisoners are deprived of their liberty not their dignity, and therefore the state should take all necessary steps in order to comply with its duty to respect the prisoners' human dignity. The prisoners shall have right to access to health services (including those available in the community) when necessary regardless their legal status, the nature of their offence as well as detention regime. Having regard the statement of the European Court of Human Rights that the increasingly high standard being required in the area of the protection of human rights and fundamental liberties correspondingly and inevitably requires greater firmness in assessing breaches of the fundamental values of democratic societies (*Mouise v France*) the author also in the concluding remarks identifies the main weaknesses in Macedonian prisoners' health care system and proposes some measures in order to its fully harmonization with the European standards.

PRILOG

CYBERCRIME IN POLAND

Jerzy Kosiński, PhD
Wyższa Szkoła Policji w Szczytnie, Polska,
kosinski@wspol.edu.pl

Summary: While accepting the appearance of Information Society (IS), the idea of Global Information Infrastructure (GII) and Global Electronic Commerce (GEC), it is necessary to notice the emergence of Risk Society (RS). The consequence of such a development is adaptation of legal normalization to appearing forms of cybercrime and threats to information security. The task of the state is to ensure that the legislation will protect citizens from cybercrime and minimize the effects of RS.

Several years ego I watched "War Games" and read about Kevin Mitnick with a profound distrust. In 1994, when preparing materials for the first in Poland conference devoted to crime with the use of modern technologies of data processing, I borrowed some pieces of information from Great Britain, France, Germany; having at the some time only two Polish examples available. Now, discussing the problem of cybercrime (or computer crime) I can make use of our own home sources. In Poland, there were many crimes included in Council's of Europe Convention on cybercrime from 2001 (ETS-185).

Such an alarming phenomenon has been reflected in alternation and establishment of new regulations.

In 1994, Copyright and Related Rights Act, owing to which within a few years **computer piracy** has become a synonym for computer crime, came into force. There are several reasons of such a situation. The most important are:

- high level of piracy (software producers' loss) – over 90% (in 1994) (in 2005 – "only" 59%, in 2010 – still 54%),
- opportunity to make use of act regulations for prosecuting criminals,
- relatively simple in understanding method of committing a crime.

According to the act, illegal distribution and publication of legally protected computer programs are prosecuted. Prosecution is carried out on private accusation and in cases when a given crime becomes permanent source of income or when a perpetrator organises or runs criminal activity – prosecution is on indictment. Criminal responsibility for violation of the act enclosed in the chapter 14, which says:

- misappropriation of authorship, falsification, labelling with trade mark of one's product are prohibited. Moreover, it is illegal to shorten, adapt and change the code of program against the will of the author (art. 115 – penalty of up to 2 years' imprisonment, restriction of liberty, or pecuniary penalty),
- it is forbidden to make any changes, against the licence, in the way of using software, e.g. one–position installation in the net or on a few

workstations. It is forbidden to make protected software for copying in the net or BBS accessible (art. 116 - penalty of up to 2 years' imprisonment, restriction of liberty, or pecuniary penalty),
- making extra illegal copies, preinstallation of protected software on hard disc are prohibited (art. 117 - penalty of up to 2 years' imprisonment, restriction of liberty, or pecuniary penalty),
- it is forbidden to purchase, accept or help with selling or hiding software carriers in order to gain material profit, called receiving of stolen property (art. 118 - penalty of up to 2 years' imprisonment, restriction of liberty, or pecuniary penalty),
- it is illegal to make exercising the right to control the process of operating a program difficult or impossible (art. 119).

The new Penal Code, which has had a binding effect since 1st September 1998, has introduced new possibilities of fighting computer piracy. Illegal obtainment of computer program (copying, duplication of a carrier, taking a carrier without authorised person's permission) – theft of other person's program aimed at gaining material profit (disposal of a copy on a computer stock market) has been considered a theft of a movable property (art. 278 §2 of the penal code). A computer program is not a movable property, however, it may become the subject of copyright property. Article 278 §2 of the penal code allows more radical prosecution of computer piracy, since it imposes penalty of imprisonment for 3 months to 5 years. Moreover, classified form of crimes under the articles 117 and 118 of the law on copyright imposes penalty of up to 3 years' imprisonment, if the crime becomes a permanent source of income, or when a perpetrator organises or runs crime activities related to computer piracy. If illegal obtainment of computer programs concerns the property of great value (200 as much as minimum salary), according to the article 294 §1 of the penal code, a perpetrator commits classified crime and he/she can be sentenced to up to 10 years. A computer program can became an intentional or unintentional receiving of stolen property (art. 291 §1 and 291 §2 of the penal code). It is illegal to help with selling, receiving or hiding pirate copy in order to gain material profit. This regulation provides for penalty of imprisonment for 3 months to 5 years. In a less serious case a perpetrator can be fined or he/she is liable to the restriction of liberty up to 1 year. What is meant by a less serious case is that a perpetrator did not want to gain any material profit and installed a program only in his/her own computer or helped with receiving or hiding a program by means of computer network. Unintentional receiving of stolen property – when perpetrator should or may assume that a program either purchased, sold or hidden has been stolen, he/she is liable to the penalty of restriction of liberty, or the penalty of up to 2 years' imprisonment. It is worth noticing, that receiving of stolen property under the article 293 §1 of the penal code is prosecuted on indictment, and under the article 118 point 1 – on the wronged person's motion.

Owning to various activities estimated level of computer piracy went down to 54% in 2010. At the same time the rise both in anti-pirate activities and instituted preparatory proceedings was observed.

It can be said, that computer piracy has become one of a few areas of computer crime where the police are effective. So far, I have not come across any evidence of applying regulations of tax law as far as collected and unrecorded software in the register is concerned.

As far as hacking is concerned, within a few years hackers have **broken into servers** and replaced WWW pages belonging to the Prime Minister and Government. Unfortunately, perpetrators have not been captured. Even if they had been captured there would have been plenty of problems with qualification of the offence. First time in 1998, people could watch on TV how a burglary to the server of the Central Bureau for Statistics was performed. In a talk-show programme an invited computer scientist broke security measures and gained access to the resources of the Central Bureau for Statistics. Heaving had a binding effect since 1st August 1998 the new penal code under XXXIII chapter – crime against the protection of information – penalised such deeds. Unlawful entry to a computer system through violation of security measures and receiving protected information (also obtaining access without authority to all or part of the computer system) is liable to the penalty of fine restriction of liberty, or penalty of up to the 2 years' imprisonment. According to the regulation mentioned above, it is illegal to receive information by an unauthorised person. What is valid, however, is whether it was an electronic, magnetic, or any specific entry. It does not matter what kind of security measure was disabled to break. Attempted hacking – checking the quality of security measures and possibilities of breaking them isn't prosecuted. It is also forbidden to alter, damage, erase any recorded information or in any way hinder an authorised person from accessing it. Also is prohibited the acquisition, sale or sharing with others a hardware or software adapted to commit these crimes, as well as computer passwords, access codes or other data enabling access to information stored on computer system or communications network (art.269b).

Computer frauds such as interfering with input data, program or output are often a black number. Afraid of having their reputation undermined, banks, offices and companies often fail to inform the police and the public about them. One of the most frequent computer frauds is tampering with output devices with credit cards. The present penal code defines computer fraud as an activity involving the obtaining of material profit or causing other harm by exerting influence on gathering, processing and transmitting information. The criminal activity can take various forms, such as alteration, erasure or input of new data into the computer information carrier (art.286 §1 of the penal code). This regulation refers to a classic fraud where, with the intent of procuring an lawful economic gain, the offender makes other person administer his/her or other person's property by inducing him/her into error or by taking advantage of his /her error or inability to undertake the right action. Thus, art.287 §1 of the code forbids any computer data interference aiming at causing economic loss of another person property.

Computer fraud is punishable by three months up to five years in prison. In less serious cases (art.287 §2 of the code) the penalty is a fine, restriction of liberty or prison sentence for up to one year.

Computer forgery - another cybercrime - can be divided into two cases:

- a computer with its programs and input-output devices is a tool used to forge typical documents or legal tenders. It is not difficult to provide evidence of this act having been committed, and this sort of crime is recognised as forgery of documents (art.270 §1 of the code) or of money (art.310, 313, 314 §1 of the code).
- documents in the form of electromagnetic record are counterfeited or forged. Under article 115 §14 of the penal code, a document is any object or recording on a computer information carrier bearing a definite title, or which

due to its contents is a proof of law, legal relationship or circumstances of legal significance. With this understanding of a document, a person forging a record on a magnetic card or other computer information carrier is also liable to penalty under art.270 §1 of the penal code.

In both cases forgery is liable to a fine, restriction of liberty or prison sentence of three months to five years.

One of few cases of computer blackmail for which documentary evidence has been supplied involves planting a logic bomb in software by a dismissed computer operator. The planting of the bomb was connected with the operator's demand to be paid for programs he was the author of. As a result of undertaken actions no **computer data or programs were damaged**.

Any tampering with computer entries with the intent to unlawfully alter, erase or suppress important computer data, or to hinder or prevent an authorised person from getting access to the data (art.268 §2 of the code) is punishable by prison sentence for up to three years. It does not make any difference how the information was damaged. The damage can be done to data-base, in the course of information processing, by putting a virus into information, program or computer network, entering a password or changing it, blocking connections in a network, or any other hinderance to accessing data by an authorised person. Alteration of computer data or programs is also punishable. The latter differs from the former in that the perpetrator unlawfully interferes with data, e.g. by entering new data or changing the existing record to break the protection system. Therefore, it is forbidden to enter any changes in important information stored in a computer system, as it breaks the integrity of data and infringes interests of the owner or other authorised person. It is connected with the right for undisturbed possession of data or the right for privacy. If the violator damages information, whereby causing grave pecuniary loss, he is liable to a prison sentence of 3 months to 5 years under art.268 §3 of the penal code. This is a qualified form of damaging information - a crime prosecuted on the wronged person's motion. If the above mentioned acts cause damage to information of particular importance for the state's defensive system or security, citizens' safety, or local government, then the offender is liable to a prison sentence of 6 months to 8 years. It should be added that besides computer sabotage, the legislator distinguishes activity with the intent to hinder or prevent automatic data acquisition or transmission.

Computer sabotage can also involve damaging or replacing the information carrier, destroying or damaging devices for automatic processing, acquiring or transferring of data (art.269 §2 of the code). Those acts are also liable to a prison sentence for up to 8 years. Since 2004, also unintentional sabotage , e.g. in case of unintentional putting of virus into the computer system or data on the carrier is liable to a prison sentence to 5 years (art.269a).

Unauthorised interception of information - computer tapping. This crime involves obtaining information by using a tapping or visual device, or other special device. Thus, it does not matter what kind of device it is, it can also be a telecommunication device plugged into teletransmission network. Neither is it important why the person enters the computer network or system. Penal sanctions for these crimes are the same as for hacking. The main purpose of security measures is to ensure the confidentiality of data transmitted or transferred with the use of technical devices, and to guarantee that every person's privacy is protected against various forms of surveillance in teletransmission networks.

Other forms of computer crime and possibilities of prosecuting them in Poland are as follows:

Telecommunication fraud - phreaking (art.285 §1 of the code). It is illegal to get connected to a telecommunication device and obtain phone impulses at somebody else's expense. The offender is liable to a prison sentence for up to 3 years.

Computer espionage or computer intelligence (art.130 §3 of the code). This crime consists in entering a computer network with the aim of gaining information which is either a state or official secret, and which - if given to another country's intelligence service - may do harm to the Polish Republic. The statutory penalty for this crime is a prison sentence for the period of 3 years or more. If an offender enters a computer network and gathers or stores the collected information, or intends to gain it for a foreign intelligence service against Poland but has not yet transferred it, then under art.130 §3 of the penal code he/she is liable to a prison sentence of 6 months to 8 years. Computer espionage of that type can also be prosecuted under hacking or computer tapping regulations, or under state or official secret protection ones. Liable to penalty is also an act harmful for an allied state, provided that the state ensures mutuality in this respect (art.138 §2 of the code).

Bringing about danger to the lives or health of many people or to property of great value (art.165 §1 of the code, point 4). This crime consists in hampering, preventing or influencing automatic processing, acquisition or transmission of data, and is liable to a prison sentence of six months to eight years. A person can be prosecuted under the same regulation for jeopardizing safety connected with the functioning of an airport, railway station, water, gas or energy supply system, monitoring of data in an intensive medical care ward, guarded bank, military or other facilities, e.g. by putting a virus into a computer program controlling the above mentioned activities.
If a person causes somebody's death or grievous bodily harm to many people, he/she can be sentenced to a prison sentence of 2 to 12 years.

Unintentional disturbance of automatic data processing resulting in bringing about public danger (art.165 §2 of the code). This crime carries a prison sentence for up to three years. However, if somebody's death or grievous bodily harm done to many people is involved, the penalty is 6 months to 8 years in prison.

Terrorist attempt on a ship or an aeroplane (art.167 §2 of the code). If a terrorist destroys, damages or disables navigational equipment used for processing indispensable data, or makes it impossible to operate it, he/she is liable to a prison sentence of 3 months to 5 years.

Cyberstalking (art.190a §1 of the code, since 2011). It is prohibited to persistent harassment (eg by Internet, phone) to another, which gives rise to the circumstances justified sense of danger or significantly affect her privacy. The penalty is up to 3 years.

Cyberstalking, phishing (art.190a §2 of the code, since 2011). It is prohibited to impersonate another person, the use of his/her image or his/her personal data in order to cause the property or personal damages. The penalty is also up to 3 years.

Offence to somebody's religious beliefs (art.196 of the code). This crime consists in insulting an object of religious worship or a place used for public performance of religious rituals, e.g. by disseminating information of this nature in computer networks.

Grooming (art.200a §1 of the code, since 2011). If someone contacts via the Internet with a minor under the age of 15 with an intention to meet with him/her, by

placing him/her in error, exploiting error or inability to properly understanding the situation or using unlawful threat, he/she is liable to a prison sentence of 3 years.

Disseminating pornography, pedophilia, sodomy (art.202 of the code). Making arrangements for sexual contacts, including pedophiliac ones, distributing pornographic materials. Since May 2004 possessing in the system or on the computer carrier pornographic materials with children under 15 is liable to a prison sentence of 3 months to 5 years.

Praising fascism in public (art.256 of the code). Propagating fascism, communism or other totalitarian ideologies, also selling, sharing symbols of them with the use of computer network (up to 2 years).

Insulting, deriding or humiliating people in public (art 262 of the code). Publicising or spreading information glorifying violence, racism, nazism, anti-semitism, etc.

The above list of computer crimes shows explicitly that these crimes are closely linked with economic activity and pose a serious threat to communication and transportation. They can jeopardize lives, health, property and safety of citizens.

2. Evidence practice concerned to Computer Crime.

Polish judiciary underestimate the possibilities given by the digital evidence, which causes that computer systems are not taken into consideration because of lack of link between crime and computer crimes catalogue. My many years' practice and experience show that the classification of crime act arises from Penal Code does not exhaust the possibilities of using the digital evidence. Contemporary crimes as commonly thefts were not so far connected to processing the information. But they are more frequently concern with existing the electronic information which has evidence or circumstantial value

In every case when the law enforcement bodies protect the document which comes from hard disc drive it can be the evidence. But Polish law does not identify the digital evidence as the special evidence which needs special treatment – different than material evidences. Formally obtaining this type of evidence has its legislative basis in article 217 § 1 of Code of Criminal Procedure, which says that the things which can be the evidence in the case should be handed over on demand of authorized law enforcement bodies. Hoverer it is impossible to demand from defendant to give the access code to protected data or to point specific data, because it is at variance with the rule: "*nemo se ipsum accusare tenetur*" binding in Polish law. Due to lack of this approval, or due to lack of submitting of the order of article 219 § 1 Code of Criminal Procedure allows to search and detaining of the thing which meets the evidence pointing article 217. The truth is that digital information is not a „thing" but it is inseparably bounded with specific information carrier (for example hard disc drive, streamer). In spite of the fact that Code of Criminal Procedure regulations concern detaining the things, so also the carrier, the carriers as „things" will not be evidence but the information which is contained there. The regularity of this type reasoning, seems to be fully well-grounded, because it is not anything new in the aspects of criminal procedure. As I can protect dactyloscopic tracks on the with the use of specialist materials, I could also protect the digital data in any case. But the correctness of the dactyloscopic activities is ensured by the appropriate procedures. Every criminologist technician, even the beginner one knows that the disclosed and protected dactyloscopic tracks can not cast doubts as for hour, date of coming into existence and the place of appearing. In the aspect of digital information, in Polish criminal procedure there is no suitable regulations. What is more – even the

Polish legislators are not prepared to standardize this type of cases, even on slim level. So it is very important to realize of the threats connected to incompetently approach to data, which needs suitable preparing to its understanding. At the present legislative state (and in principle of its lack) with reference to people who are concerned with collecting the evidence materials – there is no any official standard of using the digital evidences. It causes that even if the prosecutor's office secure the computer, where the digital evidences appear, it could not have any importance in the aspect of legal evidences because of gaps in Chain of Custody.

Fortunately the correct way of securing the digital evidences contained on data carriers in the way specified in article 148 which concerns to detain the things and determines their specific parameters in the protocol, and lets to create the chain. Potential flaws, because of lack of the detailed procedure concerned for example the form of marking the carrier will not influence on the matters of admitting the evidence, but only on its value. The lack of procedures complements also the growing consciousness of investigators and the possibility of getting the standards from the west. In particular cases Polish law allows to appoint ICT expert witness according to article 193, 198 and 205 of Code of Criminal Procedure, which can support take part in the investigations.

The issues of Chain of Custody, especially important in the case of digital evidence is regulated also only by the general legislations from the detaining protocol, where the characteristics of carrier, date and the place of detainer are described (article 148 Code of Criminal Procedure), to the storing the evidence (article 228). General legal articles do not say how to secure the digital evidence and analyze it to save its evidence value. In this aspect it is very important to apply to world's standards, especially to generating MD5 (SHA1) check sums and working on images during the analysis. The protocols and procedures worked out by us let to describe what was happening with the evidence in every time and the check sum is its digital sign.

As I mentioned above, digital evidence analysis is based mostly on expert witnesses opinions. Depending on the trial organ order, expert witness gives oral or written statement (article 200 Code of Criminal Procedure), and this opinion should contain the report from the performed investigation, observations and conclusions. Any legislations predict the form of presenting the digital evidence.

During my activity I developed the shape of expert witness opinion, based on trial experience and western standards, especially the Encase (Guidance Software) training recommendations. My experience shows that most evidences need to be printed, and the rest is enclosed in the form allocated on the CD carriers with possibility of easy analysis by the trial organ. Because the specialist knowledge of trial organs is rather limited in this scope, the opinion should be maximally legible. In any case the person giving the opinion is obliged to give the explanations.

In conclusion, it seems worth noticing that criminals are making the most of the latest developments in information technology. Computer crime should be treated as a criminological phenomenon (not necessarily regulated in separate chapters of the code) prosecuted under an adequate article depending on the act (e.g. appropriation, devastation of, or damage to property, revealing a state or official secret). Existing Polish legislative regulations leave the material and keeping its evidence value in the hands of experts so as to have to possibility of its defence during the trial.

CIP - Каталогизација у публикацији
Народна и универзитетска библиотека
Републике Српске, Бања Лука

343.85:[343.326:004.738.5(082)
343.85:327.39(4)(082)

МЕЂУНАРОДНА научностручна конференција Сузбијање криминала и европске интеграције с освртом на високотехнолошки криминал (2012 ; Лакташи)
Zbornik radova / Međunarodna naučnostručna konferencija Suzbijanje kriminala i evropske integracije s osvrtom na visokotehnološki kriminal, Laktaši, 28-30. marta 2012. godine ; [organizatori] Republika Srpska. Vlada, Ministarstvo unutrašnjih poslova, Uprava za policijsko obrazovanje, Visoka škola unutrašnjih poslova u saradnji sa Hans Zajdel fondacijom ; [glavni i odgovorni urednik Mile Šikman ; prevodilac Jelena Vignjević]. - Banja Luka : Visoka škola unutrašnjih poslova, 2012 (Banja Luka : Grafomark). - VI, 511 str. : ilustr. ; 24 cm

Radovi na srp i engl. jeziku. - Tiraž 200. - Napomene i bibliografske reference uz tekst. - Bibliografija uz svaki rad.

ISBN 978-99938-43-36-8
1. Министарство унутрашњих послова (Бања Лука)
2. Управа за полицијско образовање (Бања Лука)
3. Висока школа унутрашњих послова (Бања Лука)
4. Ханс Зајдел фондација (Минхен)

COBISS.BH-ID 2660888