Fakultet za kriminalistiku, kriminologiju i sigurnosne studije
Univerziteta u Sarajevu
KRIMINALISTIČKE TEME, Godina XIX, Broj 5
Zbornik radova
XVIII DANI KRIMINALISTIČKIH NAUKA
Međunarodna naučna konferencija
„Savremeni izazovi u cyber sigurnosti" – CFS 2019
Sarajevo, 2019.

Izdavač: Fakultet za kriminalistiku, kriminologiju i sigurnosne studije
Za izdavača: prof. dr Nedžad Korajlić, dekan
Gost urednik: prof. dr Jasmin Ahić
Redakcija: Naučni i programski odbor Konferencije
predsjednik Odbora: prof. dr Jasmin Ahić (BiH), prof. dr Nedžad Korajlić (BiH), prof. dr Dina Bajraktarević Pajević (BiH), prof. dr Marija Lučić-Ćatić (BiH), prof. dr Muhamed Budimlić (BiH), prof. dr Lada Sadiković (BiH), prof. dr Sakib Softić (BiH), prof. dr Haris Halilović (BiH), dr.sci. Beba Ešrefa Rašidović (BiH), profesor emeritus Mirsad Abazović (BiH), dr.sci. Itamara Lochard (USA), prof. dr Samim Konjicija (BiH), prof. dr Jasmin Azemović (BiH), prof. dr Ratko Duev (S. Makedonija), prof. dr Oliver Bakreski (S. Makedonija), prof. dr Vančo Kenkov (S. Makedonija), prof. dr Andrej Sotlar (Slovenija), prof. dr Gorazd Meško (Slovenija), doc. dr Ivan Toth (Hrvatska), doc. dr Ivan Nađ (Hrvatska), prof. dr Lulzim Tafa (Kosovo), dr.sci. Krunoslav Borovec (Hrvatska), prof. dr Želimir Kešetović (Srbija), prof. dr Zoran Keković (Srbija), prof. dr Nikola Dujovski (S. Makedonija), prof. dr Marjan Gjurovski (S. Makedonija), prof. dr Milan Žarković (Srbija), prof. dr Zvonimir Ivanović (Srbija), mr. Nenad Sikirica (Hrvatska); sekretar Odbora: Ermina Bakić
Organizacioni odbor Konferencije
predsjednik Odbora: prof. dr Admir Hadžikadunić, prof.dr. Goran Kovačević, prof.dr. Almir Maljević, prof. dr Muamer Kavazović, doc. dr Elvira Čekić, doc. dr Armin Kržalić, dr.sci. Adnan Fazlić, Sandra Kobajica, MA, dr.sci. Nerma Halilović-Kibrić, Kenan Hodžić, MA, Predrag Puharić, Amra Hodo; sekretar Odbora: Mirza Buljubašić, MA

Lektor: Nizama Hodžić
Štampa: _____

ISSN: 1512-5505

XVIII Dani kriminalističkih nauka

Međunarodna naučna konferencija

„Savremeni izazovi u cyber sigurnosti“ – CFS 2019

ZBORNIK RADOVA

Sarajevo, 3-4. oktobar 2019.

Kriminalističke teme
Zbornik radova
Godina XIX, Broj 5, 2019.
ISSN 1512-5505

UVODNA RIJEČ

Poštovani čitaoci,

zadovoljstvo nam je predstaviti vam posebni broj časopisa „Kriminalističke teme“ kojim su obuhvaćeni naučni i stručni radovi prezentirani na Međunarodnoj naučnoj konferenciji „Savremeni izazovi u cyber sigurnosti“ koja je u okviru XVIII Dana kriminalističkih nauka održana na Fakultetu za kriminalistiku, kriminologiju i sigurnosne studije Univerziteta u Sarajevu 3. i 4. oktobra 2019. godine.

Konferenciju je otvorio predsjedavajući Predsjedništva Bosne i Hercegovine Željko Komšić koji je naglasio da je tema „Savremeni izazovi u cyber sigurnosti“ izuzetno važna za čitav svijet, jer živimo u dobu koje nazivaju informatičkom revolucijom, dobu koje je donijelo velike promjene na globalnom nivou, pa i u Bosni i Hercegovini. Izrazio je uvjerenje da svi sigurnosni subjekti u našoj zemlji daju svoj maksimalni doprinos, da idu ukorak sa cyber izazovima koji se postavljaju pred Bosnom i Hercegovinom, ali za savremene izazove u cyber svijetu potrebni su podrška i iskustvo drugih. „U svakodnevnoj borbi protiv svih oblika kriminala i korupcije, pa tako i lakšeg kontroliranja cyber kriminala, Bosna i Hercegovina će najbolje napredovati ukoliko postane članica NATO-a i Evropske unije”, istakao je predsjedavajući Predsjedništva Željko Komšić.

„Fenomen cyber kriminala, koji je svoju ekspanziju doživio naglim razvojem kompjuterskih i informacionih sistema, veliki je izazov za moderni svijet. Žrtve ovog vida kriminaliteta doslovno mogu biti svi: od pojedinaca, privrednih subjekata do državnih institucija i vojske“, istakli su rektor Univerziteta u Sarajevu prof. dr. Rifat Škrijelj i dekan Fakulteta za kriminalistiku, kriminologiju i sigurnosne studije prof. dr. Nedžad Korajlić, te naveli da je ova konferencija na međunarodnom nivou od izuzetne važnosti kako bi se u aktuelnom momentu ponudila rješenja i odgovori kao i modeli kreiranja politika cyber sigurnosti.

Uvodno plenarno predavanje održala je prof. dr. Itamara Lochard sa George Mason University, SAD. Pored učesnika konferencije, otvaranju su prisustvovali i brojni ugledni gosti, dekani partnerskih visokoškolskih ustanova iz regiona, predstavnici diplomatskog kora u Bosni i Hercegovini, članovi akademske zajednice, predstavnici agencija za provedbu zakona, sistema krivičnog pravosuđa, privatnih i nevladinog sektora, a posebna gošća bila je komandantica NATO Štaba Sarajevo, brigadna generalica Marti Bissell sa saradnicima. U okviru konferencije održan je i Okrugli sto u partnerstvu Fakulteta i

organizacije Save the Childern na temu „*Digitalne" generacije: djeca i mladi*, kao i Master Class predavanje u partnerstvu Fakulteta i Agencije za zaštitu ljudi i imovine DSC Sarajevo na temu *Zaštita ličnih podataka u Bosni i Hercegovini, sa posebnim osvrtom na zaštitu matičnih knjiga, spisa i registra*, kao i SHOT radionica, na kojoj je prezentirana najnovija sigurnosna oprema i tehnologija.

Radovi u ovom zborniku razvrstani su prema panelima u okviru kojih su bili i predstavljeni na samoj konferenciji, a prema području istraživanja i posmatranja problematike cyber sigurnosti. Zahvalni smo svim autorima koji su svoj naučnoistraživački interes pronašli u ovoj savremenoj oblasti i ukazali na brojne sigurnosne izazove današnjeg vremena, i koji svojim radovima i učešćem na Danima kriminalističkih nauka iz godine u godinu podržavaju naučnoistraživačku djelatnost Fakulteta za kriminalistiku, kriminologiju i sigurnosne studije. Hvala svim recenzentima koji su uložili svoje vrijeme, trud i znanje u kategorizaciji prispjelih radova, kao i na svrsishodnim sugestijama i uputama autorima, a sve u cilju unapređenja kvaliteta ovog Zbornika radova.

Nadamo se da će predstavljeni radovi biti od značaja za naučnu i stručnu javnost, ali i za studente i širu čitalačku publiku.

S poštovanjem,

prof. dr. Jasmin Ahić

Kriminalističke teme
Zbornik radova
Godina XIX, Broj 5, 2019.
ISSN 1512-5505

SADRŽAJ

UVODNA RIJEČ I

BORBA PROTIV CYBER KRIMINALA: KRIVIČNOPRAVNI I KRIMINALISTIČKI ASPEKT FIGHT AGAINST CYBER CRIME: CRIMINAL LAW AND CRIMINALISTICS ASPECTS 3

NEMATERIJALNA ŠTETA KAO JEDAN OD OBLIKA KOMPJUTERSKOG KRIMINALA NASTAO VRŠENJEM KOMPJUTERSKIH DELIKATA 17

INTANGIBLE DAMAGE AS ONE OF THE FORMS OF COMPUTER CRIME CAUSED BY COMPUTER DELICTS 17

STANJE, KRETANJE I NORMATIVNO UREĐENJE RAČUNALNOG KRIMINALITETA U REPUBLICI HRVATSKOJ STATE, TRENDS AND NORMATIVE REGULATION OF CYBERCRIME IN THE REPUBLIC OF CROATIA 31

KRIMINALISTIČKI I KRIVIČNOPROCESNI ASPEKTI OTKRIVANJA, RAZJAŠNJAVANJA I DOKAZIVANJA KRIVIČNIH DJELA VISOKOTEHNOLOŠKOG KRIMINALITETA CRIME AND CRIMINAL PROCESSES, ASPECTS OF DETECTION, EXPLOITATION AND EVIDENCE OF HIGHER-TECHNICAL CRIMINALITY 55

KRIVIČNOPRAVNI ASPEKTI ZAŠTITE KOMPJUTERSKIH SISTEMA, ANALIZA STANJA I DE LEGE FERENDA PRIJEDLOZI CRIMINAL ASPECTS OF THE COMPUTER SYSTEM'S PROTECTION, SITUATION ANALISIS OF AND DE LEGE FERENDA PROPOSAL'S 67

ILEGALNE AKTIVNOSTI U NEVIDLJIVOM WEB-U ILLEGAL ACTIVITIES IN THE INVISIBLE WEB 87

KRIMINALNI POTENCIJAL FENOMENA DARKNET-A THE DARKNET PHENOMENON CRIMINAL POTENTIAL 101

DARK WEB AS A CONTEMPORARY CHALLENGE TO CYBER SECURITY 117

CYBER KRIMINAL KAO MODERNA SIGURNOSNA PRIJETNJA U BOSNI I HERCEGOVINI CYBERCRIME AS A MODERN SECURITY THREAT IN BOSNIA AND HERZEGOVINA 129

HORIZONATALNO I VERTIKALNO HIBRIDNO DJELOVANJE I/ILI RAT - STUDIJA SLUČAJA BOSNE I HERCEGOVINE HORIZONTAL AND VERTICAL HYBRID ACTION AND/OR WAR-CASE STUDY OF BOSNIA AND HERZEGOVINA 161

RADIKALIZAM I EKSTREMIZAM NA INTERNETU RADICALISM AND EXTREMISM ON THE INTERNET 181

MEĐUNARODNO PRAVO I CYBER SIGURNOST INTERNATIONAL LAW AND CYBER SECURITY 197

CYBER TERORIZAM CYBER TERRORISM 217

CYBER TERORIZAM KAO NOVI OBLIK RATOVANJA: SEKUNDARNA ANALIZA SLUČAJA „STUXNET“ I TEORETSKI OKVIRI CYBER TERORIZMA CYBER TERRORISM AS NEW WAY OF WARFARE: SECONDARY CASE ANALYSIS OF “STUXNET” AND THEORETICAL APPROACH TO CYBER TERRORISM 227

VIKTIMIZACIJA STUDENATA U SAJBER PROSTORU: ISKUSTVA IZ SRBIJE STUDENTS' EXPERIENCE IN CYBERSPACE: EXPERIENCES FROM SERBIA 247

ULOGA PSIHOLOGIJE U UNAPREĐENJU CYBER SIGURNOSTI THE ROLE OF PSYCHOLOGY IN ENHANCING CYBERSECURITY 271

POSTUPCI KRIPTOGRAFIJE I NJIHOVA ULOGA CRYPTOGRAPHY PROCEDURES AND THEIR ROLE 287

KORIŠTENJE KOMERCIJALNE TEHNOLOGIJE U SUZBIJANJU I PRAĆENJU NEZAKONITE TRGOVINE ŽIVOTINJSKIM TROFEJIMA U CYBER-KRIMINALNIM TRGOVINSKIM MREŽAMA USE OF COMMERCIAL TECHNOLOGY IN COUNTERING ILLEGAL WILDLIFE TRAFFICKING WITHIN CYBER-CRIMINAL TRADE NETWORKS 313

ZAŠTITA OD CYBER NAPADA I UPRAVLJANJE PODACIMA NA KRITIČNOJ INFRASTRUKTURI POMOĆU INOVACIONIH 3D ALATA GIS I BIM CYBER ATTACK PROTECTION AND CRITICAL INFRASTRUCTURE DATA MANAGEMENT WITH THE INNOVATIVE 3D GIS AND BIM INSTRUMENTS 331

KRIMINALISTIČKO POSTUPANJE SA DIGITALNIM DOKAZIMA U PRAKSI POLICIJSKIH AGENCIJA U BIH DIGITAL EVIDENCE HANDLING IN PRACTICE OF POLICE AGENCIES IN B&H 351

METODE OTKRIVANJA SAJBER KRIMINALA PUTEM DIGITALNE FORENZIKE THE METHODS OF DETECTION CYBER CRIME INTO DIGITAL FORENSICS 389

PRETRESANJE UREĐAJA ZA AUTOMATSKU OBRADU PODATAKA I AUTOMATSKO RAČUNARSKO PRETRAŽIVANJE PODATAKA SEARCH AND SEIZURE OF THE AUTOMATIC DATA PROCESSING DEVICE AND AUTOMATIC COMPUTER DATA SEARCH 417

NACIONALNA PLATFORMA REPUBLIKE SEVERNE MAKEDONIJE ZA IZGRADNJU SAJBER BEZBEDNOSTI 441

ZLOUPOTREBA SAJBER PROSTORA U IZBORNOM PROCESU KAO GLOBALNA POLITIČKA I SIGURNOSNA PRIJETNJA ABUSE OF CYBER SPACE IN THE ELECTION PROCESS AS A GLOBAL POLITICAL AND SECURITY THREAT 459

BEZBEDNOST I ZAŠTITA PODATAKA O LIČNOSTI U ZDRAVSTVENIM USTANOVAMA SECURITY AND PERSONAL DATA PROTECTION IN HEALTHCARE INSTITUTIONS 475

KORIŠTENJE ELEKTRONSKOG I KORESPONDENTNOG BANKARSTVA ZA AKTIVNOSTI PRANJA NOVCA USE OF ELECTRONIC AND CORRESPONDENT BANKING FOR MONEY LAUNDERING ACTIVITIES 483

SVEOBUHVATNI PRISTUP NATO-A SAJBER ODBRANI NATO'S COMPREHENSIVE APPROACH TO CYBER DEFENSE 501

METODOLOŠKA ISTRAŽIVANJA U POLITICI I SIGURNOSTI KAO DIO KOMPJUTERSKE MANIPULACIJE PODACIMA U KREIRANJU SIGURNOSNE PERCEPCIJE JAVNOSTI 515

MEDIJSKA I INFORMACIJSKA PISMENOST U SISTEMU CYBER SIGURNOSTI MEDIA AND INFORMATION LITERACY IN CYBER SECURITY SYSTEM 529

ZAKLJUČCI KONFERENCIJE 547

Kriminalističke teme
Zbornik radova
Godina XIX, Broj 5, 2019.
ISSN 1512-5505

Panel 1

Prema idealu pravde: kriminalistika i pravo u cyber prostoru

Kriminalističke teme
Zbornik radova
Godina XIX, Broj 5, 2019.
ISSN 1512-5505

BORBA PROTIV CYBER KRIMINALA: KRIVIČNOPRAVNI I KRIMINALISTIČKI ASPEKT

FIGHT AGAINST CYBER CRIME: CRIMINAL LAW AND CRIMINALISTICS ASPECTS

Pregledni naučni rad

Prof. dr. Željko Nikač[1]
Branko Leštanin, doktorant[2]

SAŽETAK

Inspiracija za rad i problem (i) koji se radom oslovljava (ju): Tehničko tehnološki razvoj ljudske civilizacije doveli su do izuma Interneta i društvenih mreža. Međutim ovi izumi nažalost su zloupotrebljeni i postali su sredstvo i način za izvršenje raznih krivičnih dela iz oblasti kompijuterskog (cyber) kriminala. *Software* predstavlja središte ovog oblika kriminala i glavno sredstvo za izvršenje dela. Normativni okvir u borbi protiv cyber kriminala čine međunarodni dokumenti i s njima usklađeno nacionalno zakonodavstvo. Organizacioni okvir čine državne institucije čija je nadležnost sprečavanje i borba protiv ovog oblika kriminala i to specijalizovane službe policije, tužilaštva, suda, ministarstva finansija i dr. Zbog specifičnog načina izvršenja, svojstva učinioca, nepostojanja mesta izvršenja kao i vremena i mesta nastupanja posledice krivičnog dela cyber kriminalia rad na otkrivanju i dokazivanju zahteva specificna znanja, veštine i obuku. Primarnu ulogu u dokazivanju ovog oblika kriminaliteta ima specifična cyber forenzika radi pribavljanja relevantnih dokaza u cilju rasvetaljavanja i hapšenja izvršioca. U radu je napravljena i analiza pojedinih počinjenih krivičnih dela iz oblasti cyber kriminala u Republici Srbiji i navedeni su značajniji rezultati u otkrivanju i dokazivanju ovih krivičnih dela. Autori u zaključnim razmatranjima, radi unapređenja pravnog i institucionalnog okvira za suzbijanje cyber kriminala, dati su predlozi *de lege ferenda*.

Ciljevi rada (naučni i/ ili društveni): Ukazati na potencijalne nove pojavne oblike cyber kriminala i njihov *modus operandi* i prikaz predloga *de lege ferenda* za unapređenje normativnog okvira, prakse i saradnje država.

Metodologija/ dizajn: Rad je temeljen na normativnom i uporedno-pravnom metodama.

Ograničenja rada/ istraživanja: Potencijalna tamna brojka izvršenih krivičnih dela cyber kriminala.

Rezultati/ generalni zaključak: Multidisciplinarni i multiagencijski pristup i međunarodna operativna saradnja policije, posebno na Zapadnom Balkanu, koja je od izuzetnog značaja za otkrivanje i borbu protiv cyber kriminala.

[1] Prof. dr. Željko Nikač je redovni profesor Kriminalističko policijskog univerziteta (KPU) u Beogradu, Srbija. zeljko.nikac@kpu.edu.rs

[2] Branko Leštanin je doktorant na Pravnom fakultetu, Univerziteta u Nišu. b.lestanin@gmail.com

Opravdanost istraživanja/ rada: Na opravdanost istraživanja utiče enormna društvena opasnost od najtežih pojavnih oblika cyber kriminala, zbog specifičnog načina izvršenja, svojstva učinioca, nepostojanja mesta izvršenja kao i vremena i mesta nastupanja posledice.

Ključne riječi
cyber kriminal, normativni okvir, međunarodna policijska saradnja, Zapadni Balkan i EU.

ABSTRACT
Reason for writing and research problem (s): The technical technological development of human civilization has led to the invention of the Internet and social networks. However, these inventions were unfortunately abused and became a means and method for the execution of various felonies in the field of cyber crime. Software is the center of this form of crime and the main mean of carrying out the crime.The normative framework in the fight against cyber crime consists of international documents and harmonized national legislation. The organizational framework consists of state institutions whose jurisdiction is the prevention and combating of this form of crime and specialized services of the police, the prosecution, the court, the ministry of finance, and others. Due to the specific manner of execution, the characteristics of the perpetrator, the absence of the crime scene and the time and place of the occurrence of the consequences of the cyber crime, the work on detection and proofing requires specific knowledge, skills and training. The primary role in proving this form of crime has specific cyber forensics in order to obtain relevant evidence in order to clarify and arrest the perpetrator. The paper also analyzes certain felonies committed in the field of cyber crime in the Republic of Serbia and provides significant results in the detection and proving of these felonies. The authors in the concluding remarks, in order to improve the legal and institutional framework for the suppression of cyber crime, have submitted *de lege ferenda* proposals.
Aims of the paper (scientific and/ or social): To point out potential new emerging forms of cybercrime and their *modus operandi* and to present the proposal *de lege ferenda* for the improvement of the normative framework, practice and state cooperation.
Methodology/ Design: The work is based on normative and comparative-legal methods.
Research/ Paper limitations: Potential dark number of committed felonies of cyber crime.
Results/ Findings: General conclusion: Multidisciplinary and multi-agency approach and international operational cooperation of the police, especially in the Western Balkans, which is of great importance for the detection and fight against cyber crime.
Research/ Paper validity: The justification of research is affected by an enormous social danger from the most serious forms of cyber crime, due to the specific way of execution, the characteristics of the perpetrator, the absence of the crime scene, and the time and place of the occurrence of the consequences.

KEY WORDS
cyber crime, normative framework, international police cooperation, Western Balkans and the EU.

1. UVOD

Početak treće decenije XXI veka obeležava do sada najveći razvoj nauke i tehnike, kao i napredak informacione tehnologije i tehničkih sistemema u ovom sektoru. Savremeni svet je danas prosto nezamisliv bez kompjutera koji već decenijama imaju primat u poslovnoj sferi, a poslednjih godina su zauzeli ogroman prostor i u privatnim životima ljudi i naročito mlade populacije. Kompjuteri su u posebno našli svoju primenu u velikim sistemima, javnoj upravi, privatnom i javnom poslovnom sektoru, pa se bez njih danas ne mogu obaviti brojni poslovi i transakcije koji donose ekonomski profit.

Međutim, pored pozitivnih učinaka razvoj informacione tehnologije je nažalost doneo i brojne negativne efekte i prouzrokovao brojne probleme u zajednici. Na personalnom planu došlo je do velike otuđenosti ljudi i posebno mladih koji su čak postali zavisni od kompjutera, interneta i društvenih mreža. Na širem planu sigurno najteži problem predstavlja zloupotreba kompjutera i informacionih tehnologija, kao i pojava cyber kriminala kao posebnog pojavnog oblika kriminaliteta. Cyber kriminal se ispoljio u različitim vidovima i oblicima kao što su: kompjuterske prevare, zloupotrebe kompjutera, kompjuterski kriminal, računarski ili informatički kriminal i ostali oblici koji čine širi pojam cyber kriminala. U novije vreme javljaju se drugi brojni vidovi napada na kompjutere i kompjuterske sistema, zatim kompjuterski virusi, zaražena elektronska pošta i dr.

Posebno su ugrožene razvijenije zemlje koje imaju značajne informacione resurse, pa su zloupotrebe tim pre veće. Naravno ugrožene su i manje zemlje, države u razvoju i posebno one u tranziciji koje tek razvijaju informatičke sisteme, kulturu i bezbednost u istoj oblasti. U tom kontekstu pominjemo i Republiku Srbiju koja je još uvek zemlja u tranziciji i u kojoj je informatička pismenost u razvoju. Srbija i ostale zemlje koje su nekada bile u sastavu ex Jugoslavije su danas samostalne mlade države, ali suočene sa cyber kriminalom, drugim pojavnim oblicima kriminala i brojnim izazovima, rizicima i pretnjama.

Države i međunarodna zajednica su pokušale da pruže adekvatan odgovor na enormni rast kriminala u svim oblastima društvenog života i posebno terorizma, organizovanog kriminala i s tim u vezi cyber kriminala. Na nacionalnom i međunarodnom nivou je usledila reakcija ovlašćenih subjekata država i međunarodnih organizacija, pre svega na legislativnom i funkcionalnom planu. Međunarodna zajednica, države i međunarodne organizacije kao najvažniji njeni subjekti usvojili su brojne međunarodne konvencije, rezolucije, deklaracije i druge dokumente koji na globalnom planu tretiraju pitanje cyber kriminala i shodno tome iziskuju međunarodnu akciju. Države kao članice međunarodne zajednice i potpisnice ovih dokumenata su se obavezale da ratifikuju potpisane akte i njihova rešenja ugrade u nacionalno zakonodavstvo, kao i olakšaju mere međunarodne krivično-pravne i svake druge saradnje u borbi protiv cyber i drugih oblika kriminala. Važan deo međunarodne krivičnoprave saradnje u širem smislu čini međunarodna policijska saradnja koja obuhvata razmenu obaveštajnih informacija, razmenu oficira za vezu,

zajedničke akcije, zajedničke istražne timove i ostale vidove borbe protiv cyber i drugih teških oblika kriminala.

Srbija se kao i ostale zemlje u tranziciji suočila sa naglim razvojem komjputerske tehnologije i s tim u vezi cyber kriminalom, kao najtežom posledicom ovog procesa. U pokušaju da se obezbedi adekavatan društveni odgovor u velikoj meri je harmonizovan nacionalni legislativni okvir sa normama međunarodnog prava, u kojem kontekstu pominjemo novele Krivičnog zakonika (KZ)[3] i inkriminaciju krivičnih dela iz oblasti računarskog (kompjuterskog) kriminala. Drugim zakonima su usvojena rešenja koja se odnose na formiranje specijalizovanih organa za borbu protiv terorizma, organizovanog kriminala i s tim u vezi visokotehnološkog kriminala (VTK), kao što su posebna odeljenja sudova, tužilaštava i policije u kojima rade lica za primenu zakona koja su edukovana u ovoj oblasti. U funkcionalnom smislu formirano je i anagažovano više expertskih tela i specijalizovanih organa za borbu protiv cyber i ostalih najtežih pojvnih oblika kriminala.

2. POJAM I KARAKTERISTIKE CYBER KRIMINALA

Cyber kriminal je noviji pojavni oblik kriminaliteta koji se manifestuje u periodu posle II sv. rata kad je došlo do modernizacije društva, tehničkog napretka i razvoja savremene tehnologije pre svega u SAD i zapadnim zemljama. Prema raspoloživim istorijskopravnim izvorima prvi slučaj cyber kriminala je zabeležen u SAD (1958, Mineapolis) kada su kompjuteri zloupotrebljeni radi falsifikovanja bankarskih podataka (Ranđelović, 2013, str. 257-265). Dalje su zabeleženi slučaj cyber kriminala u Finskoj (1968) i još nekim razvijenim zemljama Evrope, dok je u nekadašnjoj SFRJ prvi slučaj bio u Hrvatskoj (1983) i to u Istarskoj banci u Puli (Božić, Nikač, str. 281-290).

Pojam cyber kriminala nije jedinstveno određen u praksi i legislativi pa je to često dovodilo do poteškoća u primeni i različitog pravnog tretmana konkretnih dela i radnji koje čine obeležja ovih dela. Prvi pokušaj pojmovnog određenja cyber kriminal je dao jedan od pionira u ovoj oblasti, poznati američki autor Parker D. prema kojem *zloupotreba kompjutera* predstavlja „svaki događaj u vezi sa upotrebom kompjuterske tehnologije u kome žrtva trpi ili bi mogla da trpi gubitak, a učinilac deluje u nameri da sebi pribavi ili bi mogao da pribavi korist“ (Parker, 1973). Deceniju kasnije isti autor je predvideo da će cyber kriminal biti dominantna forma u bliskoj budućnosti (Parker, 1983), što se obistinilo i danas imamo eksploziju ovog pojavnog oblika kriminala.

U anglosaksonskoj literaturi cyber kriminal u etimološkom smislu obuhvata nezakonite radnje na kompjuteru, ili radnje kod kojih je kompjuter sredstvo izvršenja. Kao radnje

[3] Krivični zakonik, Službeni glasnik RS, br. 85/05-ispr,107/05– ispr,72/09, 111/09,121/12,104/13,108/14,94/16 i 35/19

izvršenja navode se nezakonit upad u tuđi kompjuterski sistem, krađa kompjuterskih podataka i korišćenje on line sistema za izvršenje krivičnog dela ili pomoć u izvršenju prevara (Encarta, 2010).

Prema legislativi EU cyber kriminal je definisan kao napad na informacione sisteme. Pod informacionim sistemom podrazumeva se uređaj ili grupa povezanih uređaja, od kojih jedan ili više njih u skladu sa programom automatski obrađuje kompjuterske podatke, kao i kompjuterske podatke skladištene, obrađene, preuzete ili prenesene od strane tog uređaja ili grupe uređaja u svrhu njegovog ili njihovog rukovanja, upotrebe, zaštite i održavanja.[4]

Sa krivičnopravnog stanovišta cyber kriminal obuhvata zloupotrebe kompjuterskih sistema, programa i podataka koji su inkriminisani u krivičnom zakonu svake zemlje. Krivična dela koja su rezultat zloupotrebe kompjutera se u doktrini najčešće dela na: 1) krivična dela kod kojih je kompjuter objekt radnje izvršenja (*computer crime*), 2) krivična dela kod kojih je kompjuter sredstvo izvršenja (*computer related crime*) i 3) krivična dela kod kojih je protivzakonita upotreba interneta (*net crime*) (Stojanović, 1987).

Za potrebe ovog referata cyber (kompjuterski, računarski) kriminal smo definisali kao oblik kriminalnog ponašanja u kojem se korišćenje kompjuterske tehnologije i informatičkih sistema ispoljava kao način vršenja krivičnih dela ili se kompjuter upotrebljava kao sredstvo ili cilj izvršenja, na koji način se ostvaruje relevantna posledica u krivičnopravnom smislu (Božić, Nikač, str. 281-290).

Karakteristike cyber kriminala možemo celovito sagledati na osnovu kriminalističke analize koja obuhvata: način izvršenja krivičnih dela, sredstva za izvršenje i posledice krivičnih dela cyber kriminala. Način izvršenja krivičnih dela iz grupe cyber kriminala obuhvata pre svega (zlo) upotrebu kompljutera i s tim u vezi kompjuteri (kompjuterski sistemi) su osnovno sredstvo izvršenja ovih krivičnih dela, dok se posledica manifestuje u vidu ostvarenja protivpravne imovinske koristi za sebe ili drugog, zatim nanošenja štete drugome, oštećenja sistema i na druge srodne načine (Aleksić, Škulić, 2007).

Krivična dela iz ove oblasti se odvijaju u posebnom informatičkom prostoru i stoga je njihova struktura veoma složena, način i sredstva izvršenja su specifični, poseban je objekt zaštite i postoji izuzetno velika društvena opasnost. Mesto izvršenja je fizički neodređeno jer se odnosi na specifičan IT prostor u kojem nema ograničenja na nacionalne prostore, dok krivična dela uvek imaju potencijalnu međunarodnu dimenziju jer ne postoje fizičke barijere i državne granice. Izvršioci krivičnih dela cyber kriminala su po pravilu lica koja imaju posebna znanja u ovoj oblasti i obično su vrhunski eksperti iz IT sektora, što naravno jako otežava procesuiranje ovih dela i izvršilaca. Kod izvršioca se

[4] Art.2.a. Directive 2013/40/EU of the EU Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA OJ L 218, 14.8.2013, p. 8–14

posebno naglašava namera da sebi ili drugom pribavi protivpravnu imovinsku - neimovinsku korist, ili da drugom nanese štetu.

Stanje i kretanje cyber kriminala ukazuje da je danas velika tamna brojka ove vrste krivičnih dela koja u velikoj meri nisu poznata ili prijavljena, što posebno otežava otkrivanje i procesuiranje izvršilaca i krivičnih dela. Problem je tim pre složeniji jer postoji veliki broj društvenih mreža i još veći broj njihovih korisnika, pa to olakšava izvršenje krivičnih dela i skrivanje izvršilaca. Prema službenim procenama najbolje kriminalističke službe na svetu, američkog FBI, manje od 1% cyber kriminala je realno otkriveno, dok je svega 12% prijavljeno (Obradović, Mijalković, Perić, Puača, 2007, str. 455-459). FBI u svom sastavu ima specijalizovano Odeljenje za borbu protiv cyber kriminala – CAT (*Cyber Action Team*),[5] koje sarađuje sa Interpolom, Europolom i drugim specijalizovanim agencijama kao što je CERT (*Computer Emergency Response Team*) (Nikač, 2015, str. 69-72).

3. LEGISLATIVNI OKVIR ZA BORBU PROTIV CYBER KRIMINALA

3.1. Međunarodni legislativni okvir

Međunarodni legislativni okvir za borbu protiv cyber kriminala čine značajniji dokumenti usvojeni pre svega na nivou SE i UN koji su posvećeni suzbijanju najtežih pojavnih oblika kriminala, međunarodnoj krivičnopravnoj saradnji i međunarodnoj policijskoj saradnji.

Zbog prostornih i drugih limita ukazujemo samo na važnije među kojima se po značaju ističe *Konvencija o Cyber kriminalu* ***Saveta Europe,*** usvojena 2001. godine u Budimpešti 2001.[6] Pored ostalog Konvencija je obavezala države potpisnice da u nacionalnom zakonodavstvu obavezno predvide i sledeća krivična dela: a) protiv poverljivosti, integriteta i dostupnosti kompjuterskih podataka i sistema, b) u vezi kompjutera (*prim. aut.* kompjuter kao sredstvo izvršenja), c) u vezi sa sadržajem and d) u vezi sa kršenjem autorskih i srodnih prava.[7] Konvencija dalje apostrofira neophodnost svestrane međunarodne saradnje država potpisnica i u tom kontekstu ističe veoma važnu uzajamnu pravnu pomoć. Republika Srbija je potpisala i ratifikovala Konvenciju posebnim *Zakonom o potvrđivanju Konvencije o visokotehnološkom kriminalu.*[8]

---

[5] Prema https://www.fbi.gov/investigate, cyber crime preuzeto 19. 07. 2019
[6] Convention on Cybercrime, CETS 185, 23. 11. 2001 dostupno na: http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_.pdf preuzeto 19.07. 2019.
[7] *Ibid.*
[8] Zakon o potvrđivanju Konvencije o visokotehnološkom kriminalu, Službeni glasnik RS br. 19/09.

U smislu implementacije Konvencije 2003. godine u Strazburu je usvojen *Dodatni Protokol uz Konvenciju o sajber kriminalu*, u vezi sa kriminalizacijom krivičnih dela rasističke i ksenofobične prirode izvršenih putem kompjuterskih sistema.[9] Pored ostalog Protokol je obavezao države potpisnice da donesu neophodna zakonska rešenja u skladu sa Konvencijom i usvoje potrebne mere za njihovu primenu. Prema Protokolu države potpisnice su se posebno obavezale da će u nacionalnom zakonodavstvu predvideti kao krivična dela sledeća ponašanja: širenje rasnog i ksenofobičnog materijala pomoću kompjuterskih sistema, pretnje putem kompjuterskih sistema motivisane rasizmom i ksenofobijom, javno vređanje lica pomoću kompjuterskih sistema zbog pripadnosti grupi koja se razlikuje prema rasi, boji kože, nacionalnom ili etničkom poreklu i veri, distribuiranje ili omogućavanje dostupnim javnosti putem kompjuterskih sistema materijala kojima se poriče, bitno umanjuju, odobravaju ili opravdavaju krivična dela genocida ili zločina protiv čovečnosti, pomaganja izvršiocima i podstrekavanja na izvršenje nekog od navedenih krivičnih dela.[10]

U širem smislu značajni su još neki **međunarodni dokumenti** u borbi protiv cyber kriminala kao što su: Konvencija UN o transnacionalnom organizovanom kriminalu,[11] Konvencija i policijskoj saradnji u Jugoistočnoj Evropi[12] i Konvencija o Centru agencija za sprovođenje zakona u Jugoistočnoj.[13]

Na nivou ***EU*** usvojeno je nekoliko značajnih dokumenata za borbu protiv cyber kriminala. Najpre je 2006. godine usvojena Direktiva 2006/24/EC Evropskog parlamenta i Saveta od 15. marta 2006. godine o zadržavanju podataka dobijenih ili obrađeni u vezi sa pružanjem javno dostupnih elektronskih komunikacionih usluga ili javnih komunikacija mreža kojom se dopunjava Direktiva 2002/58/EC,[14] posebno u cilju efikasnijeg suzbijanja cyber kriminala na osnovu elektronskih tragova i drugih dokaza. Potom je 2009. godine doneta Direktiva 2009/24/EC Evropskog parlamenta i Saveta od 23. aprila 2009. o pravnoj zaštiti kompjuterskih programa,[15] prema kojoj je izvorni kompjuterski program zaštićen u korist autora čija je to intelektualna svojina. Pored toga doneto je i nekoliko podzakonskih akata

---

[9] Dostupno na: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081 60f preuzeto 19.07.2019.
[10] *Ibid,* art. 3-7.
[11] United Nations Convention against Transnational Organized Crime (UNCATOC), dostupno na: https://www.unodc.org/unodc/treaties/CTOC/ pristupljeno 20.07.2019.
[12] Police Cooperation Convention for Southeast Europe (PCCSE), dostupno na: http://www.pccseesecretariat.si/index.php?item=9&page=static, PCC SEE 2006 2011.pdf pristupljeno 20. 07. 2019.
[13] SELEC Convention, dostupno na: http://www.selec.org/docs/PDF/SELEC%20Convention%20%5Bsigned%20on%2009.12.2009%5D.pdf pristupljeno 20. 07. 2019.
[14] Directive 2006/24/EC, Official Journal of the European Union, L 105/54, dostupno na: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32006L0024 preuzeto 20. 07. 2019.
[15] Directive 2009/24/EC, Official Journal of the European Union, L 111/16, dostupno na: **Greška! Referenca hiperveze nije ispravna.** preuzeto 20. 07. 2019.

za primenu ovih direktiva. Poslednja u nizu je usvojena Direktiva 2013/40/EU Evropskog parlamenta i Saveta od 12. avgusta 2013. o napadima na kompjuterske sisteme, koja je zamenila prethodnu Okvirnu odluka Saveta EU 2005/222/PUP[16]. Pored ostalog Direktiva nalaže državama potpisnicama da u nacionalnom zakonodavstvu inkriminišu sledeća krivična dela: Nezakonit pristup informacionom sistemu; Nazakonito mešanje u sistem; Nezakonito mešanje u podatke; Nazakonito presretanje, podsticanje, pomaganje, podržavanje i pokušaj te je propisana i odgovornost pravnog lica. Dodajemo da se Direktivom proširuje krug kažnjivih ponašanja i uvode dopunske otežavajuće okolnosti (Kokot, 2014, str. 301-327).

3.2. Nacionalni legislativni okvir Srbije

Nacionalni legislativni okvir Republike Srbije u borbi protiv cyber kriminala je utemeljen na navedenim međunarodnim dokumentima, koje je potpisala i ratifikovala Republika Srbija. U ovoj oblasti od izuzetne važnosti su norme predviđene nacionalnim krivičnim zakonodavstvom, a pre svih odredbama KZ. Značajno mesto imaju i ostali propisi iz krivičnopravne oblasti kao što su Zakonik o krivičnom postupku,[17] Zakon o organizaciji i nadležnosti državnih organa u suzbijanju organizovanog kriminala, terorizma i korupcije,[18] Zakon o oduzimanju imovine proistekle iz krivičnog dela.[19]

Odredbama aktuelnog KZ najpre su definisani pojedini značajniji pojmovi u oblasti računarske (kompjuterske) tehnologije, IT sistema i cyber kriminala. Tako je računarski (kompjuterski) podatak određen kao svako predstavljanje činjenica, informacija ili koncepta u obliku podesnom za obradu u računarskom sistemu, uključujući i odgovarajući program na osnovu koga računarski sistem obavlja svoju funkciju. Dalje se definiše računarska mreža_kao skup međusobno povezanih računara, odnosno kompjuterskih sistema koji komuniciraju razmenjujući podatke. Pod računarskim programom_smatra se uređeni skup naredbi koji služe za upravljanje radom računara, kao i za rešavanje određenog zadatka pomoću računara.[20] Istim zakonom je određen i računarski virus kao računarski program ili neki drugi skup naredbi unet u računar ili računarsku mrežu koji je napravljen da sam sebe umnožava i deluje na druge programe ili podatke u računaru ili računarskoj

[16] Directive 2013/40/EU of the European parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, dostupno na: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:218:0008:0014:en:PDF preuzeto 20. 07. 2019.
[17] Zakonik o krivičnom postupku, Službeni glasnik RS, br.72/11,101/11,121/12,32/13,45/13, 55/14 i 35/19
[18] Zakon o organizaciji i nadležnosti državnih organa u suzbijanju organizovanog kriminala, terorizma i korupcije, Službeni glasnik RS, br. 94/16.
[19] Zakon o oduzimanju imovine proistekle iz krivičnog dela, Službeni glasnik RS, br. 32/13 i 94/16.
[20] Čl. 112. st. 3. tač. 17-20. KZ

mreži dodavanjem tog programa ili skupa naredbi jednom ili više računarskih programa ili podataka.[21]

Krivična dela iz oblasti cyber kriminala su navedena u Glavi XXVII KZ – Krivična dela protiv bezbednosti računarskih podata¸ odredbe od čl. 298 do čl. 304.a, ukupno osam (8) i to:

Oštećenje računarskih podataka i programa, Računarska sabotaža, Pravljenje i unošenje računarskih virusa, Računarska prevara, Neovlašćeni pristup zaštićenom računaru, računarskoj mreži i elektronskoj obradi podataka kao i Sprečavanje i organičavanje pristupa javnoj računarskoj mreži.[22]

U kratkom osvrtu na važnija krivična dela i zaprećene kazne iz aktuelnog KZ ukazujemo da je zakonodvac u RS najpre pošao od lakšeg krivičnog dela – oštećenja računarskih podataka i programa iz čl. 298. Za navedeno delo je predviđena kazna zatvora do 3 godine ako izvršilac neovlašćeno izbriše, izmeni, ošteti, prikrije ili na drugi način učini neupotrebljivim računarski podatak ili program. Dalje je predviđena kazna zatvora od 3 meseca do 3 godine ako je delom prouzrokovana šteta u iznosu koji prelazi 450.000 RSD, dok je predviđena kazna zatvora od 3 meseca do 5 godina ako je delom prouzrokovana šteta u iznosu koji prelazi 1.500.000 RSD. Sledeće krivično delo je računarska sabotaža iz čl. 299 za koju je zaprećena kazna zatvora od 6 meseci do 5 godina. Sledi pravljenje i unošenje računarskih virusa iz čl. 300 i predviđene novčana kazna ili kazna zatvora do 6 meseci za osnovni oblik, kao i za teži oblik novčana kazna ili kazna zatvora do 2 godine ako unese računarski virus u tuđi računar ili računarsku mrežu i time prouzrokuje štetu.[23]

Zakonodavac je dalje predvideo krivično delo gde je radnja izvršenja kompleksnija kao što je to računarska prevara iz čl. 301, za koju je predviđena novčana kazna ili kazna zatvora do 3 godine. Za teži oblik je prediđena kazna zatvora od 1 do 8 godina ako je pribavljena imovinska korist koja prelazi iznos od 450.000 RSD, dok je predviđena kazna zatvora od 2 do 10 godina ako je pribavljena imovinska korist koja prelazi iznos od 1.500.000 RSD. Krivično delo pod nazivom neovlašćeni pristup zaštićenom računaru, računarskoj mreži i elektronskoj obradi podataka je predviđeno u čl. 302. i za navedeno je popisana novčana kazna ili kazna zatvora do 6 meseci za osnovni oblik. Za teži oblik je predviđena novčana kazna ili kazna zatvora do 2 godine ako snimi ili upotrebi podatak dobijen na neovlašćen način, dok je za najteži oblik predviđena kazna zatvora do 2 godine ako je došlo do zastoja ili ozbiljnog poremećaja funkcionisanja elektronske obrade i prenosa podataka ili mreže ili su nastupile druge teške posledice.[24]

---

[21] Čl. 112. st. 3. tač. 20. KZ
[22] Čl. 298 - 304a. KZ
[23] *Ibid.*
[24] *Ibid.*

Sprečavanje i ograničavanje pristupa javnoj računarskoj mreži je krivično delo iz čl. 303. i za isto je predviđena novčana kazna ili kazna zatvora do 1 godine, dok je za kvalifikovani oblik predviđena kazna zatvora do 3 godine ako delo učini službeno lice u vršenju službe. Neovlašćeno korišćenje računara ili računarske mreže je krivično delo predviđeno čl. 304. i za isto je predviđena novčana kazna ili kazna zatvora do 3 meseca. Poslednje u grupi je pravljenje, nabavljanje i davanje drugom sredstava za izvršenje krivičnih dela protiv bezbednosti računarskih podataka iz čl. 304a za koje je predviđena kazna zatvora od 6 meseci do 3 godine, odnosno novčana kazna ili kazna zatvora do 1 godine ako izvršilac poseduje sredstva s namerom izvršenja cyber crime.[25]

4. KRIMINALISTIČKI ASPEKT BORBE PROTIV CYBER KRIMINALA

Kriminalističko-operativni aspekt suzbijanja kriminala je nesporno krucijalni element borbe protiv cyber i ostalih pojavnih oblika kriminala. Glavni subjekt i nosilac aktivnosti je pre svega ***policija*** koja u svom sastavu po pravilu ima modernu organizaciju, specijalizovane linije rada i edukovane eksperte za borbu protiv najtežih pojavnih oblika kriminala. U razvijenim zemljama policija je organizovana na vrlo visokom nivou, poseduje relativno dobra ovlašćenja, modernu tehničku opremu i ima finansijsku podršku zajednice. Pored policije veoma važnu ulogu imaju ***tužilaštvo*** i ***sud*** kao državni organi u prvoj liniji borbe protiv kriminala. Rad pravosudnih organa i policije je danas baziran na opšteprihvaćenim međunarodnim standardima, normama međunarodnog prava i rešenjima razrađenim u nacionalnim propisima.

Zakonom o organizaciji i nadležnosti državnih organa za borbu protiv visoko-tehnološkog kriminala[26] uređeni su obrazovanje, organizacija, nadležnost i ovlašćenja posebnih organizacionih jedinica državnih organa radi otkrivanja, krivičnog gonjenja i suđenja za krivična dela iz grupe VTK i komplementarna krivična dela (čl. 3). Istim propisom predviđeni su Posebno tužilaštvo – Više JT u Beogradu za teritoriju RS kojim rukovodi posebni tužilac za VTK,[27] zatim nadležni Viši sud u Beogradu za teritoriju RS[28] i posebna služba u okviru MUP RS.[29] U pitanju je posebno Odeljenje za suzbijanje VTK koje je u sastavu Službe za borbu protiv organizovanog kriminala (SBPOK), koja je integralni deo jedinstvene Uprave kriminalističke policije (UKP) sedištu MUP RS u Beogradu.[30]

---

[25] *Ibid.*
[26] Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visoko-tehnološkog kriminala, Službeni glasnik RS, br. 61/05 i 104/09 (Zakon o VTK).
[27] Čl. 4-6. Zakon o VTK,
[28] Čl. 10-11. Zakon o VTK
[29] Čl. 9. Zakon o VTK
[30] www.mup.gov.rs pristupljeno 20. 07. 2019.

Policija postupa po nalogu Višeg JT, radi saglasno ZKP i ostalim normama krivičnog zakonodavstva, dok je jedino oblast rada posebna zbog specifičnog okruženja u kojem se vrše krivična dela. Izuzetno je važno da pripadnici policije budu dobro edukovani i da im je poznata metodologija izvršenja krivičnih dela iz oblasti VTK, jer se pojavni oblici VTK svakodnevno razvijaju i usavršavaju usled tehničko-tehnološkog razvoja kompjutera.

Pripadnici Odeljenja za suzbijanje VTK stalno izučavaju *modus operandi* krivičnih dela i savremene pojavne oblike među kojima su posebno atraktivni: finansijske prevare, krađa identiteta, zloupotreba podataka preko Interneta i društvenih mreža (Nikač, 2015, str. 110-112), zatim mrežna ometanja, *on-line* prevare *(fishing*), hakovanje, neovlašćeno presnimavanje na multimedijalne nosače i dr. (Nikač, Urošević, 2010, str. 53-58).

Izvršioci krivičnih dela cyber kriminala su ne samo eksperti već i veliki broj lica kojima su kompjuteri danas dostupni, a među njima ima dosta mladih. Naravno najopasnije su organizovane kriminalne grupe koje angažuju najbolje eksperte i mlade za izvršenje najtežih krivičnih dela. Grupe su veoma organizovane, koriste slabosti sistema, upadaju i kompromituju čak velike kompjuterske sisteme državnih organa najrazvijenih zemalja.

Policija i drugi subjekti preduzimaju najpre preventivne ***mere*** na suzbijanju pojavnih oblika VTK, kao što su specijalne zaštitne šifre i posebni kodovi. Dalje se preduzimaju represivne mere sa ciljem lociranja, prepoznavanja i prikupljanja dokaza o krivičnim delima i izvršiocima cyber kriminala, a potom procesuiranja pred nadležnim sudovima. Pored korišćenja tradicionalnih kriminalističko-operativnih metoda u velikoj meri se koriste specijalne istražne tehnike i metode, za koje potrebe je neophodno izraditi i usvojiti novu strategiju borbe protiv cyber kriminala u budućnosti (Sessions, 2001).

Borba protiv cyber kriminala podrazumeva multiagencijski pristup i koordinaciju na nacionalnom planu, kao i svestranu međunarodnu saradnju država i međunarodnih organizacija na globalnom planu (Nikač, Božić, 2016, str. 431-443).

5. ZAKLJUČAK

Cyber kriminalitet je najsofisticiraniji pojavni oblik kriminala u savremenom društvu i manifestuje se u različitim vidovima. Modusi izvršenja krivičnih dela ukazuju da se cyber kriminal odvija u specifičnom virtuelnom prostoru i da sa sobom nosi izuzetno visoki stepen društvene opasnosti, dok su izvšioci ne samo experti u ovoj oblasti već sva lica koja bez teškoća pristupaju kompjuterima i društvenim mrežama. To je jedan od osnovnih razloga što je dokazivanje i procesuiranje cyber krivičnih dela i izvršilaca veoma teško. Problem je još složeniji usled velike tamne brojke ovog pojavnog oblika kriminala, jer mnoga krivična dela nisu ni prijavljena.

U cilju harmonizacije pravnih normi na međunarodnom planu su usvojeni važni međunarodni dokumenti za suzbijanje organizovanog i drugih oblika kriminala. Međunarodna zajednica je reagovala na identičan način i u slučaju cyber kriminala kad je usvojena *Konvencija o kibernetičkom kriminalu* kao najvažniji pravni iyvor u ovoj oblasti na starom kontinentu. To je dalje omgoućilo da države potpsnice harmonizuju svoje zakonodavstvo, ugrade u pravni sistem najvažnija pravna rešenja iz Konvencije i donesu propise u ovoj oblasti na nacionalnom nivou. Na toj osnovi bilo je dalje moguće usvojit preventivne i represivne mere u borbi protiv cyber kriminala, uspostaviti multiagencijsku saradnju na nacionalnom nivou i uspostaviti međunarodnu saradnju na međunarodnom nivou.

Republika Srbija je potpisala i ratifikovala navedenu Konvenciju, izvršila novele KZ i ugradila posebnu glavu – krivična dela protiv bezbednosti računarskih podataka. Dalje je usvojen poseban Zakon o VTK kojim su pre svega predviđeni specijalizovani organi za suzbijanje cyber kriminala. Smatramo da treba permanentno pratiti primenu propisa i praksi i shodno tome, po potrebi, u slučaju novih pojavnih oblika cyber kriminala predvideti adekvatne novele. Treba voditi računa i o izgradnji jedinstvene pravne prakse u ovoj za nas nedovoljno poznatoj oblasti, na koji način bi se izbegla potencijalna različita pravna tumačenja srodnih ili sličnih predmeta.

Kriminalističko-operativni odgovor treba da bude komplementaran težini radnih problema, s posebnim akcentom na to da je cyber kriminal najčešće oblik organizovanog kriminala. U tom kontekstu od presudne važnosti je da države imaju dobro organizovane specijalne službe koje pak imaju dobre materijlne uslove za rad, zatim da imaju dobro edukovane kadrove i da razvijaju multiagencijsku pristup i međunarodnu saradnju u borbi protiv cyber kriminala.

LITERATURA

- Aleksić, Ž., Škulić, M. (2007). *Kriminalistika.* Beograd: Pravni fakultet.
- Božić, V., Nikač, Ž. (2017). Criminal Law and Criminalistic forensic approach to fighting Cyber Crime. In Alexandar Ioan Cuza and others (Eds.) *Conference Proceedings of the V International Scientific Conference Romaninan Educational System of Forensic Science, „Forensic Sciences between education and operational field"* (str. 281-290). Bucharest
- Directive 2013/40/EU of the EU Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing, Council Framework Decision 2005/222/JHA OJ L 218, 14.08.2013
- Directive 2006/24/EC, Official Journal of the European Union, L 105/54, dostupno na: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32006L0024 preuzeto 20. 07. 2019.
- Encarta, (2010). *World English Dictionary*, North American Edition, Microsoft Corporation dostupno na http://encarta.msn.com/encnet/refpages/search.aspx?q=computer+crime pristupljeno 20. 07. 2019.
- Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala, Službeni glasnik RS, br. 61/05 i 104/09
- Krivični zakonik, Službeni glasnik RS, br. 85/05-ispr, 107/05-ispr, 72/09, 111/09, 121/12, 104/13, 108/14, 94/16 i 35/19
- Kokot, I. (2014). Kaznenopravna zaštita računalnih sustava, programa i podataka. *Zagrebačka pravna revija,* 3, 303-330.
- Nikač, Ž., (2015). *Međunarodna policijska saradnja*. Beograd: Kriminalističko-policijska akademija.
- Nikač, Ž., Božić, V. (2016). International Cooperation of Southeast Europe in the fight against crime. in *Conference Proceedings of International scientific conference "Theory and Practice of Law Enforcement Activities".* Lviv, 431-443
- Obradović, S., Mijalković, M., Perić, D., Puača, D. (2007). Istraživanje kriminala na računarima, *Infoteh Jahorina,* 3, 455-459.
- Parker, D. (1973). *Computer Abuse.* Menlo Park: Stanford Research Institute.
- Parker, D. (1983). *Fighting computer crime.* New York: Charles Scribner's Sons.
- Ranđelović, D. (2013). *Visokotehnološki kriminal*. Beograd: Kriminalističko-policijska akademija.
- Sessions, S.W. (1991). *Kompjuterski kriminal-trend koji eskalira*, Zagreb: Priručnik, 3
- Stojanović, Z. (1987). Savremena tehnička sredstva i krivično pravo sa posebnim osvrtom na kompjuterski kriminalitet, učešće u Okruglom stolu *"Savremena tehnika i krivično pravosuđe"*, Novi Sad: XXV Savetovanje Saveza udruženja za krivično pravo i kriminologiju Jugoslavije.

Kriminalističke teme
Zbornik radova
Godina XIX, Broj 5, 2019.
ISSN 1512-5505

NEMATERIJALNA ŠTETA KAO JEDAN OD OBLIKA KOMPJUTERSKOG KRIMINALA NASTAO VRŠENJEM KOMPJUTERSKIH DELIKATA

INTANGIBLE DAMAGE AS ONE OF THE FORMS OF COMPUTER CRIME CAUSED BY COMPUTER DELICTS

Pregledni naučni rad

Sana SOFTIĆ[31]

SAŽETAK

Inspiracija za rad i problem (i) koji se radom oslovljava (ju): Neophodnost unapređenja prevencije zaštite privatnosti na internetu te povreda prava na privatnost i zakonsko regulisanje istog.

Ciljevi rada (naučni i/ili društveni): Potaknuti svijest o posljedicama i o pravima onih čije je pravo na privatnost povrijeđeno kao i djelotvorno utvrđivanje težine učinjenih povreda.

Metodologija/Dizajn: Pregled postojeće literature. Pregled internetskih izvora. Pregled sudske prakse.

Ograničenja istraživanja/rada: Ne postoje.

Rezultati/Nalazi: Sudovi u BiH u postupcima povrede prava na privatnost, nemaju jos dovoljno iskustva, niti postoji sudska praksa ni mogućnost Vrhovnog suda da ujednači razlike u procjenama sudova nižeg stepena.

Generalni zaključak: Sa naglim razvojem savremenih računarskih tehnologija putem zloupotrebe kompjutora sve češće se povrijeđuje moralno pravo te narušava nečiji ugled.

Opravdanost istraživanja/rada: Rad je ustanovio da kompjuterski kriminalitet kao velika negativna društvena pojava sve više dovodi do povreda prava na privatnost te da oštećenici ne pokazuju dovoljno interesa za neimovinske oblike popravljanja štete, te da bi se isto svakako trebalo promjeniti.

Ključne riječi

nematerijalna šteta; kompjuterski kriminal;internet; zaštita privatnosti; pravo na privatnost; intangible demage; computer criminality, Internet, privacy protection, right to privacy;

[31] Sana Softić je magistar kriminalističkih nauka, advokat u advokatskoj kancelariji Sana Softić. E –mail: adv.sanasoftic@outlook.com

ABSTRAKT

Reason (s) for writing and research problem (s): Necessity of improving the prevention of privacy protection on the Internet and violation of the right to privacy and legal regulation of the same.
Aims of the paper (scientific and/or social): To raise awareness of the consequences and rights of those whose right to privacy has been violated, as well as the effective determination of the severity of the violations committed.
Methodology/Design: Review of existing literature. Review of internet sources. Review of the case law.
Research/ paper limitations: Do not exist.
Results/ Findings: Courts in BiH in procedures of violation of the right to privacy do not have sufficient experience yet, and there is no case law or the ability of the Supreme Court to align differences in the judgments of lower courts.
General conclusion: With the rapid development of modern computer technologies through the abuse of computers, moral law is being violated more and more, thereby violating someone's reputation.
Research/paper validity: The paper found that computer crime as a major negative social phenomenon increasingly leads to violation of the right to privacy and that the injured parties do not show sufficient interest in non-property forms of reparation, and that the same should certainly be changed.

Key words

intangible demage; computer criminality, Internet, privacy protection, right to privacy

UVOD

U ovom članku je teorijski sagledan jedan od najrasprostranjenijih oblika kompjuterskog kriminaliteta koji obuvhata povredu prava na privatnost zloupotrebom društvenih mreža i naknadu nematerijalne štete kao jednog od oblika kompjuterskog kriminala nastao vršenjem kompjuterskih delikata. U današnje vrijeme su česte stručne i naučne rasprave o tome da li kriminalitet u oblasti informacionih tehnologija predstavlja nastavak klasičnih oblika kriminaliteta sa kojima se suočavamo svakodnevno ili se radi o posebnom obliku kriminaliteta koji zahtijeva novo definisanje.

U svakom slučaju kompjuterski kriminalitet predstavlja noviji oblik kriminaliteta, čije je pojavljivanje rezultat velikog napretka tehnologije u oblasti telekomunikacija.

Sve veća upotreba interneta i društvenih mreža, kao i korišćenje kompjuterske tehnike u svakodnevnom životu, predstavljaju ogroman napredak sa stanovišta društvenog razvoja.

S druge strane, upotrebom kompjuterske tehnike, posebno interneta i društvenih mreža, veliki broj korisnika je izložen svakodnevnoj viktimizaciji, u slučaju da podaci prenijeti putem društvenih mreža budu zloupotrebljeni.

Sa naglim razvojem savremenih računarskih tehnologija putem zloupotrebe kompjutera sve češće se povrijeđuje moralno pravo te narušava nečiji ugled. U današnjim, savremenim pravnim sistemima naknada nematerijalne štete je realnost.

Većina savremenih uporednih pravnih sistema, u većoj ili manjoj mjeri, bilo izričito ili posredno, uz popravljanje štete priznaje i neke druge funkcije odgovornosti za štetu:

Bitna posljedica priznanja preventivne funkcije odštetnog prava mogućnost je priznavanja viših iznosa naknada no što su one koje proizlaze samo iz funkcije popravljanja štete.[32]

Za pravilno tumačenje naknade nematerijalne štete neophodno je da se upozna sa pravima ličnosti, jer su to prava kojima se priznaje pravna zaštita pojedinca od štetnih radnji na osobi [33] odnosno povreda koje su nanesene njegovom biću, njegovoj psihi ili njegovom tijelu. Jezički smisao izraza šteta uobičajeno ne podrazumjeva samo imovinske već i moralne gubitke. Cilj naknade štete je otklanjanje štetne posljedice i naknada mora biti adekvatna šteti. S obzirom na čijenicu da nematerijalna šteta ne može imati cijenu, postavlja se pitanje da li se i kako se može izvršiti naknada štete koja je nastala povredom prava ličnosti.

Zaključak se našao u samoj sudskoj praksi, gde se na praktičnim primjerima vidi kako i na koji način se izvršava naknada nematerijalne štete i u kojoj mjeri su određene zakonske odredbe ali i sudske odluke efikasne. U tom smislu se može reći da je sud kod svih oblika nanošenja nematerijalne štete stava da je pravo na naknadu nematerijalne štete osnovano kada je radnjom štetnika određeno lice trpelo strah, bolove psihičke ili fizičke prirode ili je teško povrijeđen ugled oštećenog u sredini u kojoj živi.

Štetne posljedice suštinski se ispoljavaju na oštećenom licu koje je pogođeno protivpravnom radnjom štetnika. Ono trpi promjenu svog određenog pravnog dobra i to na gore. Po Radišiću, šteta postaje vidljiva tek ako se sravni sadašnje stanje uštrbnutih dobara sa njihovim ranijim stanjem, pri čemu se može uzeti u obzir i budući razvitak koji je već izvestan. O šteti može biti riječi samo ako postoji negativna razlika ovih stanja (Radišić, 1985).

Pod kategorijom nematerijalne štete mogu se podvesti fizički i psihički bol, kao i strah. Novčana naknada se dosuđuje oštećenom samo u slučaju manifestovanja posljedica povreda u nekom od vidova nematerijalne štete. Član 200. Zakona o obligacionim odnosima navodi mogućnost dosuđivanja pravične naknade u slučaju pretrpljenih fizičkih bolova, pretrpljenih duševnih bolova zbog umanjenja životne aktivnosti, naruženosti,

[32] MAGNUS, U., Comparative Report on the Law of Damages, Unification of Tort Law: Damages, Kluwer Law International, The Hague–London–Boston, 2001., str. 186.

[33] Štetne radnje na osobi – u te radnje spadaj: uništenje tuđeg života, ozljeda tijela i zdravlja, lišenje slobode, povreda spolnog integriteta, povreda časti i ostale povrede na osobi (ograničenje slobode volje, povreda nečijeg vjerskog uvjerenja i sl.) Modly D. Korajlić N; 2002: 805)

povrede ugleda, časti, slobode ili prava ličnosti, smrti bliskog lica kao i za strah, posebno se vrši analiza intenziteta i obima pretrpljenih fizičkih ili psihičkih bolova. Nematerijalna šteta se može dosuditi nezavisno od materijalne štete, čak i u odsustvu zahtjeva za materijalnu štetu, oštećeni može zahtijevati naknadu nematrijalne štete. "Glavni cilj naknade štete sastoji se u otklanjanju štetnih posljedica. Smatra se da se taj cilj, u izvjesnom smislu, može postići i kod nekih nematerijalnih šteta. Ipak, nesporno je da se naveći broj nematerijalnih šteta ne može popraviti putem naturalne restitucije. Stoga, dolazi u obzir jedino novčano davanje radi zadovoljenja (satisfakcija) oštećenog, a ne kao cjena prikraćenog dobra (Obradović i Kovačević, 2014). "

PRAVO NA PRIVATNOST

Pravo na privatnost predstavlja elementarno čovjekovo pravo, kako međunarodno, tako i ustavno pravo javno-pravnog značaja te lično pravo civilno-pravnog značaja kao jedan od nezamjenjivih elemenata čovjekovog postojanja koji štiti čovjeka od prekomjernog posezanja državne vlasti, javnosti i drugih pojedinaca u pojedinčevu odlučujuću duševnu, prostornu i informacijsku privatnost. Dakle, pravo na privatnost može se razmatrati s nekoliko aspekata: kao čovjekovo pravo međunarodno pravne prirode, kao temeljno ustavom zagarantirano pravo te kao lično pravo zaštićeno instrumentima građanskoga prava. Pravo na privatnost u pravnoj terminologiji najčešće je spominjano prema anglo-američkoj inačici „Right to privacy", u francuskom pravu pak najviše puta imenovano kao „pravo poštivanja privatnog življenja – droit au respect de la vie" te u Njemačkoj nazivano „Recht auf Privatheit" ili „Recht auf Privatsphäre".

Protupravnost je, pravnim rječnikom, ona granica koju pojedinac ne smije prijeći u ostvarivanju suprotnog interesa za očuvanjem nedodirljivosti prava na privatnost, odnosno prava na ličnost. Samo kršenje prava na privatnost predstavlja interes pojedinca za očuvanje vlastite privatnosti koje prevladava nad interesima kojima pojedinac u ostvarivanju prava, zadire upravo na privatnost drugog pojedinca. Postoji mišljenje da je u području prava na privatnost prvenstveno riječ o osobi i nematerijalnim vrijednostima koje predstavljaju i činjenice sadržane u ličnim podacima. Zaštitom podataka od neodgovarajuće upotrebe, štiti se u konačnici subjekt podataka, tj. osoba. Dakle, samo razgraničenje pojmova temelji se na činjenici da se ne radi o povredi podataka u klasičnom smislu već o povredi osobe. Vezano uz taj navod možemo samo ustanoviti da nažalost čovjek sve više postaje objektom i sve su manje mogućnosti da se sačuvaju njegovi interesi, prava, slobode i posebno najintimniji život. „Odredba da je sadržaj neimovinske štete povreda prava osobnosti je, međutim, od povijesnog značenja.[34]

[34] Prof. dr. Aldo Radolović, Pravo osobnosti u novom Zakonu o obveznim odnosima, Zb. Prav. fak. Sveuč. Rij. (1991) v. 27, br. 1, 129-170 (2006.)

Zaštita ličnih podataka unutar informacijskih sistema tako danas postaje jedno od najznačajnijih društvenih pitanja i ima jako bitnu ulogu. Nedopušteno otkrivanje podataka o ličnim stvarima mogu itekako negativno uticati na pojedinca. Iz tog razloga je prijeko potrebno razraditi i provesti takav mehanizam obrade podataka koji će u najvećoj mjeri garantovati kvalitetno i savjesno prikupljanje, obradu, pohranu i korištenje informacija.

Privatnost ima nekoliko aspekata, te bi se mogla podijeliti na informacijsku, komunikacijsku i prostornu privatnost. Informacijska se privatnost odnosi na lične podatke (prikupljanje podataka o sebi, upravljanje njima i njihovo korištenje), komunikacijska obuhvaća onaj dio privatnosti koji se odnosi na lične zapise i komunikaciju s drugim osobama (sloboda i tajnost osobnih zapisa te dopisivanja i bilo kojeg drugog oblika komuniciranja), a prostorna se privatnost odnosi na dom i drugi prostor u kojem osoba vodi život posebno od drugih. Svaki se aspekt prava na privatnost sastoji u očuvanju tajnosti svoje privatnosti, posebno u onome dijelu gdje se od pojedinaca zahtijeva davanje podataka u svojstvu poreznih obveznika, korisnika penziskih, zdravstvenih, socijalnih i drugih fondova, zbog statističkih analiza i praćenja, znanstvenih istraživanja i slično. Ti se podaci bez dopuštenja osobe ne smiju dalje širiti i javno otkrivati. Neki se podaci mogu i posebno dodatno štititi ako su klasificirani kao državna, vojna, službena, poslovna ili profesionalna tajna.

Podizanje razine svijesti, u cjelokupnoj javnoj vlasti i administraciji, o vrijednosti i značenju zaštite ličnih podataka, kao i o uvidu u temeljna načela i standarde na kojima se ta zaštita temelji, osnova je koja bi trebala osigurati da se ovom pitanju pristupi profesionalno i odgovorno. Pritom, odgovornost u pristupanju problemu zaštite podataka ne ovisi samo o svijesti i znanju o vrijednosti i značenju zaštite nego i o poštivanju temeljnih prava i interesa pojedinaca.

NAKNADA NEMATERIJALNE ŠTETE I PRAVO NA ISTU

Jezički smisao riječi šteta uobičajeno ne podrazumeva samo imovinske već i moralne gubitke. Za pravilno tumačenje naknade nematerijalne štete neophodno je da se upozna sa pravima ličnosti, jer su to prava kojima se priznaje pravna zaštita pojedinca od povreda koje su nanesene njegovom biću, njegovoj psihi ili njegovom tijelu. Pristupi zakonodavaca, sudske prakse i pravne teorije pojedinih država, razvijali su se, vrlo načelno govoreći, različitim tempom, ali u istom smjeru, od potpune neprihvatljivosti novčane naknade kao oblika popravljanja neimovinske štete, ka njenom priznavanju.[35]

Cilj naknade štete je otklanjanje štetne posljedice i naknada mora biti adekvatna šteti. S obzirom na čijenicu da nematerijalna šteta ne može imati cijenu, postavlja se pitanje kako

[35] Ovaj su razvoj, općenito govoreći, omogućile sudska praksa i pravna teorija, jer su zakonodavci bili u priznavanju novčane naknade za neimovinske štete, vrlo restriktivni.

se i da li se može izvršiti naknada štete koja je nastala povredom prava ličnosti. Zaključak se našao u samoj sudskoj praksi, gde se na praktičnim primjerima vidi kako i na koji način se izvršava naknada nematerijalne štete i u kojoj mjeri su određene zakonske odredbe ali i sudske odluke efikasne. U tom smislu se može reći da je sud kod svih oblika nanošenja nematerijalne štete stava da je pravo na naknadu nematerijalne štete osnovano kada je radnjom štetnika određeno lice trpjelo strah, bolove psihičke ili fizičke prirode ili je teško povrijeđen ugled oštećenog u sredini u kojoj prebiva.

Fizički i psihički bol, kao i strah mogu se podvesti pod kategorijom nematerijalne štete. Novčana naknada se dosuđuje oštećenom samo u slučaju manifestovanja posljedica povreda u nekom od vidova nematerijalne štete. Član 200. Zakona o obligacionim odnosima navodi mogućnost dosuđivanja pravične naknade u slučaju pretrpljenih fizičkih bolova, pretrpljenih duševnih bolova zbog umanjenja životne aktivnosti, naruženosti, povrede ugleda, časti, slobode ili prava ličnosti, smrti bliskog lica kao i za strah, posebno se vrši analiza intenziteta i obima pretrpljenih fizičkih ili psihičkih bolova.

Nematerijalna šteta se može dosuditi nezavisno od materijalne štete, čak i u odsustvu zahtjeva za materijalnu štetu, oštećeni može zahtijevati naknadu nematerijalne štete.

Sud posebno mora voditi računa o značaju povrijeđenog dobra i samom cilju kome služi naknada prilikom odlučivanja o zahtjevu za naknadu nematerijalne štete, kao i njenoj visini čime se ne smije voditi težnjama koje nemaju društvenu svrhu niti su spojivi sa prirodom postojanja instituta naknade nematerijalne štete.

Rezultat povijesne evolucije prava odgovornosti za štetu je i taj da građanskopravna sankcija za počinjenu štetu može biti samo imovinska, ne i osobna. [36] Načelo imovinske sankcije kao načelo koje važi za čitavo građansko (privatno) pravo[37] predstavlja, s jedne strane, izraz humanizacije građanskopravnih odnosa, ali s druge strane, ponekad izaziva nemogućnost podmirenja oštećenika.

U slučaju nastanka nematerijalne štete u nekom od vidova koji su predviđeni zakonom novčana naknada se dosuđuje oštećenom samo u slučaju kada je intenzitet i trajanje bolova ili straha opravdan što će uticati na ponovno uspostavljanje psihičke ravnoteže ili makar približno olakšanje psihičkog stanja oštećenog što se kroz praksu pokazalo kao djelimično učinkovit metod postizanja cilja postojanja naknade štete, vraćanje u pređašnje stanje. Inicirajuću postupak kod nadležnog suda oštećeni može ostvariti pravo za naknadom nematerijalne štete tužbom. Tužba za naknadu nematerijalne štete se odlikuje

[36] Tako V. Vodinelić, op. cit., str. 41., 494.-495. Povijesna evolucija dosta tvrdokorno zadržava načelo krivnje kao bitnu pretpostavku odgovornosti, ali razlozi humanizacije prava išli su u pravcu pretežitog otklanjanja osobnih sankcija; iznimno takvih (osobnih) sankcija i danas ima u građanskom pravu (neimovinsko popravljanje neimovinske štete ili iseljenje zbog protupravnog useljenja u tuđi stan).
[37] V. Vodinelić, op. cit., str. 46.-47. govori o „porodici“ građanskog prava“.

elementom određenosti vida nematerijalne štete, čak i kada je ona proistekla iz istog životnog događaja mora se navesti svaki oblik štete pojedinačno.

NAKNADA NEMATERIJALNE ŠTETE PREMA ZAKONU OOBLIGACIONIM ODNOSIMA

Nematerijalna šteta je definisana Zakonom o obligacionim odnosima koji predviđa novčanu i nenovčanu naknadu nematerijalne štete koja se dosuđuje u slučaju povrede prava ličnosti. Zakon o obligacionim odnosima posebno ističe povredu prava ličnosti u čl. 199. kao i u čl. 200. što po mišljenju autora predstavlja mnogo širi pojam koji se ne odnosi samo na fizičku bol, duševnu bol kao i strah, već ovaj termin predstavlja otvorenu kategoriju pod kojom se mogu svrstati i drugi vidovi naknade materijalne štete što omogućava svakom licu kojem je povrijeđeno pravo ličnosti da zahtijeva novčanu ili nenovčanu nanadu štete.

Član 199. Zakona o obligacionim odnosima određuje da u slučaju povrede prava ličnosti sud može odrediti da lice koje je nanijelo štetu objavi presudu, ispravku ili ipak narediti povlačenje izjave koja je izazvala povredu na trošak štetnika, isti član ZOO u dijelu "...ili što drugo čime se može ostvariti svrha koja se postiže naknadom" ostavlja prostora sudu da donese odluku koja će na najbolji način zadovoljiti oštećenu stranu u svakom konkretnom slučaju jer cilj nematerijalne naknade jeste upravo uspostavljanje narušene psihičke ravnoteže oštećenog, a s obzirom na to da je svaka individua specifična i jedinstvena ne može se nikako generalizovati način nenovčane naknade nematerijalne štete što upravo i omogućava ovaj član. ZOO pored nenovčane naknade nematerijalne štete predviđa i novčanu naknadu koja se određuje kao pravična novčana naknada. "Novčana naknada nematerijalne štete nema za svrhu reparaciju onog što je oštećeni izgubio, već da oštećeni za dosuđeni novčani iznos može sebi da pribavi ono zadovoljstvo koje mu na najbolji način omogućava da uspostavi narušenu psihičku ravnotežu." Suštinska razlika između novčane i nenovčane naknade nematerijalne štete jeste u dokazivanju, jer je oštećeni u slučaju kada traži nenovčani oblik naknade štete dužan dokazati samo povredu nekog od prava ličnosti, a u slučaju kada traži novčani oblik naknade štete oštećeni dužan dokazati povredu ličnog dobra ali i dokazati posljedicu koja je proistekla iz te povrede.

Zakon o obligacionim odnosima je taksativno regulisao oblike nematerijalne štete za koje se može dosuditi novčana naknada. Fizički bol i strah su regulisani uopšteno, jer odredbe člana 200. stav 1. Zakona o obligacionim odnosima ne regulišu pojedinačne slučajeve koje uzrokuje fizički bol i strah, za razliku od pravične novčane naknade nematerijalne štete za duševne bolove koja se može dosuditi za taksativno navedene slučajeve. Duševni bolovi su kriterijumi na osnovu kojih sud ceni da li su oni takve jačine i trajanja da predstavljaju osnovu za naknadu nematerijalne štete,a sama nematerijalna šteta je povreda nekog od prava ličnosti (prava na fizički integritete, psihički integritet, zaštitu zdravlja, dostojanstvo, slobodu).

Nematerijalna šteta za pretrpljene duševne bolove može se dosuditi i isplatiti u sledećim slučajevima: zbog umanjenja životnih aktivnosti, zbog naruženosti, povrede ugleda, časti, slobode, smrt bliskog lica, zbog naročito teškog invaliditeta bliskog lica i zbog krivičnih dela protiv dostojanstva ličnosti i morala. Ova vrsta štete regulisana je i drugim zakonima. Na sve ove zakone odnosno pojedine njihove delove, koji se tiču pojedinih slučajeva naknade štete zbog pretrpljenih duševnih bolova primenjuju se odredbe člana 200. stav 1. Zakona o obligacionim odnosima.

VRSTE NEMATERIJALNE ŠTETE

Nematerijalna šteta je definisana kao nanošenje drugome fizičkog ili psihičkog bola ili straha. U teoriji nematerijalna, neimovinska, moralna ili idealna šteta predstavlja štetu na ličnim i neimovinskim dobrima čovjeka gde se kod određenog lica izaziva psihičko uznemiravanje. Mjerilo za razlikovanje materijalne i nematerijalne štete leži u pojmu imovinskog i neimovinskog dobra, gde se pod imovinskim dobrima smatraju sva dobra čija se vrijednost može izraziti u novcu, tj. dobra koja imaju opštu vrijednost.

Nasuprot tome vrijednost neimovinskih dobara se ne može izraziti u novcu jer je njihova vrijednost vezana za lice kojem dobro pripada, dok za ostala lica ono nema nikakvu vrijednost. Oštećenom se novčana naknada zbog nanošenja nematerijalne štete može dosuditi samo u zakonom propisanim uslovima. Prema Zakonu o obligacionim odnosima (čl. 200.), nematerijalna šteta se može zahtijevati u sljedećim slučajevima:

- za pretrpljene fizičke bolove;
- povrede ugleda, časti i dostojanstva;

Povreda ugleda i časti podrazumijeva skup objektivnih i subjektivnih elemenata, koje je potrebno cijeniti u svakoj konkretnoj situaciji. Čast je skup čovjekovih vrlina i mišljenje koje pojedinac ima o sebi samom, a ugled je objektivna kategorija, gdje se za naknadu nematerijalne štete u teoriji i sudskoj praksi BiH podrazumijeva stav i mišljenje, koje ima sredina o ličnosti nekog pojedinca. Dakle, da bi se oštećenom licu priznalo pravo na novčanu satisfakciju zbog navedenog vida nematerijalne štete, potrebno je postojanje uzročno-posledične veze između događaja kojim je šteta izazvana i nastanka nematerijalne štete, kao i uvjerenje suda da je u konkretnom slučaju pravično dosuditi oštećenom licu novčanu satisfakciju.

- povrede slobode ili prava ličnosti;

Naknada štete u slučaju povrede slobode i prava ličnosti jeste jedinstven vid štete gde se obuhvataju sve štetne posledice koje su proistekle iz neosnovanog lišenja slobode a vezane su za ličnost oštećenog. Sud uzima u obzir sve subjektivne i objektivne posljedice prilikom odmeravanja štete, kao što su raniji ugled oštećenog i kasnije posljedice nastale

zbog lišenja slobode a odnose se na ponašanje sredine prema njemu. Činioci koji se još uzimaju u obzir jesu priroda, težina i trajanje psihičkih bolova koji su posljedica lišenja slobode. I ovaj vid naknade nematerijalne štete reguliše član 200. Zakona o obligacionim odnosima koji precizno i taksativno navodi u kojim se slučajevima može tražiti naknada nematerijalne štete, pa između ostalih slučajeva se spominje i povreda slobode što predstavlja osnov za pravo na novčanu satisfakciju licu koje je neosnovano lišeno slobode.

- strah;

Strah jeste emocionalan poremećaj koji ostavlja psihičke posljedice kod oštećenog kao što su narušena psihička ravnoteža i trauma." Bol je prvenstveno tjelesni osjećaj, dok je strah psihičko osjećanje reaktivne prirode. Zbog toga fizički bolovi i strah mogu, ali i ne moraju postojati istovremeno. "Strah se javlja kao primarni i sekundarni. Primarni je neprijatno mučno osjećanje koje postoji neposredno prije, za vrijeme i kratko vrijeme nakon egzistencijalno opasnih situacija, a dijeli se na lak, srednji, jak i veoma jak. Sekundarni je kasnije emocionalno stanje, nakon prolaska egzistencijalne opasnosti i najčešće postoji kod težih povreda, neophodnosti dužeg liječenja i rehabilitacije (Ćirić, 2013)." Kao pravni pojam, strah je jedan od oblika nematerijalne štete koja nastaje kad je ugroženo lično pravo pojedinca (Bikić, 2010)."

Osnovni kriterijum za dosuđivanje naknade jeste pouzdano utvrđenje intenziteta pretrpljenog straha kao i trajanja kao spoljašnjeg elementa koji opravdava dosuđivanje naknade. Dokazna sredstva koja će dokazati postojanje straha jesu najčešće veštačenja ili putem svjedoka. "Naknadu štete može ostvariti ono lice koje trpi strah zbog vlastite opasnosti, ali ne ako je strah izazvan brigom za drugoga, pa makar to bio i bliski srodnik (Krsmanović, 2003)."

OSTVARIVANJE PRAVA I PRIMJER NAKNADE NEMATERIJALNE ŠTETE IZ SUDSKE PRAKSE

Ostvarivanje prava na novčanu naknadu nematerijalne štete zbog povrede časti, ugleda, slobode ili prava ličnosti koju pruža Zakon o obligacionim odnosima predstavlja tekovinu savremenog, demokratskog društva, jer se ovim štite intimna osećanja pojedinca, njegovo pravo da se slobodno kreće, razmišlja, da živi život dostojan čoveka (Petrović i Petrović, 2012).

Prilikom odlučivanja o zahtjevu za naknadu nematerijalne štete sud bi trebalo da vodi računa o važnosti dobra koje je povređeno kao i cilju zbog kojeg postoji naknada. Da bi se kod oštećenog lica uspostavila psihička ravnoteža koja je narušena, dosudiće mu se novčana naknada ali samo u slučajevima kada jačina i trajanje bolova to opravdavaju. Da bi ostvario svoje pravo za naknadom nematerijalne štete, oštećeni inicira postupak tužbom kod nadležnog suda. Naknada nematerijalne štete sastoji se u isplati sume novca, kao satisfakciji za pretrpljenu nematerijalnu štetu, da bi se kod oštećenog uspostavila psihička i emotivna ravnoteža koja je postojala prije štetnog događaja, u mjeri u kojoj je to moguće, a prije svega da bi se uklonile štetne posljedice koje su nastale nad ličnim dobrima oštećenog.

Pravo ličnosti se može povrijediti i objavom informacije u medijima i ako bio istinitost trebala biti temelj novinarstva. Većina novinarskih udzbenika uopće ne definira istinitost jer se o njoj ne raspravlja. Vijest je ili istinita, ili nije vijest.[38] U skladu sa zaštitom koja se časti i ugledu garantuje odredbama Zakona o obligacionim odnosima, u sudskoj praksi je zauzet stav da kada je oštećeni zbog povrede časti i ugleda trpio duševne bolove, sud mu pored sankcije iz člana 199. Zakona o obligacionim odnosima, može dosuditi i pravičnu naknadu kada zbog okolnosti slučaja samo na taj način može dati pravičnu statisfakciju.

U tom smislu je i usvojen tužbeni zahtev zbog povrede ugleda i časti tužiteljice u objavljenom članku koji je potvrdio je odluku da tužiteljica ima pravo da joj se dosudi pravična novčana naknada u određenom iznosu za pretrpljene duševne bolove, s obzirom da je značajan list objavio informacije da je tužiteljica dok je obavljala funkciju vaspitačice u vrtiću zlostavljala dječake tako što ih je zaključavala u kupatilo. Protiv iste je pokrenut disciplinski postupak u kome se dokazalo da nije kriva za navedene optužbe. Direktorica vrtića je poslala listu demant međutim on nikada nije objavljen. U presudi se navodi i da su javna glasila dužna da se staraju da objavljuju istinite i potpune informacije a ne poluistine, sumnje ili neistine. Neistinita informacija koja se objavi u listu je osnov za utvrđivanje naknade nematerijalne štete zbog nanijetog psihičkog bola izazvanog povredom ugleda i dostojanstva istog, također sud je naložio da se presuda objavi u istom listu čime

[38] Skoko, Božo, Bajs, Denis, Objavljivanje neistina i manipuliranje činjenicama u hrvatskim medijima i mogućost zaštite privatnosti časti i ugleda. Politička misao, vol.XLIV (2017), br. 1, str 95

je dosuđena i nenovčana naknada nematerijalne štete, što predstavlja još jedan vid statisfakcije oštećenog lica u ovom slučaju. Kumulacija sankcija je dakle dopuštena kada okolnosti slučaja to dozvoljavaju, što znači da u svakom slučaju treba ocjenjivati da li okolnosti slučaja zaista zahtijevaju kumulaciju.

Iz ovog primjera možemo zaključiti da je iz stava sudske prakse pravo na naknadu nematerijalne štete zbog povrede časti i ugleda osnovano kada je radnjom štetnika teško povređen ugled uštećenog u sredini u kojoj prebiva.

ZAKLJUČNA RAZMATRANJA

Pravo na privatnost predstavlja jedno od osnovnih ljudskih prava, kako međunarodno, tako i ustavno pravo javnopravnog i građanskopravnog značaja, koje djeluje prema svima (erga omnes) i štiti čovjeka od uznemiravanja od strane državne vlasti i drugih ljudi.

Naknada nematerijalne štete je satisfakcija koja se daje oštećenom fizičkom licu za štetu koju je pretrpio na nekom svom nematerijalnom dobru. Naknada može biti izražena u novcu ali postoji i nenovčana naknada nematerijalne štete. Odredbom člana 200. Zakona o obligacionim odnosima priznato je pravo na pravičnu naknadu nematerijalne štete za pretrpljene: fizičke bolove, duševne bolove zbog smanjene životne aktivnosti, naruženosti, povrede ugleda ili časti, povrede polne slobode, zbog smrti ili teškog invaliditeta bliskog lica. Pravo na nenovčano popravljanje nematerijalne štete može biti objavljivanjem presude ili ispravke, ali i javno izvinjenje odnosno javno kajanje zbog učinjene nematerijalne štete nad određenim licem. Iz sudske prakse se može zaključiti da je sud u svakom konkretnom slučaju analizirao intenzitet povrede prava ličnosti ali isto tako i posljedice koje su proizvod te povrede.

Ukoliko je postojala štetna posljedica koja je proistekla iz povrede sud pristupa kumulaciji sankcija, gde je pored novčanog oblika naređuje i izvršenja nenovčanog oblika naknade nematerijalne štete, čime se postiže osnovni cilj nematerijalne štete, uspostavljanje psihičke ravnoteže oštećenog kao i uklanjanje štetnih posljedica koje su nastale radnjama štetnika. Sud posebno mora voditi računa o značaju povređenog dobra i samom cilju kome služi naknada prilikom odlučivanja o zahtijevu za naknadu nematerijalne štete, kao i njenoj visini čime se ne smije voditi težnjama koje nemaju društvenu svrhu niti su spojivi sa prirodom postojanja instituta naknade nematerijalne štete.

U slučaju nastanka nematerijalne štete u nekom od vidova koji su predviđeni zakonom novčana naknada se dosuđuje oštećenom samo u slučaju kada je intenzitet i trajanje bolova ili straha opravdan što će uticati na ponovno uspostavljanje psihičke ravnoteže ili makar približno olakšanje psihičkog stanja oštećenog što se kroz praksu pokazalo kao dijelimično učinkovit metod postizanja cilja postojanja naknade štete, vraćanje u pređašnje stanje.

Inicirajuću postupak kod nadležnog suda oštećeni može ostvariti pravo za naknadom nematerijalne štete tužbom. Tužba za naknadu nematerijalne štete se odlikuje elementom određenosti vida nematerijalne štete, čak i kada je ona proistekla iz istog životnog događaja mora se navesti svaki oblik štete pojedinačno. Poseban problem jest pitanje kriterija po kojima će se odrediti iznos pravične novčane naknade u slučajevima kada osoba zahtijeva pravičnu novčanu naknadu zbog jedne ili više povreda ličnosti. Prema ZOO-a, jedini kriteriji su težina povrede i okolnosti slučaja. Ovakvo pravno uređenje može imati za posljedicu pravnu nesigurnost i nejednakost svih pred zakonom. Problem je aktuelniji, tim što sudovi u BiH, u postupcima povrede prava ličnosti nemaju dovoljno iskustva, niti postoji sudska praksa ni mogućnost Vrhovnog suda da ujednači razlike u procjenama sudova nižeg stepena.

Smatramo da su neophodne stalne aktivnosti na mijenjanju društvene svijesti da se shvati neustavnost i protivpravnost preduzimanja radnji kojima se krše tuđa prava na život, tjelesni integritet, slobodu ili druga prava ličnosti. U tom smislu potrebno je djelovati i na građane kao i na pojedince koje reprezentuju državnu vlast da bi se određene radnje spriječile prije nego što dođe do kršenje tuđih prava i nastajanja štete.

POPIS KORIŠTENE LITERATURA

Knjige i članci

1. Bikić, Abedin.2010. Naknada štete. Sarajevo
2. Bikić, Abedin. 2007. Obligaciono pravo, Sarajevo
3. Baretić, Marko.2006. Povreda prava na slobodu. Zagreb
4. Blagojević, Milan., H a j d a r e v i ć HAJRUDIN., T a j i ć HASO., P i l i p o v i ć Dragan. 2013. Odštetno pravo i pravo osiguranja u sudskoj praksi, Sarajevo
5. Radišić, Jakov, 1985, Obligaciono pravo, Beograd
6. Kalođera, Marko.1941. Naknada neimovinske štete. Zagreb
7. Krsmanović Tomislav.2003. Aktuelna sudska praksa iz građansko-materijalnog prava. Beograd
8. Loza, Bogdan.1985. Obligaciono pravo. Sarajevo
9. Modly D., Korajlić N., 2002, Kriminalistički rječnik, Tešanj
10. Petrović, Zdravko.1996. Naknada nematerijale štete zbog povrede prava ličnosti. Beograd
11. Petrović, Zdravko., Petrović, Nataša.2012. Nadoknada nematerijalne štete. Beograd
12. Bećirović Alić Maida, Ekonomski izazovi, Zb. prav. fak. u Novom Pazaru, godina 7, broj 13, str. 140 -152.
13. Bukovac Puvača Maja, Deset godina nove koncepcije neimovinske štete, Zb. Prav. fak. sveuč. u Rij., 2015, broj 1, str 157 – 180.
14. Radolović Aldo, Pravo osobnosti u novom Zakonu o obveznim odnosima, Zb. Prav. fak. Sveuč. Rij. (1991) v. 27, br. 1, 129-170 (2006.)
15. MAGNUS, U., Comparative Report on the Law of Damages, Unification of Tort Law: Damages, Kluwer Law International, The Hague–London–Boston, 2001., str. 186.
16. Karanikić-Mirić, M., „Odmeravanje naknade štete prema vrednosti koju je ona imala za oštećenika," Crimen 1/2011, 67-87.
17. Misailović, J. (2018). Naknada štete kap posljedica nezakonitog ugovora o radu u pravu velike Britanije i Republike Srbije. Strani Pravni život, 62 (3), 197-211.
18. Obradović Goran, Kovačević-Perić Slobodanka, Novčana naknada nematerijalne štete zbog nezakonitog otkaza, zb. radova Prav fak. u Nišu, br. 67, str. 199-220, 2014.

Pravni akti

19. Ustav Bosne i Hercegovine, Službeni glasnik BiH br.25/09
20. Zakon o obligacionim odnosima, Sl. list SFRJ", br. 29/78, 39/85, 45/89 - odluka USJ i 57/89, "Sl. list RBiH", br. 2/92, 13/93 i 13/94 "Sl. Novine FBiH", br. 29/03 i 42/11

21. "Sl. list SFRJ", br. 29/78, 39/85, 45/89 - odluka USJ i 57/89, "Sl. list SRJ", br. 31/93 i "Sl. list SCG", br. 1/2003 - Ustavna povelja
22. Zakon o zaštiti ličnih podataka, Sl. glasnik BiH, broj: 49/06, 76/11 i 89/11 Presuda Vrhovnog suda Srbije, Rev.41/97

Kriminalističke teme
Zbornik radova
Godina XIX, Broj 5, 2019.
ISSN 1512-5505

STANJE, KRETANJE I NORMATIVNO UREĐENJE RAČUNALNOG KRIMINALITETA U REPUBLICI HRVATSKOJ

STATE, TRENDS AND NORMATIVE REGULATION OF CYBERCRIME IN THE REPUBLIC OF CROATIA

Izvorni naučni rad

dr. sc. Mirjana Kondor-Langer[39]
dr.sc. Krunoslav Borovec[40]
dr. sc. Stjepan Gluščić[41]

SAŽETAK

Inspiracija za rad i problem (i) koji se radom oslovljava (ju): U radu se kroz tri cjeline analiziraju odredbe Kaznenog zakona Republike Hrvatske, podaci o broju prijavljenih i razriješenih kaznenih djela prema službenoj statistici te se analiziraju rezultati provedenog istraživanja o svjesnosti računalnog kriminaliteta.

Ciljevi rada (naučni i/ili društveni): Ciljevi istraživanja nastojali su utvrditi navike mladih vezane za korištenje interneta; ispitati njihovu svijest i iskustva o opasnostima računalnog (*cyber*) kriminaliteta; utvrditi razinu viktimizacije računalnim kriminalitetom te utvrditi postoji li veza između negativnih iskustava na internetu te eventualne viktimizacije s promjenom ponašanja prilikom korištenja interneta.

Metodologija/Dizajn: Istraživanje je provedeno na prigodnom uzorku od 344 ispitanika, studenata veleučilišta i visokih škola u Republici Hrvatskoj. Rezultati dobiveni ovim istraživanjem obrađeni su u statističkom programu SPSS, a u radu su prikazani rezultati deskriptivne statistike, marginalne frekvencije odgovora ispitanika na pojedina pitanja. Radi utvrđivanja postojanja veza između negativnih iskustava na internetu te eventualne viktimizacije s promjenom ponašanja prilikom korištenja interneta korišten je hi-kvadrat test, kao test nezavisnosti dviju varijabli.

Ograničenja istraživanja/rada: ograničenja ovog istraživanja ogledaju se u činjenici da je istraživanjem obuhvaćena specifična skupina mladih (studenti visokih učilišta), čija se ponašanja i iskustva povezana s internetom ne mogu generalizirati na širu populaciju, tako da i dobivene rezultate treba promatrati u kontekstu ovog ograničenja. S druge pak strane, podaci o broju prijavljenih i razriješenih kaznenih djela, prikupljeni iz službenih policijskih statistika, također imaju ograničenje jer se ne odnose na ukupni, već samo registrirani kriminalitet.

Rezultati/Nalazi: Provedeno istraživanje pokazalo je da je 46,8 % ispitanika neprekidno na internetu te da njih 54,9 % svoje informacije na internetu ne doživljava sigurnim, a 18,4 % ispitanika bilo je žrtvom računalnog kriminaliteta.

[39] Visoka policijska škola u Zagrebu, mklanger@fkz.hr
[40] Visoka policijska škola u Zagrebu, kborovec@mup.hr
[41] Visoka policijska škola u Zagrebu, sgluscic@fkz.hr

Generalni zaključak: Podaci pokazuju vrlo visok stupanj uspješnosti u razjašnjavanju prijavljenog kriminaliteta te visok stupanj svjesnosti o opasnostima novih tehnologija ali i relativno neadekvatnu zaštitu.
Opravdanost istraživanja: Računalni kriminalitet u Republici Hrvatskoj je za policiju važno područje. U tom području mogu se postići značajni pomaci upravo jačanjem prevencije i rada sa potencijalnim žrtvama kako bi se stvorilo povjerenje između policije i građana (tamo gdje ne postoji) te kako bi se otklonile zaprjeke za prijavljivanje kaznenih djela i suradnju tijekom istraživanja istih.

KLJUČNE RIJEČI
računalni kriminalitet, kaznena djela, stanje i kretanje kriminaliteta, informacijska sigurnost

ABSTRACT
The inspiration for the paper and the problem (s) that the paper addresses: The first part of the paper gives an analysis of the provisions of the Criminal Code of the Republic of Croatia. Furthermore the paper presents data on the reported and resolved computer crime according to official statistics and the results of the conducted research on computer crime awareness.
The goals of the paper (scientific and/or social): The research goals sought to determine youth habits related to Internet use; examine their awareness and experience of the dangers of cybercrime; determine the level of cybercrime victimization and determine if there is a link between negative experiences on the internet and any possible victimization with behavior change when using the internet.
Methodology/Design: The research sample included a convenience sample of 344 respondents, students of polytechnics and colleges in the Republic of Croatia. The results obtained by this research were analyzed in the SPSS statistical program. The paper presents the results of descriptive statistics and the marginal frequency of respondents' answers to a particular question. Two tests were used to determine whether there are links between negative experiences on the Internet and possible victimization with behavioural change when using the Internet- the chi-square test and the test of the independence of two variables.
Research/the paper limitations: The limitations of this research are reflected in fact that the respondents are only students from Croatian Colleges whose behaviours and experiences related to the use of Internet cannot be generalized to the general population. Therefore, the obtained results should be viewed in the context of these limitations. On the other hand, reported and discovered crimes data were collected from official police database and they do not present total but only registered crime.
Results/findings: The conducted research showed that 46.8% of the respondents were constantly on the Internet. 54.9% of them do not consider their information on the internet to be secure, and 18.4% of the respondents were victims of cybercrime.
General conclusion: The conducted research showed a high level of success in resolving reported crime and a high level of awareness of the dangers of new technologies, but it also drew attention to the inadequate level of cybersecurity.
Research/the paper justifiability: Computer crime in the Republic of Croatia is an important area for the police. Significant progress can be made in this area by strengthening prevention and by working with potential victims. That would create trust between police and citizens (where it does not exist), remove obstacles to reporting crimes and facilitate cooperation during the investigation of those types of crime.

KEY WORDS
cybercrime, computer crime, criminal offenses, crime trends, IT security

1. Uvodne napomene

U ovom radu, koji je suštinski podijeljen u tri cjeline analiziraju se odredbe Kaznenog zakona, podaci o broju prijavljenih i razriješenih kaznenih djela prema službenoj statistici Ministarstva unutarnjih poslova Republike Hrvatske i u trećem dijelu prikazuju se i analiziraju rezultati provedenog istraživanja o svjesnosti računalnog kriminaliteta. Istraživanjem su ispitane navike mladih vezane za korištenje interneta (svijest i iskustva o opasnostima računalnog (*cyber*) kriminaliteta, razina viktimizacije računalnim kriminalitetom te veza između negativnih iskustava na internetu te eventualne viktimizacije s promjenom ponašanja prilikom korištenja interneta), (o problematici pojmovnog određenja ovog područja, vidi više: Dragičević, D. (2004); Vuković, H. (2012).; Kokot, I. (2014)).

Kaznena djela iz područja računalnog kriminaliteta u Republici Hrvatskoj normirana su Kaznenim zakonom (Narodne Novine br. 125/11, 144/12, 56/15, 61/15, 101/17, 118/18; u daljnjem tekstu KZ RH) u Glavi XXV i usko su povezana uz računalnu tehnologiju i internet. Globalna i sveopća dostupnost računalne tehnologije dovodi do povećanja kaznenih djela kod kojih računalo služi kao sredstvo počinjenja kaznenog djela (vidi: Vuletić, I. (2014); Krapac, D. (1992)). Upravo stoga vrlo značajan međunarodni izvor za normiranje računalnog kriminaliteta predstavlja Konvencija o kibernetičkom kriminalu Vijeća Europe[42] i dodatni protokol uz Konvenciju o kibernetičkom kriminalu o inkriminiranju djela rasističke i ksenofobne naravi počinjenih pomoću računalnih sustava.[43]

Tako Vojković i Štambuk-Sunjić (2006:124) navode kako je jedan od ključnih događaja stupanje na snagu Konvencije o kibernetičkom kriminalu kojom se regulira potreba vođenja zajedničke kaznene politike u sferi borbe protiv računalnog kriminala. Republika Hrvatska je ratificirala Konvenciju o kibernetičkom kriminalu te njene odredbe unijela u svoj KZ RH donošenjem Zakona o izmjenama i dopunama Kaznenog zakona (Narodne novine, br. 105/04), a koji je stupio na snagu 1. listopada 2004. godine.

2. Normativno uređenje računalnog kriminaliteta u RH

Normativno uređenje računalnog kriminaliteta u Republici Hrvatskoj može se podijeliti na tri područja. Prva dva čine područja kaznenog i kaznenog procesnog prava (o problematici dokazivanja ovih kaznenih djela kao i korištenju dostignutih tehničkih mogućnosti napisani su brojni radovi; za primjer vidi: Čizmić, J., Boban, M. (2017)). Treće se područje odnosi na posebno zakonodavstvo koje pokriva sigurnosna i organizacijska pitanja kao i pitanje uređenja zaštite specifičnih prava. Tu je niz zakona i podzakonskih akata koja

[42] https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561)
[43] (https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/090000168008160f).

uređuju informacijsku sigurnost kao na primjer: Zakon o informacijskoj sigurnosti (Narodne Novine, br. 79/07), Zakon o provedbi Uredbe (EU) br. 910/2014 Europskog parlamenta i Vijeća od 23. srpnja 2014. o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ (Narodne Novine, br. 62/17), Zakon o elektroničkoj ispravi (Narodne Novine, br. 150/05), Zakon o elektroničkom novcu (Narodne Novine, br. 64/18), Zakon o tajnosti podataka (Narodne Novine, br. 79/07, 86/12), Zakon o provedbi Opće Uredbe o zaštiti podataka (Narodne Novine, br. 42/18), Zakon o pravu na pristup informacijama (Narodne Novine, br. 25/13, 85/15), Zakon o autorskom pravu i srodnim pravima (Narodne Novine, br. 167/03, 79/07, 80/11, 141/13, 127/14, 62/17, 96/18), Zakon o elektroničkoj trgovini (Narodne Novine, br. 173/03, 67/08, 36/09, 130/11, 30/14, 32/19) Zakon o elektroničkom izdavanju računa u javnoj nabavi (Narodne Novine, br. 94/18). O značaju ovog posebnog područja govori i činjenica da je u Strategiji nacionalne sigurnosti Republike Hrvatske posebno poglavlje posvećeno kibernetičkoj sigurnosti. Osnovno stajalište o važnosti ovog područja je: „Razvoj informacijskih i komunikacijskih tehnologija omogućio je procese koji povezuju svijet i olakšavaju život, ali je stvorio i nove prijetnje i rizike. Ovisnost društava i pojedinaca o internetu i informacijskoj tehnologiji predstavljaju posebnu osjetljivost. Napadi u kibernetičkom prostoru, bez obzira na motive, sve više ugrožavaju pojedince, organizacije i države. Istodobno, organizacijska fluidnost, geografska rasprostranjenost, tehnološka difuznost i neograničena mogućnost komunikacije otežavaju identifikaciju napadača, njihovih namjera i sposobnosti. Kibernetički kriminal je u porastu, a kibernetički prostor sve se više koristi za nezakonito djelovanje. Osim moguće povrede sigurnosti klasificiranih, osobnih i osjetljivih podataka, prijetnju predstavlja i korištenje kibernetičkog prostora za izazivanje žrtava i šteta u materijalnom svijetu. Radikalne ideje i pokreti, koji prerastaju u ekstremizam i terorizam, multipliciraju se i šire na internetu i društvenim mrežama, čime poprimaju doseg i utjecaj kakav ranije nisu imali.“ Strategija nacionalne sigurnosti Republike Hrvatske (Narodne novine, br. 73/17).

Distribucija kaznenih djela izvršena je podjelom na: a) kaznena djela kod kojih računalo, odnosno računalni sustavi služe kao sredstvo počinjeno kaznenog djela u odnosu na objekt zaštite; b) kaznena djela kod kojih se štiti poseban interes; c) kaznena djela računalnog kriminaliteta („prava“ kaznena djela računalnog kriminaliteta koja su izdvojena u zasebnu cjelinu; o tome i: Škrtić, D., dostupno na: https://www.fvv.um.si/dv2012/zbornik/informacijska_varnost/skrtic.pdf; Škrtić, D. (2011); Kokot, I. (2014)).

2.1. Kaznena djela kod kojih računalo, odnosno računalni sustavi služe kao sredstvo počinjeno kaznenog djela u odnosu na objekt zaštite

Kod ovih kaznenih djela računalo, odnosno računalni sustavi služe kao sredstvo počinjenja kaznenog djela. To su kaznena djela: Uvrede (čl. 147. KZ RH), Sramoćenja (čl. 148. KZ RH) i Klevete (čl. 149. KZ RH) navedena u Glavi XV: kaznenih djela protiv časti i ugleda.

Zakon predviđa strože kažnjavanje zbog načina počinjenja kaznenih djela kojim je „uvredljiv sadržaj" postao dostupan većem broju osoba.

Zatim javno poticanje na nasilje i mržnju (čl. 325. KZ RH) navedeno u Glavi XXX: kaznenih djela protiv javnog reda i mira. Javno poticanje na nasilje i mržnju uređeno je u KZ RH i zbog potrebe implementacije Okvirne odluke 2008/91/JHA o suzbijanju određenih oblika i načina izražavanja rasizma i ksenofobije putem kaznenog prava od 28. studenog 2008. godine (o nekim pitanjima zlouporabe društvenih mreža vidi: Roksandić Vidlička, S., Mamić, K. (2018)).

U ovu grupu kaznenih djela uvrštavamo i kaznena djela iz Glave XXVII: Kaznena djela zaštite intelektualnog vlasništva, jer prema načinima počinjenja obuhvaćaju i počinjenje pomoću računalnih sustava. To su kaznena djela: Povreda osobnih prava autora ili umjetnika izvođača (čl. 284. KZ RH), Nedozvoljena uporaba autorskog djela ili izvedbe umjetnika izvođača (čl. 285. KZ RH), Povreda drugih autorskom srodnih prava (čl. 286. KZ RH), Povreda prava na izum (čl. 287. KZ RH), Povreda žiga (čl. 288. KZ RH), Povreda registrirane oznake podrijetla (čl. 289. KZ RH). Kaznena djela su usklađena s čl. 10 Konvencije o kibernetičkom kriminalu te ih posebno određuje kao specifična kaznena djela zaštite intelektualnog vlasništva.

2.2. Kaznena djela kod kojih se štiti poseban interes

U ova kaznena djela KZ RH uvrstio je: Iskorištavanje djece za pornografiju (čl. 163. KZ RH), Iskorištavanje djece za pornografske predstave (čl. 164. KZ RH), Upoznavanje djece s pornografijom (čl. 165. KZ RH) i teška kaznena djela spolnog zlostavljanja i iskorištavanja djeteta (čl. 166. KZ RH) iz Glave XVII: kaznena djela spolnog zlostavljanja i iskorištavanja djeteta. Tu su i kaznena djela iz Glave XVIII: kaznena djela protiv braka, obitelji djece i to kazneno djelo povrede privatnosti djeteta (čl. 178. KZ RH).

Kod kaznenog djela opisanog u čl. 163. KZ RH novina je inkriminiranje svjesnog pristupanja putem informacijsko komunikacijskih tehnologija bilo kakvim materijalima pornografskog sadržaja. Dakle nije potrebno da osoba spremi te podatke na svoje računalo – u tom slučaju radilo bi se o posjedovanju, već kazneno djelo postoji i kad osoba samo privremeno pristupa i gleda pornografske materijale. Uz prikazivanje prave djece inkriminira se i realno prikazivanje nepostojeće djece te prikazivanje osoba koje izgledaju mlađe od 18 godina iako to nisu. Uz čl. 9. Konvencije o kibernetičkom kriminalu ovakva ponašanja zabranjuje i čl. 20. Konvencije Vijeća Europe o zaštiti djece od spolnog zlostavljanja i spolnog iskorištavanja[44].

[44] (https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168046e1d1)

Zatim u čl. 164. KZ RH kažnjavaju se aktivnosti kojima se angažiraju djeca za sudjelovanje u pornografskim predstavama, zarađivanje na istima te gledanje pornografskih predstava u skladu sa čl. 21. Konvencije Vijeća Europe o zaštiti djece od seksualnog iskorištavanja i zlostavljanja. Kod kaznenog djela opisanog u čl. 165. KZ RH potrebno je spomenuti da je dobna granica je petnaest godina, a inkriminira se prodaja, poklanjanje, prikazivanje ili javno izlaganje, posredstvom računalnog sustava, mreže ili medija za pohranu računalnih podataka ili na drugi način činjenje pristupačnim spisa, slika, audiovizualnog sadržaja ili drugih predmeta pornografskog sadržaja ili prikazivanje pornografske predstave. Temeljnu, polaznu definiciju pornografije dao je Ustavni sud u svojoj odluci broj U-III-279/1998 od 9. listopada 1998. ali je ona za potrebe članka 165. KZ RH proširena. U odluci Ustavnog suda se navodi: „Tako kao orijentacijske točke mogu poslužiti slijedeće odrednice: namjena pornografije jest zadovoljenje nekog seksualnog interesa, njezin je pojavni oblik eksplicitno pokazivanje nekog seksualnog ponašanja na nizak, uvredljiv ili ponižavajući način, a karakteristično je da je lišena i svake političke, umjetničke ili znanstvene vrijednosti i poruke. Pri tome valja naglasiti stajalište ovog Suda kako karakter, namjena i orijentacija određene tiskovine u načelu ne može predstavljati alibi, odnosno okolnost koja bi ekskulpirala od odgovornosti za promicanje pornografije. Međutim, to onda kada se zaista nedvojbeno radi o pornografiji, odnosno kada je namjera ili postignuti efekt onog što se prikazuje – poticanje seksualnog nagona eksplicitnim pokazivanjem nekog seksualnog ponašanja.“ Odluka Ustavnog suda Republike Hrvatske broj U-III-279/1998 od 9. listopada 1998. (Narodne Novine br. 134/98). Članak 178. KZ RH usklađen je sa čl. 16. Konvencije o pravima djeteta (Narodne novine – Međunarodni ugovori, br. 12/93 i 20/97), koje određuje da dijete ima pravo na zakonsku zaštitu protiv samovoljnog ili nezakonitog miješanja u njegovu privatnost, obitelj, dom ili dopisivanje te nezakonitih napada na njegovu čast i ugled. Zaštita privatnosti odnosi se na svu djecu, a ne samo onu koja su mlađa od 14 godina te napisi u medijima moraju zaštiti identitet, odnosno prikriti identitet djeteta radi neprepoznavanja, "iznošenje ili prenošenje nečega iz osobnog ili obiteljskog života" što se odnosi na činjenične tvrdnje čija se istinitost ili neistinitost ne može dokazivati, uvedeni su i objavljivanje fotografija te otkrivanje identiteta djeteta suprotno propisima. Članak 1. Konvencije o pravima djeteta određuje da je dijete svako ljudske biće mlađe od 18 godina, osim iznimno, punoljetnost ne stječe ranije prema zakonima neke države.

2.3. Kaznena djela računalnog kriminaliteta

Računalni sustav je svaka naprava ili skupina međusobno spojenih ili povezanih naprava, od kojih jedna ili više njih na osnovi programa automatski obrađuju podatke, kao i računalni podaci koji su u njega spremljeni, obrađeni, učitani ili preneseni za svrhe njegovog rada, korištenja, zaštite i održavanja (čl. 87. st. 17. KZ RH). Računalni program je skup računalnih podataka koji su u stanju prouzročiti da računalni sustav izvrši određenu funkciju (čl. 87. st. 19. KZ RH), a računalni podatak je svako iskazivanje činjenica, informacija ili zamisli u obliku prikladnom za obradu u računalnom sustavu. (čl. 87. st. 18. KZ RH).

Ova kaznena djela normirana su u Glavi XXV: Kaznena djela protiv računalnih sustava, programa i podataka. Kaznena djela su: Neovlašteni pristup (čl. 266. KZ RH), Ometanje rada računalnog sustava (čl. 267. KZ RH), Oštećenje računalnih podataka (čl. 268. KZ RH); Neovlašteno presretanje računalnih podataka (čl. 269. KZ RH), Računalno krivotvorenje (čl. 270. KZ RH), Računalna prijevara (čl. 271. KZ RH), Zloporaba naprava (čl. 272. KZ RH) i teška kaznena djela protiv računalnih sustava, programa i podataka (čl. 273. KZ RH).

Kaznena djela su usklađena sa Konvencijom o kibernetičkom kriminalu. Specifičnost njihova počinjenja je da se čine u međunarodno javno dostupnom sustavu računala. Sukladno Konvenciji o kibernetičkom kriminalu postoje četiri grupe kaznenih djela: protiv tajnosti, nepovredivosti i dostupnosti podataka spremljenih na računalima i računalnih sustava; računalne prijevare i krivotvorenje uz pomoć računala; povrede i napadi na sadržaje i podatke na računalima; distribucija i širenje dječje pornografije i kaznena djela povrede autorskih i srodnih prava (usporedi: Pavlović, Š. Kazneni zakon (2013); Pavlović, Š. (2003).; Škrtić, dostupno na: https://www.fvv.um.si/dv2012/zbornik/informacijska_varnost/skrtic.pdf; Škrtić, D. (2011); Kokot, I. (2014)).

2.3.1. Neovlašteni pristup (čl. 266. KZ RH)

Inkriminira se nezakonit pristup tuđem računalnom sustavu, te računalnim podacima. Neovlašteni pristup jest pristup bez odobrenja. Razlog za sankcioniranje neovlaštenog pristupa je taj što je njegova realizacija najčešće preduvjet za činjenje nekog težeg kaznenog djela. Osnovni oblik kaznenog djela progoni se po prijedlogu, a kažnjiv je i pokušaj. Djelo je usklađeno sa čl. 2. Konvencije o kibernetičkom kriminalu. Naime, Zakon o kaznenom postupku Republike Hrvatske (u daljnjem tekstu ZKP RH) propisuje da se kaznena djela mogu progoniti: po prijedlogu; privatnom tužbom i po službenoj dužnosti. Progon po prijedlogu može dati ovlaštena fizička ili pravna osoba, kao i žrtva kaznenog djela. Progon se podnosi državnom odvjetniku, a daljnje postupanje državnog odvjetnika isto je kao i kod kaznenih djela za koje se progon poduzima po službenoj dužnosti. Vidi čl. 47. ZKP RH (NN 152/08, 76/09, 80/11, 91/12 - Odluka i Rješenje USRH, 143/12, 56/13, 145/13, 152/14 i 70/17). Tko s namjerom da počini kazneno djelo poduzme radnju koja prostorno i vremenski neposredno prethodi ostvarenju bića kaznenog djela, kaznit će se za pokušaj ako se za kazneno djelo može izreći kazna zatvora od pet godina ili teža kazna ili zakon izričito propisuje kažnjavanje i za pokušaj (čl. 34. st. 1. KZ RH).

2.3.2. Ometanje rada računalnog sustava (čl. 267. KZ RH)

Inkriminira se ometanje rada računalnog sustava, računalnih podataka ili programa te računalne komunikacije na način da se ovlaštenim korisnicima onemogući nesmetano korištenje njegovih resursa ili međusobna komunikacija. Ne mora ugroziti integritet ili tajnost podataka koji se nalaze unutar sustava. Radnja kaznenog djela čini se prenošenjem, oštećivanjem, brisanjem, kvarenjem, mijenjanjem ili činjenjem neupotrebljivim

računalnih podataka. Kazneno djelo usklađeno je s čl. 5. Konvencije o kibernetičkom kriminalu. Prema dostupnim analizama i podacima o ovom kaznenom djelo može se istaknuti da su počinitelji najčešće profesionalci koji iz različitih motiva ometaju rad računalnih sustava (vidi: Pavlović, Š. (2013); Šimundić, S., Franjić, S., Vdovjak, K. (2012); Bača, M., Ćosić, J. (2013)).

2.3.3. Oštećenje računalnih podataka (čl. 268. KZ RH)

Inkriminiraju se sve one radnje kojima se neovlašteno zadire u cjelovitost računalnih podataka ili programa, pri čemu nije važno je li im počinitelj neposredno pristupio ili je to učinio npr. izradom i prijenosom nekog malicioznog programa. Djelo je usklađeno sa čl. 4. Konvencije o kibernetičkom kriminalu i s čl. 4. Okvirne odluke 2005/222/JHA od 24. veljače 2005. godine (Okvirne odluke 2005/222/JHA od 24. veljače 2005. godine zamijenjena je Direktivom 2013/40/EU Europskog parlamenta i Vijeća od 12. kolovoza 2013. o napadima na informacijske sustave i o zamjeni Okvirne odluke Vijeća 2005/222/PUP, dostupno na:
https://eur-lex.europa.eu/legal-content/HR/TXT/HTML/?uri=LEGISSUM:l33193&from=HR).

2.3.4. Neovlašteno presretanje računalnih podataka (čl. 269. KZ RH)

Inkriminira se neovlašteno presretanje komunikacije prema računalnom sustavu, iz njega ili unutar njega odnosno između udaljenih računalnih sustava, njihovo snimanje, te činjenje takvih podataka dostupnim trećim osobama. Djelo je usklađeno sa čl. 3. Konvencije o kibernetičkom kriminalu. Smisao ove inkriminacije je u zaštiti nejavne komunikacije. Činjenjem ovog kaznenog djela povređuje se ili ugrožava pravo na poštovanje privatnog života, štiti se i pravo na uspostavljanje i razvijanje slobodne komunikacije (o pravu na poštovanje privatnog i obiteljskog života, doma i dopisivanja vidi: Vodič kroz članak 8. Europske konvencije o ljudskim pravima, dostupno na: https://uredzastupnika.gov.hr/UserDocsImages//dokumenti/Edukacija//Vodi%C4%8D%20kroz%20%C4%8Dlanak%208.%20Konvencije.pdf; Turkalj, K., Leppee Pažanin, D. (2018)).

2.3.5. Računalno krivotvorenje (čl. 270. KZ RH)

Inkriminira se krivotvorenje računalnih isprava zbog njihove važnosti u pravnom prometu i poslovanju. Kaznenim djelom pruža se zaštita vjerodostojnosti računalnih podataka u odnosu na sastavljača i sadržaj (vidi: Škrtić, D. dostupno na: https://www.fvv.um.si/dv2012/zbornik/informacijska_varnost/skrtic.pdf; Jelenski, M., Šuperina, M., Budiša, J. (2013); Casey E. Digital evidence and computer crime, Academis Press (2011)). Djelo je usklađeno s čl. 7. i 19. Konvencije o kibernetičkom kriminalu.

2.3.6. Računalna prijevara (čl. 271. KZ RH)

Vuletić i Nedić (2014: 680 i 683) navode da se radnja ovog kaznenog djela sastoji u manipulaciji s računalnim podacima ili programima, pri čemu se djeluje s namjerom stjecanja protupravne imovinske koristi. Ovo kazneno djelo je najučestalije u grupi računalnih kaznenih djela, a počinitelji žrtve su vrlo često iz različitih zemalja.

Postoje dva moguća shvaćanja prijevare. Prva je tzv. izravna računalna prijevara koja se sastoji u obmanjivanju žrtve, a kao sredstvo počinjenja kaznenog djela koristi se računalni sustav. Drugo shvaćanje je tzv. neizravna računalna prijevara koja se sastoji u varanju računalnog sustava. Objekt napada, „žrtva" je sam računalni sustav a onda posljedično i neka pravna ili fizička osoba. Kod ovog počinjenja neće doći do posljedičnog oštećenja neke osoba ako počinitelj prvo ne prevari računalni sustav. Vuletić i Nedić (2014) kao tipičan primjer ove prijevare navode uporabu tuđe bankovne kartice, gdje počinitelj podiže novac na bankomatu varajući računalni sustav a onda posljedično i osobu (fizičku ili pravnu) (vidi i: Sokanović, L., Orlović, A. (2017); Novoselec, P., Bojanić, I. (2007)). Djelo je usklađeno s čl. 8. i 19. Konvencije o kibernetičkom kriminalu.

2.3.7. Zloporaba naprava (čl. 272. KZ RH)

Ovim se djelom propisuje kažnjivost za pripremnu radnju poduzetu radi ostvarivanja nekog od navedenih djela. Radnja kaznenog djela sastoji se prvenstveno u izradi i/ili distribuciji različitih uređaja, računalnih programa ili podataka koji služe počinjenju nekog od kompjutorskih kaznenih djela. Takvi su uređaji za računalno krivotvorenje ili neovlašteno presretanje komunikacije, računalni programi za izradu malicioznih programa i sl. (vidi i: Dragičević, D. (2011)). To su i podaci koji počinitelju mogu poslužiti da ostvari neovlašteni pristup tuđem računalnom sustavu, poput neovlašteno pribavljenih korisničkih imena i lozinki ili pak uputa kako počiniti neko drugo kompjutorsko kazneno djelo. Odgovornost za ovo djelo uvjetuje se postojanjem namjere da se počini neko od navedenih djela kako se zbog posjedovanja takvih naprava ne bi kažnjavalo one koji ih imaju i koriste u legalne svrhe kao npr. u slučaju ovlaštenog ispitivanja ili zaštite računalnog sustava ili izrade efikasnih mjera i sredstava zaštite. „Naprava" se odnosi na bilo koji uređaj, dio ili komponentu vezanu uz računalo te sam računalni program kojim se čini radnja kaznenog djela. Radnja djela može se odnositi i na računalne zaporke, šifre ili druge podatke kojima se može pristupiti računalnim sustavima kako bi se njihovom uporabom počinilo kazneno djelo. Kazneno djelo je usklađeno s čl. 6. Konvencije o kibernetičkom kriminalu.

2.3.8. Teška kaznena djela protiv računalnih sustava, programa i podataka (čl. 273. KZ RH)

Kao teška kaznena djela određena su ona koja se čine putem tiska, radija, televizije, računalnog sustava ili mreže, na javnom skupu ili na da se drugi način javno potiče ili javnosti učini dostupnim letke, slike ili druge materijale kojima se poziva na nasilje ili mržnju

usmjerenu prema skupini ljudi ili pripadniku skupine zbog njihove rasne, vjerske, nacionalne ili etničke pripadnosti, podrijetla, boje kože, spola, spolnog opredjeljenja, rodnog identiteta, invaliditeta ili kakvih drugih osobina. Djelo čini i onaj tko javno odobrava, poriče ili znatno umanjuje kazneno djelo genocida, zločina agresije, zločina protiv čovječnosti ili ratnog zločina, usmjereno prema skupini ljudi ili pripadniku skupine zbog njihove rasne, vjerske, nacionalne ili etničke pripadnosti, podrijetla ili boje kože, na način koji je prikladan potaknuti nasilje ili mržnju protiv takve skupine ili pripadnika te skupine. Pokušaj kaznenog djela je kažnjiv.

3. Statistički pokazatelji stanja prijavljenih i razriješenih pojedinih kaznenih djela računalnog kriminaliteta u Republici Hrvatskoj

U tablici koja slijedi prikazana je prijavljivanost i razriješenost 7 kaznenih djela računalnog kriminaliteta za razdoblje od 2014. do 2018. godine na području Republike Hrvatske. Iz prikazanih podataka vidljivo je kako je u svim promatranim godinama daleko više prijavljivano kazneno djelo Računalne prijevare. U 2014. godine nakon kaznenog djela Računalne prijevare po čestini prijavljivanosti slijedi kazneno djelo Računalnog krivotvorenja, a potom slijedi podjednaka prijavljivanosti kaznenog djela Zlouporabe naprava i Neovlaštenog pristupa. Slični podaci se pronalaze i u 2015. i 2018. godini. U 2017. godini nakon kaznenog djela Računalne prijevare po prijavljivanosti slijedi kazneno djelo Računalnog krivotvorenja, a nakon njih kazneno djelo Ometanje rada računalnog sustava. Za razliku od navedenih godina u 2016. godini, nakon kaznenog djela Računalne prijevare po čestini prijavljivanosti slijedi Zlouporaba naprava i Neovlašteni pristup te tek na četvrtom mjestu Računalno krivotvorenje. Također, iz podataka prikazanih u Tablici 1. vidljiva je relativno visoka razriješenost gotovo svih prijavljenih kaznenih djela. Od prikazanih podataka potrebno je spomenuti kako je kod kaznenog djela Računalnog krivotvorenja u 2015. i 2018. godini zabilježena razriješenost veća od 100% što zapravo ukazuje da su policijskih službenici u tim godinama razriješili i nekoliko kaznenih djela koja su prijavljena u ranijim izvještajnim razdobljima odnosno godinama.

Tablica 1: Statistički pokazatelji prijavljenih i razriješenih pojedinih kaznenih djela računalnog krivotvorenja u Republici Hrvatskoj za razdoblje od 2014. do 2018. godine

Kazneno djelo	2014 Prijavljeno/ razriješeno		2015 Prijavljeno/ razriješeno		2016 Prijavljeno/ razriješeno		2017 Prijavljeno/ razriješeno		2018. Prijavljeno/ razriješeno	
Neovlašteni pristup (čl. 266. KZ RH)	16	13	29	21	115	110	7	5	16	13
	100%	81,2%	100%	72,4%	100%	95,7%	100%	71,4%	100%	81,3%
Ometanje rada računalnog sustava (čl. 267. KZ RH)	1	1	2	2	4	2	11	10	1	1
	100%	100%	100%	100%	100%	50%	100%	90,9%	100%	100%
Oštećenje računalnih podataka (čl. 268. KZ RH)	4	4	7	3	6	2	7	7	-	-
	100%	100%	100%	42,8%	100%	33,3%	100%	100%	0%	0%
Neovlašteno presretanje računalnih podataka (čl. 269. KZ RH)	3	3	5	4	1	1	1	-	-	-
	100%	100%	100%	80%	100%	100%	100%	0%	0%	0%
Računalno krivotvorenje (čl. 270. KZ RH)	169	169	80	82	52	51	37	35	32	39
	100%	100%	100%	102,5%	100%	98,1%	100%	94,6%	100%	121,9%
Računalna prijevara (čl. 271. KZ RH)	960	864	1361	1215	1365	1238	1114	915	1310	1162
	100%	90%	100%	89,3%	100%	90,7%	100%	82,1%	100%	88,7
Zlouporaba naprava (čl. 272. KZ RH)	19	18	69	69	160	157	9	7	17	17
	100%	94,7%	100%	100%	100%	98,1%	100%	77,8%	100%	100%

Izvor: Statistički pregled temeljnih sigurnosnih pokazatelja i rezultata rada u 2018., 2017. i 2015. godini (Ministarstvo unutarnjih poslova, Glavno tajništvo sektor za pravne poslove i strateško planiranje, služba za strateško planiranje, statistiku i unaprjeđenje rada, Statistički pregled temeljnih sigurnosnih pokazatelja i rezultata rada u 2018. godini, dostupno na:https://mup.gov.hr/UserDocsImages/statistika/2019/Pregled%20sigurnosnih%20pokazatelja%20u%202018%20godini/Statisticki%20pregled%202018_web.pdf, str. 56., Ministarstvo unutarnjih poslova, Glavno tajništvo sektor za pravne poslove i strateško planiranje, služba za strateško planiranje, statistiku i unaprjeđenje rada, Statistički pregled temeljnih sigurnosnih pokazatelja i rezultata rada u 2017. godini, dostupno na: https://mup.gov.hr/UserDocsImages/statistika/2018/Travanj/Statisticki%20pregled%202017.pdf, str. 48, Ministarstvo unutarnjih poslova, Glavno tajništvo sektor za pravne poslove i strateško planiranje, služba za strateško planiranje, statistiku i unaprjeđenje rada, Statistički pregled temeljnih sigurnosnih pokazatelja i rezultata rada u 2015. godini, dostupno na: https://mup.gov.hr/UserDocsImages/statistika/2016/Statistika_2015_nova..pdf, str. 42.)

U Tablici 2. prikazan je ukupan broj kaznenih djela i broj prijavljenih kaznenih djela računalnog kriminaliteta za razdoblje od 2014. do 2018. godine u Republici Hrvatskoj. Kaznena djela računalnog kriminaliteta prikazana u Tablici 2. ovog rada podrazumijevaju

prijavljena kaznena djela koja su prikazana u Tablici 1. ovog rada. Ukupan broj kaznenih djela obuhvaća i kaznena djela za koja se progon poduzima po službenoj dužnosti, ali i kaznena djela po privatnoj tužbi i izostanku prijedloga. Kod ukupnog broja kaznenih djela u promatranom razdoblju vidljiv je konstantan pad evidentiranih kaznenih djela. Za razliku od ukupnog broja kaznenih djela kod kaznenih djela računalnog kriminaliteta vidljive su značajne oscilacije u ukupnom broju prijavljenih kaznenih djela prikazanih u Tablici 1.

Naime, u periodu od 2014. do 2016. godine iz godine u godinu zabilježen je porast prijavljenih kaznenih djela računalnog kriminaliteta. U 2017. godine u odnosu na 2016. godinu zabilježen je pad broja prijavljenih kaznenih djela računalnog kriminaliteta za 30,4 % dok je u 2018. godini u odnosu na 2017. godinu zabilježen porast prijavljenih kaznenih djela računalnog kriminaliteta za 16 %.

Ukoliko se u pojedinačnim godinama pogleda udio prijavljenog računalnog kriminaliteta u ukupnom broju kaznenih djela u pojedinoj godini vidljivo je kako je relativno najveći udio računalnog kriminaliteta u ukupnom broju kaznenih djela u 2016. godini (2%), potom slijedi 2018. godina s 1,7 % te 2015. godina s 1,63 %.

To ukazuje na potrebu stalne edukacije korisnika različitih sustava temeljem kojih se čine ova kaznena djela te prevencije i jačanja svijesti. To je jednim dijelom bila i osnova istraživanja čije rezultate prikazujemo u sljedećem poglavlju.

Tablica 2. Ukupan broj kaznenih djela i broj prijavljenih kaznenih djela računalnog kriminaliteta za razdoblje od 2014. do 2018. godine u Republici Hrvatskoj

Godina	2014		2015		2016		2017		2018	
Ukupno k.d.	96877	100%	95037	100%	85620	100%	83047	100%	78922	100%
K. d. računalnog krim.	1172	1,2%	1553	1,63%	1703	2%	1186	1,4%	1376	1,7%

Izvor: Statistički pregled temeljnih sigurnosnih pokazatelja i rezultata rada u 2018., 2017. i 2015. godini (Ministarstvo unutarnjih poslova, Glavno tajništvo sektor za pravne poslove i strateško planiranje, služba za strateško planiranje, statistiku i unaprjeđenje rada, Statistički pregled temeljnih sigurnosnih pokazatelja i rezultata rada u 2018. godini, dostupno na: https://mup.gov.hr/UserDocsImages/statistika/2019/Pregled%20sigurnosnih%20pokazatelja%20u%202018%20godini/Statisticki%20pregled%202018_web.pdf, str. 1., Ministarstvo unutarnjih poslova, Glavno tajništvo sektor za pravne poslove i strateško planiranje, služba za strateško planiranje, statistiku i unaprjeđenje rada, Statistički pregled temeljnih sigurnosnih pokazatelja i rezultata rada u 2017. godini, dostupno na:https://mup.gov.hr/UserDocsImages/statistika/2018/Travanj/Statisticki%20pregled%202017.pdf, str. 1, Ministarstvo unutarnjih poslova, Glavno tajništvo sektor za pravne poslove i strateško planiranje, služba za strateško planiranje, statistiku i unaprjeđenje rada, Statistički pregled temeljnih sigurnosnih pokazatelja i rezultata rada u 2015. godini, dostupno na: https://mup.gov.hr/UserDocsImages/statistika/2016/Statistika_2015_nova..pdf, str. 1)

4. Rezultati istraživanja o svjesnosti računalnog kriminaliteta

4.1. Cilj istraživanja

Ciljevi istraživanja o svjesnosti računalnog (*cyber*) kriminaliteta bili su:

- Utvrditi navike mladih vezane za korištenje interneta;
- Ispitati svijest i iskustva o opasnostima računalnog (cyber) kriminaliteta;
- Utvrditi razinu viktimizacije računalnim kriminalitetom;
- Utvrditi postoji li veza između negativnih iskustava na internetu te eventualne viktimizacije s promjenom ponašanja prilikom korištenja interneta;
- Usporediti statističke podatke o broju prijavljenih i razriješenih kaznenih djela sa rezultatima istraživanja.

4.2. Opis uzorka

Istraživanje je provedeno na uzorku od 344 ispitanika, studenata veleučilišta i visokih škola u Republici Hrvatskoj, a u samoj strukturi uzorka 55,5% ispitanika su muškarci te 44,5% žene. Svi ispitanici bili su stariji od 19 godina, a prosječna dob iznosila je 21,5 godine. Najveći dio ispitanika studenti su preddiplomskih studija (77%), zatim diplomskih studija (21,8%), a 1,2 % integriranih studija. U odnosu na područja u kojima studiraju 47,7% ispitanika studira na visokim učilištima iz područja društvenih znanosti, 30,8% tehničkih znanosti, 8,8% interdisciplinarnih znanosti te preostalih 12,7 % iz ostalih znanstvenih područja. Većina ispitanika (66,9%) su redovni studenti, a jedna trećina (33,1%) izvanredni.

4.3. Anketni upitnik

U ovom istraživanju korišten je anketni upitnik originalno objavljen i javno dostupan kao „Cyber crime awareness Survey“ (https://www.surveymonkey.com/r/WJGH7MH). Međutim, spomenuti upitnik, koji sadrži varijable kojima se ispituje svijest o opasnostima na internetu i negativno iskustvo ispitanika vezano za korištenje interneta, modificiran je i nadopunjen varijablama koje su konstruirali autori ovog istraživanja. Spomenute varijable odnose se na navike korištenja interneta, prijavljivanje policiji kaznenih djela na internetu i poduzimanje određenih radnji (preventivnih ponašanja) u korištenju interneta nakon negativnih iskustava na digitalnim mrežama. Modificirani upitnik sadrži 30 varijabli, uključujući i varijable kojima se ispituju socio-demografska obilježja ispitanika. Skale u upitniku su nominalnog tipa.

Samo ispitivanje studenata veleučilišta i visokih škola provedeno je putem on-line ankete, na način da je upitnik dostavljen njihovim matičnim ustanovama, koje su izvršile distribuciju prema studentima. S obzirom na način odabira uzorka i uvažavajući činjenicu da su u obradu uzeti odgovori onih ispitanika koji su ispunili dostavljeni im upitnik, može se konstatirati kako se radi o prigodnom uzorku.

4.4. Metode obrade rezultata

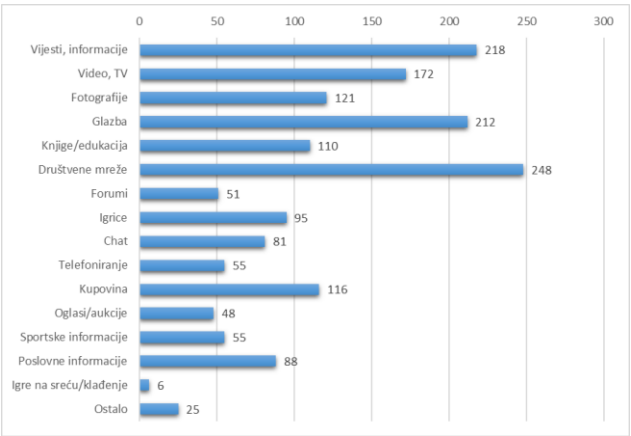
Rezultati dobiveni ovim istraživanjem obrađeni su u statističkom programu SPSS, a u radu su prikazani rezultati deskriptivne statistike, marginalne frekvencije odgovora ispitanika na pojedina pitanje. Radi utvrđivanja postojanja veza između negativnih iskustava na internetu te eventualne viktimizacije s promjenom ponašanja prilikom korištenja interneta korišten je hi-kvadrat test, kao test nezavisnosti dviju varijabli.

4.5. Rezultati istraživanja

Ovim istraživanjem ispitane su prije svega navike ispitanika vezane uz korištenje interneta. Dobiveni rezultati pokazuju da od uređaja koji ispitanici najčešće koriste je mobitel (67,4% ispitanika), zatim računalo (28,2%), dok svega 4,4% na prvome mjestu koristi neki drugi uređaj (televizor, tablet, radio i ostalo). Naravno, sukladno tome, internetu ispitanici najčešće pristupaju putem mobitela, to čini 74,4% njih, zatim putem prijenosnog računala 15,1% i stolnog računala 10,2%. Neznatan broj ispitanika internetu pristupa putem *smart* TV-a ili na druge načine. Također je interesantan podatak da studenti uključeni u istraživanje u 74,4% slučajeva internet najviše upotrebljavaju kod kuće, zatim u 21,8% na fakultetu ili poslu, a zatim 3,8% na javnom mjestu. Trećina ispitanika dnevno provede prosječno 4 sata na internetu, jedna petina više od 6 sati, a po jedna šestina 2 te 6 sati dnevno. Gotovo polovina ispitanika (46,8%) neprekidno je povezana s internetom, 27,6% internet najčešće korist navečer, 18,3% poslije podne, a 7,3 posto prije podne.

U grafikonu 1 prikazani su podaci o tome koje vrste sadržaja/aktivnosti na internetu ispitanike najviše interesiraju (ispitanicu su mogli odabrati više ponuđenih odgovora). Iz podataka je vidljiva najveća zastupljenost korištenja društvenih mreže (koristi ih 72% ispitanika), zatim pregledavanje vijesti i informacija (63% ispitanika), slušanje glazbe (62%), dok primjerice za kupovinu internet koristi 34% ispitanika itd.

Grafikon 1. Vrste sadržaja/aktivnosti na internetu koje ispitanike najviše interesiraju (N=344)

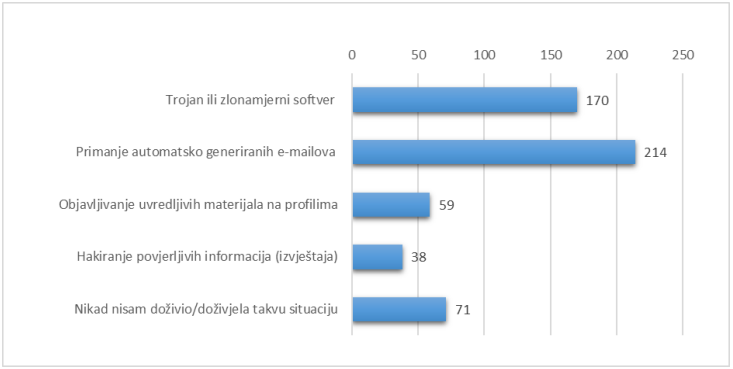


Prema dobivenim podacima velika većina ispitanika na računalu ima instaliran antivirusni program (89,8%), a njih 72,7% ima instaliran i podešen vatrozid (e*ng. Firewall*).

Nakon podataka o navikama ispitanika u vezi s korištenjem interneta, istraživanjem su prikupljeni i podaci o svjesnosti od opasnosti od računalnog kriminaliteta. Na pitanje: Koliko ste svjesni računalnog (*cyber*) kriminaliteta 43 % ispitanika odgovara da su jako dobro svjesni, 43,9 % da zna za to, a 13,1 % da i ne tako dobro. Najviše ispitanika (54,9%) svoje informacije na internetu ne doživljava sigurnima, za razliku od 33,4% njih koji ih doživljavaju sigurnima, a svega 7,8 % vrlo sigurnima, dok ostali nemaju stav o ovom pitanju. Čak 97,4 % ispitanika se slaže s tvrdnjom da je sigurnost na internetu nužna, a 94,4 % da je u vezi informacijske sigurnosti zaštita lozinke važna.

Na grafikonu 2. prikazani su podaci o negativnim iskustvima ispitanika na internetu. Vidljivo je kako je najučestalije primanje automatski generiranih e-mailova (doživjelo 62,2% ispitanika), a zatim trojan ili zlonamjerni softver (49,4% ispitanika). 20,6 % ispitanika nikada nije doživjelo neku od u istraživanju navedenih situacija.

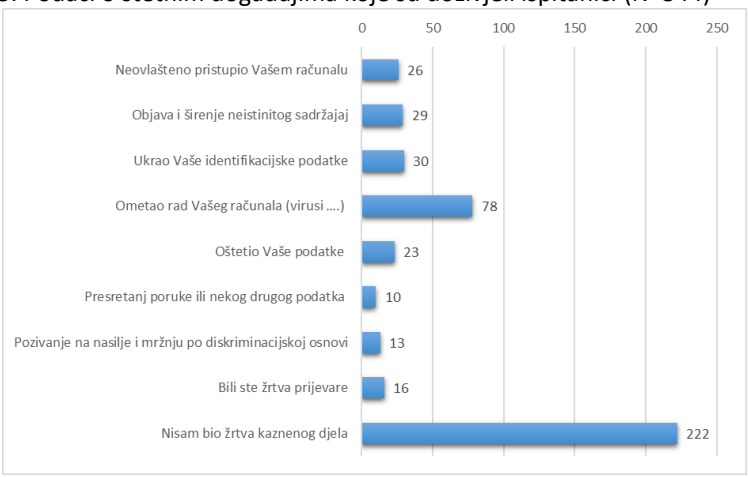
Grafikon 2. Podaci o negativnim iskustvima ispitanika na internetu (N=344)



Jedan od ciljeva istraživanja bio je i istražiti viktimizaciju povezanu s računalnim kriminalitetom te spremnost ispitanika na prijavljivanje kaznenog djela policiji. Podaci govore da od 344 ispitanika njih 18,4% su bili žrtve računalnog kriminaliteta. Ukoliko se ovaj podatak usporedi s ranijim istraživanjima u vezi s viktimizacijom u Hrvatskoj, može se zaključiti da je viktimizacija povezana s računalnim kriminalitetom puno veća nego viktimizacija drugim kaznenim djelima. Od ispitanika koji su bili žrtve kaznenog dijela većina ih je oštećena jedanput (54,6%), a 43,4 % dva ili više puta. Prema rezultatima Nacionalnog istraživanja javnog mnijenja o percepciji sigurnosti građana, postupanju policije te suradnji između policije i lokalne zajednice (GfK Croatia, 2009) dobivena je razina viktimizacije za pojedina kaznena dijela. Pa tako 3% ispitanika doživjelo je da im netko nasilno ili uz prijetnju nasilja nešto oteo ili pokušao oteti, 4 % da su bili žrtva krađe, 5% da su doživjeli provalu ili pokušaj provale u stan /kuću, 10 % da su bili prevareni, 7 % da su bili napadnuti ili im je netko prijetio napadom. U ovom istraživanju nije istraživana viktimizacija povezana s računalnim kriminalitetom.

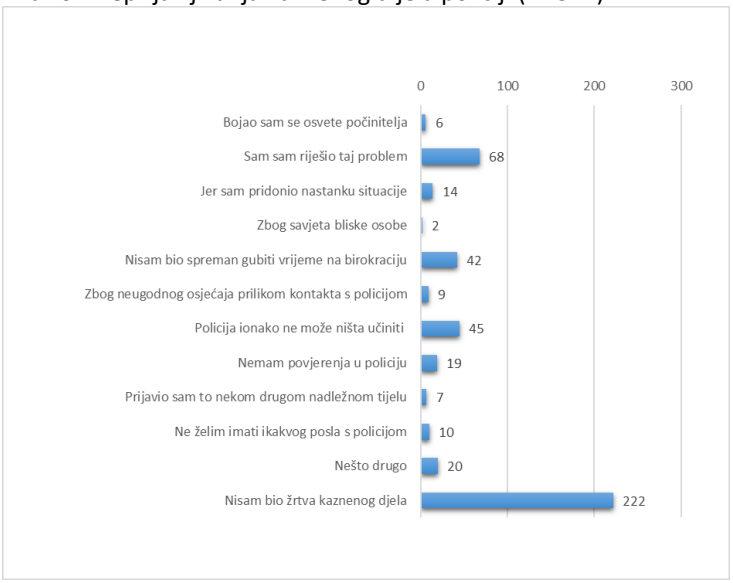
U grafikonu 3. prikazani su podaci o tome koje su štetne događaje doživjeli ispitanici iz ovog istraživanja. Iz podataka je razvidno da se štetni događaji najčešće odnose na ometanje rada računala putem zlonamjernih softvera (virusa), zatim krađu osobnih podataka, objavu i širenje neistinitih i štetnih sadržaja te neovlašteni pristup računalu. U 42,8 % slučajeva ispitanici oštećeni kaznenim dijelom računalnog kriminaliteta zna tko je počinitelj. Međutim, svega ih je 17% prijavilo to kazneno djelo.

Grafikon 3. Podaci o štetnim događajima koje su doživjeli ispitanici (N=344)



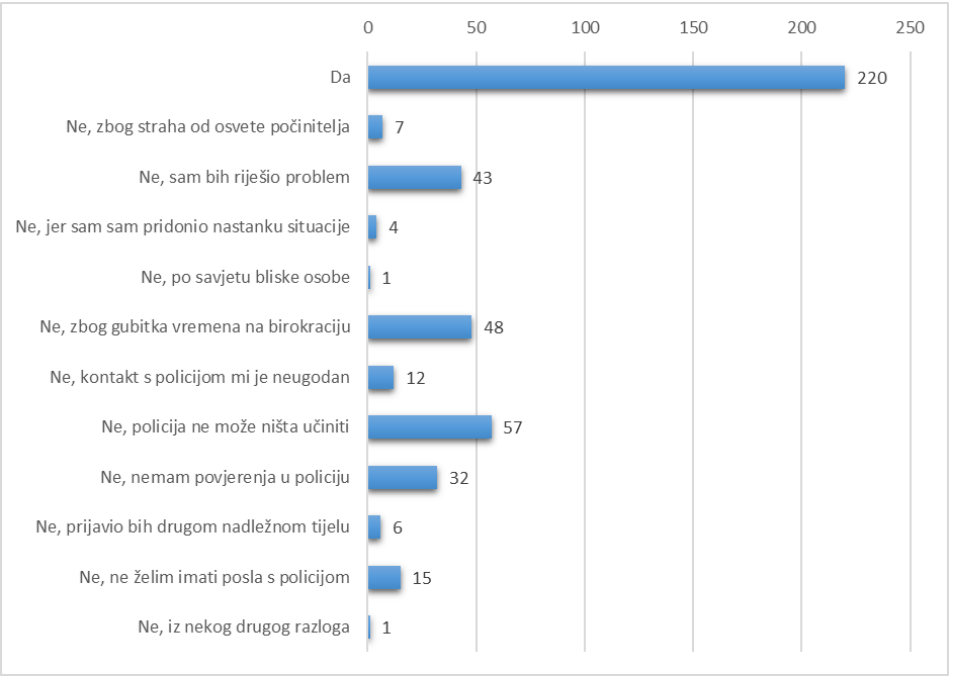
U grafikonu 4. prikazani su podaci o razlozima zbog kojih oštećeni ispitanici nisu prijavili kazneno djelo. Najčešće navedeni razlog je to što su ispitanici sami riješili taj problem, zatim nisu bili spremani gubiti vrijeme na birokraciju ili su smatrali da policija ionako ne može ništa učiniti (nemoćna je kod rješavanja takvog slučaja).

Grafikon 4. Razlozi neprijavljivanja kaznenog dijela policiji (N=344)



Za razliku od prethodnog pitanje u kojem je provjeravana reakcija na počinjeno kazneno djelo, u slijedećem pitanju napravljena je procjena spremnosti prijavljivanja računalnog kriminaliteta među svim ispitanicima, bez obzira na prethodno iskustvo (grafikon 5.).

Grafikon 5. Spremnost prijavljivanja računalnog kriminaliteta policiji (N=344)



Rezultati pokazuju da bi 64% ispitanika prijavilo djelo policiji, a od onih koji to ne bi učinili najviše je onih koji smatraju da policija ne može ništa učiniti (17%), zatim onih koji ne žele gubiti vrijeme na birokraciju (14%) ili koji bi sami riješili problem (13%).

Dobar pokazatelj viktimizacije putem računalnog kriminaliteta je i prouzročena materijalna šteta, tako da se jedna od varijabli u upitniku odnosila i na pitanje gubitka novca zbog ove vrste kriminaliteta. Prema dobivenim podacima 14,2% ispitanika pretrpjelo je materijalnu štetu. Međutim, na pitanje jesu li zbog toga prestali kupovati preko interneta većina ispitanika (60,2%) odgovara da kao mjeru koristi kupovinu isključivo preko provjerenih internetskih stranica, dok je 4,9% ispitanika donekle prestalo kupovati preko interneta.

Generalno gledajući, vezano uz sve probleme povezane s računalnim krminalitetom s kojima se ispitanici susreću na internetu, relativno je mali broj onih koji nisu ništa poduzeli (7,8%). Najviše je onih koji su prestali posjećivati nesigurne stranice (29,1%), zatim, onih koji su instalirali dodatnu zaštitu na svoj uređaj (21,2%), a mali broj onih koji su ugasili svoj račun na društvenoj mreži (6,3%).

Mišljenja ispitanika podijeljena su u oko tvrdnje da zakoni koji su na snazi mogu kontrolirati počinitelje računalnog kriminaliteta. Njih 60,8% ne slaže se s tom tvrdnjom,

24,4% ima neutralan stav (niti se slažu, niti se ne slažu), a svega 14,8% ispitanika ima pozitivno mišljenje, odnosno misli da su zakoni u tom smislu dobri.

Radi ispitivanja **povezanosti korištenja antivirusnog programa i doživljavanja kaznenog djela počinjenog preko računala**, korišten je hi-kvadrat test za dva nezavisna uzorka. Hi-kvadrat test nezavisnosti nije pokazao značajnu povezanost između posjedovanja antivirusnog programa na svom računalu i bivanja žrtvom kaznenog djela počinjenog preko računala, χ^2 (1, n=344)= 0.205, p=0,651). Jednako tako hi-kvadrat test nezavisnosti nije pokazao značajnu povezanost između posjedovanja vatrozida (*eng: firewall*) na svom računalu i bivanja žrtvom kaznenog djela počinjenog preko računala, χ^2 (2, n=344)= 2.453, p=0,293). Ovakav rezultat uvjetovan je činjenicom da velika većina ispitanika ima instaliran ili jedan ili oba oblika zaštite na svojim računalima, tako da se i nije mogla utvrditi statistički značajna razlika u odnosu na relativno mali broj onih koji ne koriste antivirusni program i/ili vartozid i bili su viktimizirani.

Jedan od ciljeva ovog istraživanja bio je i utvrditi postoji li veza između negativnih iskustava na internetu te eventualne viktimizacije putem računalne mreže s promjenom ponašanja prilikom korištenja interneta. Takva povezanost, na razini statističke značajnosti je potvrđena. Ovaj podatak pokazuje također razinu svijesti o opasnostima računalnog kriminaliteta te spremnost ispitanika na promjenu ponašanja radi smanjenja rizika i prevencije budućih kaznenih djela. U nastavku rada prikazana je povezanost **bivanja žrtvom kaznenog djela počinjenog preko računala i promjene ponašanja na internetu** utvrđena korištenjem hi-kvadrat test za dva nezavisna uzorka. Hi-kvadrat test nezavisnosti pokazuje značajnu povezanost **bivanja žrtvom kaznenog djela počinjenog preko računala i promjene ponašanja na internetu u pogledu**:

- **prestanka posjećivanja nesigurnih stranica**, χ^2 (1, n=344)= 14,180, p<0,01). Utvrđena je niska do srednje visoka veličina učinka Φ (Fi) =0,21, p<0.01.
- **prestanka spajanja na internet preko nesigurne mreže**, χ^2 (1, n=344)= 6,041, p=0,014). Utvrđena je niska veličina učinka Φ (Fi) =0,14, p<0.01.
- **brisanja računa na društvenim mrežama**, χ^2 (1, n=344)= 7,065, p=0,003). Utvrđena je niska veličina učinka Φ (Fi) =0,159, p<0.01.
- **instaliranja dodatne zaštite za svoj uređaj**, χ^2 (1, n=344)= 14,940, p<0,01). Utvrđena je niska do srednje visoka veličina učinka Φ (Fi) =0, 218, p<0.01.
- **poduzimanja nečega drugog zbog sigurnosti na internetu**, χ^2 (1, n=344)= 24,100, p<0,01). Utvrđena je srednje visoka veličina učinka Φ (Fi) =0, 275, p<0.01.

Dobiveni rezultati potvrđuju da je negativno iskustvo na internetu i viktimizacija putem računalne mreže povezana s promjenama ponašanja korisnika i njihovim navikama u daljnjem korištenju interneta.

5. Zaključak

U samom zaključku ističemo nekoliko utvrđenih činjenica, a odnose se na stalno povećanje broja počinjenih kaznenih djela računalnog kriminaliteta, što je usko vezano uz načine obavljanja svakodnevnih ali i poslovnih aktivnosti. Nadalje, vidljiv je visoki postotak razjašnjenosti prijavljenih kaznenih djela, što je u suprotnosti s rezultatima ispitivanja gdje ispitanici iskazuju da iz različitih razloga ne bi prijavili kazneno djelo policiji. Nadalje, može se zaključiti da postoji tzv. tamna broja kriminaliteta te da se upravo ta „tamna broja“ kriminaliteta dovodi u vezu s padom ukupno prijavljenog kriminaliteta.

Za policiju je svakako važno područje u kojem se mogu postići značajni pomaci upravo jačanje prevencije i rada s potencijalnim žrtvama kako bi se stvorilo povjerenje između policije i građana (tamo gdje ne postoji) te otklonile zaprjeke za prijavljivanje kaznenih djela i suradnju tijekom istraživanja istih jer kako podaci pokazuju stupanj uspješnosti u razjašnjavanju prijavljenog kriminaliteta je vrlo visok, kao što je visok stupanj svjesnosti o opasnostima novih tehnologija ali relativno neadekvatna zaštita.

LITERATURA:

1. Bača, M., Ćosić, J. (2013). Prevencija računalnog kriminaliteta, Policija i sigurnost, 22/1, str. 146. – 158.
2. Casey E.: Digital evidence and computer crime, Academis Press, 2011.
3. Cyber crime awareness Survey, dostupno na: https://www.surveymonkey.com/r/WJGH7MH
4. Čizmić, J., Boban, M. (2017). Elektronički dokazi u sudskom postupku i računalna forenzička analiza, Zbornik Pravnog fakulteta u Rijeci, 38/1., str. 23. – 50.
5. Direktiva 2013/40/EU Europskog parlamenta i Vijeća od 12. kolovoza 2013. o napadima na informacijske sustave i o zamjeni Okvirne odluke Vijeća 2005/222/PUP, dostupno na: https://eur-lex.europa.eu/legal-content/HR/TXT/HTML/?uri=LEGISSUM:l33193&from=HR, pristupljeno 26.07.2019.
6. Dodatni protokol uz Konvenciju o kibernetičkom kriminalu o inkriminiranju djela rasističke i ksenofobne naravi počinjenih pomoću računalnih sustava, dostupno na: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/090000168008160f, pristupljeno 01.08.2019.
7. Dragičević, D. Kompjuterski kriminalitet i informacijski sustavi, IBS, Zagreb, 2004.
8. Jelenski, M., Šuperina, M., Budiša, J. (2013). Kriminalitet platnim karticama (krađa identiteta, krivotvorenje i zlouporaba platne kartice), Policija i sigurnost, 22/3, str. 372. – 395.
9. Kazneni zakon Republike Hrvatske, Narodne Novine, br. 125/11, 144/12, 56/15, 61/15, 101/17, 118/18.
10. Kokot I. (2014). Kaznenopravna zaštita računalnih sustava, programa i podataka, Zagrebačka pravna revija, 3/3. str. 303. – 330.
11. Konvencija o kibernetičkom kriminalu Vijeća Europe, dostupno na: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561, pristupljeno 01.08.2019.
12. Konvencije o pravima djeteta, Narodne novine – Međunarodni ugovori, br. 12/93 i 20/97.
13. Konvencije Vijeća Europe o zaštiti djece od spolnog zlostavljanja i spolnog iskorištavanja, https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168046e1d1., pristupljeno: 26.07.2019.
14. Krapac, D. Kompjutorski kriminalitet: pregled glavnih pitanja krivičnopravne zaštite društvenih vrijednosti u postupcima elektronske obrade podataka, Pravni fakultet, Zagreb, 1992.
15. Ministarstvo unutarnjih poslova, Glavno tajništvo sektor za pravne poslove i strateško planiranje, služba za strateško planiranje, statistiku i unaprjeđenje rada, Statistički pregled temeljnih sigurnosnih pokazatelja i rezultata rada u 2018. godini, dostupno na:

https://mup.gov.hr/UserDocsImages/statistika/2019/Pregled%20sigurnosnih%20pokazatelja%20u%202018%20godini/Statisticki%20pregled%202018_web.pdf.

16. Ministarstvo unutarnjih poslova, Glavno tajništvo sektor za pravne poslove i strateško planiranje, služba za strateško planiranje, statistiku i unaprjeđenje rada, Statistički pregled temeljnih sigurnosnih pokazatelja i rezultata rada u 2017. godini, dostupno na: https://mup.gov.hr/UserDocsImages/statistika/2018/Travanj/Statisticki%20pregled%202017.pdf.
17. Ministarstvo unutarnjih poslova, Glavno tajništvo sektor za pravne poslove i strateško planiranje, služba za strateško planiranje, statistiku i unaprjeđenje rada, Statistički pregled temeljnih sigurnosnih pokazatelja i rezultata rada u 2015. godini, dostupno na: https://mup.gov.hr/UserDocsImages/statistika/2016/Statistika_2015_nova..pdf.
18. Nacionalno istraživanje javnog mnijenja o percepciji sigurnosti građana, postupanju policije te suradnji između policije i lokalne zajednice, GfK, Croatia, 2009, http://www.seesac.org/f/docs/SALW-Surveys/On-Citizen-Perception-of-Safety-and-Security-in-the-Republic-of-Croatia-BCMS.pdf, pristupljeno 30.07.2019.
19. Novoselec, P., Bojanić, I. Posebni dio kaznenog prava, Pravni fakultet Sveučilišta u Zagrebu, Zagreb, 2007.
20. Odluka Ustavnog suda Republike Hrvatske broj U-III-279/1998 od 9. listopada 1998, Narodne Novine br. 134/98.
21. Okvirna odluka 2008/91/JHA o suzbijanju određenih oblika i načina izražavanja rasizma i ksenofobije putem kaznenog prava od 28. studenog 2008. godine.
22. Pavlović, Š. Kazneni zakon, Libertin naklada, Rijeka, 2013.
23. Pavlović, Š. (2003). Kompjuterska kaznena djela u Kaznenom zakoniku – Osnove hrvatskog informacijskog kaznenog prava, Hrvatski ljetopis za kazneno pravo i praksu, 10/2, str. 625. – 664.
24. Roksandić Vidlička, S., Mamić, K. (2018). Zlouporaba društvenih mreža u javnom poticanju na nasilje i mržnju i širenju lažnih vijesti: potreba transplantiranja njemačkog zakona o jačanju provedbe zakona na društvenim mrežama?, Hrvatski ljetopis za kazneno pravo i praksu, 25/2, str. 329. – 357.
25. Sokanović, L., Orlović, A. (2017). Oblici prijevara u Kaznenom zakonu, Hrvatski ljetopis za kazneno znanosti i praksu, 24/2, str. 583. – 615.
26. Strategija nacionalne sigurnosti Republike Hrvatske, Narodne novine, br. 73/17.
27. Šimundić, S., Franjić, S., Vdovjak, K. (2012). HOAX, Zbornik radova Pravnog fakulteta u Splitu, 49/3, str. 459. – 480.
28. Škrtić, D. Kaznena djela računalnog kriminaliteta u novom Kaznenom zakonu RH, dostupno na: https://www.fvv.um.si/dv2012/zbornik/informacijska_varnost/skrtic.pdf, posjećeno 26.07.2019.
29. Škrtić, D. Kazneno pravna zaštita informatičkih sadržaja, Doktorska disertacija Sveučilište u Zagrebu, Pravni fakultet, 2011.

30. Turkalj, K., Leppee Pažanin, D. (2018). Izazovi pravnog uređenja zadržavanja podataka elektroničke komunikacije u svjetlu nedavne prakse suda EU-a, Godišnjak Akademije pravnih znanosti Hrvatske, IX/1, str. 141. – 173.
31. Vodič kroz članak 8. Europske konvencije o ljudskim pravima, dostupno na: https://uredzastupnika.gov.hr/UserDocsImages//dokumenti/Edukacija//Vodi%C4%8D%20kroz%20%C4%8Dlanak%208.%20Konvencije.pdf, pristupljeno 26.07.2019.
32. Vojković G., Štambuk-Sunjić M. (2006). Konvencija o Kibernetičkom kriminalu i Kazneni zakon republike Hrvatske, Zbornik radova Pravnog fakulteta u Splitu, str. 123 – 136.
33. Vuković, H. (2012). Kibernetska sigurnost i sustav borbe protiv kibernetskih prijetnji u Republici Hrvatskoj; Nacional security and the future, 13/3, str. 12.-31.
34. Vuletić, I. (2014). Primjenjivost tradicionalnih kaznenopravnih koncepata na računalni kriminal, Zbornik Pravnog fakulteta u Zagrebu, 64/5-6, str. 895. – 909.
35. Vuletić, I., Nedić, T. (2014). Računalna prijevara u hrvatskom kaznenom pravu, Zbornik Pravnog fakulteta u Rijeci, 35/2, str. 679. – 692.
36. Zakon o autorskom pravu i srodnim pravima, Narodne Novine br. 167/03, 79/07, 80/11, 141/13, 127/14, 62/17, 96/18.
37. Zakon o elektroničkoj ispravi, Narodne Novine, br.150/05.
38. Zakon o elektroničkom izdavanju računa u javnoj nabavi, Narodne Novine, br. 94/18.
39. Zakon o elektroničkom novcu, Narodne Novine, br. 64/18.
40. Zakon o elektroničkoj trgovini, Narodne Novine, br. 173/03, 67/08, 36/09, 130/11, 30/14, 32/19.
41. Zakon o informacijskoj sigurnosti, Narodne Novine, br. 79/07.
42. Zakona o izmjenama i dopunama Kaznenog zakona, Narodne novine, br. 105/04.
43. Zakon o kaznenom postupku Republike Hrvatske, Narodne Novine, br. 152/08, 76/09, 80/11, 91/12 - Odluka i Rješenje USRH, 143/12, 56/13, 145/13, 152/14 i 70/17.
44. Zakon o provedbi Opće Uredbe o zaštiti podataka, Narodne Novine br. 42/18.
45. Zakon o pravu na pristup informacijama, Narodne Novine br. 25/13, 85/15.
46. Zakon o tajnosti podataka, Narodne Novine br. 79/07, 86/12.
47. Zakon o provedbi Uredbe (EU) br. 910/2014 Europskog parlamenta i Vijeća od 23. srpnja 2014. o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ, Narodne Novine, br. 62/17.

Kriminalističke teme
Zbornik radova
Godina XIX, Broj 5, 2019.
ISSN 1512-5505

KRIMINALISTIČKI I KRIVIČNOPROCESNI ASPEKTI OTKRIVANJA, RAZJAŠNJAVANJA I DOKAZIVANJA KRIVIČNIH DJELA VISOKOTEHNOLOŠKOG KRIMINALITETA

CRIME AND CRIMINAL PROCESSES, ASPECTS OF DETECTION, EXPLOITATION AND EVIDENCE OF HIGHER-TECHNICAL CRIMINALITY

Stručni rad

Mile Matijević[45]
Adnan Pirić[46]

SAŽETAK

Inspiracija za rad i problem (i) koji se radom oslovljava (ju): Posmatrano sa aspekta vremena kojem pripadamo, a u vremenu koje je pred nama visokotehnološki kriminalitet svakim danom je sve izraženiji, i jedan je od najopasnijih vidova kriminaliteta uopšte. Mnoštvo je razloga koji govore u prilog ovako visokom stepenu društvene opasnosti. Među njima poseban značaj imaju sljedeći: svakim danom njegova sve veća prisutnost, i to i u najosjetljivijim institucijama društva kao cjeline; posljedice koje za sobom povlači; njegov međunarodni karakter; njegova povezanost sa najtežim oblicima kriminaliteta (slučaj prije svega sa organizovanim kriminalitetom i terorizmom gdje on postaje ne samo moćna poluga njihovog planiranja već i ključno sredstvo izvršenja); otežan način otkrivanja razjašnjavanja i dokazivanja.

Ciljevi rada (naučni i/ili društveni): Kriminalističko istraživanje je operativnog karaktera, koje se često povezuje sa iskustvom kriminalističkog istražitelja, vrlo malo i nimalo pažnje se posvećuje stručnom i naučnom proučavanju krivičnih djela uopšte, a posebno krivičnih djela visokotehnološkog kriminaliteta. Navedena percepcija navodi na zaključak da su pomenuta krivična djela oblast kriminaliteta koja je veoma kompleksna za otkrivanje, razjašnjavanje i dokazivanje. Generalni cilj kriminalistike kao nauke je da na temelju konkretnih radnji pojedinih krivičnih djela nastoji stvarati modele i temelje za uspješno otkrivanje, razjašnjavanje i dokazivanje istih. Teorijska podloga, koju postavlja predmetno istraživanje, treba da posluži unapređenju otkrivačke djelatnosti nadležnih organa kada su u pitanju ova krivična djela. Na temelju navedenih saznanja uspostavit će se interakcija kriminalističke i krivično procesne istražne djelatnosti što u konačnici treba doprinijeti efikasnijem otkrivanju, razjašnjavanju i dokazivanju krivičnih djela visokotehnološkog kriminaliteta, a posebno kroz jačanje naučnog i stručnog pristupa u suzbijanju kriminaliteta uopšte.

Metodologija/Dizajn: Prilikom pisanja ovog rada korištene su relevantne naučno istraživačke metode i tehnike, koje mogu dati najkvalitetnije rezultate u oblasti

[45] Redovni profesor Fakulteta pravnih nauka Univerziteta za poslovne studije Banja Luka. E.mail; matijevicdrmile@gmail.com, mile.m@univerzitetps.com.
[46] Docent Pravnog fakulteta Sveučilišta/Univerziteta „Vitez" Vitez. E.mail;adnan.piric@unvi.edu.ba, piricadnan@gmail.com.

istraživanja relevantnosti i efikasnosti kriminalističkih i krivično procesnih radnji u otkrivanju kriminogenih pojava, sa posebnim naglaskom na krivična djela visokotehnološkog kriminaliteta. Isto tako, nastojat će se afirmisati istraživanja koja su značajna u cilju mjerenja kvaliteta i efikasnosti istrage pomenutih krivičnih djela.

Ograničenja istraživanja/rada: Rad predstavlja dio šire naučno stručne aktivnosti sa ciljem afirmacije i primjene savremenih kriminalističkih i krivičnoprocesnih metoda, koje mogu doprinjeti efikasnijem otkrivanju, razjašnjavanju i dokazivanju krivičnih djela visokotehnološkog kriminaliteta.

Rezultati/Nalazi: Izlaganja koja će biti predstavljena u ovom radu su rezultat sistematičnog rada koji se odnosi na analiziranje uspješnosti pravosudnog sektora, kada je u pitanju otkrivanje, razjašnjavanje i dokazivanje krivičnih djela visokotehnološkog kriminaliteta.

Generalni zaključak: Izloženi zaključci predstavljaju iscrpnu sliku i identifikaciju eventualnih problema koji mogu biti od značaja za otkrivanje, razjašnjavanje i dokazivanje istih.

Opravdanost istraživanja/rada: Rezultati znanstvenih istraživanja predočeni u ovom radu daju značajan doprinos pravnim i kriminalističkim znanostima u teorijskom i u aplikativnom smislu.

Ključne riječi

kriminalistika, krivičnoprocesno pravo, otkrivanje, dokazivanje, visokotehnološki kriminal.

ABSTRACT

Reason for writing and research problem (s): Observed from the aspect of the time to which we belong, and in the time that high-tech crime is facing us every day, it is more pronounced, and it is one of the most dangerous types of crime in general. There are many reasons for supporting this high degree of social danger. Of particular importance to them is the following: every day, his growing presence, even in the most sensitive institutions of society as a whole; the consequences that it entails; its international character; its connection with the most difficult forms of crime (the case of organized crime and terrorism, where it is not only the powerful lever of their planning, but also the key means of execution); difficulty in discovering clarification and proof.

Aims of the paper (scientific and/or social): Criminal investigation is of operational character, which is often associated with the experience of a criminal investigator, very little attention is paid to professional and scientific investigation of criminal offenses in general, especially criminal offenses of high-tech criminality. This perception suggests that the crimes mentioned above are criminal areas that are very complex for detection, clarification and proofing. The general aim of criminology as a science is to try to create models and foundations for successful detection, clarification and proofing based on concrete actions of certain criminal offenses. The theoretical basis, set by the subject research, should serve to improve the detective activities of the competent authorities in the area of these crimes. On the basis of the aforementioned findings, the interaction between criminal and criminal process investigation activities will be established, which ultimately should contribute to more efficient detection, clarification and demonstration of criminal offenses of high-tech criminality, and in particular through the strengthening of scientific and professional approach in combating crime in general.

Methodology/Design: During the research, relevant scientific research methods and techniques will be used, which can provide the highest quality results in the field of investigation of the relevance and efficiency of criminal and criminal procedural actions in the detection of criminal phenomena, with special emphasis on crimes of high-tech criminality. In addition, efforts will be made to promote research that is significant in order to measure the quality and effectiveness of the investigation of the above-mentioned crimes.
Research/Paper limitation: The work is part of a wider scientific-professional activity aimed at affirmation and application of modern criminal and criminal procedural methods, which can contribute to more efficient detection, clarification and proving of criminal acts of high-tech criminality.
Results/Findings: The presentations that will be presented in this paper are the result of a systematic work related to the analysis of the success of the judicial sector in the area of detection, clarification and proving of criminal offenses of high-tech criminality.
General Conclusion: The presented conclusions represent an exhaustive picture of concrete cases individually, identification of possible problems that may be of importance for the detection, clarification and proof of the same.
Research/Paper Validity: The results of the scientific research presented in this paper give a significant contribution to the legal sciences in theoretical and applicative sense.

Keywords
criminalistics, criminal procedural law, detection, proof, high-tech crime

UVOD

Naslov rada, „Kriminalistički i krivično procesni aspekti otkrivanja, razjašnjavanja i dokazivanja krivičnih djela visokotehnološkog kriminala“, je kao takav vrlo složen i zahtjevan. Pisanja i istraživanja mnogih autora u posljednjih nekoliko godina, iako sa raznovrsnim metodologijama i ciljevima, složna su u konstataciji; da krivična djela visokotehnološkog kriminaliteta opterećuju cjelokupnu društvenu zajednicu i negativno utiču na društveni napredak. Međutim, postavlja se pitanje, šta učiniti kako bi se navedena problematika reducirala? U ovim nastojanjima, pored ostalih, najvažniju ulogu imaju policija, tužilaštvo i sudstvo, kao agenti državne prisile. Analiziranje osnovnih pojmova nastanka krivičnih djela visokotehnološkog kriminaliteta, a potom otkrivanja, razjašnjavanja i dokazivanja istih uz pomoć teorijskih i praktičnih doprinosa kriminalistike i krivično procesnog prava, kao nauka u najkonkretnijoj vezi sa uzrocima, fenomenom i tehnologijom otkrivanja i dokazivanja kriminaliteta, kao i praktično utemeljenih saznanja i informacija, od izuzetnog su značaja za cijelu društvenu zajednicu. Problematizacijom predmeta između teorije i prakse kroz uspostavljanje funkcionalnog kauzaliteta kriminalističke i krivično procesne teorije, kao i prakse u vezi sa predmetnom temom, smatramo da će dovesti do novog kvalitativnog pomaka u unapređenju efikasnosti u otkrivačkoj djelatnosti nadležnih organa.

Ovako postavljen problem determinira i predmet istraživanja: istražiti i naučno utemeljeno prezentovati sve važnije činjenice o nastanku i pojmu visokotehnološkog kriminaliteta, omjeru postojanja istog, analizirati elemenata, pojmove, tipologiju i profile učinioca, sa aspekta krivičnog prava, kriminalistike i krivično procesnog prava. Kriminalistika je nauka koja se bavi otkrivanjem i dokazivanjem krivičnih djela. Iz dosadašnjih saznanja moguće je uočiti kako tradicionalni modeli kriminalističkog istraživanja, mogu samo djelimično zadovoljiti kada su u pitanju krivična djela visokotehnološkog kriminaliteta. Počevši već od prve faze, prijavljivanja krivičnog djela u startu je upitno. Otkrivanje krivičnog djela od strane organa gonjenja ili eventualne prijave od strane trećih osoba, također se može vrlo rijetko očekivati, jer se vrlo često radi o deliktima koji se dešavaju u *„virtuelnom svijetu*". Izostanak uočljivih radnji navedenih krivičnih djela u *„vanjskom svijetu"* uveliko otežava, odnosno onemogućava da se za ista sazna neposrednim opažanjem organa gonjenja, kao i opažanjem eventualnih svjedoka. Prilikom saznanja za izvršeno krivično djelo visokotehnološkog kriminaliteta, postupak daljnjeg istraživanja, razjašnjavanja i dokazivanja je, također, veoma teško, budući da se radi o reakcijama na akt, koji nema uočljivih manifestacija u javnosti, dok bi oslanjanje na *„istinite"* izjave samih aktera bilo problematično. Uspješno otkrivanje, razjašnjavanje i dokazivanje veoma je opterećeno i nizom strukturalnih problema, kao što su manjak stručnosti kriminalističkih istražitelja i tužitelja, kao i ograničeni ljudski i materijalni resursi. S obzirom na problematizaciju i predmet istraživanja, objekti istraživanja su kriminalistika i krivično procesno pravo u svim svojim sadržajima, a u vezi sa predmetom istraživanja. Istraživanjem se nastoje ispuniti nedostaci i praznine u prethodnim percepcijama o predmetu istraživanja. Iz prethodno identificiranog problema, predmeta i objekata istraživanja implicira osnovna hipoteza rada, koja glasi; „proces otkrivanja, razjašnjavanja i dokazivanja krivičnih djela visokotehnološkog kriminaliteta uslovljen kvalitetom raspoloživih dokaza." Iz prethodne hipoteze proizilazi konstatacija da, početna saznanja o krivičnim djelima visokotehnološkog kriminaliteta često ne daju dovoljno kvalitetnih osnova za početak kriminalističko istražne djelatnosti, bez primjene dodatnih metoda i sredstava koja su specifična za otkrivanje, razjašnjavanje, dokazivanje ovih krivičnih djela. Isto tako, taktika, tehnika i metodika kriminalističkog i istražnog postupanja u otkrivanju, razjašnjavanju i dokazivanju krivičnih djela visokotehnološkog kriminaliteta je specifična i drugačija u odnosu na druge oblike kriminaliteta. U vezi s navedenim, možemo, konstatovati da naučno stručna interakcija kriminalističke i krivično procesne istražne djelatnosti, može doprinijeti efikasnijem suzbijanju krivičnih djela visokotehnološkog kriminala, a posebno kroz jačanje naučnog i stručnog pristupa u planiranju i realizaciji kriminalističke istrage konkretnih krivičnih slučajeva. Neophodno je utvrditi vezu između taktičkog, tehničkog i metodičkog kriminalističkog postupanja u otkrivanju, razjašanjavanju i dokazivanju ovih krivičnih djela, koja je specifična i drugačija u odnosu na druge oblike kriminaliteta.

U vezi sa problemom i predmetom istraživanja te postavljenom hipotezom, određena je i svrha ovog rada; društvena svrha je u neposrednoj vezi sa naučnom, društvo je sasvim sigurno zainteresovano da ovaj problem u praksi bude sveden na najniži mogući nivo. Izuzetno visok nivo nepovjerenja u državne organe nužna je pretpostavka da se na datom

planu u budućnosti mora ozbiljno raditi. Tamna brojka krivičnih djela, počinjenih upotrebom informacionih tehnologija je ogromna. Prezentacijom pojma, nastanka datih krivičnih djela, specifičnostima otkrivanja, razjašnjavanja i dokazivanja istih, odnosno profajlerskom tipologijom njihovih učinilaca, utvrdit će se najbolji načini za suzbijanje ovih krivičnih djela te primjereno i na jednostavan način predstaviti zaključci rada. U okviru sveukupnih kriminalističkih i krivično procesnih stručnih i naučnih istraživanja postoje brojni naučni i stručni radovi koji se bave predmetnom temom. Međutim, bez obzira na tu činjenicu, s obzirom da je kriminalitet, a posebno visokotehnološki veoma dinamična pojava koja mijenja oblike, forme, sukladno području djelovanja, vremenu nastanka i egzistiranja, postoji potreba i inspiracija za nove istraživačke poduhvate i korake. Predložena tema ovog rada zaslužuje stalnu inovativnost u procesu naučnog i stručnog analiziranja, sintetiziranja svih relevantnih karakteristika procesa otkrivanja, razjašnjavanja i dokazivanja, a u svrhu efikasnijeg suzbijanja kriminaliteta. Do sada dostupna istraživanja koja su mnogi autori u svojim radovima objavljivali, i pisali u svojim udžbenicima kriminalistike, kriminologije, krivičnog prava, krivično procesnog prava i srodnih nauka, dat će dragocjenu naučno stručnu osnovu za daljnja istraživanja i rad na daljnjem obogaćivanju teorijske i praktične misli u oblasti suzbijanja kriminaliteta. Iskustva iz policijsko – istražne, sudske prakse, pojedine teze, elementi, kao i mišljenja iskusnih praktičara, a prije svega utemeljena naučna shvatanja, bit će također bitan putokaz u istraživanju i analiziranju predmetne teme i donošenju relevantnih zaključaka i prijedloga. Prilikom pisanja rada korištene su relevantne naučno istraživačke metode i tehnike, koje mogu dati najkvalitetnije rezultate u oblasti istraživanja relevantnosti i efikasnosti kriminalističkih i krivično procesnih radnji u otkrivanju kriminogenih pojava, kao i ličnosti njihovi izvršioca. Isto tako, nastojat će se afirmisati istraživanja koja su značajna u cilju mjerenja kvaliteta i efikasnosti istrage ovih krivičnih djela, kroz dobijanje validnih rezultata u istražnoj, optužnoj i sudskoj praksi. Predmetno istraživanje je teorijsko empirijskog karaktera, ovaj pristup određuje predmetno istraživanje kao kriminalističke i krivično procesne aspekte otkrivanja, razjašnjavanja i dokazivanja krivičnih djela visokotehnološkog kriminala, odnosno kriminalističku i pravosudnu praksu datog istraživanja. U teorijskom dijelu, gdje god je to moguće, izlagane su i konsultirati empirijske verifikacije. Pored toga, u radu je prisutna kvalitativno - kvantitativna metoda. Prilikom pisanja ovog rada korištena je i deduktivna metoda. Izuzetan naglasak posvećen je metodama analize i sinteze. Budući da se suština istraživanja temelji na raščlanjivanju, opisivanju, istraživanju različitih odnosa, metoda analize uveliko je korištena kao osnovna metoda. U istraživanju se sintetizira i generalizira ispitivanjem jednog broja pojedinačnih slučajeva te će se njihovim povezivanjem, odnosno generalizacijom zaključivati.

VISOKOTEHNOLOŠKI KRIMINALITET - OPĆE NAPOMENE

Sadašnjost kojoj pripadamo, a u budućnosti koja je pred nama visokotehnološki kriminalitet[47] bit će sve izraženiji, i sa pravom možemo konstatovati da je danas jedan od najopasnijih vidova kriminaliteta uopšte. Mnoštvo je razloga koji govore u prilog ovoj konstataciji, odnosno visokom stepenu društvene opasnosti ove vrste kriminaliteta. Među njima poseban značaj imaju sljedeći: njegova sve veća prisutnost, i to i u najosjetljivijim institucijama društva. Dovoljno je samo navesti činjenicu o ulasku hakera u SAD u kompjuterski sistem Pentagona, u Indiji u ministarske fajlove, u Njemačkoj 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 bezbjednosti (Bejatović, 2012. str. 18); posljedice koje za sobom povlači; njegov međunarodni karakter; njegova povezanost sa najtežim oblicima kriminaliteta (organizovani kriminalitet i terorizmom gdje on postaje ne samo moćna poluga njihovog planiranja već i ključno sredstvo izvršenja). Otežan način otkrivanja i dokazivanja. U prilog ovakvom stepenu aktuelnosti društvene opasnosti ove vrste kriminaliteta treba istaći i činjenicu da je internetska povezanost ne samo svih zemalja na svijetu već skoro i njihovih najsitnijih teritorijalnih cjelina danas obilježje svijeta kao cjeline. Skoro da nema djela zemaljske kugle da nije internetom povezan sa njenim drugim djelovima, 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 čovejčanstva, 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 djelovanje visokotehnološkog kriminaliteta: 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 uspjeh 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 – prosječan 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 daleko bolje edukovanih pojedinaca sa nečasnim namjerama. Visokotehnološki kriminalitet ne samo da je postao svakodnevica, već je fantastičan razvoj tehnologija uslovio i nevjerovatnu

[47] „visokotehnološki kriminalitet“ ima isto značenje kao i „sajber kriminal (Cybercrime).“

pojavu mnoštva vrsta nedozvoljenih djela koja se mogu izvršiti njihovim korišćenjem, od onih naivnih, do veoma opasnih ponašanja koja spadaju među teška (ponekad čak i najteža) krivična djela u mnogim nacionalnim zakonodavstvima. Visokotehnološki kriminalitet je postao globalni problem, a broj djela koja se mogu podvesti čak i pod najrestriktivnije i najuže definicije sajber kriminala „*Cybercrime*" (Prlja, 2008) gotovo se svakodnevno uvećava, a šteta koja se nanosi njegovim vršenjem mjeri se na godišnjem nivou stotinama milijardi dolara (Bejatović, 2012. str. 19). Polazeći od iznesenog i posebno transnacionalnog karaktera visokotehnološkog kriminaliteta, kao i činjenice da se borba protiv njega ne može ni zamisliti bez uključivanja cijele međunarodne zajednice, odnosno bez angažovanja najuticajnijih međunarodnih institucija, po tom pitanju u posljednjih nekoliko decenija preduzimaju se značajni napori i na međunarodnom planu (Petrović, 2004, str. 51–54). Globalni napori da se uspostavi efikasna međunarodna saradnja u borbi protiv visokotehnološkog kriminaliteta dali su i konkretne rezultate u vidu pisanih dokumenata. Pored toga, tu su i brojne organizacije koje su po prirodi svog djelovanja posebno zainteresovane za ovu problematiku. Slučaj prije svega sa Interpolom kao prvom međunarodnom organizacijom koja ukazuje na potencijal visokotehnološkog kriminaliteta i poseduje operativne priručnike sa najnovijim podacima i uputstvima za istražitelje. (Bejatović, 2012. str. 20)

KRIMINALISTIČKI I KRIVIČNOPROCESNI ASPEKTI OTKRIVANJA, RAZJAŠNJAVANJA I DOKAZIVANJA VISOKOTEHNOLOŠKOG KRIMINALITETA

Ključni i neizostavni instrumenti na polju borbe protiv visokotehnološkog kriminaliteta, kao i kriminaliteta uopšte, jesu kriminalistika, krivično i krivičnoprocesno pravo. S obzirom na tako visok stepen opasnosti ove vrste kriminaliteta, ovim instrumentima 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, kvaliteta istrage, njene adekvatne primjene i stepena zloupotrebe prava, nemalo, zavisi i stepen uticaja krivičnog zakonodavstva na uspješnost ostvarivanja ciljeva kriminalne politike uopšte, a time i ciljeva kriminalne politike kod ove vrste kriminaliteta (Bejatović, 2009 str. 114–116). Ovo sve iz razloga što kriminalistika, krivično i krivičnoprocesno zakonodavstvo predstavljaju zakonsku osnovu za izgradnju onog djela kriminalne politike koji se realizuje na represivnom planu. No, kada je riječ o krivičnopravnom reagovanju i protiv ove vrste kriminala, kao i uopšte posmatrano sa aspekta zakonske norme, reakcija na opasnost od visokotehnološkog kriminaliteta treba da ide u dva pravca. Prvo, blagovremeno usvajanje adekvatne zakonodavne regulative u oblasti materijalnog i procesnog prava (Škulić, M. 2003) kako bi se stvorili pravni instrumenti za kvalitetnu istražnu djelatnost i adekvatan obračun sa visokotehnološkim kriminalitetom. Drugo, adekvatna primjena kako kriminalističkih instrumenata, tako i krivično pravnih normi. Konkretni krivičnopravni propisi da bi bili u funkciji adekvatne kriminalne politike, a time i prevencije nedozvoljenog ponašanja, moraju da odgovaraju savremenim zahtjevima borbe protiv kriminaliteta uopšte, da budu usklađeni sa stvarnošću i da budu primjenljivi, što se posebno manifestuje na polju

visoktehnološkog kriminaliteta s obzirom na pojavu stalnog širenja kako broja tako i oblika njegovog manifestovanja, kao posljedice izuzetno brzog razvoja informativne tehnike. Normativni sistem krivičnog zakonodavstva jedne države mora da bude primjenljiv, društveno racionalan i pravičan. Treba da sadrži takva rješenja koja se u praksi mogu primjenjivati, odnosno da se omogući efikasno otkrivanja razjašnjavanje i dokazivanje ovih krivičnih djela. Subjekti zaduženi za njihovu primjenu (prije svega policijske agencije tužilaštva i sudovi) treba da primjenjuju norme u mjeri koja odgovara zakonskoj intenciji i stvarnim potrebama borbe protiv kriminaliteta. Svako odstupanje od toga dovodi do nesklada između kliminalističkog, normativnog i realnog, između onog što je zakonom propisano i onog što se dešava u praktičnoj primjeni zakona. Zakon ne treba da propisuje one institute i ona rješenja koja se u praktičnoj primjeni ne mogu realizovati ili nisu društveno opravdana. Sa druge strane, organi koji primenjuju zakon ne mogu da u takvom stepenu derogiraju zakonska rješenja 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 osjećaj vrijednosti o stvarnim društvenim potrebama i kriminalnopolitičkim zahtjevima u propisivanju pojedinih instituta i rješenja uopšte i njihovoj primjeni u praksi. Samo u takvom slučaju krivično zakonodavstvo konkretne države je u funkciji željenog stepena prevencije ne samo kriminaliteta 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 primjene 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 primjenu pojedinih mjera i instituta. Rječju, preciznost sadržaja krivičnopravne norme mora da bude izuzetno visoka, a što poseban značaj ima upravo kod normi koje se tiču ove vrste kriminaliteta (Bejatović. S. 2009. str. 114-116). U nastojanju da bude u skladu sa iznesenim zahtjevima kriminalne politike, i na polju visokotehnološkog kriminaliteta u Bosni i Hercegovini po pitanjima vezanim upravo za ovu problematiku visokotehnološkog kriminaliteta posljednjih godina prisutne su, određene aktivnosti. Međutim postavlja se pitanje, kako prije svega uspostaviti efikasnu saradnju na nivou države, a potom međunarodnu saradnju bez koje nema rezultata zbog internacionalnog karaktera visokotehnološkog kriminaliteta (Ignjatović, Đ. 2004)? Kako postupati sa učiniocem koji nije dostigao starosnu granicu krivične odgovornosti (posebno u slučajevima saučesništva u izvršenju krivičnog djela na prostorima država u kojima su različite starosne granice nastupanja krivične odgovornosti)? I pored vidnog napretka, tehničke mogućnosti policije i tužilaštva kao subjekata otkrivanja – procesuiranja još uvijek nisu u skladu sa zahtjevima efikasne borbe protiv ove vrste kriminaliteta. Uspješno suprotstavljanje ovoj vrsti kriminaliteta podrazumijeva posjedovanje 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 uspješno obavi postavljeni zadatak. Kao izuzetno aktuelno i stalno otvoreno je i pitanje prevencije kao

ključnog instrumenta sprečavanja mogućnosti ove vrste kriminaliteta. 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 kriminaliteta (Udruženje javnih tužilaca i zamenika javnih tužilaca Srbije, (2010)). Statistički podaci o aktivnosti specijalizovanih organa u Bosni i Hercegovini na polju borbe protiv visokotehnološkog kriminala pokazuju da se broj krivičnih predmeta ovog karaktera povećava iz godine u godinu.

PRIMJERI IZ PRAKSE – STUDIJE SLUČAJA

U narednom dijelu ćemo predstaviti po jedan slučaj dječje pornografije, odnosno seksulanog iskorištavanja djece zloupotrebom računala, kao i jedan slučaj terorizma također počinjen zloupotrebom računala. U ovom djelu – studij slučaja se zasigurno ima što doznati o pojedinostima svakog slučaja ponaosob, a sebi za pravo uzeli smo da ove slučajeve navedemo i komentarišemo u svom kriminalističkom i pravnom stilu. Opisani slučajevi imaju za cilj da ilustruju *on-line* ponašanje pedofila odnosno osoba koje vrše krivična djela zloupotrebom informacionih tehnologija. U pojedinim slučajevima izvršioci prvo nastoje da se upoznaju sa žrtvom i na kraju istu iskorištavaju ili u najgorem slučaju zlostavljaju djecu kao žrtve. Ujedinjeni narodi su istakli kako naizgled stalnim zahtjevima zapadne Europe i sjeverne Amerike za suzbijanjem pedofilije i fotografijama maloljetnika na internetu, ne mogu stati na kraj ovim predatorima i da je potrebna cjelovita i sveobuhvatna angažiranost svijeta u suzbijanju ove pojave. (Babić 2013. str. 119).

Zvaničnici NATO-a su na vrijeme skrenuli pažnju kako *on-line* špijunaža i terorizam na internetu predstavljaju neke od najopasnijih prijetnji globalnoj sigurnosti, ali sve je ostalo u nekoj početnoj razvojnoj fazi. Svi veliki sustavi nadzora su obmanuti od strane stotine hiljada potencijalnih terorista koji kreiraju viruse i malicozne programe koji kruže internetom i napadaju kompjutere iz dana u dan. Pored toga što su iritantni ti bagovi prijete modernom životu. (Babić, 2015. str. 291).

Operacija u Španjolskoj

Dvije osobe su uhićene početkom 2005. godine pod optužbom da su uključene u seksualno iskorištavanje djece starosti 18 mjeseci. Brzom akcijom Interpola, španjolske policije i kanadske istražne agencije za borbu protiv iskorištavanja djece pronađeni su počinitelji. Sve je započelo u februaru mjesecu u Kanadi, kada je jedan kanadski policajac otkrio fotografije zlostavljene djece i prijavio Interpolu na dalju analizu. Španjolski časnik uposlenik interpola je pomogao da se potvrdi lokacija mjesta događaja, jednostavno otkrivši prema znacima na djelu tipkovnice koji se odnosi na posebna „*domaća slova*“ na računaru a vidjela su se na jednom od video zapisa. Daljnjom analizom fotografija pronađeno je još bitnih detalja koji su dali rezultate za uhićenjem zlostavljača i njegove bitne identifikacije, te saradnika koji je vršio distribuciju navedenih video isječaka i fotografija.

Ukupan broj zlostavljane i seksualno iskorištene djece u dobi od 2 – 4 godine iznosio je sedmero djece. Ta osoba zlostavljač je uglavnom bila uposlena kao beby-siter i na taj način je vrlo lako dolazila u kontakt sa malom djecom i pristupala im. Nakon ovih događaja u španjolskoj je uvedeno provjeravanje osoba koje se bave čuvanjem djece, kako bi se izbjegle situacije da osobe koje obavljaju ove poslove jednostavno i neometano mogu seksualno iskorištavati djecu koja to ne mogu ili ne znaju reći svojim roditeljima. (Babić, 2013. str. 125).

Operacija „Damask"

U jesen 2014. godine u BiH je uhićen vođa jedne od dvije najveće zajednice pripadnika radikalnog islama Husein Bosnić poznatiji kao Bilal koji je putem medija, naročito interneta pozvao mladiće iz BiH da se pridruže oružanim skupinama ISIL-a i tako uključe u džihad, kojeg vodi ta organizacija na teritoriji Iraka i Sirije. Bosnićev poziv mladim muslimanima iz BiH ostao je zabilježen na video snimkama objavljivanim na *youtube* iz svakodnevnih predavanja što ih je držao pred svojim sljedbenicima sa područja Cazinske krajine, u sjeverozapadnoj Bosni. U okviru akcije „Damask", koja je izvođena na području BiH i tijekom koje je privedeno 16 osoba osumnjičenih za vrbovanje državljana BiH za odlazak na strana ratišta, Bosnić slovi za jednog od najeksponiranijih pripadnika vehabijske zajednice u BiH. (Babić, 2015. str. 300).

ZAKLJUČAK

Svaka država nastoji da se adekvatno suprotstavi ponašanjima koja štete njenom napretku, da bi se ta nastojanja ostvarila, posebno su značajne norme krivičnog prava kojima se ustanovljava šta je to što šteti interesima zajednice i koji su uslovi za primjenu državnih mehanizama kako bi se suprotstavila devijantnim ponašanjima. Način primjene zakonskih obilježja krivičnih djela odražava se posebno u svakom konkretnom slučaju, međutim uglavnom je moguće primijetiti određene zajedničke karakteristike. U tim zajedničkim karakteristikama, odnosno objektivnim i subjektivnim sadržajima krivičnih djela, značajnu ulogu imaju kriminalistika i krivično procesno pravo. Samo određenje deliktnog ponašanja, u našem slučaju krivičnih djela visokotehnološkog kriminaliteta, gdje je u pitanju vrlo specifična oblast, najznačajnija razlika, u odnosu na sva ostala krivična djela, upravo je u specifičnom odnosu, jer uglavnom izostaje uobičajeni odnos počinitelja i žrtve. Blagovremen trenutak saznanja da je došlo do krivičnog djela visokotehnološkog kriminaliteta može biti značajan iskorak u suprotstavljanju istom. Pored toga, kroz samu percepciju ovih krivičnih djela možemo zaključiti da izvršioci istih nisu osobe koje su sklone devijantnom ponašanju, niti po bilo kojoj osnovi pripadaju profilu „*kriminalca*". Način izvršenja pomenutog krivičnog djela, odnosno njegovo ostvarenje u mnogome se razlikuje u odnosu na ostala krivična djela, što implicira da se u otkrivanju, razjašnjavanju i dokazivanju ovih delikata uvijek mogu očekivati znatne poteškoće. Sve navedeno ukazuje da se bavljenjem kriminalističkim i krivično procesnim aspektima otkrivanja, razjašnjavanja i dokazivanja krivičnih djela visokotehnološkog kriminaliteta vrijedi posvetiti izuzetno velika pažnja, koja zahtijeva multidimenzionalnost i multidisciplinarnost.

Obzirom na svojevrsnu specifičnost krivičnih djela visokotehnološkog kriminaliteta, počev od indicijalnih saznanja, konstitucije dokaznih činjenica, pa preko složenosti otkrivanja, prikupljanja relevantnih dokaza, do konačne sudske odluke, presude, smatramo da je neophodno u metodologiju rada uvesti *„savremene metode i sredstva*" otkrivanja, istrage, dokazivanja. Klasični pristup suprotstavljanja krivičnim djelima visokotehnološkog kriminaliteta, ne može niti smije biti jedini mogući način rada, suprotstavljanja. Ova krivična djela su delikti bez svjedoka, a u samom aktu involvirane su osobe koje ne odgovaraju liku *„zločinca"* kojeg karakteriše klasični kriminalitet. Pored toga, pomenuta krivična djela odlikuje visoka tamna brojka, i upravo zbog toga, klasičan pristup otkrivanju, razjašnjavanju i dokazivanju istih nije moguć, ili u najboljem slučaju, samo djelimično moguć.

LITERATURA

1. Bejatović. S. (2012) Visokotehnološki kriminal i krivično pravni instrumenti suprostavljanja Laktaši, Zbornik radova Međunarodna naučno stručna konferencija, „Suzbijanje kriminala i evropske integracije sa posebnim osvrtom na visokotehnološki kriminal“. Vlada RS, MUP RS Uprava za policijsko obrazovanje RS i VŠU u saradnji sa Hans Zajedl fondacijom, 17-29.
2. Babić, V. (2013) Dječija pornografija i internet, Vitez.
3. Babić, V. (2015) Cyber terorizam suvremena sigurnosna prijetnja, Novi Travnik.
4. Ignjatović, Đ. (2004) Suzbijanje najtežih oblika kriminaliteta u uslovima tranzicije i nesigurnosti Beograd, Zbornik radova „Teški oblici kriminala“, Institut za kriminološka i sociološka istraživanja.
5. Priručnik za trening tužilaca i sudija u oblasti visokotehnološkog kriminala (2009), Udruženje javnih tužilaca i zamenika javnih tužilaca Srbije, ATC.
6. Prlja, D. (2008), Sajber kriminal (***http://www.prlja.info/;sk2008,pdf,1.5.2009***)
7. Škulić, M. (2003) Organizovani kriminalitet – Pojam i krivičnoprocesni aspekti, Beograd.

Kriminalističke teme
Zbornik radova
Godina XIX, Broj 5, 2019.
ISSN 1512-5505

KRIVIČNOPRAVNI ASPEKTI ZAŠTITE KOMPJUTERSKIH SISTEMA, ANALIZA STANJA I DE LEGE FERENDA PRIJEDLOZI

CRIMINAL ASPECTS OF THE COMPUTER SYSTEM'S PROTECTION, SITUATION ANALISIS OF AND DE LEGE FERENDA PROPOSAL'S

Stručni rad

mr. sci. Hasan Pleh[48]

SAŽETAK

Inspiracija za rad i problem koji se radom oslovljava

Bosna i Hercegovina mora kreirati jasan i nedvosmislen krivičnopravni okvir sa krivičnopravnim sankcijama koji je usklađen sa konvencijama kojima pristupa. Tekst krivičnih djela kojima se štite kompjuterski sistemi u Bosni i Hercegovini nije usklađen sa Konvencijom Vijeća Evrope o kompjuterskom kriminalu (u daljem tekstu: Konvencija).

Ciljevi rada:

Cilj stručnog rada je da se ukaže na potrebu usklađivanja krivičnog zakonodavstva Bosne i Hercegovine sa Konvencijom.

Metodologija/Dizajn:

Metode korištene u ovom radu su metoda analize, komparativna i empirijska metoda.

Ograničenja istraživanja/rada:

Loš prevod Konvencije o kompjuterskom kriminalu na bosanski jezik.

Rezultati/Nalazi:

Rezultati koji su dobiveni analizom krivičnopravnih normi koje pružaju krivičnopravnu zaštitu kompjuterskih sistema ukazali su da postoji potreba da se krivično zakonodavstvo u Bosni i Hercegovini uskladi sa Konvencijom.

Generalni zaključak:

Osobe koje rade na izmjenama i dopunama krivičnog zakonodavstva u Bosni i Hercegovini nisu dovoljno posvećene procesu usklađivanja našeg krivičnog zakonodavstva sa konvencijama koje Bosna i Hercegovina preuizima zbog čega često moramo dopunjavati ili mijenjati naše krivično zakonodavstvo.

Opravdanost istraživanja/rada:

Nedostatak usklađenosti našeg krivičnog zakonodavstva sa Konvencijom i nejasnoća krivičnopravnih normi sadržanih u krivičnim zakonima u Bosni i Hercegovini koje se

[48] Autor je magistar pravnih nauka sa odbranjenim radom na temu „Zajednički zločinački poduhvat kao oblik krivične odgovornosti u krivičnom zakonodavstvu Bosne i Hercegovine“ i doktorant na Pravnom fakultetu Univerziteta u Sarajevu na katedri krivičnog prava. Zaposlen je kao savjetnik u Posebnom odjelu za organizovani kriminal, korupciju i privredni kriminal Tužilaštva Bosne i Hercegovine. Email adresa: pleh.hasan@gmail.com

Stavovi izraženi u ovom članku su lični stavovi autora, te niti jednim dijelom ne predstavljaju stavove Tužilaštva Bosne i Hercegovine.

odnose na kompjuterski kriminal, čine ovaj stručni rad opravdanim.

Ključne riječi

Informaciona tehnologija, kompjuterski sistemi, Konvencija Vijeće Evrope o kibernetičkom kriminalu, Dodatni protokol, Krivični zakon, Kompjuterski podatak, Evropska unija

ABSTRACT

Inspiration for the paper and addressed issue:
Bosnia and Herzegovina has to create a clear and unambiguous criminal law framework with criminal sanctions harmonised to conventions to which Bosnia and Herzegovina access. The text of the offenses protecting computer systems in Bosnia and Herzegovina is not in line with the European Council Cybercrime Convention (here after as: Convention).
Goal of the professional paper research:
The goal of the professional work is to highlight the need to harmonize the criminal legislation of Bosnia and Herzegovina with the Convention.
Methodology:
The following methods were used for the research: analysis, comparative and empirical methods
Research limitations:
The poor translation of the Convention into Bosnian appeared as a problem.
Results/Findings:
The results achieved through the analysis of the legal provisions regulating the protection of computer systems against crimes show that there is a need to amend the criminal legislation in Bosnia and Herzegovina and fully harmonize it with the Convention.
General conclusion:
Persons working on amendments to the criminal legislation in Bosnia and Herzegovina are not sufficiently committed to the process of aligning our criminal legislation with the conventions we adopt, which often leads to the need to supplement our criminal legislation.
Research justification:
The lack of harmonization of our criminal legislation with the Convention and unclear provisions of the respective Criminal Codes in Bosnia and Herzegovina relating to cybercrime make this research justifiable.

Key words

Information technology, Computer system, European Council Convention on Cybercrime, Additional protocol, Criminal Code, Computer data, European Union

I. Uvodna razmatranja

Reforma krivičnog zakonodavstva iz 2003. godine je bila sveobuhvatna u pogledu krivičnih zakona i zakona o krivičnom postupku u Bosni i Hercegovini.[49] Međunarodna zajednica, zajedno sa domaćim pravnim stručnjacima, uložila je ogromne napore da se krivično zakonodavstvo[50] Bosne i Hercegovine uskladi sa međunarodnim krivičnopravnim standardima i obavezama koje je Bosna i Hercegovina preuzela pristupajući raznim multilateralnim ugovorima, ali isto tako i sa onim kojima Bosna i Hercegovina nije pristupila, odnosno potpisala.[51]

Takav je slučaj bio i sa Konvencijom Vijeća Evrope o kibernetičkom kriminalu (u daljem tekstu: Konvencija) i njenim Dodatnim protokolom u vezi kažnjavanja djela rasističke i ksenofobične prirode učinjenih putem kompjuterskih sistema (u daljem tekstu: Protokol).[52] Krivična djela sadržana u Konvenciji postala su sastavni dio krivičnog zakonodavstva entiteta i Brčko Distrikta i prije nego što su Konvencija i Protokol bili potpisani i ratifikovani. Ovakav proaktivan pristup međunarodne zajednice govori nam da je međunarodna zajednica prepoznala važnost Konvencije i poduzela konkretne radnje kako bi se zaštita koju pruža Konvencija proširila i na građane Bosne i Hercegovine na način da je iskoristila svoj snažan uticaj na bosanskohercegovačke entitete i Brčko Distrikt, kako bi krivičnopravne odredbe iz Konvencije obuhvatili svojim krivičnim zakonodavstvima.

Međutim, ovaj uticaj nije ostvaren na državnom nivou, čime je Krivični zakon Bosne i Hercegovine ostao uskraćen za krivična djela kompjuterskog kriminala. O mogućim razlozima zbog čega je to tako moglo bi se pretpostavljati, mada bi bilo ispravnije da su radnje koje su propisane Konvencijom i Protokolom, kao krivičnopravne radnje, postale sastavni dio Krivičnog zakona Bosne i Hercegovine zbog specifičnosti krivičnih djela, jer se radi o krivičnim djelima gdje počinilac krivičnog djela može poduzimati radnju, primjera radi, u Federaciji Bosne i Hercegovine, a posljedica istovremeno nastupiti u Federaciji Bosne i Hercegovine, Republici Srpskoj, Brčko Distriktu ili van teritorije Bosne i Hercegovine. Svakako, ovakvo zakonsko rješenje nije isključilo mogućnost da se krivična djela kompjuterskog kriminala krivično gone pred Sudom Bosne i Hercegovine na osnovu člana

[49] Bosna i Hercegovina ima četiri krivična zakona i četiri zakona o krivičnom postupku. Ovako decentralizovan krivičnopravni sistem stvara pogodno tlo za pravnu nesigurnost građana, tj. može dovesti do toga da jedno krivično djelo bude propisano u jednom entitetu ili Brčko Distriktu, a da ne bude krivično djelo u drugom entitetu ili Brčko Distriktu. Slična situacija je i sa kaznenim okvirom, odnosno postoji razlika u pogledu gornjeg maksimuma i donjeg minimuma za ista krivična djela propisana entitetskim zakonodavstvom.

[50] U ovom radu pod pojmom krivično zakonodavstvo smatrat će se Krivični zakon Bosne i Hercegovine, entitetski krivični zakoni i Krivični zakon Brčko Distrikta.

[51] Bosna i Hercegovina je potpisala Konvenciju o kibernetičkom kriminalu tek 09. februara 2005. godine, dok je istu ratifikovala tek u 2006. godini. Za više vidjeti: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=dOsJKORQ (17.06.2019.)

[52] Parlamentarna skupština Bosne i Hercegovine je ratifikovala Konvenciju i Dodatni protokol 25. marta 2006. godine. Konvencija i Dodatni protokol su objavljeni u „Službenom glasniku Bosne i Hercegovine – dodatak – Međunarodni ugovori“, broj 6. od 11. maja 2006. godine.

7. stava 2. Zakona o Sudu Bosne i Hercegovine (u daljem tekstu: Zakon). Da bi se poduzelo krivično gonjenje pred Sudom Bosne i Hercegovine za krivična djela kompjuterskog kriminala na osnovu člana 7. stava 2. Zakona, potrebno je da počinjena krivična djela kompjuterskog kriminala ugrožavaju suverenitet, teritorijalni integritet, političku nezavisnost, nacionalnu sigurnost i međunarodni subjektivitet Bosne i Hercegovine, odnosno da krivična djela kompjuterskog kriminala mogu imati ozbiljne reperkusije ili štetne posljedice na privredu Bosne i Hercegovine ili mogu izazvati druge štetne posljedice za Bosnu i Hercegovinu ili mogu izazvati ozbiljnu ekonomsku štetu ili druge štetne posljedice izvan teritorije datog entiteta ili Brčko Distrikta Bosne i Hercegovine. Dakle, postoji mogućnost za krivično gonjenje na državnom nivou, ali standardi za zasnivanje nadležnosti Suda Bosne i Hercegovine prema članu 7. stavu 2. Zakona za krivična djela kompjuterskog kriminala su visoko postavljeni u odnosu na posljedicu.

Pristupanjem Konvenciji i potpisivanjem Dodatnog protokola, Bosna i Hercegovina je odredila Državnu agenciju za istrage i zaštitu (u daljem tekstu: SIPA) kao centralni organ za pružanje međunarodne pravne pomoći, dok je Zakonom o SIPA-i, koji uređuje nadležnost SIPA-e, propisano da SIPA postupa po nalogu Suda Bosne i Hercegovine i glavnog tužioca Tužilaštva Bosne i Hercegovine.[53] Također, pristupanjem Konvenciji, Bosna i Hercegovina je odredila da će kontaktna tačka za Mrežu 24/7 biti Direkcija za koordinaciju policijskih tijela Bosne i Hercegovine.[54] Razmatrajući stav Bosne i Hercegovine prema Konvenciji i Dodatnom protokolu u pogledu institucija koje su nadležne za pružanje međunarodne pravne pomoći, kao i institucija koje su nadležne za osiguranje neodložive pomoći u istragama koje su povezane sa kompjuterskim kriminalom, te činjenicu da krivično djelo može biti počinjeno s bilo kojeg teritorija Bosne i Hercegovine, a da posljedica istovremeno može nastupiti na teritoriju oba entiteta i Brčko Distrikta ili van Bosne i Hercegovine, može se zaključiti da je krivičnopravna zaštita kompjuterskih sistema, odnosno elektronske obrade podataka i drugih krivičnih djela povezanih sa internet kriminalom, trebala biti pozicionirana u Krivičnom zakonu Bosne i Hercegovine, a ne u entitetskim krivičnim zakonodavstvima i krivičnom zakonodavstvu Brčko Distrikta.

Također, Bosna i Hercegovina je država koja se odredila ka evropskim integracijama, što znači da će svoje zakonodavstvo morati prilagođavati pravnoj stečevini Evropske unije, odnosno da će Bosna i Hercegovina morati prilagođavati svoje krivično zakonodavstvo zakonodavnim aktima Evropske unije[55] (u daljem tekstu: EU) kojima se propisuju određena krivična djela. U tom pravcu, a u kontekstu kompjuterskog kriminala, neophodno je naglasiti direktive EU koje predstavljaju zakonodavni akt EU kojim se utvrđuje cilj koji sve

[53] Za više vidjeti odredbe člana 24. stava 7. i člana 27. stava 2. Konvencije.
[54] Za više vidjeti odredbe člana 35. stava 1. Konvencije.
[55] Kao zakonodavni akti Evropske unije javljaju se: uredbe i direktive. Uredba je obvezujući zakonodavni akt koji se mora u cijelosti primjenjivati u čitavoj Evropskoj uniji, dok je direktiva zakonodavni akt kojim se utvrđuje cilj koji sve države članice EU-a moraju ostvariti. Međutim, svaka država samostalno odlučuje o načinu na koji će ostvariti taj cilj. Za više vidjeti: https://europa.eu/european-union/eu-law/legal-acts_hr (18.06.2019.)

države članice EU-a moraju ostvariti.[56] Jedna od takvih direktiva je i Direktiva Evropskog parlamenta i Vijeća o napadima na informatičke sisteme i o zamjeni Okvirne odluke Vijeća 2005/222/PUP (u daljem tekstu: Direktiva).[57]

Razlozi za donošenje Direktive mogu se naći u značajnim nedostacima i razlikama u zakonodavstvima i krivičnim postupcima država članica u pogledu napada na informatičke sisteme. Iz sadržaja uvodnog teksta Direktive može se zaključiti da nedostaci i razlike, koji su sadržani u krivičnim zakonodavstvima članica EU, mogu usporiti borbu protiv organiziranog kriminala i terorizma te otežati efikasnu policijsku i pravosudnu saradnju koja je veoma bitna za borbu protiv organiziranog kriminala i terorizma, pogotovo imajući u vidu da su savremeni informatički sistemi nadnacionalni i bezgranični, te da napadi na takve sisteme imaju prekograničnu dimenziju, što čini osnov za poduzimanje hitnih mjera kako bi se uskladilo krivično pravo u toj oblasti u zemljama članicama EU.[58]

U tom smislu Direktiva traži od zemalja članica EU da ujednače svoja krivična zakonodavstva u pogledu kriminalizacije napada na informatičke, odnosno kompjuterske sisteme, utvrđivanjem minimalnih pravila o definisanju krivičnih djela i sankcija u vezi napada na informatičke sisteme olakšavanjem sprečavanja takvih djela i jačanjem saradnje između pravosudnih i drugih nadležnih tijela.[59]

U pogledu minimalnih pravila o definisanju krivičnih djela Direktiva traži od zemalja članica EU da propišu sljedeća krivična djela: nezakonit pristup informatičkim sistemima, nezakonito ometanje sistema, nezakonito ometanje podataka, nezakonito presretanje, sredstva koja se koriste za izvršenje krivičnih djela. U pravcu krivičnih sankcija, Direktiva traži da zemlje članice EU propišu efikasne, proporcionalne i odvraćajuće krivičnopravne sankcije, s tim da za izvršenje pomenutih krivičnih djela, u kojima je nastupila ozbiljna posljedica, minimalna kazna bude dvije godine zatvora. Ukoliko su krivična djela nezakonito ometanje sistema i nezakonito ometanje podataka učinjena s namjerom i korištenjem nekih od sredstava koja su namijenjena ili prilagođena za izvršenje ovih krivičnih djela, Direktiva traži da zemlje članice EU propišu minimalnu kaznu zatvora od tri godine. Ukoliko su ova krivična djela učinjena u okviru grupe za organizovani kriminal ili je izvršenjem pomenutih krivičnih djela prouzrokovana ozbiljna šteta ili su ta krivična djela izvršena protiv informatičkog sistema od ključne infrastrukture za zemlju ili zemlje članice EU, onda minimalna propisana kazna mora biti pet godina zatvora.

---

[56] Za više vidjeti: https://ec.europa.eu/info/law/law-making-process/types-eu-law_hr#primarno-zakonodavstvo-u-odnosu-na-sekundarno-zakonodavstvo (18.06.2019.)

[57] Direktiva je donesena 12.08.2013. godine i objavljena je u Službenom listu Evropske unije broj: L 218/8 od 14.08.2013. godine. Dostupna je na web adresi: https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=celex%3A32013L0040 (18.06.2019.)

[58] Za više vidjeti stav 27. uvodnog teksta Direktive.

[59] Za više vidjeti član 1. Direktive.

U okviru poglavlja sankcija, Direktiva predviđa i otežavajuće okolnosti ukoliko su krivična djela nezakonito ometanje sistema i nezakonito ometanje podataka izvršena zloupotrebom ličnih podataka druge osobe s ciljem zadobivanja povjerenja treće strane, i time nanoseći štetu legitimnom vlasniku identiteta.[60] Naravno, ove otežavajuće okolnosti se cijene prilikom izricanja kazne za počinitelje, s tim što sudija uvijek zadržava pravo da slobodno cijeni takve okolnosti zajedno s drugim činjenicama konkretnog slučaja. U pogledu definicije pojmova, Direktiva definiše četiri pojma i to: informatički sistem i računalne, odnosno kompjuterske podatke, pravnu osobu i bespravnost. Definicije pojmova informatički sistem i računalni podaci slične su definicijama kompjuterskog sistema i kompjuterskih podataka iz Konvencije. Pojmovi pravne osobe i pojam bespravnosti su novost i definicija ovih pojmova nije obuhvaćena Konvencijom.

Analizom Konvencije i Direktive dolazi se do zaključka da je Evropa, kao kontinent, a kasnije i EU kao regionalna organizacija, prepoznala značaj zaštite kompjuterskih sistema, odnosno da bi se ometanje rada ili uništenje ključnih kompjuterskih sistema bilo koje države, pogotovo bankarskog, carinskog ili bezbjednosnog kompjuterskog sistema odrazio na sve države Evrope zbog isprepletenosti poslovnih i drugih društvenih odnosa. Oba dokumenta, Konvencija i Direktiva, traže da kompjuterski sistemi koji se odnose na održavanje ključnih društvenih funkcija poput sigurnosnog, privrednog, zdravstvenog ili socijalnog sistema, moraju biti krivičnopravno zaštićeni od napada kako bi se poslala jasna poruka eventualnim počiniteljima šta ih očekuje u slučaju napada na kompjuterske sisteme koji se nalaze na evropskom kontinentu.

[60] Za više vidjeti stav 19. uvodnog teksta Direktive.

II. Analiza postojećeg stanja materijalnih odredaba u krivičnom zakonodavstvu Bosne i Hercegovine sa naglaskom na Krivični zakon Federacije BiH

Iz prethodnog poglavlja zaključili smo da krivična djela protiv kompjuterskih sistema predstavljaju novinu u našem krivičnom zakonodavstvu i temelje se na međunarodnom pravnom osnovu, odnosno na Konvenciji i konačnom Izvještaju Evropskog komiteta u vezi problema sa kriminalom.[61]

Analizom sadržaja Konvencije proizlazi da su krivična djela sadržana u Konvenciji klasificirana u četiri grupe. U prvu grupu spadaju krivična djela usmjerena protiv povjerljivosti, integriteta i dostupnosti[62] kompjuterskih podataka i sistema. Druga grupa krivičnih djela usmjerena je protiv krivičnih djela u vezi kompjutera. Treću grupu čine krivična djela u vezi korištenja kompjuterskih sistema u svrhu dječije pornografije i četvrtu, posljednju grupu, čine krivična djela protiv autorskih i njima srodnih prava. Također, Konvencija obavezuje države potpisnice da svojim krivičnim zakonodavstvom propišu krivnju i krivičnopravne sankcije za pokušaj i saizvršilaštvo u širem značenju, kao i kaznenu odgovornost za pravna lica.

Analizom krivičnopravnih odredaba Krivičnog zakona Federacije Bosne i Hercegovine (u daljem tekstu: KZ FBiH), kao i odredaba Krivičnog zakona Republike Srpske (u daljem tekstu: KZ RS) i odredaba Krivičnog zakona Brčko Distrikta (u daljem tekstu: KZ BD), a u kontekstu krivičnih djela koje Konvencija propisuje, dolazi se do zaključka da je Bosna i Hercegovina poprilično uskladila svoje krivično zakonodavstvo sa odredbama iz Konvencije.

Krivičnopravna zaštita kompjuterskih sistema pozicionirana je u glavi XXXII KZ-a FBiH, s nazivom „Krivična djela protiv sistema elektronske obrade podataka“ i razrađena je kroz šest krivičnih djela: Oštećenje računalnih podataka i programa (član 393.), Računalno krivotvorenje (član 394.), Računalna prevara (član 395.), Ometanje rada sistema i mreže elektronske obrade podataka (član 396.), Neovlašteni pristup zaštićenom sistemu i mreži elektronske obrade podataka (član 397.) i Računalna sabotaža (član 398.). Krivična djela koja su propisana KZ-om RS pozicionirana su u glavi XXXII KZ-a RS i nose naslov „Krivična djela protiv bezbjednosti kompjuterskih podataka“. Za razliku od KZ-a FBiH, KZ RS propisuje i krivično djelo Izrade i unošenja kompjuterskih virusa, ali ne propisuje krivično djelo Računalno krivotvorenje, niti daje definiciju „kompjuterskog virusa“.

---

[61] Tomić. Z., Krivično pravo II, Posebni dio, drugo izmijenjeno i dopunjeno izdanje, Pravni fakultet Univerziteta u Sarajevu, Sarajevo, 2007. godina, strana 397.

[62] Interesantno je da je u prijevodu na bosanski jezik, engleska riječ „*available“* što u prevodu na bosanski jezik znači „*dostupan*“, prevedena kao „*disponibilnost*“, što predstavlja loš i nerazumljiv prijevod ne samo u odnosu na ovu riječ nego na prijevod Konvencije u cijelosti.

Analiza krivičnopravnih odredaba između krivičnih zakona entiteta i Brčko Distrikta kojima su propisana krivična djela protiv kompjuterskih sistema, a u odnosu na Konvenciju, upućuje na zaključak da su entiteti i Brčko Distrikt propustili propisati određena krivična djela koja su predviđena Konvencijom. Primjera radi, krivično djelo Neovlaštenog presretanja kompjuterskih podataka iz člana 3. Konvencije nije propisano krivičnim zakonima entiteta i Brčko Distrikta. Iako se na prvi pogled čini da je ovo krivično djelo propisano krivičnim zakonodavstvom Bosne i Hercegovine, ozbiljnijom analizom teksta Konvencije i tekstova krivičnih zakona se ne može izvući takav zaključak.

Kriminalizacija presretanja prenosa podataka koja je sadržana u članu 393. stavu 2. KZ-a FBiH traži da se ispuni nužan uslov, a to je da postoje zaštitne mjere.[63] Ako nema zaštitnih mjera, odnosno ako se prenos podataka vrši putem Wi-Fi prenosa kroz nezaštićenu mrežu, tj. javnu mrežu, postavlja se pitanje postojanja krivičnog djela neovlaštenog presretanja podataka koji se prenose jer se radi o mreži koja nema zaštitnih mjera, odnosno mreži na koju se može priključiti bilo ko. Međutim, postavljanje zaštitnih mjera kao uslova inkriminacije nije predviđeno Konvencijom, što otvara dodatno pitanje zašto su se naši zakonodavci odlučili za ovaj uslov?

Kriminalizacijom neovlaštenog presretanja štite se podaci koji se nalaze u prijenosu. Podaci koji su u prijenosu mogu biti poslovne i lične prirode, lični podaci, podaci o broju kreditnih kartica, podaci koji se odnose na jedinstveni matični broj, brojevi bankovnih računa, odnosno može biti bilo koji podatak koji je predmet komunikacije.[64] Uklanjanjem dijela rečenice „unatoč zaštitnim mjerama“ iz teksta zakona ovog krivičnog djela omogućila bi se krivičnopravna zaštita privatnosti komunikacije bez obzira da li se prenos digitalnih podataka vrši zaštićenom ili nezaštićenom mrežom, jer se i nezaštićenom mrežom mogu slati E-mail komunikacije, prenositi datoteke putem pametnih telefona koristeći Wi-Fi prenos podataka ili bluetooth.

Također, mora se imati i u vidu da sva zakonodavstva u Bosni i Hercegovini, koja na jedan ili drugi način imaju doticaja sa privatnošću građana, moraju biti usklađena sa članom 8. Evropske konvencije o ljudskim pravima i temeljnim slobodima kojim se štiti pravo na privatnost građana, što je jedno od temeljnih ljudskih prava. S obzirom da krivično zakonodavstvo u Bosni i Hercegovini ne propisuje kao krivično djelo neovlašteno presretanje kompjuterskih podataka, postavlja se pitanje na koji bi se način sankcionisali oni koji protupravno „skidaju“ privatne komunikacije koje se odvijaju putem E-maila ili Wi-Fi sistema

---

[63] Krivični zakon Federacije Bosne i Hercegovine, „Službene novine Federacije Bosne i Hercegovine“, br. 36/03, 37/03, 21/04, 69/04, 18/05, 42/10, 42/11, 59/14, 76/14, 46/16 i 75/17
Član 393. stav 2
Ko **unatoč zaštitnim mjerama** neovlašćeno pristupi računalnim podacima ili programima ili neovlašćeno presreće njihov prijenos.....

[64] Kokot. I., Kaznenopravna zaštita računalnih sustava, programa i podataka, Pregledni znanstveni rad od 08. listopada 2014. godine. Dostupno na web adresi: https://hrcak.srce.hr/file/209347 (16.06.2019.)

prenosa podataka na javnoj mreži, odnosno oni koji protupravno narušavaju privatnost građana?

Šta je bio razlog da se propusti sankcionisanje neovlaštenog presretanja kompjuterskih podataka? Da li je to nerazumijevanje teksta Konvencije ili neposjedovanje znanja u vezi rada sa kompjuterima i korištenja tehničkih uređaja ili nešto sasvim treće od strane grupe koja je bila zadužena da izradi tekst dijela krivičnog zakona na koji se odnosi Konvencija, ostaje nepoznanica.

Iako je krivično zakonodavstvo Bosne i Hercegovine poprilično ispunilo svoje obaveze u pogledu kriminalizacije radnji koje su usmjerene protiv kompjuterskih sistema, i dalje ima prostora da se to popravi i u cijelosti uskladi sa Konvencijom, pogotovo u pogledu naziva krivičnih djela i preciziranja radnji koje proizlaze iz Konvencije. Primjera radi, u članu 2. Konvencije naslov krivičnog djela nosi naziv „Nedozvoljeni pristup", dok u krivičnom zakonodavstvu Bosne i Hercegovine nema ovakvog naziva, a sam tekst sadržan u krivičnim zakonodavstvima Bosne i Hercegovine ne odražava najjasnije tekst Konvencije jer se miješaju pojmovi kompjuterskog podatka i programa, a pojam elektronska obrada podataka nije uopšte definisan. Smatram da je inkriminacija iz člana 2. Konvencije trebala imati naziv u krivičnimm zakonodavstvima u Bosni i Hercegovini „*Neovlašteni pristup*" i glasiti: „*Ko neovlašteno pristupi kompjuterskom sistemu radi pribavljanja kompjuterskih podataka, kaznit će se....*". Na ovaj način bi naše krivično zakonodavstvo u cijelosti slijedilo tekst Konvencije.

Dalje, član 3. Konvencije ima naziv „Nezakonito presretanje", dok u krivičnim zakonodavstvima Bosne i Hercegovine nema krivičnog djela sa ovim nazivom, nego je određeni i uslovljeni oblik ove inkriminacije pozicioniran u članu 393. stavu 2. KZ-a FBiH. Krivični zakon Republike Srpske uopšte ne sadrži odredbe kojima bi se kriminalizovalo nezakonito presretanje kompjuterskih podataka. Smatram da bi se ovaj nedostatak mogao otkloniti promjenom naziva krivičnog djela u „*Neovlašteno presretanje*" i izmjenom teksta krivičnih zakona koji bi glasio: „*Ko u namjeri da pribavi kompjuterski podatak neovlašteno presretne prijenos kompjuterskih podataka ili prijenos elektromagnetske emisije koja potiče iz kompjuterskog sistema kaznit će se.....*"

Kriminalizacija presretanja podataka, koristeći elektromagnetne emisije, uopšte nije obuhvaćena krivičnim zakonodavstvima u Bosni i Hercegovini. Rad kompjutera stvara elektromagnetnu energiju koja se adekvatnom tehničkom opremom može presretnuti, rekonstruisati u kompjuterski podatak.[65] Stoga je neophodno da naš zakonodavac budućim izmjenama i dopunama krivičnog zakonodavstva obuhvati i kriminalizaciju presretanja kompjuterskih podataka putem elektromagnetne emisije, kako bi se naše krivično

[65] Za više vidjeti: Izvještaj s obrazloženjem Konvencije o kibernetičkom kriminalu, stav 57, dostupan na web adresi: https://rm.coe.int/16800cce5b (17.06.2019.)

zakonodavstvo u cijelosti uskladilo sa odredbama Konvencije kojima se prenos kompjuterskih podataka štiti od neovlaštenog presretanja.

Član 4. Konvencije ima naziv „Povreda integriteta podataka“, odnosno radi se o krivičnom djelu gdje se poduzimanjem inkrimisanih radnji nanosi šteta kompjuterskim podacima. U krivičnom zakonodavstvu Bosne i Hercegovine ovo krivično djelo nosi naziv „Oštećenje računalnih podataka i programa“. Smatram da bi bilo ispravnije da ovo krivično djelo nosi naziv „Oštećenje računalnih podataka“ jer tekst Konvencije upravo na to i upućuje. Prema definiciji kompjuterskog podatka koja je sadržana u Konvenciji, pojam kompjuterskog podatka obuhvata i kompjuterski program, pa nije jasno zbog čega je naš zakonodavac obuhvatio povredu kompjuterskog programa kada je program kompjuterski podatak. Također smatram da bi ovo krivično djelo u osnovnom značenju trebalo da glasi: „*Ko neovlašteno ošteti, obriše, izmijeni ili učini nedostupnim kompjuterski podatak kaznit će se.....*“

Slično rješenje trebalo je imati i krivično djelo iz člana 5. Konvencije koje ima naziv „Povreda integriteta sistema“, dok je u krivičnom zakonodavstvu Bosne i Hercegovine to krivično djelo obuhvaćeno „Računalnom sabotažom“. Naziv krivičnog djela „računalna sabotaža“ temelji se na Preporuci broj R (89) 9 o kompjuterskom kriminalu i konačnom izvještaju Evropskog komiteta u vezi problema sa kompjuterskim kriminalom, koji ukazuju nacionalnim zakonodavcima na vodeće principe u definiranju određenih krivičnih djela u vezi sa kompjuterskim kriminalom.[66] S obzirom da je Konvencija usvojena 2001. godine, odnosno punih 10 godina kasnije nakon što je Izvještaj objavljen, te da u Konvenciji nema krivičnog djela kompjuterske sabotaže, smatram da je naš zakonodavac trebao slijediti tekst prihvaćene Konvencije i umjesto naziva krivičnog djela „Računalna sabotaža“ istom odrediti naziv „Neovlašteno ometanje kompjuterskog sistema“, s tim da je tekst krivičnog djela u svom osnovnom značenju trebao glasiti „*Ko u namjeri da ozbiljno omete rad kompjuterskog sistema, neovlašteno unese, prenese, ošteti, obriše, izmijeni ili učini nedostupnim kompjuterski podatak kaznit će se.....*“

Što se tiče krivičnog djela iz člana 6. Konvencije „Zloupotrebe uređaja“, analizom teksta krivičnog djela iz člana 6. Konvencije u odnosu na krivično zakonodavstvo Bosne i Hercegovine, može se zaključiti da niti jedno krivično zakonodavstvo u Bosni i Hercegovini ne propisuje krivično djelo zloupotrebe uređaja na način kako je to predviđeno Konvencijom. Umjesto toga, određena vrsta pojavnog oblika ovog krivičnog djela koje je utvrđeno u Konvenciji može se pronaći u članu 393. stavu 5. KZ-a FBiH, odnosno u članu 411. stavu 4. KZ-a RS. Smatram da bi ovo krivično djelo trebalo biti posebno propisano u krivičnim zakonodavstvima Bosne i Hercegovine sa nazivom „Neovlaštena izrada sredstava radi izvršenja krivičnih djela protiv kompjuterskog sistema“, s tim da bi tekst zakona glasio:

[66] Za više vidjeti Kompjuterski kriminal i konačni izvještaj Evropskog komiteta u vezi problema sa kriminalom, Strasbourg 1990, dostupno na web adresi: http://www.oas.org/juridico/english/89-9&final%20Report.pdf (17.06.2019.)

„Ko radi izvršenja krivičnih djela iz člana 393., 394., 395., 396., 397. i 398. neovlašteno proizvodi, prodaje, nabavi radi upotrebe, uvozi, distribuira ili na drugi način učini dostupnim sredstvo, kompjuterski program, lozinku ili kod za pristup dijelu ili kompletnom kompjuterskom sistemu, kaznit će se.....“

U pogledu krivičnih djela iz člana 7. i 8. Konvencije, krivično zakonodavstvo Bosne i Hercegovine je obuhvatilo ova krivična djela, s tim da su u KZ-u FBiH propisana sa istim nazivima, dok je u KZ-u RS propisano krivično djelo „Kompjuterske prevare“, a krivično djelo „Kompjuterskog krivotvorenja“ nije.

Što se tiče radnji izvršenja krivičnih djela u vezi kompjuterskih sistema koje su propisane entitetskim krivičnim zakonima, među njima ima sličnosti ali i značajnih različitosti. Različitosti postoje i u pogledu propisanih krivičnopravnih sankcija. Također, pitanje protupravnosti, odnosno neovlaštenog pristupa za neka krivična djela uopšte nije ni propisana, iako je to Konvencijom traženo. Primjera radi, u KZ-u FBiH kod krivičnog djela „Kompjuterske prevare“ traži se „neovlašten unos“, dok u KZ-u RS „neovlaštenost“ uopšte nije potrebna. Dovoljno je samo da je unesen netačan podatak ili propušteno unošenje tačnog podataka u određenu svrhu koja je vezana za finansijsku ili drugu korist, odnosno prouzrokovanje štete, pa da krivično djelo bude učinjeno.[67] Ukoliko je unesen netačan podatak ili je propušteno unošenje tačnog podatka, a ne postoji nikakva finansijska motivacija, neće ni postojati ovo krivično djelo jer nije propisana odgovornost za nehatno činjenje ovog krivičnog djela, što je i logično jer se svima koji rade i unose podatak može desiti propuštanje zbog drugih razloga koji se, primjera radi, mogu odnositi na odsutnost koncentracije ili na neke druge životne probleme, što u konačnici rezultira propuštanjem unosa podataka ili unošenjem u kompjuterski sistem netačnih podataka.

Što se tiče krivičnopravnih odredaba KZ-a BD[68], a u kontekstu krivičnih djela usmjerenih protiv kompjuterskih sistema, rješenja sadržana u KZ-u BD identična su rješenjima iz KZ-a FBiH. U odnosu na krivičnopravne sankcije, KZ FBiH, KZ RS i KZ BD propisuju kazne zatvora i novčane kazne za krivična djela usmjerena protiv kompjuterskih sistema.

Izvršilac krivičnih djela, koja su sadržana u glavi XXXII KZ-a FBiH, može biti bilo koja osoba, odnosno radi se o *delicta communia*, što znači da ovo krivično djelo mogu uraditi i pravne osobe. Na ovaj način uvrštene su odredbe Konvencije kojima se traži kriminalizacija postupanja pravnih osoba.[69]

---

[67] Za više vidjeti odredbe člana 410. Krivičnog zakonika Republike Srpske, „Službeni glasnik Republike Srpske“, broj: 64/17 od 13.07.2017. godine.
[68] Za više vidjeti odredbe od člana 387. do člana 392. KZ-a BD, dostupno na web adresi: https://skupstinabd.ba/3-zakon/ba/Krivic--ni%20zakon%20Brc--ko%20Distrikta%20BiH/000%2033-13%20Krivic--ni%20zakon,%20prec--is--c-en%20tekst.pdf (18.06.2019.)
[69] Za više vidjeti član 12. Konvencije.

Ipak, kada se dublje analiziraju krivičnopravne odredbe u kontekstu radnji izvršenja, doći će se do zaključka da su izvršioci ovih krivičnih djela, u pravilu, osobe koje raspolažu određenim stručnim znanjima iz oblasti kompjuterske tehnologije.[70] Ovo je vrlo važno naglasiti jer je prilikom postavljanja istrage i naređivanja ovlaštenim službenim licima da poduzmu konkretne radnje, veoma bitno da se na početku suzi krug potencijalnih izvršilaca radi efikasnosti istrage i trošenja dostupnih resursa. Također, treba imati u vidu da je prilikom planiranja istražnih radnji u pogledu dokazivanja krivičnog djela, odnosno prikupljanja dokaza, neophodno imati vještaka ili stručna lica koja imaju stručna znanja iz oblasti informacionih tehnologija, koja bi svojim znanjem mogla ukazati gdje se nalaze dokazi ili koja su sredstva i na koji način korištena kako bi se izvršilo neko od krivičnih djela propisanih u glavi XXXII KZ-a FBiH.

Za krivična djela koja su usmjerena protiv kompjuterskih sistema propisane su zatvorske i novčane kazne. Najduža zatvorska kazna propisana je za krivično djelo „Računalne prijevare" i iznosi 12 godina, s tim da je ona uslovljena pribavljanjem protupravne imovinske koristi koja prelazi 50.000 KM. S druge strane, interesantno je da je zakonodavac kod krivičnog djela „Računalne sabotaže" postavio objektivni uslov inkriminacije, odnosno potrebno je da postoji šteta koja prelazi iznos od 500.00 KM. Propisana kazna zatvora za ovo krivično djelo je u rasponu od jedne do osam godina. Kada se analizira ovo krivično djelo u pogledu kazne, doći ćemo do zaključka da izvršilac ovog krivičnog djela neće odgovarati ako je pričinio štetu do 500.00 KM. Međutim, ako je počinio štetu 500.01 KM, onda učioniocu ovog krivičnog djela prijeti kazna zatvora do osam godina zatvora. Stiče se utisak da zakonodavac nije vodio računa o rasponu kazne jer je ostavio beznačajnu razliku u novčanom iznosu u odnosu na pričinjenu štetu i poduzimanje krivičnog gonjenja. Primjera radi, izvršilac ovog krivičnog djela može biti osuđen na osam godina zatvora ako je svojom radnjom pričinio štetu u iznosu od 500.01 KM, a ako je pričinio štetu 500.00 KM neće biti krivično gonjen?!? Smatram da se kazneni okvir trebao prilagoditi šteti, čime bi kazna za osnovni oblik izvršenja ovog krivičnog djela u stavu 1. za pričinjenu štetu do 5.000,00 KM bila kazna zatvora do jedne godine i novčana kazna do 10.000,00 KM, u stavu 2. od dvije do pet godina ako je učinjena šteta veća od 5.000,00 KM i u stavu 3. ako učinjena šteta prelazi 50.000,00 KM učinilac će se kazniti najmanje tri godine.

Suprotno ovome, postojeći kaznenopravni okvir upućuje na zaključak da je on postavljen paušalno, bez ozbiljne analize između uslova za poduzimanje krivičnog gonjenja i kazni za pričinjenu štetu, što u konačnici dovodi do toga da sudovi putem sudske prakse grade kaznenu politiku koja je, sudeći po trenutnom stanju stvari, blaga i nije polučila očekivane rezultate u pogledu svrhe kažnjavanja, što proizilazi iz sadržaja dokumenta „Struktura

[70] Tomić. Z., op. cit. str. 399.

kriminala“ 2018. godina, kojeg je objavilo Visoko sudsko i tužilačko vijeće Bosne i Hercegovine.[71]

Uvidom u izvještaj Visokog sudskog i tužilačkog vijeća koji sadrži strukturu krivičnih djela, može se zaključiti da Bosna i Hercegovina ima relativno mali broj predmeta koji se odnose na krivična djela usmjerena protiv kompjuterskih sistema. Tako je u periodu 2018. godine, broj primljenih krivičnih prijava za krivična djela iz glave XXXII KZ-a FBiH iznosio 18. Od toga, osam prijava se odnosilo na krivično djelo iz člana 395. „Računalna prevara“, dvije prijave su se odnosile na krivično djelo iz člana 396. „Ometanja rada sistema i mreže elektronske obrade podataka“ i osam prijava se odnosilo na krivično djelo iz člana 397. „Neovlašteni pristup zaštićenom sistemu i mreži elektronske obrade podataka“. Što se tiče podignutih optužnica u 2018. godini, tužilaštva u Federaciji Bosne i Hercegovine podigla su ukupno sedam optužnica od kojih je samo 4 potvrđeno, prema dostupnim podacima. Optužnice su podignute za krivična djela „Računalne prevare“ (četiri optužnice), „Neovlašteni pristup zaštićenom sistemu i mreži elektronske obrade podataka“ (dvije optužnice) i jedna optužnica za „Oštećenje kompjuterskih podataka i programa“. U konačnici, donesene su dvije presude za krivična djela „Kompjuterske prevare“ i jedna presuda za krivično djelo „Neovlašteni pristup zaštićenom sistemu i mreži elektronske obrade podataka“. Kazne koje su izrečene za ova krivična djela su **uslovne kazne**.[72] U 2017. godini donesene su tri presude sa izrečenim **uslovnim kaznama.**

Kao što je već prethodno pomenuto, analizom sadržaja krivičnopravnih normi kojima se štite kompjuterski sistemi, u krivičnim zakonodavstvima Bosne i Hercegovine može se zaključiti da je Bosna i Hercegovina dijelom ispunila preuzete obaveze iz Konvencije, kao i obaveze iz Dopunskog protokola, s tim da niti jedan od entitetskih krivičnih zakona, kao ni Krivični zakon Brčko Distrikta, nije definisao šta se smatra: kompjuterskim sistemom[73], kompjuterskim podatkom[74] ili davaocem usluge, rasističkim ili ksenofobskim materijalom, ili pak dječijom pornografijom.

Razrađujući analitički krivičnopravne odredbe koje su sadržane u Krivičnom zakonu Federacije Bosne i Hercegovine od člana 393. do člana 398., koje se odnose na krivična djela

[71] Sadržaj je dostupan na web adresi: https://vstv.pravosudje.ba/vstv/faces/kategorije.jsp?ins=141&modul=1198&kat=1363&kolona=114475 (18.06.2019.)
[72] Za više vidjeti: https://vstv.pravosudje.ba/vstv/faces/kategorije.jsp?ins=141&modul=1198&kat=1363&kolona=114475 (20.06.2019.)
[73] Zakon o krivičnom postupku Bosne i Hercegovine („Službeni glasnik Bosne i Hercegovine“ broj 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, 93/09, 72/13 i 65/18) u članu 20. stavu 1. tački u) definiše pojam kompjuterski sistem, ali samo za potrebe Zakona o krivičnom postupku koiji se dijelom podudara sa definicijom kompjuterskog sistema koja je data u Konvenciji.
[74] KZ RS pod pokretnom stvari podrazumijeva i kompjuterski podatak ili program. Za više vidjeti član 123. stav 1. tačku 18.

vezana za kompjuterske sisteme, dolazi se do zaključka da su one dijelom neodređene što može kod tužilaca izazvati dvojbe u pogledu poduzimanja krivičnog gonjenja, a samim tim i do arbitrarnosti u postupanju, u smislu da će za istu radnju jedno tužilaštvo poduzeti krivično gonjenje jer smatra da je to „organ vlasti od značaja", a drugo tužilaštvo neće smatrati da se ne radi o „organu vlasti od značaja" ili nisu „prouzrokovane teške posljedice", pa samim tim nema ni krivičnog djela.

U pravcu neodređenosti krivičnog djela skrenut će se pažnja na tekst odredbe koji je sadržan u članu 398. (Kompjuterska sabotaža): „*znatno omete postupak elektronske obrade podataka značajnim organima vlasti*". Smatram da krivičnopravna radnja nije jasno određena, odnosno u suprotnosti je sa načelom *lex certa*. Postavlja se pitanje šta znači *značajnim organima vlasti*? Koji su to organi vlasti značajni a koji nisu? Možda je zakonodavac htio propisati *od značaja za organ vlasti*. Dalje, zašto značajan ili od značaja, šta bi bio standard za utvrđivanje značaja, odnosno na osnovu čega bi se utvrdio taj „značaj". Slično je i sa pojmom „znatno" - koliko je „znatno" pa da bi se radilo o krivičnom djelu. Isto tako, u naslovu „Ometanja rada sistema i mreže elektronske obrade podataka" - kojeg sistema, kompjuterskog ili....? Dalje, u krivičnom djelu „Neovlašteni pristup zaštićenom sistemu i mreži elektronske obrade podataka" imamo radnju izvršenja neovlašteno uključivanje, a u naslovu krivičnog djela neovlašteni pristup?!?

Dakle, samo u članu 398. koji propisuje krivično djelo Računalne sabotaže postoji niz pitanja koja mogu stvoriti dvojbu ili već jesu u pogledu primjene ove krivičnopravne norme. Slično tome, u KZ-u FBiH nema definicije šta se smatra elektronskom obradom podataka, pa se postavlja pitanje kako se može ometati rad onoga čije značenje nije određeno krivičnim zakonodavstvom? Isto tako, u članu 397. stavu 1. KZ-a FBiH krivično djelo počinje *ko se neovlašteno uključi u sistem*? U koji sistem, kompjuterski ili sistem obrade podataka? Konvencija uopšte ne propisuje radnju uključivanja. Vjerovatno je zakonodavac mislio „*ko neovlašteno pristupi kompjuterskom sistemu*", ali to tako nije propisano.

Pomenute nejasnoće mogu imati uticaja na poduzimanje krivičnog gonjenja za krivična djela koja su usmjerena protiv kompjuterskih sistema, odnosno određene krivičnopravne radnje mogu ostati nekažnjene zbog kvaliteta teksta zakona. U pogledu kvalitete teksta zakona, Evropski sud za ljudska prava (u daljem tekstu: ESLJP), je kroz nekoliko svojih odluka naglasio da zakon mora biti dostupan, jasan i predvidljiv jer se na takav način sprečava rizik od njegove proizvoljne primjene.[75] U tom pravcu neophodno je da naš zakonodavac slijedi standarde koje je ESLJP utvrdio u svojim odlukama, kako bi naši zakoni ispunjavali standard kvalitete zakona.

[75] Za više vidjeti odluke ESLJP: Kennedy protiv Velike Britanije, stav 151; Rotaru protiv Romunije, stav 52; Amann proti Švajcarske, stav 50; Kruslin protiv Francuske, stav 27; Odluke su dostupne na web adresi: https://hudoc.echr.coe.int/eng# (20.06.2019.)

III. Zaključak

Analiza krivičnog zakonodavstva Bosne i Hercegovine ukazuje da krivično zakonodavstvo Bosne i Hercegovine pruža krivičnopravnu zaštitu kompjuterskim sistemima i sistemima elektronske obrade podataka kako bi se ostvarilo njihovo neometano korištenje od strane vlasnika ili ovlaštenog korisnika.

Također, naše krivično zakonodavstvo Bosne i Hercegovine kažnjava bilo koje lice koje koristi kompjutere kao sredstvo za izvršenje krivičnih djela: dječije pornografije, pranja novca terorizma i drugih krivičnih djela koja su povezana sa internet aktivnostima. Dakle, propisivanjem krivičnih djela kojima se štite kompjuterski sistemi i podaci stvoren je osnov za poduzimanje krivičnog gonjenja, s tim da efikasnost krivičnog gonjenja ovisi o mnogim uslovima, a prevashodno od jasnoće normi koje su sadržane u krivičnom djelu.

Sve ovo upućuje da Bosna i Hercegovina, kao država koja je na putu da se pridruži zajednici evropskih država, postepeno usklađuje svoje krivično zakonodavstvo sa obavezama koje je preuzela pristupajući multilateralnim ugovorima.

Ipak, analiza krivičnog zakonodavstva Bosne i Hercegovine u odnosu na Konvenciju je ukazala na nedovoljnu posvećenost osoba koje se bave usklađivanjem domaćeg krivičnog zakonodavstva sa međunarodno preuzetim obavezama.

S tim u vezi, postoji potreba da se naše entitetsko krivično zakonodavstvo, kao i krivično zakonodavstvo Brčko Distrikta Bosne i Hercegovine, dodatno uskladi i dopuni sa određenim krivičnim djelima i definicijama koja su propisane Konvencijom i Dodatnim protokolom, ali i određenim mjerama sigurnosti i pravnim posljedicama osude koje se pojavljuju kao nužna potreba, cijeneći ciljeve kriminalne politike.

Također, potrebno je da krivični zakoni u Bosni i Hercegovine usklade nazive sa nazivima krivičnih djela i propisanih radnji iz Konvencije. Primjera radi, da se propiše krivično djelo „*Neovlašteni pristup*“ koje je predviđeno članom 2. Konvencije, „*Neovlašteno presretanje*“ koje je predviđeno članom 3. Konvencije, da se krivično djelo propisano članom 393. KZ-a FBiH uskladi sa tekstom iz Konvencije i da nosi naziv „Oštećenje računalnih podataka“ umjesto „Oštećenje računalnih podataka i programa“ jer kompjuterski podatak obuhvaća kompjuterski program.

Također, potrebno je da se tekst i naziv krivičnog djela iz člana 398. KZ-a FBiH „Računalna sabotaža“ uskladi sa nazivom iz člana 5. Konvencije „Neovlašteno ometanje kompjuterskog sistema“ i da se tekst krivičnog djela uskladi sa tekstom iz Konvencije i preciznije odredi. Isto tako, potrebno je da se krivično djelo iz člana 6. Konvencije „Zloupotrebe uređaja“, posebno propiše u krivičnim zakonodavstvima Bosne i Hercegovine sa nazivom „Neovlaštena izrada sredstava radi izvršenja krivičnih djela protiv kompjuterskog sistema“.

U odnosu na mjere sigurnosti potrebno je da krivično zakonodavstvo u Bosni i Hercegovini propiše mjeru zabrane pristupa kompjuterskim sistema i internetu, kao i da se u posebnim zakonima propiše nastupanje pravnih posljedica osude za lica koja su osuđena za krivična djela protiv kompjuterskih sistema, kako se takva lica ne bi mogla zaposliti na pozicije IT administratora ili imati pristup kompjuterskim sistemima.

Neophodno je da krivično zakonodavstvo u Bosni i Hercegovini definiše pojmove kompjuterskog sistema, kompjuterskih podataka, davaoca usluge, prenosa kompjuterskih podataka i drugih pojmova koji su propisani Konvencijom.

I na kraju, potrebno je da tekst prevoda bilo koje konvencije, koju Bosna i Hercgovina ima namjeru potpisati ili potpiše kako bi istu mogla ugraditi u svoje zakonodavstvo, radi grupa koja se sastoji od iskusnih prevodilaca i pravnika iz oblasti na koju se konkretna konvencija odnosi. U suprotnom, imat ćemo pogrešno preveden i nerazumljiv tekst ili neprevedene dijelove teksta, kao što je to slučaj sa Konvencijom o kompjuterskom kriminalu, jer pogrešno preveden tekst ili nepotpuno preveden tekst može imati ozbiljne posljedice po zakonodavstvo jedne države kada koristi tekst konvencije kao podlogu za izradu zakona.

LITERATURA

- Komentari krivičnih/kaznenih zakona u Bosni i Hercegovini, Knjiga I, Zajednički projekat Vijeća Evrope i Evropske komisije, Sarajevo, 2005.
- Kokot. I., Kaznenopravna zaštita računalnih sustava, programa i podataka, Zagrebačka pravna revija Vol 3. br. 3., Pregledni znanstveni rad od 08. listopada 2014. godine.
- Lazarević. Lj., Komentar Krivičnog zakonika, drugo izmijenjeno i dopunjeno izdanje, Beograd 2011. godina;
- Tomić. Z., Krivično pravo II, Posebni dio, drugo izmijenjeno i dopunjeno izdanje, Pravni fakultet Univerziteta u Sarajevu, Sarajevo, 2007. godina;

ZAKONSKI I PODZAKONSKI OKVIR

- Krivični zakon Bosne i Hercegovine, „Službeni glasnik Bosne i Hercegovine“, br. 3/03, 32/03, 37/03, 54/04, 61/04, 30/05, 53/06, 55/06, 32/07,8/10, 47/14, 22/15, 40/15 i 35/18;
- Krivični zakon Federacije Bosne i Hercegovine, „Službene novine Federacije Bosne i Hercegovine“, br. 36/03, 37/03, 21/04, 69/04, 18/05, 42/10, 42/11, 59/14, 76/14, 46/16 i 75/17;
- Krivični zakonik Republike Srpske, „Službeni glasnik RS“, br. 64/17;
- Krivični zakon Brčko Distrikta, „Službeni glasnik Brčko Distrikta“, br. 33/13 prečišćeni tekst
- Zakon o krivičnom postupku Bosne i Hercegovine, „Službeni glasnik Bosne i Hercegovine“, 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, 93/09, 72/13 i 65/18;

MEĐUNARODNE KONVENCIJE, DOKUMENTI I ZAKONODAVNE ODLUKE EU

- Konvencija Vijeća Evrope o kibernetičkom kriminalu;
- Dodatni protokol Konvencije o kibernetičkom kriminalu, a u vezi sa kažnjavanjem djela rasističke i ksenofobične prirode učinjenih putem kompjuterskih sistema;
- Izvještaj s obrazloženjem Konvencije o kibernetičkom kriminalu;
- Kompjuterski kriminal i konačni izvještaj Evropskog komiteta u vezi problema sa kriminalom, Strasbourg 1990;
- Direktiva Evropskog parlamenta i Vijeća o napadima na informacijske sisteme i o zamjeni Okvirne odluke Vijeća 2005/222/PUP

WEB STRANICE

- https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=dOsJKORQ
- https://europa.eu/european-union/eu-law/legal-acts_hr
- https://ec.europa.eu/info/law/law-making-process/types-eu-law_hr#primarno-zakonodavstvo-u-odnosu-na-sekundarno-zakonodavstvo
- https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=celex%3A32013L0040
- https://hrcak.srce.hr/file/209347
- https://rm.coe.int/16800cce5b
- http://www.oas.org/juridico/english/89-9&final%20Report.pdf
- https://skupstinabd.ba/3-zakon/ba/Krivic--ni%20zakon%20Brc--ko%20Distrikta%20BiH/000%2033-13%20Krivic--ni%20zakon,%20prec--is--cen%20tekst.pdf
- https://vstv.pravosudje.ba/vstv/faces/kategorije.jsp?ins=141&modul=1198&kat=1363&kolona=114475
- https://hudoc.echr.coe.int/eng#

Kriminalističke teme
Zbornik radova
Godina XIX, Broj 5, 2019.
ISSN 1512-5505

Panel 2

RASVJETLJAVANJE I RASPETLJAVANJE CYBER SIGURNOSTI: DARKWEB, DARKNET I DEEPWEB

Kriminalističke teme
Zbornik radova
Godina XIX, Broj 5, 2019.
ISSN 1512-5505

ILEGALNE AKTIVNOSTI U NEVIDLJIVOM WEB-u
ILLEGAL ACTIVITIES IN THE INVISIBLE WEB

Pregledni naučni rad

spec.krim. Marjanović Marjan[76]

Sažetak

Inspiracija za rad: Uloga hakera u vršenju ilegalnih aktivnosti pod okriljem nevidljivog dijela World Wide Web-a podstakla je autora na promišljanje o povezanosti ovih specifičnih delikvenata sa skrivenim oblastima savremene informatičke sfere.
Ciljevi rada: Autor svoja razmišljanja posvećuje ustanovljavanju veze, koju hakeri sasvim moguće imaju sa potencijalnim mogućnostima okruženja Deep Web-a.
Metodologija/dizajn: Analiza pojmova *haker* i *nevidljivi Web*, kroz njihovu fenomenološku uzajamnost, opredijelila je metodološki napore autora u svom istraživanju.
Ograničenja rada/istraživanja: Ograničenja u prikazivanju potpune slike temeljnih pojmova u ovom radu mogu predstavljati njihovi tekući vidovi ispoljavanja, koje autor zbog tehničke nemogućnosti sagledavanja cjelokupnog varijetata njihovih pojavnih oblika nije bio u mogućnosti da predstavi.
Rezultati: Veza hakera sa Deep Web-om, kako smatra autor, postoji u brojnim oblicima kriminalnih aktivnosti, od kojih će u radu biti akcentovani neki od hakerskih napada i terorizam.
Generalni zaključak: Nevidljivi deo Web-a, a posebno njegova tamna zona tzv. Darknet, čine naročitu pogodnost za djelovanje hakera *ante delictum*, kao i *post delictum*, čineći istovremeno optimalno informatičko okruženje za razmjenu podataka koji vode ka pripremanju ilegalne aktivnosti, baš kao i ka kapitalizovanju štete nastale hakerskim napadom.
Opravdanost istraživanja/rada: Ukazivanjem na postojanje veze hakera sa skrivenim dijelom World Wide Weba, autor nastoji da utiče na pojačavanje opreza i unapređivanje zaštite od hakerskih napada određivanjem preventivnog postupanja, koje svaki korisnik savremene globalne komunikacije može upotrijebiti na ličnom planu u razmjeni podataka putem Interneta.

Ključne riječi

haker, hakerski napad, Internet, terorizam, Deep Web, Dark Web

Summary

Reason for writing and research problem (s): The very role of hackers while dealing with illegal activities within surroundings of the invisible part of the World Wide Web motivated the author to analyze relations between this special kind of offenders and hidden areas of modern informatics sphere.

[76] Institut za procjenu rizika i kritičnu infrastrukturu, Podgorica, Crna Gora, marjan.marjanovic@iprki.me, marjan@securityguardmn.com

Aims of the paper (scientific and/or social): The author focused his attention to establishing of link that, very possible, connects hackers to the potential opportunities of the Deep Web zone.
Methodology/Design: Analyze of terms *hacker* and *invisible Web*, done through their phenomenological mutuality, prevailed the author's methodological efforts in this research.
Research/Paper limitation: Actual forms of exposing basic terms in the paper are probable limitation to have them presented completely, because of technical lack of the author's capability to make the full-scaled overview of their existing modalities.
Results/Findings: According to the author's opinion, the link between hacker and the Deep Web exists in the various types of criminal activities having hackers' attacks and terrorism as highlighted in the paper.
General Conclusion: Invisible part of Web and its dark zone so-called the Darknet, especially, make specific suitability for hacker's activity *ante delictum*, just as *post delictum*, having at the same time optimal informatics surroundings enabled for the data exchanging as ground of illegal activities preparation and likewise of getting profit out of damage committed by hacker's attack.
Research/Paper Validity: By pointing out on existing of connection between hacker and hidden part of the World Wide Web, the author tends to get caution heightened and to enhance protection considering hackers' attacks by defining preventive proceedings that can come in handy in exchanging personal data of every user of Internet global communication network.

Keywords
hacker, hacker's attack, Internet, terrorism, the Deep Web, the Dark Web

UVOD

Opseg Interneta daleko premašuje njegov vidljiv površinski dio, koji mnogi od nas dnevno posjećuju u svojim, gotovo, rutinskim pretragama. Drugi njegovi segmenti sadržani su u ukupnosti informatičko-komunikativnih mogućnosti nevidljivog dijela World Wide Web-a, koji ostaje skriven za standardne pretraživače, kao što je Googl. Ovaj virtuelni prostor za razmjenu informacija, nezamislivih granica, nazivamo Deep Web i on predstavlja izraz želja i neophodnosti različitih društvenih individualnih i grupnih, kako resornih tako i vanresornih, subjekata za diskretnom razmjenom podataka. Ovaj duboki i nevidljivi Web, ogromnih razmjera i neuporedivo prostraniji od svog vidljivog i svima dostupnog antipoda, pored legitimne namjene može imati i svoju tamnu stranu oličenu u njegovom skrivenom dijelu poznatom kao Dark Web ili Darknet. Ovaj tamni i nedostupni dio Web-a ima sve predispozicije za kreiranje informatičkog okruženja podesnog za skrivenu komunikaciju između kriminalnih grupa i pojedinačnih nosilaca kriminalnih aktivnosti. Pomoću naročitih softvera, kao što je The Onion Router (TOR), korisnici tamnog dijela Web-a uz zametanje tragova svog prisustva korišćenjem velikog broja računara drugih korisnika, krstare informatičkim vodama Deep Web-a tražeći mogućnosti za svoje ilegalno djelovanje (Finklea, 2017). Sajtovi za pretraživanje u nevidljivom Web-u olakšavaju surfovanje kroz Darknet, nudeći kategorizovane sadržaje koji se odnose na ilegalni promet opojnim drogama, krijumčarenje i nezakonito pribavljanje vatrenog oružja, organizovanje

trgovine falsifikovanim proizvodima, obezbeđivanje krivotvorenog novca ili ličnih dokumenata.[77] Načini komunikacije u Deep Web-u odnosno Darknet-u odvijaju se kao i na površinskom dijelu Web-a, razmjenom poruka posredstvom TOR-a, upotrebom zaštićenih elektronskih adresa, pa čak i brže kroz četovanje. Informatički alat, poput TOR-a, čija svrha je obezbjeđivanje anonimnosti sadržaja i aktivnosti u okolnostima nevidljivog Web-a, služi istraživačima i stručnjacima iz oblasti bezbjednosti da konstanto razvijaju i unapređuju načine i sredstva za otkrivanje skrivenih servisa i pojedinaca, koji vrše kriminalne aktivnosti u Darknet-u, kao tamnom i skrovitom dijelu Deep Web-a.

Okruženje dubokog Web-a pogoduje širokoj skali legalnih i nedozvoljenih aktivnosti, od očuvanja privatnosti korisnika do trgovine ukradene robe, uz upotrebu virtuelne valute Bitcoin (Finklea, 2017). Servisi kojima se eksploatiše Deep Web služe izbjegavanju zabrana, pristupu nedozvoljenim sadržajima,[78] ali i zaštiti tajnosti osjetljive komunikacije ili poslovnih planova. Ipak, veliki broj zlonamjernih učesnika, od nosilaca klasične kriminalne aktivnosti do članova terorističkih ćelija, pojedinačnih terorista, subjekata obavještajne djelatnosti odnosno aktera industrijske špijunaže, uzrokovao je da se u tamnom Webu odvijaju forumi za konverzaciju, razmjenu podataka, dogovore, koordiniranje kriminalnih aktivnosti i samo izvršenje krivičnih djela.

Međutim, baš kao što delinkventska populacija može koristiti anonimno okruženje Deep Web-a, tako ono služi i potrebama organa krivičnog gonjenja, ali i vojnih i obavještajnih subjekata u svrhu obavljanja nadzora i kontrole. Naravno, ovakve opcije omogućuju i hakerima da izvode svoje napade radi obaranja sajtova, prekida komunikacije, neovlašćenog upadanja u zaštićene sisteme, korišćenja tuđih ličnih podataka, krađe identiteta, pristupa poslovnim podacima, preusmjeravanja legalnih i ilegalnih novčanih tokova i preduzimanja drugih aktivnosti na ugrožavanju sistema za komunikaciju i skladištenje podataka u uslovima nevidljivog Web-a i njegovog skrivenog segmenta Darknet-a.

HAKERI I NEVIDLJIVI WEB

Internet je danas prepun prijetnji po bezbjednost korisnika. Hakeri i virusi vrebaju pod maskama raznovrsnih reklama i obavještenja čijim pregledom se aktiviraju hakerski upadi. Otvaranjem takvog sadržaja lozinka korisnika, istorija njegovih pretraga, elektronske poruke, ali i neke lične sklonosti i interesovanja, dolaze u ruke anonimnih delikvenata koji se nalaze bilo gdje u svijetu (Omand, 2016). Nakon toga dragocjeni podaci bivaju zlonamjerno prodati ili razmijenjeni u nevidljivom Web-u. Višestruko veći od površinskog Web-a koji je izraz uobičajene predstave redovnog korisnika Interneta, skriveni Web je informatičko okruženje koje okuplja sve one kojima je neophodna anonimnost. Pristupom preko TOR-a, koji se može besplatno preuzeti, omogućeno je kretanje kroz brojne serverske mreže koje su interkontinentalno rasprostranjene. U tamnom dijelu nevidljivog

[77] Kao što je npr. „Hidden Wiki".
[78] Ovde se misli na iskorišćavanje djece u pornografske svrhe.

Web-a, zvanom Darknet, zainteresovani korisnik pronaći će sadržaje kojima nije moguće neopaženo pristupiti u vidljivom Web-u, a koji se odnose na ilegalnu trgovinu oružjem, dječju pornografiju, ilegalnu ponudu opojnih droga, kompjuterske viruse, ukradene kreditne kartice, filmsku i muzičku pirateriju, uz mogućnost anonimnog plaćanja nabavke navedenog digitalnim novcem.

Prvi hakeri bili su srednjoškolci i studenti, koji su svoj informatički talenat usmjerili na zbijanje šala sa računarski povezanim sistemima.[79] Problem je uzrokovan činjenicom da se gotovo svaki sistem, od banke i bolnice do kritične infrastrukture, odjednom digitalizovao. Ovo je doprinijelo mogućnosti lake zarade i velikog profita za hakere (Pagliery, 2015). Njihova aktivnost postala je ilegalna, ali ih to nije sprečavalo da neovlašćeno preuzimaju, koriste i prodaju podatke. Što je više subjekata i informacija bilo povezano putem Interneta, rasle su mogućnosti i informatički volumen nevidljivog Web-a i njegovih hakerskih korisnika.

Pojam haker prati podrazumijevajuće loša konotacija, ali nemaju svi hakeri loše namjere u svojim postupanjima. Zapravo, neki autori smatraju da postoji hakerska etika čiji parametri prate nivo bunta protiv tehnološke dominacije u jednom društvu (Martin i Newhall, 2016). Haker može biti svako ko posjeduje znanje i vještine da putem informatičkog programa izbjegava bezbjednosne mjere koje štite lični računar, tehnički uređaj ili računarsku mrežu. Hakerski upad u računarski sistem ili sam računar je ilegalan čin, izuzev ako nije učinjen uz pristanak vlasnika. Šta je to što potiče hakera da prodre u nečiji računar i otuđi ili uništi lične podatke ili čak preusmjeri tuđa finansijska sredstva? „Thycotic“, softverska kompanija koja je specijalizovana za zaštitu pristupnih lozinki, sprovela je istraživanje u kome je postavljeno pitanje američkoj hakerskoj grupi „Black Hat“ zašto čine ovakve zlonamjerne akte.[80] Tom prilikom je 51% hakera izjavilo da ih neovlašćeni upadi u tuđe zaštićene sisteme uzbuđuje i zabavlja, njih 19% u svojim odgovorima bilo je opredijeljeno za finansijsku dobit kao smisao hakerisanja, etičkim razlozima rukovodilo se 29% ispitanika, a preostalih 1% imalo je želju da budu ozloglašeni (Williams, 2015).

Hakere možemo klasifikovati u tri grupe. Kompanija za tehnološku bezbjednost „Norton Security“, svaku od grupa simbolično je predstavila šeširom određene boje. Tako se razlikuju „bijeli“, „sivi“ i „crni šeširi“, kao tri esencijalno različite grupe hakera. Ovi nazivi potiču od crnih šešira koje su u filmovima o Divljem Zapadu nosili tzv. „loši momci“, dok su šešire bijele boje nosili oni koji su poštovali zakon. Termin „sivi šešir“ odnosio bi se na sve one hakere koji se ne mogu svrstati kategorično na navedene opozitne strane. Inače, hakeri su označeni na pomenuti način prema razlozima koji ih pokreću u njihovim postupanjima, kao i u odnosu na to da li su njihovi akti nezakoniti (Kovacs, 2015). „Bijeli šeširi“ koriste svoje znanje u oblasti informatičke tehnologije isključivo u dobre svrhe. Često ih nazivaju „etičkim hakerima“ jer ih kompanije plaćaju radi rešavanja problema i ojačavanja mjera bezbjednosti u svrhu zaštite programa, koje koriste u svom radu (Kovacs, 2015).

[79] Tako je jedan od prvih računarskih virusa načinio diplomac američkog Univerziteta Cornell.
[80] Bilo je ispitano 127 osoba.

Primjer ove vrste hakerisanja je program sa nazivom „HP Tipping Point“, koji je pokrenut 2005. godine radi detektovanja manjkavosti u sistemu zaštite Interneta. Neki autori navode da je ovakav „lovački“ program podešen da prima preporuke za prevenciju upada u sistem (Zetter, 2013). U tom smislu, nedostaci u zaštiti sistema pogodni su za korigovanje, na koje „bijeli hakeri“ ukazuju programerima konkretne kompanije. „Sivi šeširi“ su posvećeni traženju propusta u zaštiti sistema i njegova ranjivost služi im za zabavu. Kada jednom otkriju „rupu u brani“ ova vrsta hakera će učiniti dvije stvari: obavijestiće kompaniju ili pojedinca o postojećoj slabosti što će naplatiti manjim novčanim iznosom radi otklanjanja nedostatka ili će o ovakvom problemu obavijestiti javnost putem Interneta (Kovacs, 2015). Na prikazani način francuske komanije „Vupen“ i „Zerodium“, koje su specijalizovane za otkrivanje propusta u on-line bezbjednosti (Zetter, 2016), uspješno su detektovale dvije slabosti u Crome's Pwn2Own zaštitnom programu i pomogle rešavanje ovog problema (Zetter, 2012). „Crni šeširi“ su najopasnija vrsta hakera. Ovi hakeri su, također, vrlo vješti u upadima u računarske mreže jer umiju da naprave zlonamjerne programe (malware) putem kojih ostvaruju pristup u mrežne informatičke sisteme (Kovacs, 2015). Postoji veliki broj hakerskih grupa „crnih šešira“ u svijetu, koji neprestano izvode nedozvoljena hakerska postupanja. Jedna od najpoznatijih su „Anonymous“ koji operišu kroz pojedinačne akcije kojima se drugi pridružuju, te tako udruženi postižu uspjeh (Norton, 2012).

Veliki je broj preduzetih istraživanja psihološke pozadine hakerske motivisanosti za potčinjavanjem sistema. Prema riječima jednog od rukovodilaca u kompaniji „Thycotic“,[81] otkrivanje razloga zašto je neko zainteresovan za krađu podataka ili hakovanje sistema je vrhunski prioritet u obezbjeđivanju zaštite pristupa tajnim dokumentima. Zaštita informacija je uvek od najveće važnosti, obzirom da terorističke grupe ulažu stalne napore kako bi izvršile upade u mrežne sisteme i uništile ili neovlašćeno preuzele povjerljive informacije.

Dakle, možemo zaključiti da nevidljivi Web ima dvostruku ulogu u odnosu na hakersku aktivnost. Najprije, pruža mogućnosti za njihovo djelovanje uz postojanje svojih tamnih zona oličenih u Darknetu, kao garanciji anonimnosti i skrivenosti prisutnih korisnika. Zatim, obezbjeđuje utočište i zametanje tragova brojnim nosiocima kriminalnih aktivnosti u cyber okruženju, između kojih i hakerima. S druge strane, hakeri koriste neslućene razmjere Deep Web-a, pogotovo njegovog tamnog dijela Darkneta, kako bi svoje napade izvodili kako na ciljeve površinskog Weba, tako i na određene mete iz kriminalnog miljea dubokog Weba. Tako se, naprimjer, preusmjeravanje finansijskih sredstava može vršiti i sa skrivenih računa članova organizovanih kriminalnih grupa, ali se mogu blokirati i cyber aktivnosti terorističkih ćelija, te ometati njihova diskretna komunikacija i vođenje poslova, kojima se finansiraju.

[81] Riječ je o ekspertu po imenu Jonathan Cogley.

ZNAČAJ TAMNOG WEB-a

Dark Web je informatički prostor u kome se odvija najviše on-line kriminalnih aktivnosti i nalazi se daleko van efektivnog domašaja organa krivičnog gonjenja. Anonimnost je pravilo za postupanje i kretanje u okruženju tamnog Web-a, a identitet i pozicija korisnika skriveni su i od najupornijih nastojanja policije i obaveštajnih agencija (Omand, 2016).

Darknet funkcioniše prema različitim kriterijumima u odnosu na ostale djelove Interneta. Uobičajeno je da korisnik upotrebljava pretraživač kao što je Google, koji omogućuje pristup traženoj adresi na Web-u. Željena destinacija biće dostignuta jer je sadržaj na vidljivom površinskom Web-u indeksirana, zbog čega je pretraživački programi mogu automatizovano eksploatisati i održavati neprestano sakupljajući i klasifikujući podatke. Ovo olakšava globalni Domain Name sistem, koji pojednostavjuje registrovanje Web adrese u jedinstveni 32-bitni, a u današnje vrijeme i 128-bitni digitalni numerički zapis, u smislu Internet protokola odnosno IP adrese, kako bi usmjerio server da uputi korisnički zahtjev na odgovarajući sajt. Ipak, ovaj površinski Web je samo mali dio Interneta, čak 500 puta manji od njegove ukupnosti. Preostali dio, tzv. duboki Web, nije dostupan redovnom korisničkom protokolu jer mu nije ni namijenjen.

Moglo bi se napraviti poređenje nevidljivog segmenta Interneta sa dijelom grada u kome se nalaze poslovne kompanije, istraživačke laboratorije i vladine agencije, kojima prosječan građanin nije ovlašćen da pristupi. Očigledno je da to može da učini samo određena osoba uz posebnu propusnicu (Omand, 2016). Prateći dalje naš zamišljeni grad, Darknet bi predstavljao kvart „crvenih fenjera“ sa veoma malim brojem zgrada, koje bi inače bilo teško pronaći, jer skriveni operateri ne žele da eksponiraju aktivnosti koje se odvijaju u „zgradama“. U nekom trenutku, ovde se mogu pronaći noćni klubovi, kockarnice, narkomanska svratišta ili bordeli, ali i mjesta okupljanja siromašnih mladih slikara i pisaca, radikalnih političara i disidenata (Omand, 2016). Zbog navedenog, može se zaključiti da je tamni Web ukupnost sajtova koji mogu biti dostupni i vidljivi smo onim korisnicima koji baš njih i traže, naravno pod određenim uslovima zaštite bezbjednosti operatera sajtova i njihovih posjetilaca. Jaka enkripcija i protokoli koji garantuju anonimnost obezbjeđuju skrivenost IP adresa servera pokretača sajtova Darkneta, tako da se ne može utvrditi ko ih posjećuje čak i kada bi ovi sajtovi bili locirani i stavljeni pod prismotru.

Početnim istraživanjima ustanovljeno je da Deep Web, time i Darknet, predstavlja najveći izvor svježih informacija na Internetu. Sajtovi koji ih sadrže, po prirodi, su malog obima ali kompleksne dubine, u poređenju sa regularnim sajtovima površinskog Web-a. Paradoksalno, ali istinito, zaštićenost sadržaja sajtova tamnog Web-a doprinosi njihovom većem kvalitetu i vrijednosti od onih u vidljivoj zoni Interneta. Više od polovine sadržaja nevidljivog Web-a smješteno je u naročite direktorijume, kao što je www.thehiddenwiki.net, što ih čini dostupnijim i preciznijim odredištima pretrage (Sui, Caverlee i Rudesill, 2015).

Zbog svega navedenog, Darknet je izuzetno nekontrolisan dio Interneta. U okruženju tamnog Web-a anonimnost je primarna karika u protokolarnom lancu ostvarivanja pristupa, kako bi se operateri i ostali korisnici osigurali da ničije pretraživanje Darkneta ne bude praćeno od strane policije ili nekog drugog bezbjednosnog subjekta (Omand, 2016).

HAKERSKI NAPADI I TERORIZAM

Terorizam je akt upotrebe sile i prijetnje radi zastrašivanja i prisile. Godinama smo svedoci terorističke prijetnje na svjetskom planu, koja se neprestano razvija. U poslednje vrijeme, sa tehnološkim napretkom, ova prijetnja postala je još prisutnija i destruktivnija.

Internet je postao neodvojivi dio svakodnevnog života u gotovo svakom kutku naše planete, što je pogodovalo prijetnji sajber terorizma da dostigne viši nivo nego ikada. Terorističke grupe poput ISIS-a i Al-Qaeda, sada, imaju mogućnost prikrivanja u debelim sjenkama digitalnog svijeta Darkneta i koriste enkriptovane poruke za širenje ekstremizma. Tamni Web nudi ovim radikalnim grupama nevidljivi prostor za regrutovanje i radikalizaciju, širenje propagande, uvećavanje finansijskih sredstava i koordiniranje akcija i napada (Weimann, 2016).

Na hiljade foruma i soba za četovanje, kako na površinskom tako i u tamnom Web-u, dostupno je potencijalnim sledbenicima radikalne i ekstremističke ideologije da stupe u kontakt i komuniciraju sa terorističkim ćelijama, te razmjenjuju sa njima podatke uz potpuno skrivanje svog identiteta. Još 2001. godine, Al Qaeda je svoj prvi forum plasirala na Internetu, koji jeste bio uklonjen, ali je pregršt drugih sajtova nasilih i ekstremnih islamista nastavilo da postoji čak i u vidljivom Web-u uz kontakte visoke frenkventnosti (Cox, 2015). Ova mjesta za on-line susrete nije moguće detektovati, niti im pristupiti sa globalnog korisničkog nivoa, zbog čega se mogu posmatrati kao virtuelna zona islamskih ekstremista. Kako bi što više širile svoje poruke i regrutovale nove sledbenike, terorističke grupe promovišu upotrebu ovakvih enkriptovanih i anonimnih sajtova. Naprimjer, ISIS-ov medijski predstavnik sa nazivom Al-Hayat Media Center postavio je link i smjernice za pristup novom sajtu u Dark Web-u (Weimann, 2016).

Inače, terorističke organizacije koriste tamni Web kao informatički prostor u kome skrivaju svoje finansije, uvećavaju zaradu, vrše novčane transfere, ilegalno nabavljaju eksplozivna sredstva i oružje, pri čemu koriste virtuelni novac (Weimann, 2016). Obzirom da se može transferisati bez mogućnosti praćenja tokova transfera, Bitcoin je kao izmišljena valuta postao neka vrsta terorističke monete. Terorističke grupe ostvaruju prihode, iz kojih finansiraju napade, putem donacija od simpatizera ili prodajom ukradene robe. Dark Web podstiče rast i razvoj terorizma i to od malih grupa, koje djeluju na određenoj geografskoj lokaciji, do globalne prijetnje. Sa svakodnevnim tehnološkim progresom, prijetnja terorizma se sve više širi i uvećava bez obzira na napore vlada u svijetu da održe korak u ovoj borbi sa nevidljivim protivnikom.

Povezanost hakera sa terorizmom dolazi od mogućnosti da u tamnom Web-u hakeri prodaju kodove za pristup određenim osjetljivim sistemima,[82] nudeći ih onome ko najviše ponudi na kriminalnom tržištu. Kupci mogu biti terorističke grupe, pojedini ekstremisti, diktatorski režimi, državne obaveštajne službe, organizovane kriminalne grupe, kao i sajber ratnici[83] (LeFrancois i sar., 2018). Primjer za ovakvu vezu hakerskih napada i terorizma upravo je prodavanje koda „Zero-day".

Kod „Zero-day" odnosi se na ranjive softvere odnosno one sa nedostacima, koji su zbog toga pogodni za eksploatisanje ili napadanje uz upotrebu zloćudnih kodova radi plasiranja virusa, trojanaca odnosno drugih malware-a. Naziv „Zero-day" potiče od broja dana u kojem vremenskom periodu je otkrivena slabost softvera od strane njegovog tvorca ili prodavca. Obzirom da su osjetljive tačke u ovakvim slučajevima nepoznate autorima i prodavcima softvera, oni su veoma opasni po računarske sisteme jer sistemi zaštite od malware-a prilikom ažuriranja nisu u mogućnosti da ustanove propust i da detektuju prostor za hakerski napad kroz taj propust. Ovo je razlog zašto je „Zero-day" kod dragocjen za hakere dajući im prilike za izvođenje napada, ali istovremeno i rijedak da se pribavi (Zetter, 2014).

Hakeri su uvijek korak ispred u traženju opcija za napade na Web-u. Tako su u prilici da pronađu ovu vrstu koda, koja ukazuje na postojanje rupa u zaštitnoj strukturi softvera. Kada hakeri otkriju propust u softveru, sačine kod za probijanje zaštite, posle čega odlučuju šta će da učine sa tim podacima i kodom. Dok neki od njih o ovome obavještavaju prodavce softvera, drugi pronađeno prodaju bilo kome, od organizovanih kriminalnih grupa do zloglasnih pojedinaca koji vode diktatorske režime (Goodman, 2016).

Velikim tržištem za pronalaženje propusta u softverima upravljaju obavještajne službe jer su ovakvi kodovi izuzetno vrijedni, ne samo „crnim hakerima" već i državnim obavještajnim subjektima, kao i onim sajber ratnicima koji su resorno angažovani[84] (Greenberg, 2015). Primjera radi, u Sjedinjenim Američkim Državama, National Security Agency (NSA) je zbog velikog broja „Zero-day" propusta u programima bila prinuđena da ih detektuje i popravi do nivoa na kome ova ranjivost više nije ugrožavala američku nacionalnu bezbjednost (Greenberg, 2015). Naravno, postojeća prijetnja od terorističkih napada samo je pojačala ovu budnost vladinog sektora na međunarodnom planu.

[82] Kao što su to sistemi javnog transporta, koji podrazumijevaju drumski, železnički, vodni i vazdušni saobraćaj.
[83] Grupni naziv za individualne korisnike Interneta, koji svojim napadima nanose štetu ostalim korisnicima uz široku lepezu motivacije za ovakvo zlonamjerno postupanje na World Wide Web-u.
[84] Poput onih koje angažuju američke National Security Agency (NSA) i Cyber Command.

MOGUĆNOST ZAŠTITE OD SAJBER NAPADA

Hakerski napadi postaju sve češći i uobičajeniji jer ih olakšava činjenica da je sve više uređaja uvezano u informatičkom prostoru, koji neki autori nazivaju „Internetom stvari" (Thielman i Hunt, 2016). Malware-i mogu ugroziti svaki od umreženih uređaja, od aparata za kafu do frižidera, a da mjere zaštite zataje zbog nedovoljne brzine u odgovoru na prijetnju (Thielman i Hunt, 2016).

Poznavanje specifične opasnosti hakerskih napada i upućenost u brojne modalitete njihovih prijetnji, nisu dovoljni za formiranje konačnog odgovora na pitanje: „Kako da riješimo problem hakerisanja?" Prije nego što se posvetimo razmišljanju o zaštiti od hakerske prijetnje na pojedinačnom planu, važno je razmotriti na koji način će kompanije najprije na Web-u napraviti sigurne sajtove za svoje korisnike. Dugi niz godina, kompanije su zanemarivale značaj formulisanja poslovne strategije u kojoj je integrisano praktikovanje sajber bezbjednosti. Normativni poredak pati od nejasnoća, promjenjivih kriterijuma, te nestandardizovanih rešenja. Ukratko, proaktivan pristup poslovnih subjekata i dalje je nesistematičan i ad hoc determinisan, bez imperativa prilagođavanja okolnostima u nevidljivom Web-u u svrhu zaštite svojih korisnika od sajber napada, što u izvjesnoj mjeri pokazuje nemar kompanija prema održavanju stepena povjerenja konzumenata njihovih produkata (Lipka, 2015). Ipak, postoje i primjeri kako su neki segmenti u organizaciji društvenog života ozbiljno shvatili opasnost sajber prijetnji. Tako je, na Floridi, uspostavljen sistem upozoravanja na hakerske upade (LeFrancois i sar., 2018). U osnovi ovog sistema je kriterijum da se u lične podatke pored jedinstvenog broja socijalnog osiguranja i broja kreditne kartice, ubrajaju i elektronska adresa, kao i zaštitna pitanja i odgovori. Također, na Floridi se od kompanija zahtijeva da obavijeste tužioca ukoliko je više od pet stotina individualnih korisnika pogođeno sajber prijetnjom (LeFrancois i sar., 2018).

U svakom slučaju, koncept sajber bezbjednosti morao bi da predstavlja više od obavještavanja pojedinca da je bio izložen napadu hakera, u kojem su mu otuđeni podaci. Bez toga, primjer sa Floride ostaje na reaktivnom nivou jer se odnosi na amortizovanje posljedica problema, do koga je već došlo. Odgovarajući pristup u zaštiti od hakerisanja podrazumijeva proaktivnost i prilagodljivost koncepta, koji prati tehnološki razvoj, izmjenu normative i trendove poslovne prakse i koji bi, prije svega, bio preventivno usmjeren na samu realizaciju hakerskog napada.

Kompanije mogu primijeniti nekoliko strategija u svojim poslovnim planovima radi zaštite podataka svojih korisnika. Najprije, mogu da upotrebe postupak dvostruke potvrde prilikom pristupanja računima. Naprimjer, studentski portal američkog Univerziteta James Madison zahtijeva od korisnika unošenje podataka o korisničkom imenu i lozinki, poslije čega je neophodno odgovoriti na prethodno određeno zaštitno pitanje ili upotrebiti jednokratnu lozinku koja je dostavljena na korisnikovu elektronsku adresu (LeFrancois i sar., 2018). Pored ovog načina zaštite, kompanije mogu enkriptovati podatke koji se šalju putem javnih mreža ili se pohranjuju na mobilne uređaje, da bi potom od korisnika bilo

zahtijevano da izmijeni inicijalnu lozinku posle izdavanja računa (LeFrancois i sar., 2018). Naravno, ovi protokoli zaštite se uče i vježbaju, zbog čega je neophodno vršiti obuku zaposlenih bar na godišnjem nivou kako bi sigurnosne mjere bile uvijek odgovarajuće i ažurirane. Važno je da kompanije imaju zaštitne procedure koje ispunjavaju uslove obezbjeđivanja privatnosti i sigurnosti na svojim sajtovima. Između ostalog, to je garant održavanja povjerenja u takvu kompaniju, njen uspon na tržištu i zaštitu pojedinačnih korisnika od opasnosti sajber prijetnji.

Teško je predvidjeti nove moduse rizika koje sa sobom donosi brz tehnološki napredak, ali to ne znači da koncepti sajber bezbjednost ne budu integrisani u sisteme zbog čega kreatori zaštite moraju da komuniciraju sa poslovnim jedinicama i pravnim savjetnicima, kako bi ovi sistemi zaštite bili efikasni i ostvarivi. Kada se u kompanijama uspostavi zaštitni sistem za prepoznavanje prijetnje od hakerskih napada, neophodno je upozoriti pojedinačne korisnike o koracima koje moraju preduzeti kako bi se osigurali u on-line okruženju (Miller, 2016).

Funkcionisanje protokola sajber bezbjednosti je krupan zalogaj za kompanije i pojedince. Upotreba Interneta u obrazovanju i organizovanju svakodnevnog života je veliki zahtjev (Freedman, 2016). Elektronsko bankarsko poslovanje, kao i on-line kupovina, postali su neophodnost našeg doba. Trgovinska mreža gotovo u potpunosti se nalazi u okruženju World Wide Web-a. Sajber napadi ne završavaju se odredišnom destinacijom on-line transakcije. Neovlašćeni pristup podacima i hakovanje u on-line saobraćaju nanosi štetu globalnoj ekonomiji u svijetu u iznosu koji premašuje 400 milijardi američkih dolara godišnje (Johnson, 2016). Lični podaci, kao što su ime, prezime, adresa prebivališta, elektronska adresa, telefonski broj, dostupni su na Internetu. Distribucija ličnih podataka je uslovljena stepenom kulturnog razvoja jednog društva i običajnog miljea u kome se odrasta. Naša civilizacija uveliko počiva na imperativu on-line prisutnosti na World Wide Web-u, kako na privatnom, tako i na profesionalnom planu, a time i izloženosti napada iz dubokog i tamnog Web-a. Sve dok svjetska Internet mreža bude izgledala zabavno i bezopasno, postojaće i tamna strana globalnog Web-a, zbog čega je nužna zaštita sigurnosti svakog korisnika, bio on pojedinac ili kompanija, jedan od prioriteta vremena.

ZAKLJUČAK

Deep Web i Darknet sve više postaju predmet interesovanja istraživača, organa krivičnog gonjenja i donosilaca političkih odluka. Međutim, jasan uvid u prirodu i kvantitet ovih slojeva Interneta nije moguć. Anonimnost je vrlo često podržana pretraživačkim servisima kao što je TOR i skriva korisnike Interneta koji teže destinacijama u najdubljim zonama Web-a, što takođe doprinosi zamagljivanju prave slike stanja u nevidljivom Web-u, baš kao i nestalnost sajtova koji se u njemu hostuju. Individualni korisnici, poslovni subjekti i vlade mogu imati i koristi od razmjene podataka u Deep Web-u. U njegovom tamnom prostoru odvijaju se legalne, baš kao i nezakonite, aktivnosti i to od obezbjeđivanja diskretnog komuniciranja po osjetljivim temama sa najvišom oznakom povjerljivosti do

krijumčarenja zabranjenih proizvoda poput opojnih droga, oružja, ličnih podataka i kodova putem kojih se prolazi kroz zaštitu softvera.

Uprkos zahtjevima za povećanjem zaštite privatnosti i podizanjem nivoa bezbjednosti u on-line okruženju, možemo se pitati i da li će korespondencija između individualnih korisnika izmijeniti svoj tok prevashodno u smislu upotrebe servisa koji obezbjeđuju anonimnost, kao što je TOR (Ciancaglini i sar., 2015). Još uvijek se ne očekuje preovlađujući podsticaj za upotrebom pretraživača u okruženju anonimnih platformi za razmjenu podataka, ali je vrlo vjerovatno da će tehnološki razvoj doprinijeti da se još više poveća stepen zatamnjivanja Darkneta (Ciancaglini i sar., 2015). Naravno, ovo će uzrokovati da se organi krivičnog gonjenja i donosioci političkih odluka preispitaju u kom pravcu će se boriti sa negativnom stranom tehnološkog napretka i njegovim efektima u uslovima nevidljivog Web-a, kako bi efikasno suzbijali zloupotrebu sajber prostora uključujući i okruženje tamnog Web-a.

Dark Web je, po svojoj prirodi, anoniman i u njemu nije moguće praviti razliku između korisnika koji teže privatnosti svog boravka na Internetu i nosilaca kriminalnih aktivnosti. Pred agencijama za primjenu zakona je težak zadatak da otkriju delinkvente, a da pri tom ne naruše pravo na privatnost onih koji ne postupaju kriminalno. Sasvim je moguće da najbolji način za rješavanje ovakvog problema otkrivanje ilegalnih sajtova, a ne zlonamjernih korisnika (Chertoff, 2017). Pod plaštom svojih zakonskih ovlašćenja, državni hakeri mogu demaskirati posjetioce nezakonitih sajtova postavljanjem naročitih softvera u pokretačke programe njihovih računara. S druge strane, ukoliko državni organa zatvori neki sajt, umjesto njega pojaviće se nekoliko novih sa nezakonitim sadržajima. Vjerujemo da bi krivično gonjenje korisnika ilegalnog sajta obeshrabrilo druge korisnike, koji bi zbog opreza da ne budu otkriveni izbjegavali da rizikuju sa traženjem takvih destinacija u nevidljivom Web-u. Vjerujemo da bi ovo na svoj način doprinijelo umanjenju nedozvoljenih radnji u informatičkom prostoru Deep Web-a, a time i njegovog tamnog dijela Darkneta.

LITERATURA

- Chertoff, M. (2017). A public policy perspective of the Dark Web. *Journal of Cyber Policy*, Vol. 2, No. 1, 26-38.
- Ciancaglini, V., et al. (2015). Below the Surface: Exploring the Deep Web. *Trend Micro*, June 2015, 1-48.
- Finklea, K. (2017). Dark Web. *Congressional Research Service*, March 10, 1-16.
- Freedman, E. (2016) As holidays approach, keeping information safe from hackers becomes even more important. *The Breeze*. Dostupno na: https://www.breezejmu.org/news/as-holidays-approach-keeping-information-safe-from-hackers-becomes-even/article_eb892b64-b774-11e6-934d-cfbde922b479.html, preuzeto 21.06.2019.
- Goodman, M. (2016). *Future crimes: Inside the digital underground and the battle for our connected world*. New York: Anchor Books.
- Greenberg, A. (2015). New dark-web market is selling zero-day exploits to hackers. *Security*. Dostupno na: https://www.wired.com/2015/04/therealdeal-zero-day-exploits/, preuzeto 19.06.2019.
- Johnson, K. (2016). Managing cyber risks. *Georgia Law Review*, Vol. 50:547 2016, 547-592.
- LeFrancois, D., Reilly, C., Munn, R., Strasel, A., Garcia, J., & Chiles, L. (2018). Hackers and the dark net: A look into hacking and the deep web. *James Madison Undergraduate Research Journal,* 2017-2018, Vol. 5, Issue 1, 33-43.
- Lipka, M. (2015). Percentage of companies that report systems hacked. *Money Watch*. Dostupno na: https://www.cbsnews.com/news/percentage-of-companies-that-report-systems-hacked/, preuzeto 29.05.2019.
- Miller, K. (2016). What we talk about when we talk about "Reasonable Cybersecurity": A proactive and adaptive approach. *The Florida Bar Journal*, September/October 2016, 23-31.
- Kovacs, E. (2015). What is the difference between black, white and grey hackers? *Emerging Threats*. Dostupno na: https://us.norton.com/internetsecurity-emerging-threats-what-is-the-difference-between-black-white-and-grey-hat-hackers.html, preuzeto 19.05.2019.
- Martin, B., & Newhall, J. (2016). Technology and the guilty mind: when do technology providers become criminal accomplices? *Journal of Criminal Law & Criminology*, Vol. 105, No. 1, 95-148.
- Norton, Q. (2012). How Anonymous picks targets, launches attacks, and takes powerful organizations down. *Wired*. Dostupno na: https://www.wired.com/2012/07/ff-anonymous/, preuzeto 21.06.2019.
- Omand, D. (2016). The Dark Net: Policing the Internet's underworld. *World Policy Journal*. Winter 2015/2016, 74-82.
- Pagliery, J. (2015). The evolution of hacking. *CNN Business*. Dostupno na: https://edition.cnn.com/2015/03/11/tech/computer-hacking-history/, preuzeto 15.05.2019.

- Sui, D., Caverlee, J. & Rudesill, D. (2015). The Deep Web and the Dark Net: A look inside the Internet's massive black box. *Science and Technology Innovation Program*, STIP 03, August 2015, 1-17.
- Thielman, S., Hunt, E. (2016). Cyber Attack: Hackers 'Weaponised' Everyday Devices With Malware. *The Guardian*. Dostupno na: https://www.theguardian.com/technology/2016/oct/22/cyber-attack-hackers-weaponised-everyday-devices-with-malware-to-mount-assault, preuzeto 24.05.2019.
- Weimann, G. (2016). Going dark: Terrorism on the Dark Web, *Studies in Conflict & Terrorism*, Vol. 39, No. 3, 195-206.
- Williams, W. (2014). What motivates modern hackers? *Betanews*. Dostupno na: https://betanews.com/2014/08/14/what-motivates-modern-hackers/, preuzeto 01.06.2019.
- Zetter, K. (2012). Chrome owned by exploits in hacker contests, but Google's $1M purse still safe. *Wired*. Dostupno na: https://www.wired.com/2012/03/pwnium-and-pwn2own/, preuzeto 07.06.2019.
- Zetter, K. (2013). IE11 Preview bug bounty. *Wired*. Dostupno na: https://www.wired.com/2013/06/microsoft-bug-bounty-program/, preuzeto 05.06.2019.
- Zetter, K. (2016). Hacker Lexicon: What are white hat, gray hat, and black hat hackers? *Wired*. Dostupno na: https://www.wired.com/2016/04/hacker-lexicon-white-hat-gray-hat-black-hat-hackers/, preuzeto 09.06.2019.

Kriminalističke teme
Zbornik radova
Godina XIX, Broj 5, 2019.
ISSN 1512-5505

KRIMINALNI POTENCIJAL FENOMENA DARKNET-a
THE DARKNET PHENOMENON CRIMINAL POTENTIAL

Pregledni naučni rad

Sergej Uljanov[85]
Milan Milošević[86]

Sažetak

Inspiracija za rad: Mogućnosti savremene globalne komunikacije inspirisale su autore da usmere pažnju na pogodnosti delova svetske informatičke mreže za kriminalno delovanje.
Ciljevi rada: Sledstveno tome, cilj ovog rada posvećen je istraživanju kriminalnog potencijala skrivene zone World Wide Web-a.
Metodologija/dizajn: Poštujući metodološki model utvrdjivanja fenomenoloških determinanti od opšteg preko posebnog ka pojedinačnom, autori nastoje da odrede pojmovni volumen najzagonetnijeg dela skrivenog Web-a čineći distinkciju pojmova Worl Wide Web, Web i Deep Web kroz sagledavanje njihovog odnosa. Finalno, u pojedinačnom segmentu, autori prikazuju fenomen Darknet-a i specifičnost njegove relacije sa Deep Web-om.
Ograničenja rada/istraživanja: Autori su svesni ograničenja ovakvog istraživanja, koje mogu predstavljati neosnovane predstave o globalnoj komunikaciji kao nasušnom vidu socijalizovanog ispoljavanja ljudskih prava i sloboda.
Rezultati: Kriminalni potencijal Darknet-a autori utvrđuju posredstvom uticaja intenziteta međunarodne prisutnosti pojava kriminalnih čvorišta, kriminalnih tržišta i dejstva faktora polikriminaliteta.
Generalni zaključak: Ukazivanje na postojanje Darknet-a, te njegov kriminalni potencijal, kako smatraju autori, čini neophodnu osnovu za dalja istraživanja skrivenih načina globalne komunikacije i njihovo kriminalizovanje.
Opravdanost istraživanja/rada: Upravo zato, autori nedvosmisleno ovim radom pokušavaju da jasno prikažu kriminalnu opasnost skrivenih zona mogućnosti globalne komunikacije i njen razorni uticaj na vrednosti savremene društvene zajednice.

Ključne riječi

Darknet, Deep Web, World Wide Web, kriminalno čvorište, kriminalno tržište, polikriminalitet

[85] Zaposlen u Ministarstvu unutrašnjih poslova Republike Srbije i docent Fakulteta za poslovne studije i pravo Univerziteta "Union – Nikola Tesla", Beograd, sputnik970@gmail.com
[86] Fakultet za poslovne studije i pravo Univerztiteta „UNION - Nikola Tesla", Beograd, Republika Srbija, milanmilos@gmail.com

Summary

Reason for writing and research problem (s): Nowadays global communication possibilities have inspired the authors to pay attention to having parts of world informatics network suitable enough to be exposed criminally.
Aims of the paper (scientific and/or social): Subsequently, the article's goal sticks to research of the criminal potential of a zone hidden within the World Wide Web.
Methodology/Design: Following the methodological model of establishing the phenomenological determinants from general through special to unique, the authors try to define terminological range of the most inscrutable bit within the hidden Web by doing distinction among the terms of the World Wide Web, the surface Web and the Deep Web with scoping their relation. Finally, at unique stage, the authors show the Darknet phenomenon and particularity of its relation to the Deep Web.
Research/Paper limitation: The authors are fully aware of the exploration limits that could be supportive to the arbitrary clues on global communication as necessary mode of human rights and freedoms being exposed socialized like.
Results/Findings: The criminal potential of the Darknet is to be established by the authors through influences of criminal hubs, criminal markets and poly-criminality being presented intensively as much as internationally.
General Conclusion: Pointing to the Darknet existence and its criminal potential, as the authors deem, creates essential ground to further researching of clandestine ways to communicate globally and their criminalization.
Research/Paper Validity: Thus, the authors intend undoubtedly to show in the article clearly the criminal danger of hidden zones of possibility to communicate globally and its devastating influence to the values of modern society.

Keywords

the Darknet, the Deep Web, the World Wide Web, criminal hub, criminal market, poly-criminality.

UVOD

Danas, gotovo, da je uvreženo mišljenje da se pretragom na Googl-u može doći do traženog podatka prema kriterijumu zadatog pojma. Ipak, postoji čitavo on-line more informacija, koje je van domašaja Googl-a i ostalih javno dostupnih pretraživača Interneta. Zbog nepoznavanja okruženja i uslova koji kriminalno određuju taj nepoznati sajber prostor za traganje za podacima i razmenu informacija, akcije organa krivičnog gonjenja bivaju suštinski ograničene bez značajnije podrške donosilaca političkih odluka koji bi kreirali i javno promovisali koncept podizanja svesti na širem planu.

Razmere ovog nevidljivog dela Interneta su bezgranične. Broj web sajtova koji nisu indeksirani, kao što je slučaj u opšte poznatom i dostupnom površinskom delu World Wide Web-a, ispunjava Deep Web za koji se procenjuje da je 400 do 500 puta obimniji od svog vidljivog opozita. U vidljivom Web-u web sajtovi su registrovani i dostupni javnim pretraživačkim servisima, dok u tamnoj zoni Interneta odnosno dubokom Web-u to nije slučaj. Diskretnost ispod površinskog Web-a, svakako, pogoduje onim savesnim i dobronamernim korisnicima Interneta čije aktivnosti nisu kriminalne a anonimost čini imperativ u

njihovom delovanju, kao što je slučaj sa istraživačkim novinarstvom, političkim oponentima i uzbunjivačima. Međutim, postoji i tamni deo nevidljivog Web-a, čiiji informatički prostor neutvrđenog volumena sadrži podatke koji se dovode u vezu sa ilegalnim aktivnostima. Ova skrivena zona, poznata kao Dark Web ili Darknet, služi kao komunikacioni kanal imeđu organizovanih kriminalnih grupa, terorističkih ćelija, kao i onih korisnika Interneta koji tragaju za nedozvoljenim proizvodima. U njoj su virtuelna kriminalna tržišta, koja nude *inter alia* krijumčarenu robu, opojne droge, falsifikovane dokumente, ukradeno vatreno oružje, podatke o kreditnim karticama, te sadržaje u vezi sa iskorišćavanjem dece i maloletnih osoba u pornografske svrhe.

Obzirom na stalno uvećavanje nevidljivog Web-a i njegovog skrivenog pratioca Darkneta, eksponencijalno raste i rizik od podizanja efikasnosti ilegalnih aktivnosti zbog nemogućnosti kontrole njihove pripreme i organizovanja. Odgovor na ovakve izazove mora biti multidisciplinaran i zasnovan na platformi strategije nacionalne bezbednosti, jer sajber pretnje podjednako ugrožavaju ljudska prava i slobode, zaštitu života i zdravlja čoveka, kao i međunarodne tokove globalne ekonomije.

Uprkos ostvarenom napretku u geografskom determinisanju sveta i dalje postoje predeli naše planete koji nisu u potpunosti dokumentovani. Slično tome, novi virtuelni svet nepoznatih granica određen kao sajber prostor i pored naših napora da ga spoznamo u proteklih par decenija, ostaje zatvoren i nevidljiv za veliku većinu korisnika Interneta. Nažalost, masovno nepoznavanje informatičkog okruženja u kome živimo i dalje odnosi prevagu nad pojedinačnom upućenošću u mogućnosti i strukturu World Wide Web-a. Korišćenje pretraživača poput Googl-a i Bing-a, je samo plovidba uz obalu sajber mora čije granice nismo sposobni da sagledamo. Čitav jedan novi svet, sa svojim relacijama, okolnostima, uslovima i okruženjem, još uvek čeka da bude istražen, a činjenica njegove virtuelnosti nimalo ne umanjuje ovu potrebu.

STRUKTURA SVETSKOG WEB-a

Kako razumeti fenomen World Wide Web-a? Da li zamišljeni prostor može biti struktuiran? Da li in esentio virtuelnost može imati neku materijalnu komponentu? Za početak valja odrediti gradivnu jedinicu World Wide Web-a. Mišljenja smo da je to informacija jer se u ovom virtuelnom sajber prostoru konstantno razmenjuju podaci za kojima tragaju zainteresovani korisnici Interneta. Adrese na kojima se do potrebnih podataka može doći dostupne su na površinskom Web-u odnosno u vidljivoj zoni World Wide Web-a. Ovo dalje znači da svetsko informatičko more, pored svoje površine, mora imati i svoj dubinski deo nevidljiv i nedostupan za redovno pretraživačko postupanje.

Kao i u fizičkom svetu, odnos prostranstva površine i volumena dubine mora nije ravnomeran, pogotovo ukoliko dubina nije određena već daleko premašuje granice mogućnosti našeg saznanja obzirom na virtuelnost svoje prirode. Analogno tome, strukturu World Wide Web-a možemo zamisliti kao more podataka, čiju površinu predstavlja vidljivi Web, dok skriveni duboki Web oslikava njegovu nepoznatu dubinu neshvatljivih razmera. Tako

bi dve osnovne komponente svetskog Web-a bile razgraničene faktorom vidljivosti i dostupnosti na površinski i Deep Web.

Tehnički nije moguće izmeriti obim dubokog Web-a, ali ako pođemo od činjenice da Google svojim pretraživačkim kapacitetom pokriva do 16% površinskog Web-a, a da samo na 60 najvećih sajtova u Deep Web-u ima 40 puta više pohranjenih podataka nego u celom vidljivom delu World Wide Web-a, tada možemo makar grubo predstaviti sliku strukture svetskog Web-a i međusobni odnos njenih ključnih delova (Sui, Caverlee i Rudesill, 2015).

Kao što u tmini morskih dubina postoje rasedi u podmorju, tako i duboki Web ima svoju tajnovitu tamnu oblast tzv. Dark Web ili Darknet, koji okuplja sve destinacije za pretragu koje se ne mogu dostići putem Interneta na redovan način. Tamna strana Deep Web-a ima brz rast, koji je direktno uslovljen anonimnim šerovanjem fajlova preko mreže sa adresama koje nisu indeksirane i koje nisu vidljive za standardne pretraživače površinskog Web-a. Kao faktor uvećavanja volumena dubokog Web-a, Darknet postaje njegova ključna komponenta zbog čega ga posmatramo kao još jedan od kompleksnih slojeva višedimenzionalne strukture World Wide Web-a.

Za razliku od informatičkog saobraćaja u vidljivom Web-u, ali i od nekih delova Deep Web-a, sajtovi Darkneta mogu se posetiti isključivo anonimno. Imajući u vidu da duboki Web raspolaže najvećim brojem „živih" informacija na Internetu, struktura njegovih sajtova više je determinisana vertikalno nego horizontalno pružajući mogućnost dubinskih pretraga koje nisu izvodljive na površinskom Web-u. Uslovi dubokog i tamnog Web-a nameću zbog težeg pristupa podacima njihovu veću zaštićenost, zbog čega su eksploatisani kako od strane timova uposlenih na poverljivim resornim projektima, tako i od pojedinaca i grupa koji se dovode u vezu sa najširim spektrom kriminalnih aktivnosti predstavljajući svojevrsan izazov za hakerske napade usmerene na obe navedene kategorije korisnika.

DUBOKI I TAMNI WEB

Ekspanziji Deep Weba i Darkneta doprinose brojne informatičke tehnologije. Tako, volumen dubokog Web-a uvećavaju ubicomp, cloud i mobilno računarstvo, ali i sistemi umreženih senzora, dok rast tamnog Web-a podstiču razvoj u obezbeđivanju anonimnog i bezbednog pristupa hosting servisima, Dark Wallet platforma za omogućavanje anonimnih transakcija virtuelne valute Bitcoin i unapređivanje crimeware-a kao zloćudnih softvera za automatsko izvođenje on-line sajber napada radi istovremenog slanja zaraženih poruka na veliki broj elektronskih adresa, krađe podataka i iznude. Razne vrste virtuelnog novca, kao što su Bitcoin, Darkcoin ili Peercoin u upotrebi su pri izvršenju anonimnih transakcija u svrhu poslova koji se odvijaju na kriminalnim tržištima Darkneta. Hakeri skriveni iza ponuda za posao i višejezičkih centara za upućivanje poziva, takođe, ubrzavaju širenju dimenzije tamnog Web-a. Pored navedenog, Darknetove mogućnosti legitimno koriste novinari, uzbunjivači i zaštitnici ljudskih prava, kojima je anonimnost neophodna radi sopstvene zaštite i garanta uspeha u radu (Sui, Caverlee i Rudesill, 2015).

Za istraživanje Deep Web-a i Darkneta potrebni su posebni informatički alati i tehnike. Neki od njih su slični onima za pretraživanje površinskog Web-a. U korelaciji sa namerama i željama korisnika, različite dubine svetskog Web-a iziskuju upotrebu određenih informatičkih tehnika. U najvećem broju slučajeva, generalno se primenjuju dva posebna ali međusobno povezana protokola pristupanja dubokom i tamnom Web-u. Najpre, moguće je doći do ovih naročitih protokola upotrebom regularnih pretraživača, kao što su Internet Explorer, Firefox ili Chrome Safari. Ali, postoje specifični protokoli kojima se može pristupiti samo preko pretraživača TOR. Valja napomenuti da postoje grupe korisnika koje razvijaju protokole pristupa kreiranjem posebnih pretraživača linkova odnosno primenom softvera za komunikaciju putem aplikacija ili drugih različitih komponenti komunikacijskih softvera. Ovi alternativni modusi za ulazak u nevidljivi Web prilagođeni su potrebama okruženja različitih zona Deep Web-a. Ipak, pravi izazov predstavlja činjenica da svi do sada kreirani protokoli mogu samo da ostvare ulaz u mali deo dubokog Web-a (Sui, Caverlee i Rudesill, 2015). Zbog toga je i dalje neophodno posećivati tačno određene on-line direktorijume odnosno skrivene grupe web sajtova koji su diskretno popisani prema traženoj destinaciji korisnika, kao što je npr. https://sites.google.com/site/howto-accessthedeepnet/working-links-to-the-deep-web. Obzriom da ovi web sajtovi nisu indeksirani, oni ne mogu biti pronađeni putem regularnih pretraživača. Međutim, njihove web adrese mogu biti locirane na alternativne načine, tako da im se posle otkrivanja može pristupiti upotrebom standardnog pretraživača iako se nalaze u dubokom Web-u.

Neke od javnih baza podataka nalaze se u nevidljivom Web-u jer se najveći deo njihovog sadržaja ne može pretražen redovnim protokolima. Veliki broj korisnika Interneta dolazi u situaciju da ostvari interakciju sa delovima Weep Web-a upotrebom standarnih načina pretrage, a da nikada to ne sazna. Tako je npr. biblioteka američkog Kongresa sadržana u on-line bazi podataka na adresi www.loc.gov i može joj se pristupiti na standardan način iz površinskog Web-a, a da se pri tom ova baza podataka nalazi u Deep Web-u. Postoji veliki broj sajtova na kojima su ekonomski podaci, a koji su deo dubokog Web-a, kao što su: FreeLunch.com, Census.gov, Copyright.gov, PubMed, Web of Science, WWW Virtual Library, Directory of Open Acces Journals, FindLaw, te Wolfram Alpha (Sui, Caverlee i Rudesill, 2015).

Postoje, takođe, brojne baze podataka kojima se ne može pristupiti besplatno, kao npr. Westlaw i LexisNexis, te baze podataka sa obaveznim registrovanjem korisnika, što je slučaj sa velikim brojem on-line univerzitetskih biblioteka, koje su u oba navedena slučaja nalaze u Deep Web-u. U zoni nevidljivog Web-a nalazi se i veliki broj ličnih podataka koji su obezbeđeni lozinkama, poput PayPal računa. Pristup u ove delove dubokog Web-a je tehički limitiran i pravno zaštićen.

Sa opštom upotrebom Web 2.0, unapređene verzije Web-a, i mobilnih telefona sa višestrukom namenom, ogroman broj informacija pohranjen je na različite društvene mreže. Ovim podacima ne može se pristupiti upotrebom standardnih pretraživača. Neophodna je prethodna autorizacija korisnika kroz registrovanje ili ostvarivanje tzv. „prijateljstva“ sa drugim određenim grupama korisnika. Neki drugi servisi, kao što su Twitter i Facebook,

omogućuju javno dostupnu aplikaciju, kako bi korisnici mogli da pribave podatke preko takvih društvenih mreža u širem obimu. Ali mnoge od ovakvih društvenih mreža, poput YikYak i Wechat, zahtevaju pristupnu identifikaciju korisnika i ograničavaju dostupnost svojim masivnim bazama podataka iz razloga održavanja bezbednosti i poštovanja privatnosti.

U zonama Deep Web-a ostvaruje se i instant razmenjivanje poruka, kao još jedan od izvora podataka. Od prethodne forme on-line soba za razgovore, instant razmena poruka prerasta u komunikaciju između dva korisnika koja se ne arhivira, te tako privatnost razmenjenih podataka ostaje nenarušena. Ovaj prinic je u širokoj upotebri u on-line razgovorima i pružanju tehničke podrške.

U današnje vreme, neke mobilne aplikacije dozvoljavaju korisnicima da sačuvaju pregled razmene poruka na lokalnom nivou, tako da u slučaju potrebe mogu da pristupe ovom pregledu. Ipak, instant razmenjivanje poruka sve više postoje bazirano multimedijski, što otežava arhiviranje pregleda primljenih i poslatih poruka. Pristup ovom delu dubokog Web-a u kome se mogu pohraniti podaci iz razmenjenih poruka, moguć je ukoliko se u trenutku obavljanja konverzacije izvrši snimanje desktopa odnosno video zapisivanje.

Kao deo Deep Web-a, u poslednje vreme, Darknet sve češće služi za dogovaranje poslova, vođenje razgovora, distribuciju pojedinačnih podataka i fajlova, te transfere virtuelnog sredstva plaćanja. Potpuna anonimnost skrivenih kutaka Darkenta obezbeđuje privatnost on-line aktivnosti korisnika i za očekivati je progresivan rast njihovog prisustva u ovom tamnom delu Web-a. Da bi ovakav protokol pristupa web stranama u zoni Darkneta mogao biti realizovan, neophodna je upotreba specijalizovanog nestandardnog pretraživača, kao što je TOR, koji obezbeđuje anoniman pristup web adresama u Darknetu uz istovremeno maksimalno otežavanje eventualnog praćenja nečijih on-line aktivnosti u okviru protokola TOR-a. Za razliku od uslova u kojima se odvija komunikacija među korisnicima na površinskom Web-u, Darknet destinacije u okviru TOR-ove pretraživačke mreže često nisu stabilne jer bivaju nedostupne satima ili danima, a ponekad mogu i da nestanu uz neizvesnost ponovnog pojavljivanja. Često se sporo otvaraju, obzirom da TOR pravi konekciju kroz nasumično selektovane servere kako bi garantovao anonimnost prisustva korisnika.TOR pretraživač predviđen je za operativne sisteme mobilnih uređaja Android i iOs, što ih čini nebezbednim i manje preporučljivim za upotrebu prevashodnog broja prosečnih korisnika. Ovo se svakako odnosi i na TOR-ove dodatke za druge vrste pretraživača, što samo pojačava izazove i neizvesnost kretanja korisnika kroz duboke i tamne vode nevidljive sfere World Wide Web-a (Sui, Caverlee i Rudesill, 2015).

KRIMINALNI ATRIBUTI DARKNET-a

Poslednjih godina, Darknet je postao jedna od tema o kojoj se vrlo često raspravljalo u krugovima sajber bezbednosti. S jedne strane, skrivene komunikacione mreže na Internetu su znak dostignute slobode građana, dok s druge strane, ove mogućnosti nisu ništa drugo do platforme za ispoljavanje i ispunjavanje želja korisnika rukovođenih kriminalnim

intencijama. Uopšte uzev, mediji profilišu Darknet kao okruženje za nesmetano odvijanje kriminalnih aktivnosti, koje zato ima predominantne kriminogene predispozicije (Mirea, Wang i Jung, 2019). Brojne medijske agencije ističu da se tamni Web i njegov prateći pretraživački servis TOR prevashodno upotrebljavaju za vršenje ilegalnih radnji (Chandran, 2015; Farell, 2017; McGoogan, 2016; Moloney, 2016; Samson, 2017; Wiesmann, 2015). Kao primer navodimo dva novinska naslova koja upućuju na navedeno mišljenje o kriminogenosti Darkneta, a to su „Darknet može da predstavlja rizik od urušavanja sektora Interneta" (Samson, 2017) i „TOR pretraživač Dark Web-a se gotovo sasvim koristi u kriminalne svrhe, prema istraživanjima" (McGoogan, 2016). Ova negativna percepcija Darkneta naširoko se plasira od strane državnih organa, ali i korisnika koji su vođeni strahom od nepoznatog informatičkog okruženja tamnog Web-a (Murray, 2014). Tako je npr. jedan od rukovodilaca bezbednosno obaveštajne agencije britanske Vlade i oružanih snaga (Government Communications Headquarters-GCHQ) uporedio Darknet sa Divljim Zapadom, tvrdeći da je neophodno uspostaviti kontrolu nad ovom skrivenom zonom dubokog Web-a (Omand, 2016).

U akademskim krugovima, prva kriminološka istraživanja ukazala su na vezu Darkneta sa kriminalnim aktivnostima označavajući tamni Web kao „piratsko skrovište" za učinioce krivičnih dela, navodeći kao primer anonimni promet nedozvoljenom robom, poput narkotika, koji se plaća virtuelnim novcem kao što je Bitcoin (Buxton i Bingham, 2015). Prema nekim autorima, ilegalna trgovina opojnom drogom, zaista, je jedna od izuzetno čestih nedozvoljenih aktivnosti na Darknetu (Dolliver, 2015; Owen i Savage, 2015). Početkom 2016. godine, ukupan prihod od opijata na Darknetovom kriminalnom tržištu opojnih droga bio je procenjen na iznos od 12.000.000 do 21.100.000 američkih dolara (Kruithof i sar., 2016). Ovo skriveno kriminalno tržište za ilegalni promet opojnom drogom predstavlja ozbiljnu brigu za organe za primenu zakona širom sveta (Horton-Eddison i Di Cristofaro, 2017). Druge ilegalne transakcije na ovakvim tržištima odnose se na nedozvoljenu trgovinu oružjem, kreditnim karticama i drugim ličnim podacima, te egzotičnim životinjskim vrstama (Chertoff i Simon, 2015; Holm, 2017). Ovo nam daje za pravo da tvrdimo da je polikriminalitet jedan od ključnih kriminalnih atributa Darkneta, kao i da okolnosti tamnog Web-a koje garantuju anonimnost korisnika afirmativno deluju na formiranje virtuelnih kriminalnih čvorišta kao pratećeg efekta usmerene razmene informacija u svrhu pripremanja, organizovanja, koordiniranja i činjenja kriminalnih aktivnosti na međunarodnom nivou.

Širenje „crnih" tržišta na Darknetu pomognuto je razvojem informatičkih tehnologija, koje obezbeđuju komunikacione mreže bazirane na anonimnosti, privatnosti i upotrebi virtuelnog novca (Mirea, Wang i Jung, 2019). Prema nekim mišljenjima, anonimna priroda prisustva korisnika u zoni Darkneta pojačava rizik od krađe identiteta (Holms, 2017). U tom pravcu postoje i shvatanja da obim rizika i pretnji, koji vrebaju iz okruženja Darkneta, još uvek nije dovoljno istražen (Byrne i Kimball, 2017). Najveći broj istraživanja Darkneta, do sada, bio je usmeren na kriminalne aktivnosti i njihove tehničke aspekte (Qaing i sar., 2014; Wright, 2008; Zheng i sar. 2013). Samo nekoliko projekata bilo je posvećeno pokušajima formiranja slike o sociološkoj i psihološkoj strani Darkneta (Everett, 2015; Lacson i Jones, 2016; Van Hout i Bingham, 2013).

Darknet je, po svemu sudeći, ispunjen nekontrolisanim zloćudnim informatičkim sadržajima i služi kao zaklon za mnoge uznemirujuće aktivnosti ispod vidljivog površinskog dela World Wide Web-a. Analizom vodećih ponuđača u nevidljivom Web-u, uočen je intenzivan ilegalni promet lakom opojnom drogom, zabranjenim sintetičkim drogama, te prepisanim lekovima kao što su Ritalin i Xanax. Za pristup sajtovima u Darknetu najviše se koriste protokoli van standardnih paramatera HTTP/HTTPS, kao što su IRC, IRCS, Gopher, XMPP i FTP. Hiljade sumnjivih sajtova može se dostići putem navedenih neregularnih protokola radi ostvarivanja pristupa sadržajima koji se nalaze u vezi sa zaraženim reklamnim materijalima, načinima za ulazak na blokirane web destinacije i iskorišćavanjem dece u pornografske svrhe. Agresivne grupe malware-a, kao što su VAWTRAK i CryptoLocker, koriste TOR kao komponentu svoje konfiguracije i tako se plasiraju u sisteme korisnika koji se kreću kroz okruženje Darkneta.

Ukidanje kriminalnih tržišta na Darknetu nije trajno rešenje koje će doprineti smanjenju intenziteta i obima ilegalne trgovine opojnom drogom jer će ona biti nastavljena kroz online radnje i forume koji su tematski usmereni. U tamnom Web-u rasprostanjena je upotreba virtuelne valute Bitcoin, ali i njenog „perača“ kao što je EasyCoin u svrhu još većeg skrivanja kretanja virtuelnih novčanih tokova. To je siguran pokazatelj da su u Darknetu, time i u Deep Web-u, prisutni nosioci kriminalnih aktivnosti, koji trguju ukradenim računima, putnim ispravama i identitetima posredstvom lažnih poslovnih foruma, kojom prilikom ističu kompletan opis ponuđene robe uz njenu cenu. Pored toga, prisutne su i ponude za usluge plaćenih likvidacija maskirane poslovnim uslugama na kriminalnim tržištima Dark Web-a (Ciancaglini i sar., 2015).

Kriminalna tržišta nedvosmislen su primer kriminalizovanosti Darknet okruženja, u kome se krije identitet učesnika transakcije zabranjenim proizvodima, obavljaju poslovi putem upotrebe virtuelnog novca i na svaki način izbegava regularnost u postupanju. Tržište opojnom drogom kao što je Silk Road bilo je primer informatičkog prostora u kome su se na Darknetu vršile nelegalne transakcije, koje su podrazumevale promet krijumčarenom robom. Čak i ako je reč o legalnim proizvodima u uslugama, na Darknetu se njihova nabavka i prodaja vrše uz izbegavanje plaćanja taksi i izbegavanje kontrole nad njihovim uvozom i izvozom (Sui, Caverlee i Rudesill, 2015). Dark Web služi ne samo kao deo dubokog Web-a kome se izvode ilegalne transakcije roba i usluga, te trendovskih hakerskih alata, već je i bojno polje u kome se vode sajber bitke i obračunavaju pojedinačno i grupno nosioci sajber špijunaže (Goodman, 2015).

Pogodnosti za realizovanje kriminalnih aktivnosti očigledan su preduslov za postojanje kriminalnih predispozicija nekog dela World Wide Web-a. S tim u vezi, prema nekim tvrdnjama Darknet je primer informatičkog okruženja čiji uslovi su više nego afirmativni za odvijanje široke skale raznolikih nezakonitih postupanja. Dark Web služi kao paravan, neutvrđenih razmera, za plasiranje i ilegalnu trgovinu opojnom drogom, oružjem, retkim životinjskim vrstama, te ukradenom robom i podacima, čime se ostvaruje kriminalni profit. Uz navedeno, prisutni su i kockarski sajtovi, mogućnost iznajmljivanja lopova i ubica, te čitava skladišta sa sadržajima koji se odnose na iskorišćavanje dece u pornografske

svrhe (Chertoff i Simon, 2015). Ipak, još uvek nema saznanja o širini rasprostanjenosti ovakvih sajtova na Darknetu. Tek 1,5% korisnika TOR-a posećuje ove kategorije destinacija u Dark Web-u (Greenberg, 2015). I dalje je nepoznat udeo adresa koje su u vezi sa kriminalnim tržištima u tamnom Web-u, a još manje je jasno koliko je pristupa sajtovima sa ilegalnim sadržajima ostvareno putem TOR-a (Finklea, 2017).

Istraživači sa britanskog Univerziteta Portsmouth ispitivali su saobraćaj pretraživača TOR usmeren ka serivisima skrivenim u Darknetu, kojom prilikom su angažovali 40 kompjuterskih radnih jedinica za ostvarivanje pristupa putem TOR-a. Na taj način došli su do kontakta sa čak 45.000 on-line skrivenih servisa, kojima su mogli pristupiti u bilo kom trenutku (Greenberg, 2014). Istraživači su utvrdili da je oko 2% sajtova u TOR-ovoj pretraživačkoj mreži bilo identifikovano u vezi sa pedofilskim sadržajima, ali da je 83% poseta skrivenim sajtovima bilo usmereno na sajtove sa ovakvim sadržajima, što bi značilo da je u periodu u kome je vršeno istraživanje potražnja za nevedenim sajtovima bila višestruko veća od ponude. Ovakva nesrazmera može se objasniti, u nekom stepenu, prisustvom policije u Darknetu, ali i hakera koji iz brojnih razloga posećuju ovu vrstu sajtova, od namere da ih unište do krađe i preprodaje njihovih sadržaja (Greenberg, 2014).

Još jedno istraživanje sa londonskog Univerziteta King's College bilo je posvećeno otkrivanju skrivenig usluga u TOR-ovoj pretraživačkoj mreži. Upotrebom dva popularna pretraživača u Dark Web-u po imenu Ahmia i Onion City, istraživači su uspeli da identifikuju 5.205 „živih" web sajtova (Moor i Rid, 2016). Od ovog broja utvrđen je sadržaj njih 2.723 i oni su klasifikovani prema prirodi svojih sadržaja. Dalje je utvrđeno da 1.547 ovakvih sajtova ima nedozvoljen sadržaj. Ovo je bio uzorak na web sajtovima na kojima se u okviru TOR-a nude skrivene usluge. Preko ovog uzroka, istraživači su kontaktirali čak 300.000 web sajtova sa 205.000 jedinstvenih adresa u okviru TOR-ove mreže skrivenih servisa. Na dnevnom nivou, oko 30.000 ovakvih servisa bilo je povezano sa TOR-om, pri čemu je utvrđeno da saobraćaj koji se ostvaruje prema ovim servisima čini samo 3,4% ukupne aktivnosti koja se odvija u TOR-ovoj pretraživačkoj mreži. U narednoj fazi istraživanja broj utvrđenih dnevnih aktivnosti skrivenih servisa porastao je na 50.000 do 60.000 (https://metrics.torproject.org/, 2017).

Darknet je, svojom skrivenom pozicijom u okviru dubokog Web-a i kriminalnim atributima koje poseduje, uključen u veliki broj kriminalnih aktivnosti. On služi kao forum sa sobama za razgovor i komunikacionim servisima u svrhu planiranja i koordinacije u vršenju nelagalnih radnji. Tako su se na Darknetu, primera radi, razmenjivala mišljenja o izbegavanju poreza i načinima kako da se to izvede (Krebs, 2015). Okruženje tamnog Web-a obezbeđuje i platformu za krijumčarenje nedozvoljenim proizvodima, kao i robom koja potiče iz izvršenih krivičnih dela. Iz okrilja Darkneta vrše se neovlašćeni upadi u sisteme, pa se tako frekventno plasiraju malware-i radi lociranja kreditnih i debitnih kartica da bi se tako dobijeni podaci zloupotrebljavali, prodavali i kupovali na kriminalnim tržištima tamnog Web-a (Finklea, 2017). Upravo tako se RAM scrapers, kao jedna vrsta malware-a, može nabaviti i posredno pokrenuti za štetno delovanje okviru prodajnih sistema (Zetter, 2014).

Ukradeni podaci prodaju se na Darknetu i tako se ostvaruje zarada od ilegalnih aktivnosti (Finklea, 2017). Nakon jednog većeg upada u prodajne sisteme, na „crnim" tržištima Dark Web-a došlo je do poplave ponuđenih podataka sa ukradenih kreditnih i debitnih kartica, čiji broj je premašivao jedan milion, dok su se one prodavale za 20 do 100 američkih dolara po komadu (Krebs, 2013). Ove ponude otuđenih podataka sa platnih kartica, iz tzv. radnji sa karticama, samo su jedan od primera specifičnosti funkcionisanja kriminalnih tržišta na Darknetu (Wueest, 2015).

Ne samo što podaci mogu biti ukradeni i prodati u tamnom Web-u, već se to čini izuzetno brzo. Ponuđač BitGlass izveo je istraživanje načinivši tzv. trezor sa ukradenim podacima, koji je bio lažan, u kome se nalazilo 1.500 imena, brojeva socijalnog osiguranja, brojeva kreditnih kartica i drugih ličnih podataka, naravno izmišljenih za navedenu potrebu istraživanja. Potom je „trezor" plasiran na DropBox i drugih sedam poznatih „crnih" tržišta na Darknetu. U periodu od dvanaest dana, ovim podacima je pristupljeno oko 1.100 puta u 22 države (Jackson Higgins, 2015).

PERSPEKTIVE TAMNOG WEB-a

Podizanje javne svesti o postojanju Darkneta može dovesti do njegove povećane upotrebe radi ostarivanja nelegalnih ciljeva. Ipak, ne smatramo da u budućnosti korisnici imaju dovoljno razloga da ostvaruju svoje regularne pretrage pod velom anonimnosti u okruženju tamnog Web-a. U međuvremenu, više je verovatno da će tehnološki razvoj u polju informatike dovesti do još većeg umanjenja vidljivosti tamnih delova Deep Web-a. U ovom trenutku, vodi se trka između pobornika neograničenih građanskih sloboda i organa za primenu zakona, u kojoj je primetno traganje za novim modusima podizanja nivoa anonimnosti i skrivanja tragova kretanja u okruženju Dark Web-a. Međutim, nesumnjivo je da trgovina nedozvoljenim proizvodima predstavlja jednu od najčešćih aktivnosti u dubokom Web-u, te da će anonimnost korisnika skrivenih servisa, kriminalnih tržišta i transakcija virtuelnim novcem, još više dobiti na značaju u izgradnji poverenja između prodavaca i kupaca bez postojanja posredničke uloge banke.

U dolazećim vremenima, možemo očekivati potpuno decentralizovana tržišta koja funcionišu prema blockchain tehnologiji, koja isključuje posredničku ulogu bilo koje firme ili banke u obavljanju transakcije između prodavca i kupca. Na ovaj način već funkcionišu tokovi virtuelnih valuta koji nisu određeni domicilno jer takva valuta, kao npr. Bitcoin, nije nacionalno određena kao sredstvo plaćanja. Ova tehnologija bazira na principima primene teorije igara u ekonomiji i finansijama i otklanja teret koji predstavljaju posrednički subjekti u kreiranju i održavanju novčanih tokova. U ovako idealnoj postavci jedini problem može predstavljati činjenica da virtuelni novac neizostavno čini sredstvo plaćanja u dubokom i tamnom Web-u zbog čega će njegovi tokovi biti sve manje vidljivi i mogući za praćenje. Opasnost dolazi i od naprednih malware-a, koji će na svaki način pokušati da ugroze i eksploatišu blokchain tehnologiju koristeći odsustvo kontrole posredničkog subjekta u finansijskim kretanjima (Ciancaglini i sar., 2015).

U kriminalnoj sferi, naručioci likvidacije visoko profilisane mete činiće to uz jake garancije da se njihovom postupanju ne može uću u trag. Ne može se očekivati da će trgovci opojnom drogom želeti da svoja kriminalna tržiša postavljaju na on-line lokacije, na kojima ona mogu lako biti uočena od strane policije odnosno na adresama čiji „blizanci" već postoje na površinskom Web-u. Anonimnost će biti primaran uslov i prilikom prodaje ukradenih pasoša i kreditnih kartica, te ličnih podataka u vezi sa adresama i kontakt detaljima (Ciancaglini i sar., 2015).

Ali, pored diskretnosti u vršenju kriminalnih aktivnosti, postoje i drugi brojni razlozi zbog kojih korisnici žele da budu anonimni prilikom posete sajtova uz tendenciju da se njihovo kretanje na Internetu ne može pratiti, te da se lokacije takvih sajtova ne mogu utvrditi. Korisnici kojima je neophodno da zaštite svoju komunikaciju u odnosu na mere kontrole državnih organa, uvek će insistirati na skrivenosti koju pružaju okolnosti Darkneta. Uzbunjivači neće pristati da svoje insajderske informacije dele sa novinarima i da pri tom ostavljaju bilo kakav trag o tome. Politički neistomišljenici u restriktivnim režimima zahtevaće anonimnost prilikom obaveštavanja svetske javnosti o kršenju ljudskih prava i ograničavanju sloboda u svojim matičnim državama.

Na osnovu navedenog možemo zaključiti da ni svaki korisnik Darketovog okruženja ne mora biti samo zbog toga podrazumevan kao potencijalni nosilac ileganih aktivnosti. Anonimnost Darkneta ne mora u svakom slučaju biti preduslov sajber napada ili formiranja kriminalnog tržišta. Prema nekim mišljenjima, Darknet doprinosi razvoju konstruktivnih socijalnih i političkih vrednosti jer uslovljava poštovanje prava privatnosti i naprednog korišćenja virtuelnih valuta u legalne svrhe (Mirea, Wang i Jung, 2019). Ove činjenice ne umanjuju, kako smatramo, moguću kriminalizovanost Darkneta, ali svakako čine temelj za razvoj perspektive tamnog Web-a, kako u smislu davanja prostora za punu slobodu delovanja ljudske kreativnosti, tako i za jačanje razornog dejstva njenog kriminalnog antipoda.

ZAKLJUČAK

Da li ćemo ikada dosegnuti krajnje granice World Wide Web-a i potpuno razumeti kapacitete Deep Web-a i Darkneta? U ovom trenutku, sasvim su izvesna tehnička i pravna ograničenja koja nas u ovome sputavaju. Neophodno je ovo pitanje razmatrati kao jednu od obaveznih tema za javne debate u kojima učestvuju, kako eksperti iz prakse tako i akademski istraživači, kako bi se makar približili spoznaji o multistrukturalnoj dimenzionalnosti i uticajima nevidljivog Web-a, te konstantnom porastu njegove nepristupačne dubinske komponente. U svakom slučaju, postavljanje balansa između imperativa zaštite sloboda i prava građana i brige za nacionalnu bezbednost obeležiće eru informatičke tehnologije, u kojoj će nesagledivi broj podataka skrivenih u dubokom Web-u predstavljati stalni izazov kreatorima politike u savremenom društvu.

Mišljenja smo da bi sledeći koraci mogli da budu neka vrsta putokaza u pokušajima našeg nesigurnog hoda kroz neprozirno prostranstvo dubokog i tamnog Web-a. Ab initio,

državni resor mora biti odgovoran za sajber bezbednost jer njime rukovode donosioci političkih odluka. U tom smislu, poželjno je odrediti nacionalnog koordinatora za pitanje sajber bezbednosti, određenog inokosno ili timski, koji će usmeravati aktivnosti na održavanju sajber bezbednosti. Zbog efikasnosti, nacionalno telo nadležno za sajber pretnje mora biti centralizovano i sa jedinstvenom bazom podataka. Naravno, temelj za delovanje protiv kriminalnih aktivnosti u sajber prostoru mora biti u posebnom normativnom sistemu, koji će biti posvećen zaštiti kritičke infastrukture i podataka koji se na nju odnose, te činiti osnov za uspostavljanje i delovanje agencija i organa za realizovanje sajber bezbednosti (Kovacs, 2018). Okvir strategije nacionalne sajber bezbednosti trebalo bi da bude određen harmonizovanjem postojećih propisa sa najboljom praksom na međunarodnom planu u oblasti procene rizika i pružanja usluga. Na taktičkom i operativnom nivou važno je izgraditi kapacitete za efikasno reagovanje u slučajevima sajber napada, pri čemu bi nosioci ovih aktivnosti bili za to posebno određeni resorni subjekti. Neophodnost podizanja svesti o sajber bezbednosti mora biti praćena sistemom obuka i planskom edukacijom, kao neizostvanim delovima koncepta nacionalnog obrazovnog sistema. Pored predominantno određene uloge državnih resursa u ostvarivanju sajber bezbednosti, nužno je zasnovati partnerstvo sa privatnim sektorom koje je funkcionalno i pouzdano, te fokusirano na različite oblasti koje mogu biti izložene sajber pretnjama (Kovacs, 2018). Naposletku, ali ne i manje značajno, jeste pitanje međunarodne saradnje, koje se nedvosmisleno i posledično nameće zbog činjenice nemogućnosti sprečavanja sajber pretnji u okvirima državnih granica, a time i olakšanog vršenja široke lepeze kriminalnih aktivnosti na svetskom planu.

Uvereni smo da bi efektivna međunarodna saradnja, u kojoj učestvuju funkcionalne nacionalne strategije sajber bezbednosti koncipirane na najboljim iskustvima inostranih resornih i vanresornih partnera, mogla da odredi dobar početak usmernih napora ka smanjivanju rizika od sajber opasnosti koja dolazi iz skrovitih delova nevidljivog Web-a.

LITERATURA

- Buxton, J., & Bingham, T. (2015). The rise and challenge of dark net drug markets. *Global Drug Policy Observatory*, January 2017, Policy Brief No. 7, 1-24.
- Byrne, J.M., & Kimball, K.A. (2017). Inside the darknet: techno-crime and criminal opportunity. *Criminal Justice Technology in the 21st Century*, 3rd ed., 206–232.
- Chandran, N. (2015). From drugs to killers: exploring the deep web. *CNBC*. Dostupno na: http://www.cnbc.com/2015/06/23/from-drugs-to-killers-exploring-the-deep-web.html, preuzeto 04. 05. 2019.
- Chertoff, M., & Simon, T. (2015). The impact of the dark web on internet governance and cyber security. *Global Commission on Internet Governance*, February 2015, Paper Series No. 6, 1-8.
- Ciancaglini, V., et al. (2015). Below the surface: exploring the deep web. *Trend Micro*, June 2015, 1-48.
- Dolliver, D.S. (2015). Evaluating drug trafficking on the tor network: silk road 2, the sequel. *International Journal of Drug Policy*, 26 (11), 1113–1123.
- Everett, C. (2015). Should the dark net be taken out? *Network Security*, 2015 (3), 10–13.
- Farrell, P. (2017). Inside the darknet: where australians buy and sell illegal goods. *The Guardian*. Dostupno na: https://www.thegu ardia n.com/techn ology/2017/jul/04/inside-the-darknet-where-australians-buy-and-sell-illegal-goods, preuzeto 16.05.2019.
- Finklea, K. (2017). Dark web. *Congressional Research Service*, March 10, 1-16.
- Goodman, M. (2016). *Future crimes: Inside the digital underground and the battle for our connected world*. New York: Anchor Books.
- Greenberg, A. (2014). Over 80 percent of dark-web visits relate to pedophilia, study finds. *Security*. Dostupno na: https://www.wired.com/2014/12/80-percent-dark-web-visits-relate-pedophilia-study-finds/, preuzeto 16.05.2019.
- Greenberg, A. (2015). No, department of justice, 80 percent of tor traffic is not child porn. *Security*. Dostupno na: https://www.wired.com/2015/01/department-justice-80-percent-tor-traffic-child-porn/, preuzeto 18.05.2019.
- Holm, E. (2017). The Darknet: A new passageway to identity theft. *International Journal of Information Security and Cybercrime*, 6 (1), 41–50.
- Horton-Eddison, M., & Di Cristofaro, M. (2017). Hard interventions and innovation in crypto-drug markets: the escrow example. *Global Drug Policy Observatory*, August 2017, Policy Brief No. 11., 1-11.
- https://metrics.torproject.org/, preuzeto 28.05.2019.
- Jackson Higgins, K. (2015). What happens when personal information hits the dark web. *Information Week*. Dostupno na: https://www.darkreading.com/attacks-breaches/what-happens-when-personal-information-hits-the-dark-web/d/d-id/1319801?, preuzeto 09.05.2019.
- Kovacs, L. (2018). National cyber securiry as the corner stone of national security. *Land Forces Academy Review*, Vol. XXIII, No. 2 (90), 113-120.

- Krebs, B. (2013). Cards stolen in target breach flood underground markets. *Krebs on Security*. Dostupno na: https://krebsonsecurity.com/2013/12/cards-stolen-in-target-breach-flood-underground-markets/, preuzeto 12.05.2019.
- Krebs, B. (2015). Tax fraud advice, straight from the scammers. *Krebs on Security*. Dostupno na: https://krebsonsecurity.com/2015/03/tax-fraud-advice-straight-from-the-scammers/, preuzeto 23.05.2019.
- Kruithof, K., Aldridge, J., Décary-Hétu, D., Sim, M., Dujso, E., i Hoorens, S. (2016). *Internet-Facilitated Drugs Trade—An Analysis of the Size, Scope and the Role of the Netherlands*. Santa Monica, CA: Rand Europe.
- Lacson, W., & Jones, B. (2016). The 21st Century darknet market: lessons from the fall of silk road. *International Journal of Cyber Criminology*, 10 (1), 40–61.
- McGoogan, C. (2016). Dark web browser tor is overwhelmingly used for crime, says study. *The Telegraph*. Dostupno na: http://www.telegraph.co.uk/technology/2016/02/02/dark-web-browser-tor-is-overwhelmingly-used-for-crime-says-study/, preuzeto 28.05.2019.
- Mirea, M., Wang, V., & Jung J. (2019). The not so dark side of the darknet: a qualitative study. *Security Journal*, June 2019, Vol. 32, Issue 2, 102-118.
- Moloney, P. (2016). Dark net drug marketplace begin to emulate organised street crime. *The Sidney Morning Herald*. Dostupno na: http://www.smh.com.au/technology/technology-news/dark-net-drug-marketplaces-begin-to-emulate-organised-street-crime-20160111-gm3k1i.html, preuzeto 22.05.2019.
- Moore, D., & Rid, T. (2016). Cryptopolitik and the darknet. *Survival*, February 2016, Vol. 58, No. 1, 7-38.
- Murray, A. (2014). The dark web is not just for paedophiles, drug dealers and terrorists. *The Independent*. Dostupno na: http://www.independent.co.uk/voices/comment/the-dark-web-is-not-just-for-paedophiles-drug-dealers-and-terrorists-9920667.html, preuzeto 22.06.2019.
- Omand, D. (2016). The dark net: policing the internet's underworld. *World Policy*, Winter 2015/2016. Dostupno na: http://www.worldpolicy.org/journal/winter2015/dark-net, preuzeto 27.05.2019.
- Owen, G., & N. Savage. (2015). The tor dark net, *Global Commission on Internet Governance*, September 2015, Paper Series No. 20, 1-9.
- Paganini, P. (2015). How far do stolen data get in the deep web after a breach? *Security Affairs*. Dostupno na: https://securityaffairs.co/wordpress/35902/cyber-crime/propagation-data-deep-web.html, preuzeto 07.06.2019.
- Qiang, B., Zhang, R., Wang, Y., He, Q., Li, W., & Wang, S. (2014). Research on deep web query interface clustering based on hadoop. *Journal of Software*, 9 (12), 3057–3062.
- Samson, A. (2017). Dark net may pose 'disruptive risk' to internet sector—goldman. *Financial Times*. Dostupno na: https://www.ft.com/content/d045b27e-0842-3686-800e-080d8 ca883ae, preuzeto 01.06.2019.

- Sui, D., Caverlee, J., & Rudesill, D. (2015). The deep web and the dark net: a look inside the internet's massive black box. *Science and Technology Innovation Program*, STIP 03, August 2015, 1-17.
- Van Hout, M.C., & Bingham, T. (2013). 'Silk road', the virtual drug marketplace: a single case study of user experiences. *International Journal of Drug Policy*, 24 (5), 385–391.
- Weissman, C.G. (2015). The creepiest and most bizarre stories told by people who explored the internet's hidden websites. *Business Insider UK*. Dostupno na: http://uk.businessinsider.com/creepy-and-weird-deep-web-stories-from-reddit-2015-6?r=USand IR=T, preuzeto 24.06.2019.
- Wright, A. (2008). Searching the deep web. *Communications of the ACM*, 51 (10), 14–15.
- Wueest, C. (2015). Underground black market: thriving trade in stolen data, malware, and attack services. *Symantec*. Dostupno na: https://www.symantec.com/connect/blogs/underground-black-market-thriving-trade-stolen-data-malware-and-attack-services, preuzeto 10.05.2019.
- Zetter, K. (2014). How ram scrapers work: the sneaky tools behind the latest credit card hacks. *Security*. Dostupno na: https://www.wired.com/2014/09/ram-scrapers-how-they-work/, preuzeto 11.05.2019.
- Zheng, Q., Wu, Z., Cheng, X., Jiang, L., & Liu, J. (2013). Learning to crawl deep web. *Information Systems*, 38 (6), 801–819.

Kriminalističke teme
Zbornik radova
Godina XIX, Broj 5, 2019.
ISSN 1512-5505

DARK WEB AS A CONTEMPORARY CHALLENGE TO CYBER SECURITY

Pregledni naučni rad

Tanja MILOSHEVSKA, PhD[87]

ABSTRACT

Inspiration for work:
This paper looks specifically at the dark net which has become notorious in the media for being a hidden part of the web where all manner of illegal activities take place. Precisely, it draw attention to the 'black market' of the Internet–the dark web that represents such a hidden space, being the largest deployed anonymity network.
Goals of paper:
This article analyzes and highlights the major roles played by the Dark Web as a market; as a communication platform; as an enabler of cybercrime; as an enabler of anonymous financial transactions and as a proxy to a surface web.
Methodology/Concept:
The paper is managed by looking at current literature in academic journal databases and own research in dark web. The motivation behind this literature review is to estimate the current state and development of the dark web in relation to the roles it plays and explore how the dark web enables cybercrime.
Limits of the research/work:
It contributes to the space of the dark web by assisting as a citation document and by suggesting a research agenda to renew study on this phenomenon and allow for better projections on how it may reveal over time and as technology expands.
Results/Conclusions:
Criminality on the dark web spans multiple areas and involves a wide range of criminal commodities. An effective countermeasure will therefore require a suitably coordinated, cross-cutting response, involving investigators with equally diverse expertise. This will likely require additional capacity building and training of officers not involved in computer crime. And while though this awareness may not necessarily stop national security threats from the Dark Web, it can certainly shine a spotlight on the issue and facilitate a larger conversation on how the global community can address these emerging threats.
Accontability of the research:
The unique nature of Dark Net markets as highly anonymous and secretive, as well as loyal and intelligent, makes them an ideal test case for the unrestrained online marketplace. There is a need for a global strategy and accountabilty to address the abuse of

[87] Ss. Cyril and Methodius University – Skopje, Faculty of Philosophy, Institute of Security, defense and peace, E-mail: tanja@fzf.ukim.edu.mk

the dark web and other emerging platforms for illicit trade.

Key words
dark web, cyber crime, cyber security, networks, illegal activities

Introduction

The internet can broadly be divided into three parts: surface, deep and dark among which the latter offers anonymity to its users and hosts. The dark web has become notorious in the media for being a hidden part of the web where all manner of illegal activities take place. The more restrictions placed upon the free exchange of information, goods and services between people the more likely there exist hidden spaces for it to take place. The 'black market' of the interet – the dark web - represents such a hidden space.

One such digital environment on the internet is the *Dark Web* or *Darknet,* with the *Tor Network* being the largest deployed anonymity network (The Tor Project, 2018a). This overlay network – a distributed system – affords its users anonymity and makes attribution for activities challenging by encrypting and routing users' traffic via multiple nodes (The Tor Project, 2018b). The most popular version of the dark web – The Onion Routing (Tor) network and protocol – has become a haven for criminals to conduct their operations, including sharing illegally-acquired information, trading illicit contraband, and recruiting others – all with disregard for borders and legality (Vogt, 2017).

The Dark Web began with ARPANET, the Internet's progenitor that was developed by the Pentagon in 1969. As the inter-computer interaction began to grow, "a number of isolated, secretive networks started to appear alongside ARPANET" (McCormick, 2013). These networks eventually became the medium of choice for the U.S. Naval Research Laboratory, which introduced a browser called The Onion Router. Tor, as it is called now, "conceals the location and IP addresses of users who download the software" (McCormick, 2013) in order to protect overseas American operatives and dissidents. However, the software became available for public consumption in 2004, and Tor domains dedicated to drug dealing, child pornography, and terrorism began cropping up.

The Dark Web encompasses a vast amount of information on the Internet, the majority of which is inaccessible to the average user. Tor, the most popular Dark Web browser, which was initially created as a security measure by the U.S. Navy, is now the medium of choice for illegal sites ranging from drug dealing to assassination and terrorism (Lascon and Jones, 2016).

Last year, law enforcement dealt online criminal markets on the dark web a significant blow when two major operations, led by the FBI, the US Drug Enforcement Agency (DEA) and the Dutch National Police, with the support of Europol and a number of other law enforcement agency partners, dismantled two of the largest Darknet markets: AlphaBay

and Hansa. Until that point, along with the Russian Anonymous Marketplace (RAMP), these three markets had accounted for 87% of all Darknet market activity (Chainnalysis, 2018).

Providing easy access to a wide range of illicit commodities and services, these markets are key enablers for other crimes.

Darknet/hidden services

The *dark web*, also known as *darknets* or *hidden services,* is a subset of the network not indexed by search engines because it requires the use of special software for access. It consists of both public and private elements, i.e. accessible publicly or by only those with credentials – provided the correct software is in use. The key difference between the dark web and surface or deep web lies in the lack of accountability present on the dark web. Users are unidentifiable to the network – or anyone monitoring – and their actions are thus effectively anonymised. Furthermore, the dark web allows for hosting of web services (hidden services) which remain anonymous with regards to their true IP address, and thus location, even to the users who use those web services. The difference thus between the dark and deep web is that the former is characterised by unique technology-enabled protocols and anonymity, whereas the latter is more reliant on authentication and thus a lack of public access. Anonymity is not a feature of the deep, and surface, web and both have their unauthenticated parts readily indexed by search engines. By conferring anonymity, private engagements between people have been institutionalised by the dark web.

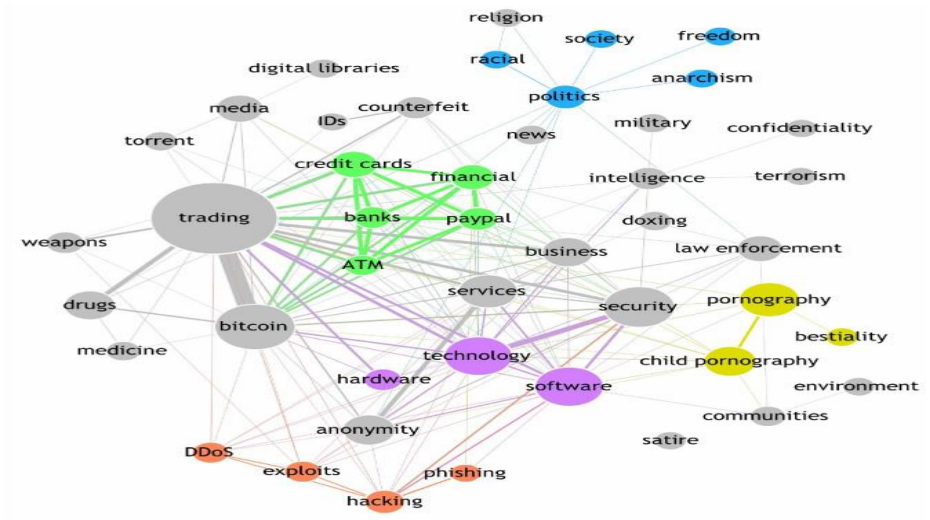


Figure 1: A topic taxonomy of Tor hidden services (Spitter at all, 2014)

The Dark Web has been cited as facilitating a wide variety of crimes. Illicit goods such as drugs, weapons, exotic animals, and stolen goods and information are all sold for profit. There are gambling sites, thieves and assassins for hire, and troves of child pornography (Chertoff and Simon, 2015). Data on the prevalence of these Dark Web sites, however, are lacking. Tor estimates that only about 1.5% of Tor users visit hidden services/Dark Web pages (Tor Project Blog, 2015).

Cybercriminals can victimize individuals and organizations alike, and they can do so without regard for borders. How criminals exploit borders is a perennial challenge for law enforcement, particularly as the concept of borders and boundaries has evolved (Finklea, 2017).

Physical Borders. For law enforcement purposes, jurisdictional boundaries have been drawn between nations, states, and other localities. Within these territories, various enforcement agencies are designated authority to administer justice. When crimes cross boundaries, a given entity may no longer have sole responsibility for criminal enforcement, and the laws across jurisdictions may not be consistent (Richman, 2000). Criminals have long understood these phenomena—and exploited them.

Physical–Cyber Borders. The relatively clear borders within the physical world are not always replicated in the virtual realm. High-speed Internet communication has not only facilitated the growth of legitimate business, but it has bolstered criminals' abilities to operate in an environment where they can broaden their pool of potential targets and rapidly exploit their victims. Frauds and schemes that were once conducted face-to-face can now be carried out remotely from across the country or even across the world. For instance, criminals can rely upon botnets to target victims across the globe without crossing a single border themselves.

Cyber Borders. While cyberspace crosses physical borders, boundaries within cyberspace—both jurisdictional and technological—still exist. Some web addresses, for instance, are country-specific, and the administration of those websites is controlled by particular nations. Another barrier in cyberspace involves the lines between the Surface Web and the Deep Web. Crossing these boundaries may involve subscriptions or fee-based access to particular website content. Certain businesses—news sites, journals, file-sharing sites, and others—may require paid access. Other sites may only be accessed through an invitation.

The Dark Web can play a number of *roles* in malicious activity. As noted, it can serve as a forum—through chat rooms and communication services—for planning and coordinating crimes. For instance, there have been reports that some of those engaged in tax-refund fraud discussed techniques on the Dark Web (Krebs, 2015).

Roles played by the Dark Web

Illicit online markets, both on the surface web and on the dark web, provide criminal vendors the opportunity to purvey all manner of illicit commodities, with those of a more serious nature typically found deeper, in the dark web. Many of these illicit goods and services, such as cybercrime toolkits or fake documents, are enablers for further criminality.

Broad Role	**Specific Cases**	**Description**
As a Market	Illicit drugs traded on markets	All range of drugs from marijuana to cocaine are being sold on eBay-like platforms, e.g. Silk Road 3.0. (Tzanetakis, 2018).
	Malware and exploits – zero-day + known vulnerabilities traded on markets	Exploits targeting a wide range of systems – from specific low-popularity software to prevalent operating system bugs, e.g. WannaCry Ransomware, Eternal Blue exploit. (Armin et al., 2015).
	Credit card, identities, breached data made traded on markets	Stolen credit card info, medical profiles, personally identifying information (PII) allowing identify theft. (Denic, 2017)
	Child Abuse media made available on markets or being sold separately	Child sexual abuse images and videos, available for sale. E.g. on the now-defunct Playpen12. (Kirkpatrick, 2017).
	Weapons traded on markets	Guns for sale, especially in countries where banned (Rhumorbarbe et al., 2018).

Broad Role	**Specific Cases**	**Description**
As a Communication platform	Forums for discussion	Sharing ideas, knowledge, propaganda, recruitment, training. Used by hackers, terrorists, journalists, citizens concerned about sensitive topics. (Sapienza et al., 2018).
	Chat for real-time communication	Instant Messaging/Chat facilitated by Tor, e.g. TorChat13, or end-to-end encrypted chat software, e.g. Telegram14 and Signal15, known to be in use for private communication in real-time. (Maddox et al., 2016).

Broad Role	**Specific Cases**	**Description**
As an enabler of Cybercrime	Malware-as-a-Service business model for criminal services	DDoS and Ransomware is available for use as a service and hosted as Tor Hidden Services (Huang et al., 2017).
	Command-and-Control (C2) servers deployed as hidden services	Botnets are being controlled by C2 services hosted as Tor Hidden Services. (Owen and Savage, 2016).
	Terrorism Operations conducted in conjunction with other roles	Recruitment, training, radicalisation, planning, fundraising for known terrorist organisations, e.g. ISIL (Broadhurst, 2017).

Broad Role	**Specific Cases**	**Description**
As a source of Threat Intelligence	Scanning Forums & Marketplaces for threat intelligence	Generating leads on the type of attacks that may be imminent based on exploits being sold and discussed. (Robertson et al., 2017).

Broad Role	**Specific Cases**	**Description**
As an enabler of anonymous Financial Transactions	Using Bitcoin over Tor for anonymity	Added layer of anonymity and precaution (DiPiero, 2017).
	Money Laundering of cryptocurrencies via tumbling services	Specific services to launder money, e.g. via bitcoin conversion (Dalins et al., 2017).

Broad Role	**Specific Cases**	**Description**
As a Proxy to the Surface Web	Avoid censorship by circumventing blocks	Civilians engaging in ethical behaviour while protecting privacy, e.g. bypassing China's firewall (Chertoff and Simon, 2015).
	Protection from persecution by local authorities due to browsing anonymity	Journalists writing about sensitive topics pertaining to a country which is known for an oppressive regime. (Moore and Rid, 2016).

According to the European Monitoring Centre for Drugs and Drug Addiction (EMCDDA, 2018) and Europol, Germany, the Netherlands and the United Kingdom were the most important countries with regards to the EU-based Darknet drug supply, in terms of sales revenue and volumes. Other research indicates that vendors of certain drugs commodities, such as cannabis and cocaine, are primarily located in a small number of highly active consumer countries. This further suggests that most Darknet market vendors are 'local' retailers serving the 'last mile' for drug trafficking routes (Dittus, Wright and Graham, 2018). This is supported by other research that Darknet markets are mostly used for mid or low-volume market sales or sales directly to consumers. Large-volume sales (wholesale) on Darknet markets are relatively uncommon (Europol, 2018).

The closure of any market will inevitably lead to the migration of customers and vendors to new or existing markets. Prior to the official announcement of the joint market seizures, Alphabay had been offline for several weeks. This had already resulted in a 25% increase in the number of listings appearing on Hansa, as it presumably absorbed the business from its chief competitor. Three months after Alphabay went offline and following the closure of Hansa and RAMP, several of the remaining markets had similarly displayed considerable growth in the number of listings they advertised. Dream Market, the largest remaining English language market, had grown by 20%, while several of the smaller markets such as Wall Street, TradeRoute and T-Chka/P-int had grown by 290%, 475% and 840% respectively (Europol, 2018). However, even collectively these markets did not meet the former scale of Alphabay, suggesting an overall decrease in dark web activity. Industry reporting supports this by highlighting that the value of Bitcoin transactions to Darknet markets fell by two thirds in the aftermath of the takedown operations (Chainalysis, 2018).

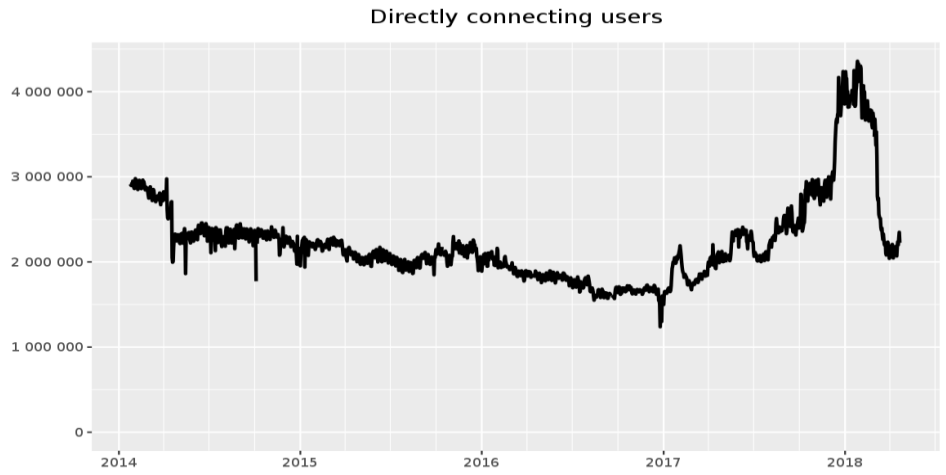


Figure 2*:* Number of users directly connected to Tor (last four years) (Top Project, 2018).

Regardless of attempts to control and curb the growth of Tor, it remains the biggest anonymising network and has had at least 2 million active users connecting directly to the service, with bursts of up to 4 million (Figure 2 above) over the last year.

Compromised data - key commodity on Darknet markets

Compromised personal, medical and financial data is a key commodity for the commission of cyber-dependent crime, but even more so for cyber-enabled crime. It plays a crucial role in activities such as frauds, phishing, identity theft and account takeovers. The prominence of data on Darknet markets reflects this. Data is often the second or third largest category of commodity listed and one of the more common commodities highlighted by law enforcement.

In last year's Europol report (2018), was described the large number of automated credit card shops on the surface web. These are online stores which sell large quantities of compromised payment card data using a fairly standardised automated shopping interface. While a large number of these sites still exist on the surface web, there are a growing number of reports of such sites migrating to the dark web.

Emerging Trends Pertaining to National Security

Whereas the last section of this paper discussed observations so far, this section of the paper will delve into the possibilities of how the Dark Web may evolve to affect national security in years to come. Rather than listing a series of discrete possibilities (as the possibilities are literally endless), we will instead put forth a categorical framework that covers the types of Dark Web national security threats that defense professionals are likely to encounter. Before diving in, we want to make it very clear that no framework is infallible. It is very likely that there are categories of Dark Web threats and possible trends that we did not cover in this framework. We are aware that the threat landscape could change in the blink of an eye as emerging technologies such as quantum computing, digital currency, and 3-D printing continue to evolve. Given these caveats, our understanding of the historical threat landscape, and our research into emerging Dark Web trends, the following is our proposed framework:

Proliferation - Kinetic Weapons

The anonymity facilitated through the Dark Web fosters an ideal trading ground for would-be buyers and sellers of dangerous weapons. This is more than just theoretical – it is a fact that has been proven through observation time and time again. Uranium, dangerous chemical compounds, military grade firearms à these are sample subset of the types of weapons that have been listed on the Dark Web. In response to these listings, the global law enforcement community has been aggressively pursuing would be buyers and sellers of weapons on the Dark Web – and in many cases they have been successful in thwarting potential attacks. In 2016, the U.S. Federal Bureau of Investigation (FBI) collaborated with Irish law enforcement authorities to stop an Irish Republic Army (IRA)

militant from procuring handguns, grenades, and plastic explosives from a Dark Web marketplace (Aliens, 2018). And while the national security community can claim minor victories with these types of preventative operations, those interested in anonymously buying and selling kinetic weapons have begun to shift their methodology.

Over the coming years, we assess that there will be two major evolutions to the ways that kinetic weapons are traded on the Dark Web. The first is that buyers and sellers of Dark Web weapons will likely move their business away from some of the more popular open-access marketplaces (such as Dream Market) and over to other marketplaces that require a higher degree of vetting to enter (such as Demon Forum and OG-Users Forums). This is likely to happen for two primary reasons. The first is that the individuals who engage in the weapons trade are becoming more wary of undercover law enforcement presence and the possibility that they are being lured into a trap. The second is that the major marketplaces are likely becoming less tolerant of the risk they incur by allowing weapons listings on their marketplaces. Weapons listings have historically attracted the attention of the global law enforcement community, which has resulted in undercover officers perusing markets looking for leads. Beyond the increased risk, the marketplace profit margin for the weapons trade is relatively low when compared to the profit margins of other high-volume illicit goods such as drugs and fraud. According to two studies conducted by RAND (2016), global drug sales on the Dark Web were estimated to be between $12-$21.1 million per month in 2016, while the global arms trade was $80k per month in 2017. (RAND, 2017). Below is an image from the Dark Web listing some of the locations where threat actors can still purchase weapons:

Weapons / Оружие	
Guns	Guns and Ammo / Пистолеты и боеприпасы
Pistols	Your european arms dealers / Поставка европейского оружия
Weapons	Guns,Pharmacy,Counterfeits / Оружие, наркотики, подделки валют
Guns Store	Verified marketplace for Guns and other weapons, worldwide shipping / Склад оружия,доставка по всему миру
Lucky47	Weapons from Ukraine / Оружие с Украины
GG Club	Stocks every type of rifle to meet your needs / Оружие и боеприпасы для ваших нужд
Darkseid guns shop	Rifles, Handguns, Silencers, Body Armour / Винтовки, пистолеты, глушители, бронежилеты

Image 5: Examples of Limited Access Dark Web Marketplaces (Rivera and Arcy, 2019)

Whereas the Dark Web is most well-known for hosting illicit economic trade, it has become clear that the Dark Web also holds some very serious national security implications that will affect most nations throughout the globe. The proliferation of cyber and kinetic weapons, the facilitation of terrorism, intelligence gathering, extortion, malicious services-for-hire à all of these illicit activities are occurring on the Dark Web, and the evidence put forth in this paper suggests that these activities may occur at increasing rates in the coming future.

Reflections

Criminality on the dark web spans multiple areas and involves a wide range of criminal commodities. An effective countermeasure will therefore require a suitably coordinated, cross-cutting response, involving investigators with equally diverse expertise. This will

likely require additional capacity building and training of officers not involved in computer crime. And while though this awareness may not necessarily stop national security threats from the Dark Web, it can certainly shine a spotlight on the issue and facilitate a larger conversation on how the global community can address these emerging threats.

However, even with all three top markets sensationally being taken offline by police in the space of a few months, the will or desire to migrate from the familiar territory of Tor to another, potentially safer digital environment still does not appear to be there. It therefore seems unlikely that this will come to pass in the foreseeable future.

The almost inevitable closure of large, global Darknet marketplaces has led to an increase in the number of smaller vendor shops and secondary markets catering to specific language groups or nationalities.

The unique nature of Dark Net markets as highly anonymous and secretive, as well as loyal and intelligent, makes them an ideal test case for the unrestrained online marketplace.

There is a need for a global strategy to address the abuse of the dark web and other emerging platforms for illicit trade.

References

- Armin, J., Foti, P., Cremonini, M. (2015). 0-day vulnerabilities and cybercrime, in: Availability, Reliability and Security (ARES), 10th International Conference On.
- Broadhurst, R. (2017). Cyber Terrorism Research Review Cyber Terrorism: Research Review Research Report of the Australian National University. doi: https://doi.org/10.13140/RG.2.2.19282.96964
- C. Aliens. (2018). "More Details Revealed In The Dublin Explosives Case", Deep Dot Web. doi: https://www.deepdotweb.com/2018/08/05/more-details-revealed-in-the-dublin-explosives-case/.
- Chainalysis. (2018). The changing nature of cryptocrime, Chainalysis: Darknet Market Activity Nearly Doubled Throughout 2018, Crypto Crime Report. doi: https://e-cryptonews.com/chainalysis-darknet-market-activity-nearly-doubled-throughout-2018/.
- Chertoff, M., Simon, T. (2015). The Impact of the Dark Web on Internet Governance and Cyber Security, Global Commission on Internet Governance, The Royal Institute od International Affairs, Centre for International Governance Innovation and Chatham House, No. 6. doi: https://www.cigionline.org/sites/default/files/gcig_paper_no6.pdf.
- Dalins, J., Wilson, C., Carman, M. (2017). Criminal motivation on the dark web: A categorisation model for law enforcement. Digit. Investig.
- Denic, N. V. (2017). Government Activities to Detect, Deter and Disrupt Threats Enumerating from the Dark Web, thesis presented to the Faculty of the U.S. Army Command and General Staff College, Fort Leavenworth, Kansas.
- DiPiero, C. (2017). Deciphering Cryptocurrency: Shining a Light on the Deep Dark Web. U. Ill. L. Rev.1267.
- Dittus, M., Wright, J., Graham, M.. (2018). Platform Criminalism: The 'last-mile' geography of the darknet market supply chain, in WWW 2018, Lyon: France.
- European Monitoring Centre for Drugs and Drug Addiction (2018). doi: http://www.emcdda.europa.eu/drugs-library/emcdda-europol-working-arrangement-2018_en.
- Finklea, K. (2017). The Interplay of Borders, Turf, Cyberspace, and Jurisdiction: Issues Confronting U.S. Law Enforcement, CRS Report R41927.
- Huang, K., Siegel, M., Madnick, S. (2017). Cybercrime-as-a-Service: Identifying Control Points to Disrupt.
- Internet Organized Crime Threat Assessment (2018), Europol, European Union Agency for Law Enforcement Cooperation 2018. doi: www.europol.europa.eu.
- "International arms trade on the dark web". (2017). RAND Corporation. doi: https://www.rand.org/randeurope/research/projects/international-arms-trade-on-the-hidden-web.html.
- Kirkpatrick, K. (2017). Financing the Dark Web. Commun. ACM 60, 21–22.
- Krebs, B. (2015). "Tax Fraud Advice, Straight From the Scammers," Krebs on Security.

- Maddox, A., Barratt, M.J., Allen, M., Lenton, S., (2016). Constructive activism in the dark web: cryptomarkets and illicit drugs in the digital 'demimonde.' Inf. Commun. Soc. 19, 111–126. doi: https://doi.org/10.1080/1369118X.2015.1093531
- McCormick, T. (2013). The Darknet. Foreign Policy, (203), 22-24.
- Moore, D., Rid, T. (2016). Cryptopolitik and the Darknet. Survival (Lond). 58, 7–38.
- Owen, G., Savage, N. (2016). Empirical analysis of Tor hidden services. IET Inf. Secur. 10, 113–118.
- Rhumorbarbe, D, at all., (2018). Characterising the online weapons trafficking on cryptomarkets. Forensic Sci. Int. 283, 16–20.
- Richman, D. (2000). "The Changing Boundaries Between Federal and Local Law Enforcement," Boundary Changes in Criminal Justice Organizations, pp. 81-111, http://www.ncjrs.gov/criminal_justice2000/vol_2/02d2.pdf.
- Rivera, J., Archy, W. (2019). The Role of the Dark Web in Future Cyber Wars to Come, Small War Journal. doi: https://smallwarsjournal.com/jrnl/art/role-dark-web-future-cyber-wars-com.
- Robertson, J., at all. (2017). Darkweb Cyber Threat Intelligence Mining. Cambridge: University Press.
- Sapienza, A. at all, (2018). Early Warnings of Cyber Threats in Online Discussions. arXiv Prepr. arXiv1801.09781.
- Spitters, M., Verbruggen, S., van Staalduinen, M. (2014). Towards a comprehensive insight into the thematic organization of the tor hidden services, in: Intelligence and Security Informatics Conference (JISIC), 2014 IEEE Joint.
- "Taking Stock of the Online Drugs Trade". (2016). RAND Corporation. doi: https://www.rand.org/randeurope/research/projects/online-drugs-trade-trafficking.html.
- The Tor Project. (2018a). Tor Metrics [WWW Document]. Tor Proj. doi: https://metrics.torproject.org/
- The Tor Project. (2018b). Tor Project [WWW Document]. doi: https://www.torproject.org/
- Tor Project Blog. (December 30, 2014) Tor: 80 Percent of ??? Percent of 1-2 Percent Abusive.
- Tzanetakis, M. (2018). Comparing cryptomarkets for drugs. A characterisation of sellers and buyers over time. Int. J. Drug Policy.
- Vogt, S.D. (2017). The Digital Underworld: Combating Crime on the Dark Web in the Modern Era. St. Cl. J. Int'l L. 15.
- Wesley L., Jones, B. (2016). The 21st Century DarkNet Market: Lessons from the Fall of Silk Road, International Journal of Cyber Criminology (IJCC).

Kriminalističke teme
Zbornik radova
Godina XIX, Broj 5, 2019.
ISSN 1512-5505

CYBER KRIMINAL KAO MODERNA SIGURNOSNA PRIJETNJA U BOSNI I HERCEGOVINI

CYBERCRIME AS A MODERN SECURITY THREAT IN BOSNIA AND HERZEGOVINA

Pregledni naučni rad

Amina SMAILHODŽIĆ[88]

SAŽETAK

Inspiracija za rad i problem (i) koji se radom oslovljava (ju): Razvojem informacijske tehnologije cyber kriminal egzistira kao netrpeljiv vid kršenja zakona i zloupotreba. Posjeduje specifične karakteristike koje ga izdvajaju od drugih kriminalnih delikata i pri tome predstavlja oblik kriminala koji nema granice i kao takvog ga je teško otkriti. Posljedice nastale cyber kriminalom su velike kako za pojedince, tako i za državu. Cyber kriminal je poprimio globalno obilježje i širokim razmjerama uništava poslovne sisteme stvarajući enormne finansijske troškove. Cyber kriminal ocrtava kriminalnu djelatnost počinjenu upotrebom računara, mreža i računarskih sistema. Veliki broj incidenata uzrokovanih cyber kriminalom odnosi se na bankarske prevare i na zloupotrebu identiteta na društvenim mrežama.

Ciljevi rada (naučni i/ili društveni): Tema ovog rada se obrađuje sa naučnog i društvenog aspekta. Trebaju se objasniti činjenice koje se odnose na problem cyber kriminala u Bosni i Hercegovini. Naučni cilj istraživanja treba da iskaže odgovarajući nivo naučnog saznanja o cyber kriminalu u Bosni i Hercegovini. Društveni cilj istraživanja odnosi se na informisanje o cyber kriminalu kao modernoj sigurnosnoj prijetnji u Bosni i Hercegovini, odnosno da se građani Bosne i Hercegovine, a i šire upoznaju sa karakteristikama i prisutnostima cyber kriminala u Bosni i Hercegovini.

Metodologija/Dizajn: U ovom istraživanju se analizira cyber kriminal kao moderna sigurnosna prijetnja u Bosni i Hercegovini. Paradigma kojoj istraživanje pripada jeste pozitivizam. Primjenom analize sadržaja dokumenata izvršen je pregled dostupne literature o cyber kriminalu. U istraživanju je zastupljena i hipotetičko-deduktivna metoda, induktivna, metoda analize, sinteze, metoda apstrakcije, metoda deskripcije i statistička metoda.

Ograničenja istraživanja/rada: Cyber kriminal je kompleksan i prekriva različite kriminalne djelatnosti u koje su uključeni napadi na računare, kompjuterske sisteme i podatke. Istraživanje će se usredočiti na prostor Bosne i Hercegovine.

Rezultati/Nalazi: Rezultati istraživanja trebaju opravdati naučni i društveni značaj istraživanja. Rezultatima naučnog istraživanja iskazana je ozbiljnost posljedica koje cyber kriminal proizvodi. Na internetu se svakodnevno ugrožava sigurnost putem društvenih mreža, web sajtova, kao i elektronske trgovine.

[88] Amina Smailhodžić, MA, Fakultet za kriminalistiku, kriminologiju i sigurnosne studije Univerziteta u Sarajevu, magistar sigurnosnih studija, aminasmailhodzic@fkn.unsa.ba

Generalni zaključak: Cyber kriminal označava negativnu društvenu pojavu savremenog doba. Istraživanje cyber kriminala u Bosni i Hercegovini treba se analizirati u kontinuitetu. Cyber kriminal nije nacionalno, geografsko i vremensko ograničen. Zbog dinamičnog razvoja informacijskih tehnologija neophodno je stalno posmatranje promjena koje se odigravaju da bi se uspješno suprotstavilo izazovima cyber kriminala. Prevencija se treba ogledati na preduzimanju djelatnosti da bi se otklonili propusti koji su naklonjeni zloupotrebi računarskih podataka i sistema. Prevencija podrazumijeva i preduzimanje aktivnosti i pripremanje plana osoblja koje radi na sistemu tehnologije kako bi se spriječio neovlašten pristup sistemu. Uspješno suprotstavljanje cyber kriminalu je moguće ukoliko se uključi cijela međunarodna zajednica.
Opravdanost istraživanja/rada: Rezultati istraživanja cyber kriminala kao moderne sigurnosne prijetnje u Bosni i Hercegovini trebaju opravdati naučni i društveni značaj. Naučna i društvena opravdanost ogleda se u povećanju naučnih saznanja iz oblasti cyber kriminala. Istraživanje je naučno opravdano, jer nas upućuje u problem, a ukoliko dobro poznajemo problem na putu smo da ga riješimo ili bar smanjimo posljedice uzrokovane cyber kriminalom. Naučna opravdanost ide u pravcu i heurističkog i verifikatornog rezultata. Pružanje doprinosa koji je heuristički kroz proučavanje cyber kriminala u Bosni i Hercegovini od velike je važnosti za cjelokupnu državu. Kada je u pitanju verifikacijski rezultat, u pravcu verifikacije se ide jer se istraživanje svodi na potvrdu teze da u Bosni i Hercegovini postoji cyber kriminal. Tendencija razvoja cyber kriminala predstavlja veliki problem koji kod većine građana stvara osjećaj nesigurnosti i zabrinutosti.

Ključne riječi
cyber kriminal, sigurnost, društvene mreže, elektronska trgovina

ABSTRACT
Reason for writing and research problem (s): By developing information technology, cybercrime exists as an intolerable aspect of violation of law and abuse. It has specific characteristics that distinguish it from other criminal delinquencies and is a form of crime that has no boundaries and as such is difficult to detect. The consequences of cybercrime are great for individuals as well as for the state. Cybercrime has taken a global dimension and broadly destroys business systems by creating enormous financial costs. Cybercrime illustrates the criminal activity committed by using computers, networks and computer systems. A large number of cybercrime incidents are related to bank fraud and the abuse of identity on social networks.
Aims of the paper (scientific and/or social): The theme of this paper is being studied from a scientific and social point of view. The facts related to the cybercrime problem in Bosnia and Herzegovina need to be explained. The scientific aim of the research should show the appropriate level of scientific knowledge about cybercrime in Bosnia and Herzegovina. The Social Objective of Research relates to information on cybercrime as a modern security threat in Bosnia and Herzegovina, respectively that citizens of Bosnia and Herzegovina, and beyond, are introduced to the characteristics and the presence of cybercrime in Bosnia and Herzegovina.
Methodology/Design: This research analyzes cybercrime as a modern security threat in Bosnia and Herzegovina. The paradigm to which research belongs is positivism. By using the method of analyzing the content of documents, a review of accessible cybercrime literature was performed. The hypothetical-deductive method, the inductive, the analysis method, the synthesis, the abstraction method, the descriptive method and the statistical method are represented in the research.

Research/Paper limitation: Cybercrime is complex and covers various criminal activities that involve attacks on computers, computer systems, and data. The research will be centered on the territory of Bosnia and Herzegovina.
Results/Findings: Research results should justify the scientific and social significance of research. The results of scientific research have shown the seriousness of the cybercrime consequences. The Internet is endangered on a daily basis through social networks, web sites, and e-commerce.
General Conclusion: Cybercrime means a negative social phenomenon of the contemporary age. Cybercrime research in Bosnia and Herzegovina needs to be analyzed in continuity. Cybercrime is not national, geographic, and time constrained. Due to the dynamic development of information technology, it is imperative to constantly observe the changes that are taking place in order to successfully counter the challenges of cybercrime. Prevention should be reflected in the take-up of activities in order to overcome the failures of abusing computer data and systems. Prevention also implies undertaking activities and preparing staff plans for the technology system to prevent unauthorized access to the system. Successful cybercrime is possible if the entire international community is involved.
Research/Paper Validity: Cybercrime findings as modern security threats in Bosnia and Herzegovina should justify scientific and social significance. Scientific and social justification is reflected in the increase of scientific knowledge in the field of cybercrime. The research is scientifically justified because it points to the problem, and if we know the problem in the way we are to solve it or at least reduce the consequences of cybercrime. Scientific justification goes in the direction of heuristic and verifiable results. Providing a heuristic contribution through cybercrime research in Bosnia and Herzegovina is of great importance to the entire country. When it comes to the verification result, the verification is going because the research is lowered to confirm the thesis that cybercrime exists in Bosnia and Herzegovina. The tendency to develop cybercrime is a major problem that creates a sense of insecurity and concern for most citizens.

Keywords
cyber crime, security, social networks, electronic commerce

1. UVOD

Najpotpunija definicija cyber kriminala data je u dokumentu „Kriminal vezan za kompjutersku mrežu“ (Report of Committee II, Workshop on crimes related to the computer-network) sa Desetog Kongresa Ujedinjenih nacija, posvećenog prevenciji kriminala i tretmanu počinilaca koji je održan u Beču od 10 do 17. aprila 2000. godine (Tenth United Nations Congress on the Prevention of Crime and Treatment of Offenders, Wienna, 10-17 April 2000. godine). Radna grupa eksperata u sadržaju izvještaja pod cyber kriminalom podrazumjeva „kriminal koji se odnosi na bilo koji oblik kriminala koji se može izvršavati sa kompjuterskim sistemom i mrežama, u kompjuterskim sistemima i mrežama ili protiv kompjuterskih sistema i mreža (Porobić i Bajraktarević, 2012, str. 15)“.

Na Desetom kongresu UN o sprečavanju zločina i postupanju sa prestupnicima, koji je održan 2000. godine zaključeno je da se cyber kriminal pojavljuje u užem i širem smislu. U užem smislu cyber kriminal se može posmatrati kao protivpravno ponašanje koje je potaknuto na elektronsko obavljanje sigurnosti računarskih sistema, kao i podataka koji se obrađuju, dok cyber kriminal u širem smislu se posmatra kao protivpravno ponašanje koje je povezano za mrežu i računarski sistem, a obuhvata i protivpravno davanje i dijeljenje informacija preko mreže i računarskih sistema. Cyber kriminal predstavlja oblik kriminala gdje se kao sredstvo izvršenja kriminalnog djela javljaju računarske mreže. Ovaj vid kriminalnog ponašanja većinom vrše pojedinci, dok nije rijetkost da su i same kriminalne organizacije uključene u ovaj vid kriminala, koji za posljedicu ima neovlašten pristup informacijama sa stepenom povjerljivosti, ali i njihovo objavljivanje. Cyber kriminalom mijenjaju se računarski podaci. Cyber kriminal sadrži široki spektar protivpravnih djelatnosti kako neovlašteni pristup računarskoj mreži tako i maloljetničkoj pornografiji, zloupotrebi platnih kartica, ali isto tako i krivičnim djelima koja ugrožavaju sigurnost internet korisnika.

U današnjem svijetu sve više se koristi pojam „cyber“, a da u stvari i ne znamo šta on znači. Pojam „cyber“ prvo se pojavio u vojnoj terminologiji, u smislu predviđanja budućih oblika ratovanja. „Cyberwar“ predstavlja ratovanje znanjem, odnosno informacijama. Radi se o ratu visoke tehnologije, koji se odnosi na prikupljanje povjerljivih informacija (Gligorević, 2014, str. 164). Cyber rat predstavlja događaj koji se dešava u cyber prostoru i ima elemente konvencionalnog rata. Pojedini teoretičari smatraju da je operacija Orchard, koju je Izrael iskoristio aktivacijom komponenti ugrađenih u informacioni sistem kako sirijski radari ne bi bili u mogućnosti da uoče izraelske zrakoplove na sirijskoj teritoriji predstavljala cyber rat. Zagovornici povećanih proračunskih izdvajanja za osposobljavanje američke vojske za vođenje operacija u cyber-prostoru nerijetko pokušavaju uvjeriti javnost da je cyber-rat već otpočeo i pritom se koriste metaforom „cyber Pearl Harbor”. No, dok o tome tko je, kada, gdje i kako izveo stvarni napad na Pearl Harbor nema nikakve dvojbe, kao ni o trenutnim i dugoročnim posljedicama koje je taj napad imao na odvijanje i ishod 2. svjetskog rata, o tome tko je i kada izveo „cyber Pearl Harbor”, kao i o tome je li se to uopće dogodilo, suglasnosti nema. Uvjerljivost te metafore, koja je u opticaj stavljena 1990-ih, bitno je umanjena terorističkim napadima na New York i Pentagon 11. rujna 2001. Te napade svi su vidjeli i broj njihovih žrtava mjeri se tisućama. Vidljivih razornih posljedica i ljudskih žrtava cyber-napada nema i stoga je javnost teško uvjeriti da je cyber-rat već otpočeo (Kovačević, 2013, str. 92). Riječ kibernetika, engl. Cybernetics nema isto značenje kao riječ cyber. Cyber u riječniku stranih riječi označava osnovnu materiju koja je povezana za svijet imaginarne stvarnosti nastalu preko kompjutera. Kibernetika se može definisati kao “sustavno proučavanje komunikacije i upravljanja u organizacijama svih vrsta“ (Deutsch, 1966, str. 76).

Veoma težak put predstavlja ulazak u trag kriminalnim počiniteljima koji koriste specifičan način, kao i sredstvo za izvršenje krivičnog djela cyber kriminala pomoću računara. Na tom putu je zaista potrebno uložiti mnogo zalaganja. Kriminalni počinitelji su osobe koje su veoma dobro upoznate sa savremenom tehnologijom. Kriminalni počinitelji cyber

kriminala sa predumišljajem nastoje drugima nanijeti štetu i ostvariti sebi ili drugima imovinsku ili neimovinsku korist. Lica koja se bave ovim nelegalnim radnjama su, uglavnom, studenti, informatički stručnjaci, bivši inspektori kriminalističkih službi i brojni drugi koji dobro poznaju savremenu tehnologiju (Gligorević, 2014, str. 166). Cyber kriminal predstavlja visokotehnološki kriminal i počinioci ovog vida kriminala su veoma obrazovana lica. Kriminalna lica koriste svoja stručna znanja kako bi ostvarili svoje motive. Najčešće se kao motiv ističe novac, odnosno sticanje imovinske koristi. Pojam cyber kriminal se može definisati kao oblik kriminalnog ponašanja za čije izvršenje se koristi računarska oprema. Lica koja obavljaju takve kriminalne radnje su cyber kriminalci. Uglavnom su to muškarci između 19 i 30 godina starosti. Postoji veoma mali broj žena koje se bave ovim nedozvoljenim radnjama, ali se one uglavnom pojavljuju kao saučesnici (Mesarović, 2006). Cyber kriminal čini lice koje nezakonito uđe u tuđu bazu informacija i obavlja unošenje, izmjenu, sakrivanje, kopiranje, upotrebu, objavu, onemogućavanje upotrebe programa korisnika i unošenje nekog podatka ili virusa. 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 (Krstić, 2009).

I najmanji propust cyber kriminalcu pruža pogodak za lakšu zloupotrebu povjerljivih informacija." 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 i sajber kriminal na nivou pojedinaca (Cornish, Hughes, Livingstone, 2009). Tradicionalne kriminalne grupe i organizacije modernizuju se korišćenjem ICT, a *cyber prostor* postaje sredina u kojoj deluju i koja im istovremeno služi kao skrovište (Porobić, i Bajraktarević, 2012, str. 13). Kibernetski prostor određujuće je obilježje suvremenog života i ključno područje svjetskog gospodarstva (Vuković, 2012). U listopadu 2006. Združeni stožer oružanih snaga SAD-a definirao je kibernetski prostor kao „područje koje karakterizira upotreba elektroničkog i elektromagnetskog dijapazona za pohranjivanje, modificiranje i razmjenjivanje podataka putem mrežnih sustava i povezanih fizičkih infrastruktura" (Wynne, 2006).

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 (Radnović, Ilić, i Radović, 2012, str. 131).

Kako bi se prikrile nedozvoljene radnje kompjuterska mreža predstavlja idealno oruđe za izvođenje napada poput trgovine ljudima, trgovine drogom, dječije pornografije, pedofilije i sl. Većinom počinitelji u obavljanju krivičnog djela cyber kriminala vrše DOS napade, odnosno napade na kompjuterski servis kako bi korisnicima bilo onemogućeno korištenje i ubacuju štetni softver. Trojanski konj, računarski crv, špijunski softver, oglašivački softver, keylogger, računarski virus, lažni antivirusni programi predstavljaju samo neke od štetnih programa kako bi se preuzela kontrola nad korisnikovim računarom.

Trojanski konj sposoban je obavljati razne radnje kao što su krađa brojeva sa platne kartice, zloupotreba lozinki i ostale informacije koje se zatim šalju drugom licu. Trojanski konj većinom se koristi da bi se preuzela datoteka ili nekoliko njih, a odmah nakon preuzimanja se instalira zlonamjerni softver na zaraženom računaru. Napadač može samostalno izgraditi ili kupiti od drugog napadača Trojanskog konja. Naročito su opasni bankarski Trojanski konji, koji imaju za cilj udar na bankarske sisteme i berze dionica kojima je Internet oslonac. Glavna funkcija bankarskih Trojanskih konja je zloupotreba korisnikovih ličnih podataka, preuzimanje kontrole nad računarom u potpunosti ili djelimično i krađa brojeva platnih kartica i PIN-ova. Trojanski konji su specifični jer se dijele u nekoliko porodica i različiti su po oruđu koje koriste za izvođenje napada i djelovanju zaraženog korisnika. Računarski crv označava zlonamjernu vrstu programa koja se rasprostire mrežom i obično se rasprostiru putem elektronske pošte. Špijunski softver predstavlja zlonamjerni program koji prikuplja podatke o korisnikovom korištenju računara i na osnovu toga preuzima kontrolu nad računarom. Oglašivački softver predstavlja softver koji korisniku pokazuje oglase i u vremenu kada uopšte nije povezan sa internetom.

Keylogger predstavlja zlonamjerni špijunski program čija je osnovna svrha praćenje unosa korisnika putem tastature. Programi praćenja se odlažu na poseban računar, koji napadač koristi. Osim toga, keylogger na klik miša korisnika može da uzima snimak sa ekrana i na osnovu toga se vidi program koji korisnik koristi i šta pretražuje na internetu. Keylogger se pojavljuje kao aparat koji se ugrađuje u pojedine dijelove računara i kao oruđe u formi programskih paketa. Računarski virus predstavlja program kojim se zaraze programi i datoteke, dok lažni antivirusni programi imaju namjeru da navedu korisnika na kupovinu simulacijom pretraživanja korisnikovog računara. Kao mogući ciljevi cyber kriminala mogu se navesti napad na hardver, napad na softver, napad na programe kako bi se uništila, prisvojila ili nanijela šteta kompjuterskom sistemu i kako bi se neovlašteno koristila informaciona sredstva. Veoma su česte prevare putem e:mail adresa, plaćanje preko interneta, prevare platnim karticama, lažni identitet. 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 (Radnović, Ilić, i Radović, 2012. str. 137).

Veliki broj djela cyber kriminala posjeduje međunarodnu dimenziju. Počinitelji cyber kriminala ne moraju biti prisutni na određenom mjestu gdje je prisutna žrtva, a u skladu sa time istrage cyber kriminala zahtijevaju međunarodnu saradnju. „Budući da na sadašnjem stepenu razvoja nije moguće ostvariti apsolutnu sigurnost kompjuteriziranih i međusobno povezanih informacijskih sistema, bez obzira na poduzete fizičke, tehničke (hardverske i softverske) i druge mjere, nužno je uz postojeće mjere, metode i sredstva zaštite, osigurati efikasnu pravnu zaštitu koja će se provoditi u suradnji s nadležnim organizacijama i ustanovama drugih zemalja širom svijeta“ (Hamidović, Hamidović, i Zajmović, 2016, str. 561).

2. CYBER SIGURNOST

Cyber sigurnost je upala u žarište zainteresovanosti usljed raširenog korištenja interneta. Cyber kriminal orijentisan je protiv sigurnosti informacionog sistema kako bi kriminalno lice pribavilo sebi korist a istovremeno nanijelo štetu drugome. Cyber sigurnost treba se odnositi na zaštitu od zloupotrebe informacionog sistema. Neke od mjera tehničke zaštite predstavljaju lozinke, identifikatori korisnika i slično. Kako bi korisnici stekli povjerenje u korištenje informacione tehnologije potrebno je da informacioni sistemi pruže sigurnost korištenja informacione tehnologije. Mnoge osobe strahuju da njihovi podaci ne budu predmet zloupotrebe. Neprikladno primjenjivanje mjera sigurnosti predstavlja razlog za ugrožavanje sigurnosti. Neizostavno je da organizacija koja ima ozbiljan pristup za informacijsku sigurnost da:

1. posjeduje razvijeni plan za otkrivanje, izvještaj i procjenu nastalu incidentima,
2. odgovori nastalim incidentima obuhvatajući određene mjere zaštite kako bi se spriječili i smanjili negativni uticaji,
3. nauči iz nastalih incidenata i u budućnosti unaprijedi sistem manipulisanja incidenata.

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 (Milašinović, Mijalković i Amidžić, 201. str. 31). Za suprotstavljanje cyber kriminalu neophodno je usvajanje adekvatne zakonske regulative u području materijalnog i procesnog prava i adekvatno primjenjivanje tih normi. Kompjuterska mreža služi kao dokaz u postupku dokazivanja cyber kriminala. U suprotstavljanju cyber kriminalu postoji nekoliko mehanizama da bi se objasnile i opisale faze kojima se djeluje na suzbijanje cyber kriminala.

U Bosni i Hercegovini ne postoje odgovarajući mehanizmi za suprotstavljanje cyber kriminalu. Nedostatak novca za ulaganje u sigurnosne sisteme predstavlja ogroman problem kada je u pitanju odgovarajuća i uspješna borba protiv cyber kriminala u Bosni i Hercegovini. Suprotstavljanje cyber kriminalu predstavlja neizostavan dio Strategije Bosne i Hercegovine za prevenciju i borbu protiv terorizma od 2010.-2013. godine, gdje

je zabilježeno da nema pouzdanih pokazatelja u kom obimu i u kolikoj mjeri je ova moderna sigurnosna prijetnja zastupljena u Bosni i Hercegovini. Na nivou entiteta u Bosni i Hercegovini zakonski su regulisana djela protiv sistema mreže elektronske obrade podataka, dok je na državnom nivou nedozvoljeno korištenje autorskih prava usko vezano za kompjuterski kriminal. U krivičnom zakonu Federacije Bosne i Hercegovine nalaze se krivična djela protiv sustava elektronske obrade podataka.

Član 393. (Oštećenje računalnih podataka i programa)

(1) Ko ošteti, izmijeni, izbriše, uništi ili na drugi način učini neupotrebljivim ili nepristupačnim tuđe računalne podatke ili računalne programe, kaznit će se novčanom kaznom ili kaznom zatvora do jedne godine.

(2) Ko unatoč zaštitnim mjerama neovlašćeno pristupi računalnim podacima ili programima ili neovlašćeno presreće njihov prijenos, kaznit će se novčanom kaznom ili kaznom zatvora do tri godine.

(3) Kaznom iz stava 2. ovog člana kaznit će se ko onemogući ili oteža rad ili korišćenje računalnog sustava, računalnih podataka ili programa ili računalnu komunikaciju.

(4) Ako je krivično djelo iz st. od 1. do 3. ovog člana učinjeno u odnosu na računalni sustav, podatak ili program organa vlasti, javne službe, javne ustanove ili privrednog društva od posebnog javnog interesa, ili je prouzrokovana znatna šteta, kaznit će se kaznom zatvora od tri mjeseca do pet godina.

(5) Ko neovlašćeno izrađuje, nabavlja, prodaje, posjeduje ili čini drugom dostupne posebne naprave, sredstva, računalne programe ili računalne podatke stvorene ili prilagođene radi učinjenja krivičnog djela iz st. od 1. do 3. ovog člana, kaznit će se novčanom kaznom ili kaznom zatvora do tri godine.

(6) Posebne naprave, sredstva, računalni programi ili podaci stvoreni, korišćeni ili prilagođeni radi učinjenja krivičnih djela, kojima je krivično djelo iz st. od 1. do 3. ovog člana učinjeno, oduzet će se.

Član 394. (Računalno krivotvorenje)

(1) Ko neovlašćeno izradi, unese, izmijeni, izbriše ili učini neupotrebljivim računalne podatke ili programe koji imaju vrijednost za pravne odnose, s ciljem da se upotrijebe kao pravi ili sam upotrijebi takve podatke ili programe, kaznit će se novčanom kaznom ili kaznom zatvora do tri godine.

(2) Ako je krivično djelo iz stava 1. ovog člana učinjeno u odnosu na računalne podatke ili programe organa javne službe, javne ustanove ili privrednog društva od posebnog

javnog interesa, ili je prouzrokovana znatna šteta, kaznit će se kaznom zatvora od tri mjeseca do pet godina.

(3) Ko neovlašćeno izrađuje, nabavlja, prodaje, posjeduje ili čini drugom pristupačnim posebne naprave, sredstva, računalne programe ili računalne podatke stvorene ili prilagođene radi učinjenja krivičnog djela iz st. 1. i 2. ovog člana, kaznit će se novčanom kaznom ili kaznom zatvora do tri godine.

(4) Posebne naprave, sredstva, računalni programi ili podaci stvoreni, korišćeni ili prilagođeni radi učinjenja krivičnih djela kojima je učinjeno krivično djelo iz stava 1. ili 2. ovog člana, oduzet će se.

Član 395. (Računalna prijevara)

(1) Ko neovlašćeno unese, ošteti, izmijeni ili prikrije računalni podatak ili program ili na drugi način utiče na ishod elektronske obrade podataka s ciljem da sebi ili drugom pribavi protupravnu imovinsku korist i time drugom prouzrokuje imovinsku štetu, kaznit će se kaznom zatvora od šest mjeseci do pet godina.

(2) Ako je krivičnim djelom iz stava 1. ovog člana pribavljena imovinska korist koja prelazi 10.000 KM, učinitelj će se kazniti kaznom zatvora od dvije do deset godina.

(3) Ako je krivičnim djelom iz stava 1. ovog člana pribavljena imovinska korist koja prelazi 50.000 KM, učinitelj će se kazniti kaznom zatvora od dvije do dvanaest godina.

(4) Ko krivično djelo iz stava 1. ovog člana učini samo s ciljem da drugog ošteti, kaznit će se novčanom kaznom ili kaznom zatvora do tri godine.

Član 396. (Ometanje rada sustava i mreže elektronske obrade podataka)

Ko neovlašćenim pristupom u sustav ili mrežu elektronske obrade podataka izazove zastoj ili poremeti rad tog sustava ili mreže, kaznit će se novčanom kaznom ili kaznom zatvora do tri godine.

Član 397. (Neovlašćeni pristup zaštićenom sustavu i mreži elektronske obrade podataka)

(1) Ko se neovlašćeno uključi u sustav ili mrežu elektronske obrade podataka kršenjem mjera zaštite, kaznit će se novčanom kaznom ili kaznom zatvora do jedne godine.

(2) Ko upotrijebi podatak dobijen na način iz stava 1. ovog člana, kaznit će se kaznom zatvora do tri godine.

(3) Ako su krivičnim djelom iz stava 2. ovog člana prouzrokovane drugom teške posljedice, učinitelj će se kazniti kaznom zatvora od šest mjeseci do pet godina.

Član 398. (Računalna sabotaža)

Ko unese, izmijeni, izbriše ili prikrije računalni podatak ili program ili se na drugi način umiješa u računalni sustav, ili uništi ili ošteti naprave za elektronsku obradu podataka s ciljem da onemogući ili znatno omete postupak elektronske obrade podataka značajnim organima vlasti, javnim službama, javnim ustanovama, trgovačkim društvima ili drugim pravnim osobama od posebnog javnog interesa, pa time prouzrokuje štetu u iznosu većem od 500.00 KM, kaznit će se kaznom zatvora od jedne do osam godina.[89]

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 (Vasić, Šarić i Jovanić, 2012, str. 183).

U krivičnom zakonu Republike Srpske, glava XXXIV, navedena su krivična djela protiv bezbjednosti kompjuterskih podataka:

Član 407. (Oštećenje kompjuterskih podataka i programa)

(1) Ko neovlašteno izbriše, izmijeni, ošteti, prikrije ili na drugi način učini neupotrebljivim kompjuterski podatak ili program, kazniće se novčanom kaznom ili kaznom zatvora do jedne godine.

(2) Ako je djelom iz stava 1. ovog člana prouzrokovana šteta u iznosu koji prelazi 10.000 KM, učinilac će se kazniti kaznom zatvora od šest mjeseci do tri godine.

(3) Ako je djelom iz stava 1. ovog člana prouzrokovana šteta u iznosu koji prelazi 50.000 KM, učinilac će se kazniti kaznom zatvora od jedne do pet godina.

---

[89] *Krivični zakon Federacije Bosne i Hercegovine*. Glava XXXII. Krivična djela protiv sustava elektronske obrade podataka, Službene novine Federacije BiH, br. 36/2003, 21/2004-ispr., 69/2004, 18/2005, 42/2010, 42/2011, 59/2014, 76/2014, 46/2016 i 75/2017

(4) Uređaji i sredstva kojima je izvršeno krivično djelo iz st. 1. i 2. ovog člana oduzeće se.

Član 408. (Kompjuterska sabotaža)

Ko unese, uništi, izbriše, izmijeni, ošteti, prikrije ili na drugi način učini neupotrebljivim kompjuterski podatak ili program ili uništi ili ošteti kompjuter ili drugi uređaj za elektronsku obradu i prenos podataka sa namjerom da onemogući ili znatno ometa postupak elektronske obrade i prenosa podataka koji su od značaja za republičke organe, javne službe, ustanove, privredna društva ili druge subjekte, kazniće se kaznom zatvora od šest mjeseci do pet godina.

Član 409. (Izrada i unošenje kompjuterskih virusa)

(1) Ko napravi računarski virus u namjeri njegovog unošenja u tuđi kompjuter ili kompjutersku ili telekomunikacionu mrežu, kazniće se novčanom kaznom ili kaznom zatvora do šest mjeseci.

(2) Ko unese računarski virus u tuđi kompjuter ili kompjutersku mrežu i time prouzrokuje štetu, kazniće se novčanom kaznom ili kaznom zatvora do dvije godine.

(3) Uređaj i sredstva kojima je izvršeno krivično djelo iz st. 1. i 2. ovog člana oduzeće se.

Član 410. (Kompjuterska prevara)

(1) Ko unese netačan podatak, propusti unošenje tačnog podatka ili na drugi način prikrije ili lažno prikaže podatak i time utiče na rezultat elektronske obrade i prenosa podataka u namjeri da sebi ili drugom pribavi protivpravnu imovinsku korist i time drugom prouzrokuje imovinsku štetu, kazniće se novčanom kaznom ili kaznom zatvora do tri godine.

(2) Ako je djelom iz stava 1. ovog člana pribavljena imovinska korist koja prelazi iznos od 10.000 KM, učinilac će se kazniti kaznom zatvora od jedne do osam godina.

(3) Ako je djelom iz stava 1. ovog člana pribavljena imovinska korist koja prelazi iznos od 30.000 KM, učinilac će se kazniti kaznom zatvora od dvije do deset godina.

(4) Ko djelo iz stava 1. ovog člana izvrši samo u namjeri da drugog ošteti, kazniće se novčanom kaznom ili kaznom zatvora do šest mjeseci.

Član 411. (Neovlašteni pristup zaštićenom kompjuteru, kompjuterskoj mreži, telekomunikacionoj mreži i elektronskoj obradi podataka)

(1) Ko se, kršeći mjere zaštite, neovlašteno uključi u kompjuter ili kompjutersku mrežu ili neovlašteno pristupi elektronskoj obradi podataka, kazniće se novčanom kaznom ili kaznom zatvora do šest mjeseci.

(2) Ko snimi ili upotrijebi podatak dobijen na način utvrđen u stavu 1. ovog člana, kazniće se novčanom kaznom ili kaznom zatvora do dvije godine.

(3) Ako je usljed djela iz stava 1. ovog člana došlo do zastoja ili ozbiljnog poremećaja funkcionisanja elektronske obrade i prenosa podataka ili mreže ili su nastupile druge teške posljedice, učinilac će se kazniti kaznom zatvora do tri godine.

(4) Kaznom iz stava 1. ovog člana kazniće se i ko izradi, pribavi, proda ili da na korištenje uputstvo ili sredstvo koje je namijenjeno za ulaženje u kompjuterski sistem.

Član 412. (Sprečavanje i ograničavanje pristupa javnoj kompjuterskoj mreži)

(1) Ko neovlašteno sprečava ili ometa pristup javnoj kompjuterskoj mreži, kazniće se novčanom kaznom ili kaznom zatvora do jedne godine.

(2) Ako djelo iz stava 1. ovog člana učini službeno lice u vršenju službe, kazniće se novčanom kaznom ili kaznom zatvora do tri godine.

Član 413. (Neovlašteno korištenje kompjutera ili kompjuterske mreže)

(1) Ko neovlašteno koristi kompjuterske usluge ili kompjutersku mrežu u namjeri da sebi ili drugom pribavi protivpravnu imovinsku korist, kazniće se novčanom kaznom ili kaznom zatvora do šest mjeseci.

(2) Gonjenje za djelo iz stava 1. ovog člana preduzima se po prijedlogu.[90]

U krivičnom zakonu Brčko distrikta Bosne i Hercegovine, glava XXXII, nalaze se krivična djela protiv sistema elektronske obrade podataka. Prema članu 387. krivičnog zakona Brčko distrikta Bosne i Hercegovine (***Oštećenje računarskih podataka i programa)***:

(1) Ko ošteti, izmijeni, izbriše, uništi ili na drugi način učini neupotrebljivim ili nepristupačnim tuđe računarske podatke ili računarske programe, kaznit će se novčanom kaznom ili kaznom zatvora do jedne godine.

[90] *Krivični zakon Republike Srpske*. Glava XXXIV. Krivična djela protiv bezbjednosti kompjuterskih podataka. Službeni glasnik Republike Srpske broj: 64/17 i 104/2018-odluka US

(2) Ko unatoč zaštitnim mjerama neovlašteno pristupi računarskim podacima ili programima ili neovlašteno presreće njihov prenos, kaznit će se novčanom kaznom ili kaznom zatvora do tri godine. Kaznom iz stava 2. ovoga člana kaznit će se ko onemogući ili oteža rad ili korištenje računarskog sistema, računarskih podataka ili programa ili računarsku komunikaciju.

(3) Ako je krivično djelo iz stavova od 1. do 3. ovoga člana počinjeno u odnosu na računarski sistem, podatak ili program tijela vlasti, javne službe, javne ustanove ili trgovačkog društva od posebnog javnog interesa, ili je prouzrokovana znatna šteta, kaznit će se kaznom zatvora od tri mjeseca do pet godina.

(4) Ko neovlašteno izrađuje, nabavlja, prodaje, posjeduje ili čini drugome dostupne posebne sprave, sredstva, računarske programe ili računarske podatke stvorene ili prilagođene radi počinjenja krivičnog djela iz stavova od 1. do 3. ovoga člana, kaznit će se novčanom kaznom ili kaznom zatvora do tri godine.

(5) Posebne sprave, sredstva, računarski programi ili podaci stvoreni, korišteni ili prilagođeni radi počinjenja krivičnih djela, kojima je krivično djelo iz stavova od 1. do 3. ovoga člana počinjeno, oduzet će se.

Član 388. (Računarsko krivotvorenje)

(1) Ko neovlašteno izradi, unese, izmijeni, izbriše ili učini neupotrebljivim računarske podatke ili programe koji imaju vrijednost za pravna lica, s ciljem da se upotrijebe kao pravi ili sam upotrijebi takve podatke ili programe, kaznit će se novčanom kaznom ili kaznom zatvora do tri godine.

(2) Ako je krivično djelo iz stava 1. ovoga člana počinjeno u odnosu na računarske podatke ili programe tijela, javne službe, javne ustanove ili trgovačkog društva od posebnog javnog interesa, ili je prouzrokovana znatna šteta, kaznit će se kaznom zatvora od tri mjeseca do pet godina.

(3) Ko neovlašteno izrađuje, nabavlja, prodaje, posjeduje ili čini drugome pristupačnim posebne sprave, sredstva, računarske programe ili računarske podatke stvorene ili prilagođene radi počinjenja krivičnog djela iz stavova 1. i 2. ovoga člana, kaznit će se novčanom kaznom ili kaznom zatvora do tri godine.

(4) Posebne sprave, sredstva, računarski programi ili podaci stvoreni, korišteni ili prilagođeni radi počinjenja krivičnih djela, kojima je počinjeno krivično djelo iz stavova 1. ili 2. ovoga člana, oduzet će se.

Član 389. (Računarska prevara)

(1) Ko neovlašteno unese, ošteti, izmijeni ili prikrije računarski podatak ili program ili na drugi način utiče na ishod elektroničke obrade podataka s ciljem da sebi ili drugome pribavi protivpravnu imovinsku korist i time drugome prouzrokuje imovinsku štetu, kaznit će se kaznom zatvora od šest mjeseci do pet godina.

(2) Ako je krivičnim djelom iz stava 1. ovoga člana pribavljena imovinska korist koja prelazi 10.000 KM, počinilac će se kazniti kaznom zatvora od dvije do deset godina.

(3) Ako je krivičnim djelom iz stava 1. ovoga člana pribavljena imovinska korist koja prelazi 50.000 KM, počinilac će se kazniti kaznom zatvora od dvije do dvanaest godina.

(4) Ko krivično djelo iz stava 1. ovoga člana počini samo s ciljem da drugoga ošteti, kaznit će se novčanom kaznom ili kaznom zatvora do tri godine.

Član 390. (Ometanje rada sistema i mreže elektroničke obrade podataka)

Ko neovlaštenim pristupom u sistem ili mrežu elektroničke obrade podataka izazove zastoj ili poremeti rad toga sistema ili mreže, kaznit će se novčanom kaznom ili kaznom zatvora do tri godine.

Član 391. (Neovlašteni pristup zaštićenome sistemu i mreži elektroničke obrade podataka)

(1) Ko se neovlašteno uključi u sistem ili mrežu elektroničke obrade podataka kršenjem mjera zaštite, kaznit će se novčanom kaznom ili kaznom zatvora do jedne godine.

(2) Ko upotrijebi podatak dobijen na način iz stava 1. ovoga člana, kaznit će se kaznom zatvora do tri godine.

(3) Ako su krivičnim djelom iz stava 2. ovoga člana prouzrokovane drugome teške posljedice, počinilac će se kazniti kaznom zatvora od šest mjeseci do pet godina.

Član 392. (Računarska sabotaža)

Ko unese, izmijeni, izbriše ili prikrije računarski podatak ili program ili se na drugi način umiješa u računarski sistem, ili uništi ili ošteti sprave za elektronsku obradu podataka s ciljem da onemogući ili znatno omete postupak elektronske obrade podataka značajnih organima vlasti, javnim službama, javnim ustanovama, trgovačkim društvima ili drugim pravnim licima od posebnog javnog interesa, kaznit će se kaznom zatvora od jedne do osam godina.[91]

Uspješno suprotstavljanje cyber kriminalu zahtijeva znatno ozbiljniji pristup i zaštitu korisnika interneta, između ostalog i stalno praćenje, upotrebom moderne sigurnosne opreme za suprotstavljanje cyber kriminala i proširivanje znanja o cyber kriminalu. Za uspješno reagovanje na cyber kriminal potrebno je preduzeti mjere prevencije da bi se suzbio ovaj vid kriminala kao i povećala svijest o opasnosti koji cyber kriminal sa sobom pruža. Za uspješnu borbu neophodna je također međunarodna saradnja državnih organa koji imaju zadatak otkrivanja i progona izvršilaca krivičnog djela cyber kriminala. Krivično pravo predstavlja neizostavni element u borbi kriminala. Pravovremeno usvajanje zakonskih propisa da bi se obezbijedio mehanizam za obračun sa cyber kriminalom, kao i uspješna upotreba takvih propisa trebaju predstavljati zakonsku podlogu izgradnje kriminalne politike kada su u pitanju represivne mjere. Moguće je otkriti računar na koji program šalje prikupljene podatke obavljanjem dinamičke analize upotrebom programa za analizu ponašanja nedobronamjernih programa i simulacijom nedobronamjernih programa u kontrolisanom okruženju. Podaci dobiveni na takav način mogu se iskoristiti za automatsko otkrivanje računara za odlaganje podataka koje je prikupio program za praćenje unosa znakova s tastature. Upotreba ove tehnike vrlo je uspješna (Porobić, i Bajraktarević, 2012, str. 112).

Prvi potpuni dokument koji se odnosi na probleme cyber kriminala jeste Konvencija o kibernetičkom kriminalu Vijeća Europe, koja je potpisana 23. novembra 2001. godine, a stupila na snagu 1. jula 2004. godine. Konvencija o kibernetičkom kriminalu Vijeća Europe ima formu međunarodnog ugovora. Konvenciju je potpisalo tridesetosam zemalja, dok je Bosna i Hercegovina istu ratifikovala 25. marta 2006. godine. Odredbe Konvencije nisu direktno primjenjive. „Brza zaštita pohranjenih kompjuterskih podataka (član 16.) je mjera koju članice konvencije trebaju propisati kako bi omogućile svojim organima da izdaju naredbe ili na neki drugi način nametnu brzu (hitnu) zaštitu elektronskih podataka koji su pohranjeni u kompjuterskom sistemu“ (Selimović, 2015, str. 74).

Vijeće Europe je donijelo 28. januara 2003. godine Dodatni protokol uz Konvenciju o kibernetičkom kriminalu o kriminalizaciji akata rasizma i ksenofobije koje su počinjene

[91] *Krivični zakon Brčko distrikta Bosne i Hercegovine*. Glava XXXII. Službeni glasnik Brčko distrikta BiH br. 33/2013 - prečišćen tekst, 47/2014 - ispravka 26/2016, 13/2017 i 50/2018

pomoću pojedinih kompjuterskih sistema. Četiri skupine krivičnih djela Konvencija o kibernetičkom kriminalu Vijeća Europe je predvidjela, i to:

- krivična djela protiv povjerljivosti, integriteta i disponibilnosti kompjuterskih podataka i sistema (nedozvoljen pristup, nezakonito presretanje, povreda integriteta podataka, povreda integriteta sistema i zloupotreba uređaja),
- kompjuterska krivična djela (kompjutersko krivotvorenje, kompjuterska prevara, krivična djela u vezi sa sadržajem, krivična djela koja se odnose na dječiju pornografiju),
- krivična djela u vezi napada na intelektualnu svojinu i odnosna prava (krivična djela koja se odnose na kršenje autorskih i njima sličnih prava).

Analizom sadržaja odredbi državnih i nedržavnih zakona se može zaključiti da se obaveza preuzeta potpisom i ratifikacijom Konvencije u pogledu krivično materijalnog prava uglavnom ispoštovala i da su krivična djela predviđena odredbama Konvencije u modificiranoj formi i sadržaju ugrađena u nove glave i odredbe nedržavnih krivičnih zakona u Bosni i Hercegovini (Porobić, i Bajraktarević, 2012, str. 23). Na osnovu Konvencije o kibernetičkom kriminalu Vijeća Europe i Direktive Savjeta Europske Zajednice Bosna i Hercegovina je konstituisala pravnu regulativu koja se primjenjuje u području otkrivanja i sprečavanja cyber kriminala.

3. METODE ISTRAŽIVANJA

Metodom istraživanja dolazimo do naučnog saznanja. Disciplinarna prednost teme *Cyber kriminal kao moderna sigurnosna prijetnja u Bosni i Hercegovini* spada u područje metodologije društvenih nauka. Metodom analize sadržaja dokumenata analiziranjem sadržaja sa interneta, sadržaja iz knjiga, časopisa, prikupili su se različiti podaci informacijskog materijala. Glavni zadatak ovog rada je analiza dostupnih izvještaja o informaciji o stanju sigurnosti i izvodi na području Bosne i Hercegovine da bi se detaljnije upoznali sa stanjem cyber kriminala na području Bosne i Hercegovine. Istraživanje se bavi uporednim pokazateljima krivičnih djela u određenom vremenskom periodu.

Hipotetičko-deduktivna metoda se primjenjuje zbog toga što se predmet odnosi na društvenu stvarnost. Deskripcija se primjenjuje u početnoj fazi istraživanja i predstavlja postupak opisivanja činjenica o cyber kriminalu. Apstrakcijom se odvajaju nebitne, a ističu bitne osobine određene pojave istraživanja, u ovom istraživanju pojave cyber kriminala. U istraživanju je zastupljena i induktivna metoda, metoda analize, sinteze i statistička metoda.

Metodologija prikupljanja podataka bazirala se na kvalitativnom i kvantitativnom istraživanju. Kvalitativno istraživanje sastoji se u sekundarnoj analizi kvalitativnih podataka sadržanih u publikacijama o cyber kriminalu, dok se kao metod prikupljanja kvantitativnih podataka sproveo intervju. Osnovni cilj istraživanja jeste da se na osnovu

prikupljenih podataka dođe do saznanja o dinamici cyber kriminala. Namjera je da se u analizu uzmu predmeti koji se odnose na cyber kriminal u Bosni i Hercegovini i to za vremenski period od 01. 01. 2015. do 31. 12. 2018. godine. Uzorci koji će biti podvrgnuti analizi u ovom istraživačkom projektu jesu izvještaji grupe eksperata o cyber kriminalu u Bosni i Hercegovini u vremenskom periodu 01. 01. 2015.-31. 12. 2018. godine. Za potrebe ovog istraživanja konsultovali su se iskazi najcitiranijih eksperata u Bosni i Hercegovini, izneseni u dostupnoj literaturi. Na temelju navedenih podataka ne možemo reći da je uzorak reprezentativan. S obzirom na navedene podatke o krivičnim djelima protiv sistema elektronske obrade podataka za uzorak možemo reči da je ilustrativan. Uzorci koji su podvrgnuti analizi jesu godišnji izvještaji podataka Federalne uprave policije o stanju cyber kriminala, Ministarstva unutrašnjih poslova Republike Srpske i Ministarstva unutrašnjih poslova Brčko distrika Bosne i Hercegovine i informacije o stanju sigurnosti Bosne i Hercegovine, koja je sačinjena u okviru nadležnosti Ministarstva sigurnosti Bosne i Hercegovine na osnovu dostupnih podataka sigurnosnih agencija (Državne agencije za istrage i zaštitu, Granične policije BiH, Službe za poslove sa strancima, Obavještajno-sigurnosne agencije, entitetskih Ministarstava unutrašnjih poslova i Policije Brčko distrikta Bosne i Hercegovine).

Prostorno određenje cyber kriminala kao moderne sigurnosne prijetnje u Bosni i Hercegovini se odnosi na teritoriju Bosne i Hercegovine, odnosno na entitete Federaciju Bosne i Hercegovine i Republiku Srpsku i Brčko distrikt Bosne i Hercegovine. Osim ovog istraživanja napravljena je anketa na populaciji od šezdeset ispitanika starijih od 18 godina kako bismo spoznali da li su građani glavnog grada Bosne i Hercegovine bili ikada žrtve cyber kriminala, da li često mijenjaju svoje lozinke, da li imaju instaliran anti virus na svojim uređajima, obavljaju li kupovinu online i da li su korisnici internet bankarstva. 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 (Pena, i Mitrović, 2012, str. 93). Cyber kriminal po osobinama veoma je sličan sa protivpravnim radnjama prevare i otuđivanja tuđe stvari.

4. REZULTATI

Prema Ministarstvu sigurnosti Bosne i Hercegovine djela koja se klasificiraju pod pojmom cyber kriminala su ometanje rada sistema i elektroničke obrade podataka, prevare na internetu, neovlašten pristup zaštićenom sistemu i mreži elektroničke obrade podataka, krivotvorenje kreditnih i ostalih kartica bezgotovinskog načina plaćanja, posjedovanje i distribucija dječije pornografije, kaznena djela u vezi sa zloupotrebama wireless mreža te društvenih mreža, kaznena djela povrede autorskih prava. Također, u Bosni i Hercegovini sve češća je pojava ekonomske špijunaže, širenja malware – a, neovlaštenog upada u zaštićene sisteme, krađe bankovnih kartica, a najčešča pojava je slučajeva koji se tiču internet prevare (Šakić, 2016, str. 1). Glavna hipoteza autora u istraživanju glasi: „*Cyber kriminal predstavlja modernu sigurnosnu prijetnju u Bosni i Hercegovini i izražen je u formi kriminala vezanog za kompjuterske mreže i upada u kompjuterski sistem.“* Pomoću

kompjuterske mreže napad se provodi na sadržaj i servis koji je na mreži sa ciljem zloupotrebe podataka, ali i uništenja mreže. Cyber kriminalci imaju cilj da navedu osobe da otkriju što više podataka o sebi kako bi ih zloupotrijebili za usluge bez korisnikovog znanja. Uništenje mreže može biti djelimično ili u cjelosti. Upad u kompjuterski sistem vrše hakeri služeći se internetom. Hakere motiviše finansijska dobit. Internet cyber kriminalcima olakšava krađu platnih kartica, krađu identiteta i obavljanje drugih nezakonitih radnji.

„Postoje mnogobrojni inkriminisani primjeri u praksi koji su se desili a da je prethodno slobodni prostor korištenja interneta i mogućnost korištenja lažnog identiteta pored nebrojeno provedenih sati za računarom, upravo psihički „okidač" da osoba nekome ili nečemu nanese neko zlo ili štetu. Često su prisutne ucjene i razne prijetnje objavljivanja kompromitujućih sadržaja neke osobe putem interneta ukoliko se ne plati određeni iznos novca ili se ne učini neka usluga itd. Pored ovakvih, postoje još i ekstremniji slučajevi. Naime, internet u današnje vrijeme služi kao veoma moćno sredstvo za teroriste, kao i za vršenje krivičnih djela, ali, isto tako, internet služi i kao sredstvo propagande, širenja nemoralnih sadržaja, raznih nacionalističkih, retrogradnih i drugih društveno i globalno neprihvatljivih ideja" (Blagojević i Guska, 2016, str. 18).

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. 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 (Milašinović, Mijalković i Amidžić, 2012, str. 34). Na području Bosne i Hercegovine cyber kriminal postepeno dominira. BiH je 2006. godine raficirala Konvenciju o kibernetičkom kriminalu Vijeća Evrope iz 2001. godine. Odredbe Konvencije su uključene u entitetske zakone (poput odredbi o oštećenju računarskih podataka i programa; računarska sabotaža). Sadržajem odredaba državnog Zakona o krivičnom postupku i entitetskih zakona o krivičnom postupku nisu preuzeta krivično procesna rješenja sadržana u Konvenciji, što za posljedicu ima brojne dileme u provedbi krivičnih odredbi iz oblasti (Porobić i Bajraktarević 2012). Unutar Federalne uprave policije u okviru Sektora kriminalističke policije djeluje Odjel za borbu protiv organiziranog kriminala, u okviru kojeg rade istražitelji cyber kriminala, a koji postoji od 2008. godine, dok u Ministarstvu unutrašnjih poslova Republike Srpske postoji od 2010. godine. Policija Brčko distrikta Bosne i Hercegovine u sastavu Jedinice kriminalističke policije, u okviru odsjeka za Droge i organizovani kriminalitet i odsjeka za krim. obavještajnu podršku i terorizam, bavi se istragama koje su vezane za cyber kriminal. U posmatranom vremenskom periodu od 01. 01. 2015. do 31. 12. 2018. godine izvršena je analiza izvještaja podataka Federalne uprave policije o stanju cyber kriminala, Ministarstva unutrašnjih poslova Republike Srpske i Ministarstva unutrašnjih poslova Brčko distrika Bosne i Hercegovine i informacije o stanju sigurnosti u Bosni i Hercegovini.

Najčešći oblici načina izvršenja krivičnog djela iz oblasti kompjuterskog kriminala su:

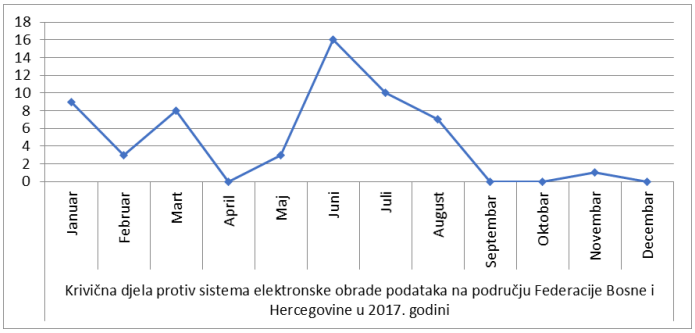
- neovlašteno dolaženje do pasvorda i korištenje istih bez dozvole stvarnih vlasnika a u cilju pribavljanja protivpravne materijalne koristi ili drugih benefita (zloupotreba informacija u cilju diskreditacije vlasnika ili sakrivanja stvarnog autora informacija preko drugih IP adresa...)
- neovlašteno sprečavanje ili ometanje pristupa javnoj mreži,
- izrada i unošenje računarskih virusa u namjeri njegovog unošenja u tuđi računar ili računarsku mrežu ili telekomunikacionu mrežu,
- unos netačnih ili propuštanje unosa tačnih podataka ili na drugi način uticanje na rezultat elektronske obrade i prenosa podataka u namjeri pribavljanja protivpravne imovinske koristi,
- zloupotreba audio-vizuelnih sadržaja.[92]

Najčešće prevare u svijetu, ali i u BiH su CEO (Chief Executive Officer) i BEC (Business E-mail Compromise) prevare. U CEO prevarama, napadač korištenjem autoriteta osobe u nekoj privrednoj organizaciji šalje podređenom instrukcije za plaćanje sa maila unaprijed kreiranog tako da se predstavlja kao autoritet pod oznakom hitnosti. Ovaj bez provjeravanja namjera svog nadređenog šalje novac na račun, većinom je to Velika Britanija. Iz Velike Britanije se redirektuje u Afriku, to je u skladu sa istragama, ne mora biti uvijek. I BEC prevare, to je najčešće i u BiH i u svijetu, kada napadač preuzima korištenje e-maila od privrednih subjekata u BiH, primjera, i u dijelu maila u forwarding stavlja svoj mail. Ovo je jedna tehnika, da napomenem. Čitavo vrijeme prati korespondenciju između privrednog subjekta iz BiH i njegovog dobavljača, recimo iz Njemačke, daću primjer. U jednom momentu kada dođe do plaćanja, avansnog ili nešto slično, šalje fakturu, odnosno mijenja dio fakture koji se odnosi na plaćanje. Predstavljaju se kao taj dobavljač, šalje žrtvi, žrtva uplaćuje novac i tek shvati, kada roba nije isporučena ili kada dobije žalbe svog dobavljača, da je prevarena". U BiH do sada najveća takva prevara iznosila je 900.000 konvertibilnih maraka (KM), a u Evropi oko 40 miliona eura. U takvim prevarama nije teško pratiti digitalne i tragove novca, ali je veoma teško kada su to napadači iz Afrike, što se u većini slučajeva i dešava... U BiH, uz CEO i BEC prevare, postoje i mnoge druge, kao što su prodaja robe nevjerovatnih svojstava, tačnije nepostojeće robe.[93]

Prema analitičkim pokazateljima Federalne uprave policije Bosne i Hercegovine najrasprostranjeniji slučajevi cyber kriminala na području Federacije Bosne i Hercegovine su: krađe novca posredstvom bankovnih kartica, sabotiranje poslovnih e-mail računa, kriptiranje informacijskih sistema korisnika, odnosno napadi koji se vrše putem malicioznih

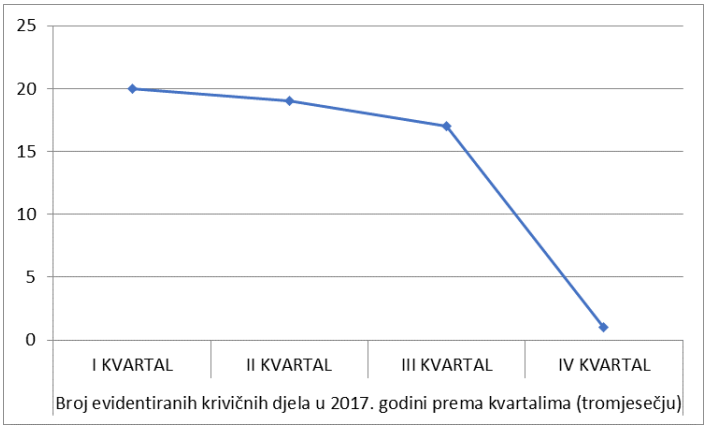
[92] Više pogledati: *Informacija o stanju sigurnosti u Bosni i Hercegovini u 2017. godini*. Bosna i Hercegovina, Ministarstvo sigurnosti. Januar-decembar 2017. Sarajevo, juni 2018.
[93] Više pogledati: Intervju na temu „Cyber kriminal sve češća pojava u BiH: Informisati se o opasnostima interneta" sa Saša Petrović, istražitelj za borbu protiv kompjuterskog kriminala u Federalnoj upravi policije (FUP).

programa na IT sistem. Prema podacima o stanju sigurnosti u Bosni i Hercegovini u 2015. godini na području Federacije Bosne i Hercegovine je izvršeno ukupno 18 krivičnih djela protiv sistema elektronske obrade podataka, a za ista krivična djela prijavljeno je samo 6 lica. Tokom 2016. godine broj krivičnih djela je naglo porastao na 26 krivičnih djela (računalna prijevara i neovlašćeni pristup zaštićenom sistemu i mreži elektronske obrade podataka) i prijavljeno je 16 lica, na osnovu čega možemo zaključiti da od ukupnog broja izvršenih krivičnih djela broj prijava opada. Kada je u pitanju broj otkrivenih djela protiv sistema elektronske obrade podataka u toku 2016. godine od ukupnog navedenog broja otkriveno je samo 18 krivičnih djela što znači da je kada je u pitanju ukupan broj otkriveno 69,23% krivičnih djela protiv sistema elektronske obrade podataka, dok se u toku 2017. godine bilježi znatan porast kako u povećanom broju krivičnog djela tako i u rasvijetljenosti 39 krivičnih djela, odnosno 68,42%.



Ilustracija 1

Ilustracija 1. pokazuje broj krivičnih djela izvršenih po mjesecima u toku 2017. godine. Uzimajući u obzir cijelu 2017. godinu na području Federacije Bosne i Hercegovine evidentirano je 57 krivičnih djela protiv sistema elektronske obrade podataka (računalna prijevara i neovlašćeni pristup zaštićenom sistemu i mreži elektronske obrade podataka), što znači da opšta sklonost ka krivičnim djelima protiv sistema elektronske obrade podataka za 2016/17. godinu iznosi 119, 23%.



Ilustracija 2.

U ilustraciji 2. su prikazana krivična djela protiv sistema elektronske obrade podataka raspoređena po kvartalima. Primjetno je opadanje broja krivičnih djela tokom IV kvartala. Na području Federacije Bosne i Hercegovine tokom 2018. godine evidentirano je 21 krivično djelo protiv sistema elektronske obrade podataka. Otkriveno je 14 krivičnih djela, što iznosi 66,67% od ukupnog broja krivičnih djela protiv sistema elektronske obrade podataka.

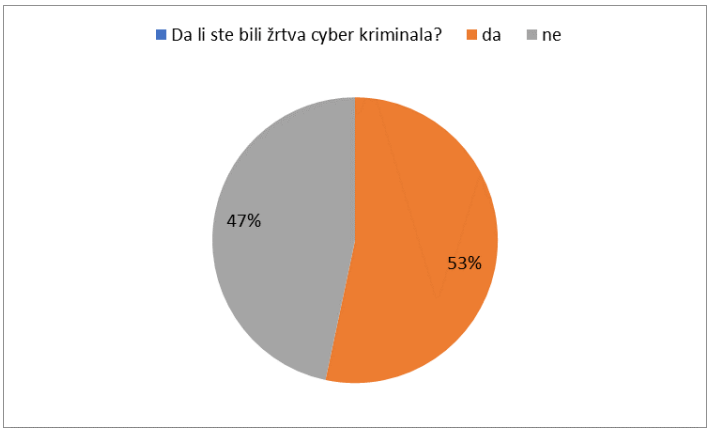
Prema dostupnim analitičkim pokazateljima Izvještaja o radu Ministarstva unutrašnjih poslova Republike Srpske najrasprostranjeniji slučajevi cyber kriminala na području Republike Srpske su: računarske prevare, izrađivanje i unošenje računalnih virusa, iskorištavanje djece i maloljetnika za pornografiju, neovlašten pristup zaštićenom računalu, računalnoj i telekomunikacijskoj mreži i elekronskoj obradi podataka, falfiskovanje kreditnih i kartica za bezgotovinsko plaćanje, kompjuterska sabotaža i oštećenje računarskih podataka i programa. Tokom 2015. godine na području Republike Srpske prijavljeno je 11 krivičnih djela cyber kriminala, dok je otkriveno svega 9 krivičnih djela cyber kriminala. Tokom 2016. godine zabilježeno je dvostruko više krivičnih djela cyber kriminala (izrada i unošenje računalnih virusa, računarske prevare, neovlašten pristup zaštićenom računalu, računalnoj i telekomunikacijskoj i elektronskoj obradi podataka, falsifikovanje kreditnih kartica i kartica za bezgotovinsko plaćanje, proizvodnja, posjedovanje i prikazivanje dječje pornografije, iskorištavanje djece i maloljetnih lica za pornografiju u odnosu na prethodnu godinu. Prijavljeno je 20 osoba što itekako predstavlja povećanje kriminala u odnosu na 2015. godinu. Tokom 2018. godine na području Republike Srpske je otkriveno 50 krivičnih djela iz oblasti cyber kriminala, što je za 19 krivičnih djela više u odnosu na 2017. godinu, gdje su dominirale računarske prevare, neovlašten pristup zaštićenom računaru, računalnoj i telekomunikacijskoj i elektronskoj obradi podataka, oštećenje računarskih podataka i programa i proizvodnja, posjedovanje i prikazivanje dječje pornografije.

Prema mišljenju eksperata iz oblasti cyber sigurnosti najrasprostranjeniji slučajevi cyber kriminala na području Brčko distrikta Bosne i Hercegovine su računarske prevare i oštećenja računarskih podataka i programa. Na području Brčko distrikta Bosne i Hercegovine prema informaciji o stanju sigurnosti u Bosni i Hercegovini tokom 2015. i 2016. godine nije bilo evidentiranih krivičnih djela protiv sistema elektronske obrade podataka, dok je u 2017. godini evidentirano jedno krivično djelo protiv sistema elektronske obrade podataka. Prema informaciji o stanju sigurnosti u Bosni i Hercegovini nije navedeno koje od navedenih krivičnih djela protiv sistema elektronske obrade podataka je evidentirano. Kada je u pitanju 2018. godina za sada nema dostupnih podataka koliki je tačan broj krivičnih djela protiv sistema elektronske obrade podataka na području Brčko distrikta Bosne i Hercegovine.

Pozitivna zakonska praksa u Bosni i Hercegovini suočava se sa izrazito kompliciranim vrstama krivičnih djela cyber kriminala. Cyber kriminal postaje najopasniji vid kriminala kako zbog veće prisustva u institucijama društva, tako i otežanog načina dokazivanja i otkrivanja. Vrste, kao i broj krivičnih djela cyber kriminala i finansijsku štetu koju uzrokuje cyber kriminal zaista je teško procijeniti. Narednih godina u Bosni i Hercegovini izvjesno je očekivati naglu ekspanziju krivičnih djela protiv sistema elektronske obrade podataka budući da informacijska tehnologija brzo napreduje.

Osim toga u istraživanju su zastupljeni i stavovi građana (N=60) na području Sarajeva tokom mjeseca juna 2019. godine. Istraživanje se svodi na glavni grad Bosne i Hercegovine[94]. S obzirom na provedenu anketu koja je obuhvatila Sarajevo, glavni grad Bosne i Hercegovine, koji ulazi u sastav Federacije Bosne i Hercegovine za navedeni uzorak ne može se reći da je reprezentativan, jer ne odražava stavove građana kroz osvrt na sve administrativne jedinice Bosne i Hercegovine U okviru empirijskog istraživanja koristila se i metoda analize sadržaja dokumenata i metoda ispitivanja. Pošto građani koriste internet svakodnevno za instrument istraživanja se sproveo intervju, kreiran za tu priliku. U ovom dijelu rada možemo saznati koliko je građana od ukupno šezdeset ispitanih lica na području glavnog grada Bosne i Hercegovine starijih od 18 godina bilo žrtva cyber kriminala, da li često mijenjaju svoje lozinke, imaju li instaliran antivirus na svojim uređajima, kupuju li online i da li koriste internet bankarstvo. Svi ispitanici koriste internet.

[94] Bosna i Hercegovina je država sastavljena iz dva entiteta: Federacije Bosne i Hercegovine i Republike Srpske i Distrikta Brčko. Glavni i najveći grad Bosne i Hercegovine je Sarajevo. Iako Sarajevo ulazi u sastav Federacije Bosne i Hercegovine, cilj ankete je bio spoznati stavove građana u glavnom gradu države Bosne i Hercegovine. Zbog toga je anketa provedena u Sarajevu.

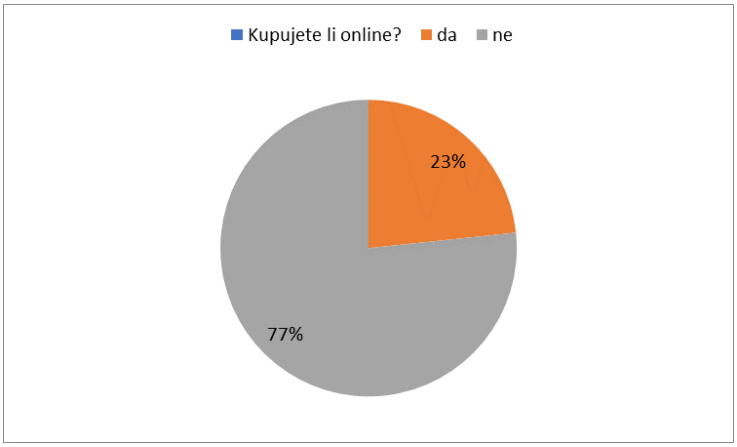


Ilustracija 3.

U ilustraciji 3. prikazano je da od ukupnog broja ispitanika (N=60) na području Sarajeva 53% ispitanika je bilo žrtva cyber kriminala, dok 47% ispitanika nije bilo žrtva krivičnog djela cyber kriminala. Od ukupnog broja ispitanika koji su bili žrtve cyber kriminala pet ispitanika je bilo žrtva računarskih virusa, dva ispitanika su bila žrtve krađe novca posredstvom bankovne kartice, dok je ostalim ispitanicima izvršen upad na korisnički profil na društvenoj mreži Facebook.

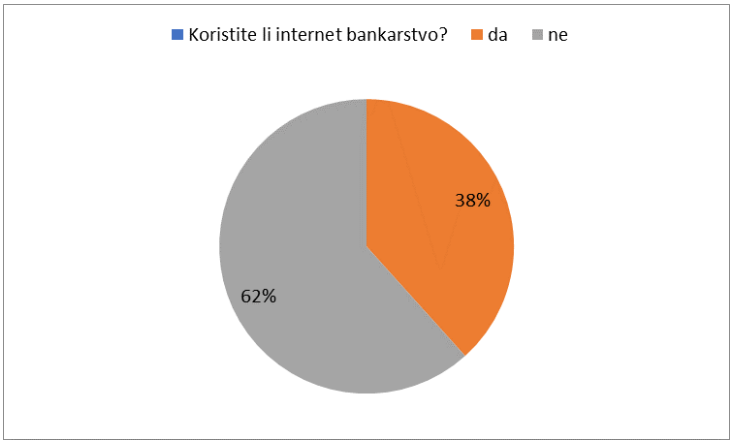
Ilustracija 4.

Ilustracija 4. pokazuje da od ukupnog broja ispitivanih lica, 70% građana na području glavnog grada Bosne i Hercegovine često mijenja svoje lozinke na korisničkim računima, dok 30% građana je odgovorilo da ne mijenja često svoje lozinke. Od ukupnog broja ispitanika na području glavnog grada Bosne i Hercegovine svi ispitanici imaju instaliran antivirus na svojim uređajima.



Ilustracija 5.

Ilustracija 5. pokazuje da 23% od ukupnog broja ispitanika kupuje online, dok 77% ispitanika ne kupuje online.



Ilustracija 6.

Ilustracija 6. pokazuje da 62 % ispitanika ne koristi internet bankarstvo, dok 38% ispitanika koristi usluge internet bankarstva. Na osnovu provedene ankete građani u glavnom gradu Bosne i Hercegovine su se susreli sa krađom novca posredstvom bankovnih kartica, računarskim virusima i upadima na korisnički profil na društvenoj mreži Facebook.

U vezi navedenog problema zaključujemo da su društvene mreže novo poprište cyber kriminala. Jednostavno trebamo biti oprezni koje stranice otvaramo. Većina stranica nas

potiče na davanje ličnih podataka, kao i za razmjenu informacija putem interneta. Lica sklona cyber kriminalu traže osobe koje otkrivaju previše ličnih informacija, koristeći manipulisanje da bi naveli osobu da prezentira svoje lične podatke, a potom ih nezakonito koriste bez znanja osobe koja otkrije svoje lične podatke. Pomoću kupovine online, kriminalna lica oglašavaju usluge koje ili nisu njihove ili ne postoje u stvarnosti kako bi uvjerili korisnika na direktno plaćanje na njihov račun. Neophodno je prije nego se odlučimo na kupovinu online istražiti poslodavce kako bismo sa sigurnošću mogli utvrditi njihovu pouzdanost. Ono što se dešava online ima uticaj i posljedice na stvarni, offline svijet-Internet jeste stvarni život. Upravo zbog toga, online napade treba shvatiti kao stvarne i obezbijediti adekvatnu zaštitu.[95] Čovjek igra značajnu ulogu kada je u pitanju cyber sigurnost. Internet predstavlja jednak prostor za sve korisnike tako da svi korisnici interneta kako građani, pravna lica tako i javni organi trebaju razviti osnovne uslove kako bi zaštitili svoje uređaje i sve informacije na njima i time djelovali nesmetano na internetu. Potrebno je pratiti tehnološki napredak iz oblasti cyber sigurnosti i modernizirati kako tehnologiju tako i sistem da bismo potisli moguće napade. Samo praćenje tehnologije neće dati odgovarajuće rezultate ukoliko se ne primjene od strane određenih stručnjaka koji svoje znanje paralelno usavršavaju sa principima svih novosti koji su izraženi u oblasti cyber sigurnosti. Za bezbjedno korištenje interneta i zaštitu na računaru neophodno je zaštiti e-mail od poruka koje su sumnjivog sadržaja, ne otvarati sumnjive e-mailove, napraviti sigurnosnu kopiju podataka, upotrebljavati kompleksne lozinke, koristiti programe koji su legalni, biti oprezan u korištenju javne WiFi mreže, računar ugasiti kada ga ne koristimo, upotrebljavati operativne sisteme koji su legalni, instalirati i ažurirati antivirusni program, držati anti virusni program uključen, skenirati vanjske uređaje koji se priključuju na računar, USB i sl.

5. RASPRAVA

Internet je postao sastavni dio svakodnevnice. Građani Bosne i Hercegovine svjedoci su da su svakodnevno prisutne prevare preko interneta. Internet se sve više koristi u poslovnoj sferi. Kako se povećava broj korisnika interneta tako se povećava i broj internet prevara. Prezentirani podaci o fenomenu cyber kriminala ukazuju da trebamo biti oprezniji kada koristimo internet jer veoma lako možemo postati žrtva cyber kriminala. Postoji značajna povezanost između cyber kriminala i kompjuterske mreže. Kompjuterske mreže koje su meta napada mogu se iskorištavati u različite svrhe. Postoji značajna povezanost između cyber kriminala i kompjuterskog sistema. Kompjuterski sistem predstavlja uređaj ili skup uređaja koji su međusobno povezani gdje jedan od njih ili nekoliko njih obavlja automatsku obradu podataka. Kod krivičnih

[95] Više pogledati: Lejla Gačanica i Marija Arnautović, *„Mehanizmi zaštite od online nasilja“*. Sarajevo: Mediacentar. 2018., str. 10

djela protiv sistema elektronske obrade podataka radnja izvršenja krivičnog djela sadržana je u neovlašćenom pristupu u tuđu kompjutersku bazu podataka.

Prezentirani statistički podaci vezani za izvještaj o evidentiranim krivičnim djelima protiv sistema elektronske obrade podataka na području Federacije Bosne i Hercegovine, Republike Srpske i Brčko distrikta Bosne i Hercegovine ne predstavljaju dovoljno tačan pokazatelj kojim se može predstaviti opseg cyber kriminala na području Federacije Bosne i Hercegovine, Republike Srpske i Brčko distrikta Bosne i Hercegovine. Prezentirani statistički podaci predstavljaju trenutne pokazatelje krivičnih djela protiv sistema elektronske obrade podataka na području Federacije Bosne i Hercegovine, Republike Srpske i Brčko distrikta u Bosni i Hercegovini. Rezultati provedenog istraživanja ukazuju da trend krivičnih djela protiv sistema elektronske obrade podataka u Bosni i Hercegovini varira. Na osnovu predstavljenog istraživanja možemo sa sigurnošću utvrditi da tokom određenog posmatranog vremenskog perioda u Bosni i Hercegovini cyber kriminal je najmanje izražen u Brčko distriktu Bosne i Hercegovine. Uporedo sa prezentiranim podacima o krivičnim djelima protiv sistema elektronske obrade podataka izneseni su stavovi građana na području glavnog grada Bosne i Hercegovine. Na osnovu iznesenih stavova uočavamo da su svi ispitanici svjesni opasnosti da veoma lako mogu postati meta nekog štetnog programa. Da bi izbjegli takav scenario svi ispitanici su instalirali antivirus na svojim uređajima.

Rezultat istraživanja treba proširiti naučno teorijsko saznanje o ovoj pojavi. U ovom istraživanju naučna opravdanost ide u pravcu i heurističkog i verifikatornog rezultata. Doprinos istraživanja je heuristički u dijelu opisivanja spoznaja provedenog istraživanja na području Bosne i Hercegovine. Kada je u pitanju verifikacijski rezultat istraživanja, u pravcu verifikacije se ide jer se istraživanje svodi na potvrdu teze da cyber kriminal predstavlja modernu sigurnosnu prijetnju u Bosni i Hercegovini i izražen je u formi kriminala vezanog za kompjuterske mreže i upada u kompjuterski sistem.

6. ZAKLJUČAK

Cyber kriminal kao fenomen modernog doba posebna je vrsta kriminala koja se ispoljava u različitim oblicima zloupotreba informacionih tehnologija. Nijedna osoba ne može garantovati da će njegovi/njeni podaci biti zaštićeni od zloupotrebe. Može se zaključiti da je internet proizveo ogromnu brojku sigurnosnih rizika kako zbog razvoja programa tako i različitih internet prevara. Posljedice koje nastaju zloupotrebom ličnih podataka internet korisnika su ogromne. Bosna i Hercegovina je država korisnica globalne mreže. Cyber kriminal uključuje krivična djela koja se izvršavaju kako protiv pojedinaca tako i protiv države kao organizovane društvene zajednice koja je uređena političkim sistemom.

Kako bi se ublažio problem fenomena modernog doba cyber kriminala neophodno je da se poboljša rad informacijske sigurnosti kako od organizacija tako i od lica koja koriste internet. Otkrivanje krivičnih djela protiv sistema elektronske obrade podataka postaje sve više složenije. Bosna i Hercegovina u pogledu nacionalne sigurnosti u cilju borbe protiv cyber kriminala treba da sprovodi mjere zaštite na operativnoj, državnoj, proizvodnoj, tehničkoj i organizacionoj razini. Osobitost cyber kriminala zahtijeva odgovarajući oblik edukacije operativnih lica koja koja su uključena u borbu protiv cyber kriminala. Zaštitne mjere ogledaju se u primjenjivanju najmodernijih sredstava kako bi se zaštitili podaci od zloupotrebe. Uspješno suprotstavljanje cyber kriminalu zahtijeva potpun krivičnoprocesni sistem otpora na cyber kriminal. Neophodno je razmjenjivanje informacija na međunarodnom nivou između organa za borbu protiv cyber kriminala. Brzo djelovanje po saznanju da je počinjeno krivično djelo od velike je važnosti za otkrivanje počinilaca i obezbjeđivanje dokaza. Neophodno je i da građani povećaju svijest o opasnostima koje cyber kriminal proizvodi kako bi zaštitili svoje lične podatke, što znači da su oprez i informiranost od krucijalnog značaja.

BIBLIOGRAFIJA

- Blagojević, G. i Guska, G. (2016). *Zavisnost od interneta-predrasude ili realnost*. Edukator Travnik: Univerzitet u Vitezu,12-20.
- 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
- Deutsch, Karl W. (1966). *The Nerves of Government: Moñels of Political Communication and Control*, 2nd ed.. New York
- Gačanica, L. i Arnautović, M. (2018). *Mehanizmi zaštite od online nasilja*. Sarajevo: Mediacentar
- Gligorević, R. (2014). *Cyber kriminal*. Digitalna ekonomija-Digital Economics, 163-174.
- Hamidović, H, Hamidović, A. i Zajmović, M. (2016). *Okvir za rješavanje problema cyber kriminala*. INFOTEH-JAHORINA, 557-562.
- Kovačević, B. (2013). *Cyberwar-Američka izlika za novi hladni rat?* Polemos, 91-110.
- Krstić, O. (2009). *Maloljetnička delinkvencija*. Banja Luka: Fakultet za bezbjednost i zaštitu
- Mesarović, S. (2006). *Motiv i profil izvršilaca*. Zbornik Ziteh '06. Beograd. IT veštak
- Milašinović, R, Mijalković, S. i Amidžić, G. (2012). *Bezbednost i internet*. Zbornik radova. Laktaši. Visoka škola unutrašnjih poslova, Bulevar Živojina Mišića 10A. Banja Luka, 31-42.
- Pena, U. i Mitrović, D. (2012). *Značaj digitalnih dokaza u krivičnom postupku*. Zbornik radova. Laktaši. Visoka škola unutrašnjih poslova, Bulevar Živojina Mišića 10A. Banja Luka, 93-108.
- Porobić, M. i Bajraktarević, M. (2012). *Cyber kriminal, pranje novca i finansijske istrage.* Sarajevo
- Radnović, B. Ilić, M. i Radović, N. (2012). *Ekonomski sajber kriminal u Srbiji-aspekt zaštite internet potrošača*. Zbornik radova. Laktaši. Visoka škola unutrašnjih poslova, Bulevar Živojina Mišića 10A. Banja Luka, 129-142.
- Selimović, M. (2015). *Implementacija procesnih odredbi Konvencije o kibernetičkom kriminalu u Zakonu o krivičnom postupku Federacije Bosne i Hercegovine*. Kriminalističke teme, str. 74, 71-83.
- Šakić, D. (2016). *Cyber kriminal*. Edukator. God 3. Br. 4. Travnik. Univerzitet Vitez.
- Vasić, G., Šarić, B. i Jovanić, V. (2012). *Kompjuterski kriminalitet*. Zbornik radova. Laktaši. Visoka škola unutrašnjih poslova, Bulevar Živojina Mišića 10A. Banja Luka, 181-192.
- Vuković, H. (2012). *Kibernetska sigurnost i sustav borbe protiv kibernetskih prijetnji u Republici Hrvatskoj*. NATIONAL SECURITY AND THE FUTURE, 12-31.

Ostali korišteni izvori:

- Informacija o stanju sigurnosti u Bosni i Hercegovini u 2015. godini. (2016). Bosna i Hercegovina. Ministarstvo sigurnosti. Sarajevo
- Informacija o stanju sigurnosti u Bosni i Hercegovini u 2016. godini. (2017). Bosna i Hercegovina. Ministarstvo sigurnosti. Sarajevo
- Informacija o stanju sigurnosti u Bosni i Hercegovini u 2017. godini. (2018). Bosna i Hercegovina. Ministarstvo sigurnosti. Sarajevo
- Krivični zakon Brčko distrikta Bosne i Hercegovine. Glava XXXII. Službeni glasnik Brčko distrikta BiH br. 33/2013 - prečišćen tekst, 47/2014 - ispravka 26/2016, 13/2017 i 50/2018
- Krivični zakon Federacije Bosne i Hercegovine. Glava XXXII. Krivična djela protiv sustava elektronske obrade podataka, Službene novine Federacije BiH, br. 36/2003, 21/2004-ispr., 69/2004, 18/2005, 42/2010, 42/2011, 59/2014, 76/2014, 46/2016 i 75/2017
- Krivični zakon Republike Srpske. Glava XXXIV. Krivična djela protiv bezbjednosti kompjuterskih podataka. Službeni glasnik Republike Srpske broj: 64/17 i 104/2018-odluka US

Internet izvori:

- Cyber kriminal sve češća pojava u BiH: Informisati se o opasnostima interneta. (2019). https://akos.ba › cyber-kriminal-sve-cesca-pojava-u-bih-informisati-se-o-o...
- Wynne, M.W. (2006). *Cyberspace as a Domain in Which the Air Force Flies and Fights*, govor s C4ISR Integration Conference. Dostupno na: https://www.af.mil›About Us › Speeches Archive
- https://www.msb.gov.ba
- https://www.mup.vladars.net
- https://www.fup.gov.ba
- https://www.policijabdbih.gov.ba

Kriminalističke teme
Zbornik radova
Godina XIX, Broj 5, 2019.
ISSN 1512-5505

Panel 3

NOVI MEDIJI, NOVE PRIJETNJE? MEĐUNARODNI ZLOČINI, RADIKALIZAM I EKSTREMIZAM U DIGITARNOJ ERI

Kriminalističke teme
Zbornik radova
Godina XIX, Broj 5, 2019.
ISSN 1512-5505

HORIZONATALNO I VERTIKALNO HIBRIDNO DJELOVANJE I/ILI RAT - STUDIJA SLUČAJA BOSNE I HERCEGOVINE

HORIZONTAL AND VERTICAL HYBRID ACTION AND/OR WAR-CASE STUDY OF BOSNIA AND HERZEGOVINA

Izvorni naučni rad

Prof. dr. Jasmin Ahić[96]
Prof. dr. Bakir Alispahić[97]

SAŽETAK

Inspiracija za rad i problem (i) koji se radom oslovljava (ju): Ako polazišno uporište postavimo na način da je hibridno djelovanje zapravo model širenja utjecaja u kojem se koriste sofisticirane aktivnosti za, informacijske i medijske operacije, te subverzivno interesno djelovanje, onda je neminovno da i odredimo njegove premise. Autor (i) iznosi osnovne kriterije po kojima je hibridno djelovanje, u većini slučajeva, u potrebno kategorizirati u horizontalnom i vertikalnom smislu unutar samom objekta na koji se odnosi (država, zajednica, sistem). Napadi i diverzije na informacione sisteme vlada i/ili sigurnosnih istraživačkih centara predstavljaju novi oblik ratovanja koji zamjenjuje konvencionalno oružje i seli se iz prirodnog u digitalno okruženje. Potreba za preveniranjem i odbranom je neupitna.

Ciljevi rada (naučni i/ili društveni): Studija daje uvid u nove načine borbe od hibridnog djelovanja do ratovanja i to protiv uspostavljenih državnih i nacionalnih sistema. Rezultati mogu poslužiti kao smjernice i uvidi u događanja u skorijoj budućnosti koja će postati tehnološki naprednija, samim time i ranjivija.

Metodologija/Dizajn: Empirijsko istraživanje u formi studije slučaja predstavlja primarnu analizu događaja koji su klasifikovani kao rad obavještajnih agencija i pojedinaca u domeni hibridnog djelovanja/ratovanja i uspostavljanja političkih pritisaka na druge regionalne aktere.

Ograničenja istraživanja/rada: Horizontalno i vertikalno hibridno djelovanje predstavlja dinamičnu kategoriju čiji se elementi kreću na političkom spektru od borbe za primarnim secesionističkim interesima do opravdanog preventivnog napada. Jasna i tačna klasifikacija svakog od događaja ima notu favorizovanja i osuđivanja aktera što može ući u domen političke korektnosti i državne favorizacije određenih subjekata. Rad predstavlja hipotetički okvir događaja koji se mogu i dešavaju, i koji su uslovljeni i direktno vezani za trenutnu političko sigurnosnu klimu.

Rezultati/Nalazi: Rezultati prezentirani u radu predstavljaju prognostiku i predviđanje budućih događaja koji nastaju kao rezultat anarhije hibridnog i cyber prostora i

[96] FKKSS, UNSA, Bosna i Hercegovina
[97] FKKSS, UNSA, Bosna i Hercegovina

međusobnog obavještajnog rata državnih i paradržavnih aktera u borbi za dominaciju nad regionalnom i globalnom politikom.
Generalni zaključak: Ranjivost cyber prostora omogućava različitim akterima da djeluju protiv nacionalnih i državnih sistema kao primarnih meta koje omogućavaju brz i efikasan povrat informacija o uspješnosti napada. Pritisci nastali od strane terorističkih organizacija i njihovog obavještajnog sistema na države ili vlade imaju poguban karakter jer se u pitanje dovodi nacionalni opstanak. Promijenjen je samo front djelovanja, od postavljanja bombi u tržne centre u postavljanje virusa i malware programa u nuklearna postrojenja, hidrocentrale i finansijske sisteme.
Opravdanost istraživanja/rada: Radom su prikazani mogući elementi i načini izvršenja hibridnog djelovanji ratovanja te aktivnosti koji mijenjaju modus operandi i prelaze na društveno i nacionalno opasnije akte poput rušenja političkog sistema, diverzija npr. infrastrukure i pristupa tajnim informacijama. Hibridno djelovanje uvijek ima strateške ciljeve stvaranja utjecaja ili preusmjeravanja političkih procesa. Današnji medijski, informacijski, propagandno politički kontekst u Bosni i Hercegovini, te otvorena destrukcija i nepovjerenje u državne institucije stvaraju dobru atmosferu za prihvaćanje dezinformacija koje mogu imati određeni strateški utjecaj. Kada strateški utjecaj počne davati rezultate onda je potrebno govoriti „i/ili“ o hibridnom ratovanju???

Ključne riječi
hibridno djelovanje, horizontalno i vertikalno djelovanje, hibridni rat

ABSTRACT
If we set the starting point in a way that hybrid action is actually a model of the expansion of influence in which sophisticated activities for information and media operations are used, and subversive interest, then it is inevitable to determine its premises. The author presents the basic criteria according to which the hybrid action, in most cases, is to be categorized in the horizontal and vertical sense within the object itself (state, community, system). Hybrid action always has the strategic goals of influencing or redirecting political processes. Today's media, information, propaganda political context in Bosnia and Herzegovina, and open destruction and mistrust in state institutions create a good atmosphere for accepting misinformations that may have a certain strategic impact. When the strategic impact begins to give results then it is necessary to speak "and/or" of hybrid warfare. ???

Key Words
Hybrid action, Horizontal and Vertical Action, Hybrid War, Bosnia and Herzegovina

UVOD

Hanibal, veliki vojskovođa svoga vremena je malom vojnom silom potpomognut slabim saveznicima napao jake rimske snage na Apeninskom poluostrvu. Uspješnom primjenom različitih oblika i kombinacija napadnih djelovanja ozbiljno je zaprijetila rimskoj vojsci i čitavoj tadašnjoj Rimskoj republici koja je imala 38 legija (preko 120.000 vojnika nasuprot oko 40.000 hiljada pripadnika kartagenske vojske). Rat, kao najsloženija društvena pojava, određena je uticajima različitih faktora povezivajući se sa svim sociološkim,

tehnološkim i historijskim pojavama, dostignućima i interesima. Poznati pruski general Clausewitz izjavio je da je rat politika drugim sredstvima, i da je rat produžena ruka politike. Tako danas i mi možemo napraviti paralelu da je neoružani rat – rat drugim sredstvima, odnosno produžena ruka oružanog rata. Tehnološka (r)evolucija dovodi do ratnih revolucija. Rat je u suštini svoje društveno-historijske konstante ostao isti, samo su se neka sredstva promjenila i prilagodila, odnosno pridodala. S obzirom, da rat predstavlja društvenu konstantu, nesumnjivo je da su se društvene promjene, izazvane procesom globalizacije, odrazile i na sam fenomen rata, prije svega na način njegovog vođenja kao historijskog društvenog činioca i pratioca tehničkog razvoja. Historija pojave *Hibridni rat* je pojava koja predstavlja sociološku i epistemiološku promjenu praktikovanja i poimanja rata, odnosno historijski poznatog konvencionalnog oružanog sukoba. Trenutna tranzicija ratovanja nije prva u hronologiji razvoja i tipologiji određenja, ali je po mnogo čemu svojstvena i značajnija u odnosu na prethodne. Kao što sve u prirodi teži ravnoteži, izjednačavanju i jednakosti kao preduslovu harmoniji i stabilnosti kao održivosti u vječnosti, tako je i rat kroz svoj razvoj doživio stupanj izjednačenosti protivnika, bez obzira na materijalnu veličinu i snagu. Koncept hibridnog ratovanja nije novi, pošto su države i njihove obavještajne agencije u prošlosti koristile iste subverzivne tehnike i alate. KGB je koristio dezinformacije i propagandu kao sredstvo asimetričnog rata u Hladnom ratu zbog velikih granica svog stanovništva i regiona koji su pali pod njenu sferu uticaja, kao što je i CIA činila da spriječi širenje komunizma u SAD i zapadnoj sferi uticaja. Međutim, hibridni rat je preuzeo potpuno novu dimenziju sa pojavom savremene tehnologije i digitalnog svijeta gde bi se cyber prostorom moglo manipulisati za širenje propagande i oružja u obliku cyber hakovanja. Hibridni rat-uz spajanje konvencionalne ratne tehnike i nekonvencionalne tehnologije sa konvencionalnim metodama postala je nova preovlađujuća generacija alata sa kojim se svijet polako suočava. Dakle, kada nema upotrebe (i) konvencionalnog oružja, tada nema ni rata. Sve se može svesti na konflikt, sukob i na kraju na rat. Konflikt ne mora uvijek da dovede do sukoba, a sukob ne mora uvijek da izazove rat, ali rat je uvijek posljedica postojanja konflikta i sukoba. Nije isto djelovanje i ratovanje. Ukoliko se svaki pojam zasebno jasno definiše, nije problem formulisati i odrednicu – hibridni rat, jer on je samo kombinacija dostupnih mogućnosti, poput i svakog drugog hibrida. Sve šta je uključeno u rat pored konvencionalnog oružja; nekonvencionalno (kao najčešće sredstvo prijetnje, prinude i/ili odvraćanja), cyber operacije, ekonomski medijski i politički pritisci, migracije i demografske eksplozije, itd. može se nazvati logističkom podrškom ratne operacije, odnosno oružane operacije ratnog djelovanja, a uključuje se u rat zbog niže cijene, lakšeg opravdanja ili veće efikasnosti pri postizanju određenih ciljeva.

Hibridni rat je možda i najširi pojam do sada, jer se sa globalizacijom i evolucija rata proširila sa bojnog polja, na kojem je taktika i asimetrija ratnih lukavstava mijenjala tokove i ishode bitaka i ratova, rastući do međunarodnih granica zatim regionalnih i na kraju globalnih, šireći se od sukoba u koje su bili uključeni samo vojnici, do granica cijelog, čak i globalnog, međunarodnog društva, i svih njegovih institucija, potencijala i resursa. Rat je u suštini svoje društveno-historijske konstante ostao isti, samo su se neka sredstva promijenila i prilagodila, odnosno pridodala. Razvojem saobraćaja, tehnologije, tehnike i

informatike, kao i medija i međunarodnih odnosa (može se reći globalizacijom) omogućeno je da logističke operacije (od dovoženja kamenja za katapulte, zatim hrane za ratnike i konje, do kasnijeg prevoza energenata, itd.) prerastu u logističke operacije. Hibridni rat je samo novi stepen u razvoju rata koji je uvek pratio razvoj društva. Kako današnje društvo karakteriše visok stepen razvijenosti i razgranatosti, a mali stepen precizne definisanosti i uređenosti, odnosno relativne opšte haotičnosti i potpune izmiješanosti, isto je i sa ratom i raznolikošću i isprepletenošću njegovih akcija i operacija. Hibridni rat nije vojni, već državni koncept ratovanja, u kojem mogu da se angažuju svi društveni potencijali države agresora, a da se napadnu svi društveni resursi države žrtve. Kao što je slučaj opasnosti od svjetskog rata zahtijevao formiranje sistema opšte narodne (civilne) odbrane, tako slučaj opasnosti od hibridnog rata zahtijeva formiranje sistema opšte društvene (sistemske i sistematske) odbrane. Što se tiče i samog naziva i samog postojanja i održivosti koncepta hibridnog rata vodi se dosta polemike sa brojnim zanimljivim argumentima *pro et contra* gde se debatuje o mjestu i ulozi novog vida rata koji je po definiciji protivna opštoj definiciji rata kao oružanom međudržavnom sporu. Očigledno je priča o ,,hibridnom ratu" dospjela u žižu interesovanja zbog međusobnih optužbi najvećih svjetskih sila za ono šta obje, ili sve tri sa Republikom Kinom, rade. Ako je treći svjetski rat bio Hladni, onda je četvrti Hibridni[98]. I, kao što Drugi vuče korjene iz Prvog, tako i Hibridni ima utemeljenje u Hladnom ratu. Hibridni rat je neograničeni rat, od beskontaktnog do totalnog. Hibridni rat može biti neograničeni rat, ali to nije novina. Rat je, zapravo oduvijek bio neograničen, ali je spektar mogućnosti bio ograničen. Nismo oduvijek imali meki ili tvrdi pristup, ekonomske sankcije, međunarodne pritiske, medijske manipulacije, cyber špijunažu i napade, itd. Rat je neograničen od nastanka, ali su se granice stalno pomjerale, odnosno mogućnosti umnožavale i unapređivale. Hibridno ratovanje je sinergija i prirodno i historijski posljedično nasljedno objedinjavanje hladnog rata i malih ratova, koji karakterišu period poslije dva velika sukoba svjetskih razmera. Hladni rat je bio hibridni svjetski rat. Hibridni rat je počeo sa Hladnim ratom, odnosno sa završetkom Drugog svjetskog rata, i još uvek traje. Svi ratovi u drugoj polovini 20. vijeka i prvoj polovini 21. vijeka su zapravo – hibridni ratovi. Ako je 20. vijek bio vijek svjetskih ratova, 21. vijek će biti vijek hibridnih ratova. Danas, nije moguće utvrditi da li je u pitanju novi ,,hladni" rat, ili je stari bio zapravo samo uvod u novi. U svakom slučaju, evidentno je da je novi nastavak starog u kojem je težište bilo prije svega na sukobu dva takmaca svjetske bezbjednosti i politike koji su se nadmetali i međusobno sputavali u svim društvenim segmentima. Novi oblik svjetskog sukoba - hibridni rat, kao da ne poznaje granice; ni vremenske, ni prostorne, niti društvene.

Za razliku od hibridnog, tzv. specijalni rat je izraz kojim se opisuju neprijateljske aktivnosti jedne suverene države ili više njih prema drugoj suverenoj državi koje po svojim ciljevima odgovara ratu, ali koje ne uključuju element neposrednog oružanog, odnosno konvencionalnog sukoba, odnosno u kome je direktna akcija zamijenjena širokim rasponom

[98] Teorija 4GW (*engl. Fourth Generation Warfare*) – četvrta generacija rata, promoviše neograničen i složeni rat.

ekonomskih, obavještajnih, propagandnih i sličnih operacija kojima se posredno ciljana država nastoji uništiti ili oslabiti kroz subverziju.

1. Geneza hibridnog djelovanja i/ili ratovanja

Tokom osamdesetih američka vojna doktrina, možda najbolje da bi uslijedila kroz čitanje Vojnog pregleda, najviše se fokusirala na teme koje se prisjećaju tzv. sukobi srednjeg do visokog intenziteta - rat i totalni rat u različitim oblicima. Autori mnogih generacija i tipova Oružanih snaga SAD-a pokušavali su, od izdavanja do izdavanja, opisati i objasniti pojmove poput "produžavanje bojnog polja", "borba u vazduhu" ili vještine vazdušnih operacija - Operativna umjetnost AirLand bitke. Nešto manje pažnje posvećeno je fenomenu tzv. sukobi niskog intenziteta, premda, kako su svojedobno primijetili general Donald R. Morelli i general pukovnik Michael M. Ferguson, vjerovatnoća takvih sukoba bila je veća od one sukoba srednjeg i visokog intenziteta za koje su se prvenstveno pripremale američke oružane snage. Usmjerenost američke vojne misli u to vrijeme na „velike“ konvencionalne sukobe ili klasične međudržavne ratove (sa ili bez upotrebe nuklearnog oružja) bila je sasvim razumljiva u kontekstu kontinuiranog i teškog višedimenzionalnog nadmetanja sa SSSR-om, čije su oružane snage, barem u nekim aspektima (prije svega kvantitativno) nadmašio američke oružane snage.

S druge strane, u pretposljednjoj deceniji prošlog vijeka, na periferiji "Fronte" sučeljavanja blockchaina - u Južnoj Americi, Africi, Južnoj i Jugoistočnoj Aziji - bile su pogođene mnoštvom sukoba niskog intenziteta čiji su potencijalni ishodi u velikoj mjeri zamijenili geostrateške položaje i interese obje supersile.

1.1 Determiniranje i definiranje pojmova

U američkoj stručnoj i doktrinarnoj literaturi sukob niskog intenziteta tretira se kao "ograničena političko-vojna borba za postizanje političkih, socijalnih, ekonomskih ili psiholoških ciljeva". Sukob niskog intenziteta "često je dugotrajan, u rasponu od diplomatskog, ekonomskog i socio-psihološkog pritiska, pa sve do terorizma i pobune". Obično je "ograničen na jedno geografsko područje i često je karakteriziran ograničenjima na oružje, taktiku i nivoima nasilja". U radu iz 1984. godine Moreli i Ferguson naveli su niz oblika upravljanja sukobom niskog intenziteta (preko dvadeset) - od političkih i ekonomskih sukoba (naprimjer, kartela i ekonomskih sankcija), do nacionalnih i subnacionalnih sukoba (recimo, granica incidenti, taoci, ubistva, terorizam i protuterorizam), za otvaranje ograničenih sukoba (naprimjer, revolucije, gerile, kontrapobune, vanjsko vojno uplitanje). Kao što se može primijetiti, kada je u pitanju sukob niskog intenziteta, riječ je o pojmu vrlo širokog opsega i ne baš jasnih granica.

Njegova definicija, kao i njegova upotreba, dobili su ozbiljnu kritiku, kako unutar samih Sjedinjenih Država, tako i izvan njih. Iako kontroverzan s gledišta logike (metodologije) i vojne nauke, koncept sukoba niskog intenziteta ipak je pridonio potrebnoj pažnji

istraživača i analitičara na poljima ratovanja i međunarodnih odnosa u mnoštvu geografski ograničenih, često dugotrajnih i polimorfnih oružanih sukoba. Kako su tenzije iz hladnog rata opadale, tako se pojavila i pojava tzv. mali ratovi postajali su sve zanimljiviji istraživačkim institucijama u AF-u različitih zemalja, kao i akademskoj zajednici, posebno u SAD-u i Evropi. U oktobru 1989., kada je rušenjem Berlinskog zida simbolično bilo okončano vrijeme hladnog rata, tekst pet američkih autora istovremeno se pojavio u magazinu Marine Corps i Vojnom časopisu o promjenjivoj fizionomiji rata i tzv. do četvrte generacije ratnih dejstava. Među tim autorima najznačajniji je svakako William S. Lind, američki konzervativni mislilac po obrazovanju, historičar. Do trenutka objavljivanja ovog djela, Lind je već pročitao knjigu posvećenu Manevarskom ratu - Priručnik o manevarima s manevrom, koja je prvi put objavljena 1985. godine. Lind i koautori (oficiri američke vojske) tumače evoluciju prirode ratovanja u modernom dobu kao rezultat interaktivnog efekta bezličnog tehnološkog napretka i taktičkih (kasnijih i operativnih) inovacija u oružanim borbama. Prva ratna generacija (koju simbolično simbolizira glatka musketa) je rođena u razdoblju prije Napoleonove pojave, a sa ratovima koji je vodio dostigla je vrhunac. Akcenat se stavlja na masu ljudi, organizovanu kroz takte linija i kolona. Druga generacija ratovanja kulminira s prvim svjetskim ratom. Taktika se temelji na vatri i pokretu, ali u osnovi ostaje linearna. Masovna vatrena snaga zamjenjuje se masovnom radnom snagom. Treća generacija ratnih dejstava (prisutna u konturama krajem 1918. godine), izašla je na vidjelo tijekom Drugog svjetskog rata, zahvaljujući velikim dijelom njemačkim taktičkim inovacijama. Na osnovu manevra, umjesto iznude, taktike treće generacije su prva istinski nelinearna taktika. Umjesto neposrednog uništenja, napad se zasniva na infiltraciji i obilaznici, dok je odbrana postavljena u dubini ali je bitno istaći da se određene taktičke i operativne ideje uvijek prenose sa generacije na generaciju.

Prema američkim autorima, naracije na generiranje ratnih dejstava, ovaj princip sukcesije primjenjuje se i kada je u pitanju četvrta generacija rata. Četiri središnje ideje koje prenose na najnoviju generaciju ratnih dejstava su naredbe za misije, smanjenje zavisnosti o centraliziranoj logistici, veći naglasak na manevru i pad neprijatelja kolabiranja neprijatelja iznutra. U odnosu na prvu ideju, vjerovatno je da će se buduće ratište vjerojatno proširiti na čitavo neprijateljsko društvo, tako da će za rasipanje snaga na bojnom polju biti potrebna izuzetna fleksibilnost i najniži nivo (sastav) kad djeluju na osnovu namjere zapovjednika. Kada je u pitanju logistika, američki autori zaključuju da će navedena disperzija zahtijevati sposobnost opstanka na štetu terena i neprijatelja. Veći naglasak na manevariju podrazumijeva da masa, bila ljudska ili vatrena, više neće biti odlučujući faktor. Male, vrlo pokretne i okretne trupe obično će dominirati. Konačno, umjesto da fizički uništimo neprijatelja, cilj će biti srušavanje iznutra, a meta će postati takve pojave, kao što su popularna podrška ratu ili neprijateljska kultura. Prema Lindu i koautorima, u budućnosti bi se razlika između mira i rata mogla zamagliti do tačke nestajanja. Upravo, to podrazumijeva nemogućnost preciznog definiranja bojnog polja ili fronta, kao i nestanak razlike između civila i vojnika. Inače, smatraju, sve gore navedene karakteristike već su u određenoj mjeri bile prisutne u trećoj generaciji ratnih dejstava, dok su u četvrtoj bile tek izraženije. Ipak, u odnosu na tzv. Treća generacija ratnih dejstava, postoje određeni novi faktori čija akcija omogućuje identifikaciju ratne četvrte generacije. Prije svega, to je

pojava novih tehnologija čija primjena u borbenim operacijama može radikalno promijeniti taktiku i uopće način vođenja rata. U središtu predstave o četvrtoj generaciji ratnih sukoba nalaze se brojčano male, visoko mobilne jedinice, opremljene najmodernijim dodacima (komunikacija i posmatranje), koji traže ciljeve, i vojne i civilne, duž čitave dubine bojišta (pozadine gotovo da i nema!) a ponekad ih i sami uništavaju.

Psihološke operacije imaju posebno mjesto u ovoj vrsti ratnih dejstava, koja „mogu postati dominantno operativno i strateško oružje u obliku medijskih / informativnih intervencija". U tekstu se predviđa raširena upotreba kompjuterskih virusa, manipulacija medijima da bi se promijenilo javno mišljenje, dok televizijske vijesti tvrde da ih je moguće pretvoriti u „moćna" sredstva manipulacije i djelovanja.

Konačno, Lind i koautori vjeruju da znanje o određenim pojavama, poput terorizma, također može uvelike olakšati razumijevanje koncepta rata četvrte generacije. Sam terorizam, prema njihovom mišljenju, ne predstavlja ratovanje četvrte generacije, ali neki od njegovih elemenata sigurno mogu biti sastavni dijelovi ove nove vrste rata. Jer, kako vjeruju, globalni Zapad više ne dominira svijetom, niti definira modele ratovanja, može doći do rata četvrte generacije.

1.2 Tradicionalistički pristupi

U okviru zapadnjačkih tradicija , ali i islamske ili azijske, kojima se mogu pribjegavati zbog tehnološke zaostalosti koja im onemogućuje ravnomjerno vođenje konvencionalnih ratova sa zapadnim silama. Budući da bi u ratu četvrte generacije čitavo društvo postalo bojno polje, jer bi granica između prednje i stražnje strane bila zamagljena, a borbene jedinice logistički bi preživjele na štetu terena ili plijena, očito je da je u nekim aspektima terorizam i to nova vrsta rata veoma povezane pojave. Teroristi djeluju i u cjelokupnom društvu, živeći na štetu tog društva i, što je najvažnije, pokušavajući neprijatelja poraziti iznutra, zaobilazeći njegovu vojnu silu i direktno udarajući civilne ciljeve. Na kraju teksta Lind i koautori kažu da njegova svrha nije odgovaranje, već postavljanje pitanja, pa nije neobično da je definicija rata četvrte generacije izostala, iako je njihov rad bio pionirski. Umjesto definicije nude se opisi pojava i njegove geneze. Opis karakteristika fenomena i njegova pojava mogu pružiti dobru osnovu za formulisanje jedinstvene, analitičko-genetske definicije rata četvrte generacije. Međutim, do danas ne postoji takva definicija, iako postoje valjani epistemološki preduslovi za njenu formulaciju. Jasno je i na prvi pogled da koncept rata četvrte generacije dijeli više zajedništva s idejom sukoba niskog intenziteta (nekonvencionalna upotreba ljudskih i materijalno-tehničkih sredstava u borbenim operacijama, pribjegavanje ekonomskim, psihološkim i propagandnim akcijama, asimetrija između suprotstavljenih strana). Uzimajući u obzir tu činjenicu, može se reći da su pojmovi sukoba niskog intenziteta i rata četvrte generacije u konceptu povezani sa supstancom.

U vrijeme objavljivanja ovog članka poznati izraelski vojni teoretičar Martin van Creveld, napisao je studiju o transformaciji rata. Kako sam kaže u predgovoru, tekst knjige formulisan je u periodu 1989-1990., što znači da je Kreveld imao priliku upoznati rad Linda i njegovih koautora, s obzirom na to da je najvjerovatnije imao pristup američkoj vojnoj periodici. Ipak, Kreveld ovaj tekst ne navodi na popisu literature, iako čini nekoliko tačaka koje su po sadržaju vrlo bliske onome Linde i koautora. Prema Kreveldu, od kraja Drugog svjetskog rata tzv. mali ratovi ili, kako on kaže, sukobi niskog intenziteta, koji su možda bili "dominantni instrument za izazivanje političkih promjena". Bitne karakteristike ovih sukoba (brojni revolucionarni i građanski ratovi, višegodišnje terorističke kampanje) su sljedeće: oni se odvijaju u manje razvijenim dijelovima svijeta (postoji takva težnja); rijetko uključuju redovnu vojsku s obje strane; većina sukoba niskog intenziteta ne oslanja se prije svega na visokoj tehnologiji. Također je vrlo značajno, a Kreveld na više mjesta u svojoj knjizi ističe (i potvrđuje) da u sukobima slabog intenziteta moderni sustavi oružja i uopće moderne vojske postaju uglavnom irelevantni (Kreveld: 2010:13).

Govoreći o trendovima u narednim desetljećima, Kreveld je predvidio da "rat u budućnosti neće voditi vojske, nego grupe koje danas nazivamo teroristima, gerilcima, banditima i razbojnicima (nesumnjivo će koristiti još izbirljivija imena da se opišu). Njihove organizacije vjerovatno će počivati na harizmatičnoj, a ne na institucionalnoj osnovi i manje će biti motivirane profesionalizmom nego fanatičnom, ideološki utemeljenom lojalnošću. " Polazeći od pretpostavke da je sukob slabog intenziteta "val budućnosti", Kreveld ukazuje na nekoliko velikih promjena u ratovanju. U njegovom razumijevanju nestaće strategija u klasičnom smislu.

Jasno je da postoje određene sličnosti između Kreveldovih stavova i onih iza koju su Lind i kolege formulisali. U oba razumijevanja naglasak se mijenja priroda ratovanja, zamagljivanje granice između postojećih "stabilnih" kategorija vještine samo rata (front / background, borac / civil), kao i zemljopisni okvir fenomena (sukob slabog intenziteta ili rat četvrte generacije) - zemlje trećeg svijeta. S druge strane, postoje i neke razlike - Lind i koautori imaju veći naglasak za naglasiti važnost psiholoških (medijskih) operacija i upotrebe pojedinačnih (ul-savremene tehnologije). Zanimljivo je i da Kreveld ne daje vlastitu definiciju sukoba niskog intenziteta već koristi tu sintagmu slobodno bez preliminarne idejne definicije.

2. Hibridna politika i hibridno ratovanje

Tokom proteklog desetljeća vojni teoretičari i analitičari iz područja nacionalne sigurnosti aktivno su se bavili pitanjima suvremenih sigurnosnih ratova, i pokušajima da predvide ono što dolazi u budućnosti. Tako su u analizama događaja u svijetu koji su obilježili protekli period, a u cilju prikazivanja različitosti konvencionalnog od nekonvencionalnog odnosno savremenog ratovanja u leksikone nacionalne sigurnosti i nauke o sigurnosti uvršteni mnogi novi pojmovi.

Naime, ti događaji, kao što su primjerice revolucionarne promjene i oružani sukobi u zemljama Sjeverne Afrike, Bliskog Istoka i zemljama bivšeg Sovjetskog Saveza potvrdili su pojavu novih oblika i metoda ostvarivanja vlastitih političkih ciljeva, odnosno potvrdili su da se nastavlja trend razvoja ratovanja o kojem elaboriramo u prethodnom dijelu.

Srž promjena nije promjena političkih ciljeva koji su i danas gotovo identični kao i na samim začecima ratovanja, srž promjena je pomak u načinu na koji se ti ciljevi ostvaruju, i to se prvobitno odnosi na gravitacijsko središte. To u smislu hibridnog ratovanja njegovih slabosti i širenja vlastitog narativa. U kontekstu ruskog pripajanja Krima i ruske prikrivene intervencije u Istočnoj Ukrajini kao događaja koji su potaknuli Zapad na analiziranje koncepta „hibridnih" načina (metoda) organizacije i provedbe oružane agresije jedne zemlje na drugu, zaključeno je da hibridno ratovanje nije novi fenomen (Radkovets, 2015a: 2). Hibridno ratovanje nije revolucionaran pristup jer izučavanjem povijesti možemo identificirati veliki broj ratova koji sadržavaju elemente hibridnog rata, što ćemo istraživati i u ovom radu. Međutim, iako sami faktori koji definiraju hibridni rat nisu novi, već su uglavnom svi već prije korišteni u nekim od povijesnih ratova, ruski hibridni model sadržava neke dosad neizučavane aspekte – velika nepredvidivost i dinamičnost i fleksibilnost u primjeni različitih faktora, rastuća uloga informacijskog, ekonomskog, energetskog i drugih aspekata koji u savremenom hibridnom modelu postaju gotov jednako (ako ne i više) važni od klasičnog vojnog aspekta. To zapravo podrazumijeva odmak od tradicionalnog uništavanja protivnika primjenom vojne sile do korištenja kombinacije nevojnih metoda s ciljem dezintegracije protivnika, eksploatacije njegovih unutrašnjih resursa.

Izučavanjem dostupne literature jasno je da već postoji značajan broj stranih teoretičara i vojnih analitičara koji su u svojim međunarodno priznatim knjigama i člancima obradili pojam hibridnog rata, kao što su Martin van Creveld, David Kilcullen, Frank Hoffman, Karber, McCulloh, Janis Berzins i Robert Gates. Oni su u svojim radovima koristeći različite pristupe definirali ključne faktore, preduvjete, faze razvoja i elemente hibridnog rata kao operativnog pristupa za ostvarivanje nekih ciljeva o kojima teorija hibridnog rata ne govori ništa. Međutim, uočen je manjak naučnih radova koji se bave pojmom hibridne politike i hibridnog djelovanja koja skriva prave ciljeve i namjere, jer dobro poznata i ranije spomenuta korelacija politike i rata - kaže da je rat nastavak politike. Iako pojam hibridne politike zasada nije opsežno izučavan, za potrebe ovog rada i analize savremenog hibridnog modela prepoznata je nepobitna važnost hibridne politike kao polazišne tačke hibridnog djelovanja/ratovanja koja je kreirana i implementirana puno ranije od operacionalizacije samog rata (tokom 1. pripremne faze rata). Stoga je ovaj element sadržan u jednom od tri teorijska okvira na kojima i počiva ovaj rad.

Tvrdnje pruskog generala i vojnog teoretičara Carla von Clausewitza „rat je nastavak politike drugim sredstvima" i „vojska se mora podrediti političarima" i danas relevantno govori o utjecaju politike na kreiranje strategije i na samo ratovanje. Clausewitzeve teorije, ali i teorije drugih ranije spomenutih filozofa i mislioca o strategiji, taktici i filozofiji ratovanja su značajno utjecale na razvoj vojnih i nauke o sigurnosti zapadnih zemalja, a

mnogi njihovi radovi se i danas koriste na vojnim akademijama i sigurnosnim studijama te čine jedan od važnih temelja sigurnosno-obavještajnog promišljanja.

Ako u okvirima ovog istraživanja govorimo o hibridnom ratovanju kao nastojanju jedne strane da korištenjem hibridnog oblika ratovanja prvenstveno ostvari svoje političke ciljeve izvan teritorija vlastite države, onda zaključujemo da se politička dimenzija hibridnog ratovanja manifestuje kroz vanjsku politiku te države – pa je u ovom kontekstu izučavanja hibridnog ratovanja prikladno o vanjskoj politici neke države govoriti kao o „hibridnoj politici". Promatrajući gore navedene definicije rata u kontekstu hibridnog ratovanja, nameće se pitanje – kako definirati hibridnu politiku, te koja je bit, sadržaj i usmjerenje hibridne politike Ruske Federacije u odnosu na članice i partnere Europske unije i NATO saveza? Odnosno, koja je bit, sadržaj i usmjerenje vanjske politike Republike Srbije u odnosu na Bosnu i Hercegovinu. Hibridna politika je ciljana kompleksna upotreba političke, diplomatske, ekonomske (uključujući finansijske, energetske, i vojno-tehničke aspekte) razmjene, kao i informacijska propaganda i druge nekonvencionalne (asimetrične) mjere jedne države (ili saveza više država) s ciljem potkopavanja unutarnje i vanjske politike druge države, i to uz pomoć širokog raspona prikrivenih metoda i mehanizama potkupljivanja, zastrašivanja i ucjenjivanja vodstva političkih i gospodarskih elita, političkih stranaka i društvenih grupa, kao i cjelokupne populacije te države (Radkovets, 2015: 8). Hibridna politika provodi se tokom svih faza hibridnog rata, a započinje u pripremnoj fazi hibridnog rata (Radkovets, 2015: 8).

Volodymyr Horbulin analizira problem konceptualiziranja hibridnog rata u kontekstu geostrateških napora Ruske Federacije čiji krajnji cilj je nametanje ruskog utjecaja na međunarodnoj sceni (Horbulin, 2015) – čime njegov članak sadrži začetke promišljanja koji dovode hibridno ratovanje u izravnu vezu sa hibridnom (geo)politikom i hibridnom strategijom (Radkovets, 2015). Bugajski u svojoj knjizi Eurasian Disunion – Russia's Vulnerable Flanks kaže da ruski napad na Ukrajinu i cijepanje ukrajinskog teritorija nisu izolirana operacija, već da je to dio šireg strateškog plana s ciljem ponovne izgradnje bloka moći sa središtem u Moskvi i natjecanja sa Zapadom (Bugajski, 2016: 10). Ubrzana realizacija neo-imperijalističkog projekta ruskog predsjednika Vladimira Putina predstavlja sigurnosni izazov za nekoliko regija koje graniče s Ruskom Federacijom, te je privukla pažnju zapada na vanjsku politiku Rusije (Denyer, 2015). Glavni cilj ruske hibridne politike je obnoviti status Rusije kao centra moći u multipolarnom i multicentričnom svijetu.

Tablica 3: Gerasimova strategija - temeljne razlike između konvecionalnog i hibridnog rata

Tradicionalne vojne metode	**Nove vojne metode**
Vojna operacija počinje nakon strateškog razmještanja snaga (objave rata)	Vojnu operaciju pokreću grupe snaga za vrijeme razdoblja mira (uopće nema klasične objave rata)
Frontalni sudari velikih oružanih jedinica uglavnom se sastoje od zemaljskih snaga	Sudari visoko manevarskih interspecifičnih borbenih skupina bez stvarnog kontakta

Povećavanje snaga, paljbene moći, preuzimanje nadzora nad dijelom teritorija i granica s ciljem ostvarivanja teritorijalnog nadzora	Uništavanje protivničke vojne i ekonomske moći pomoću kratkotrajnih visoko preciznih udara na stratešku vojnu i civilnu infrastrukturu
Uništavanje ekonomske moći i pripajanje teritorija	Masivna upotreba oružja visoke preciznosti i specijalnih operacija, robotike, i oružja koja koriste nove fizikalne principe (laseri, kratkovalna radijacija i sl.)
Upravljanje snagama kroz postojanje stroge vojne hijerarhije	Korištenje naoružanih civila (četiri civila na jednog vojnika) Simultani udari na protivničke postrojbe i infrastrukturu na cjelokupnom teritoriju Simultane bitke na zemlji, moru, zraku i informacijskom prostoru Korištenje asimetričnih i neizravnih metoda Upravljanje snagama u unificiranoj informacijskoj sferi

Izvor: izradio autori(i) prema: Gerasimov, 2013.

Kao rezultat toga u ratovima nove generacije dominira informacijsko i psihološko ratovanje pomoću kojega se postiže superiornost nad konvencionalnim vojnim snagama, te se moralno i psihološki potiskuje vojna sila i populacija protivničke strane (Berzins, 2014: 2). Berzins navodi da je u trenutnom geopolitičkom poretku glavni protivnik Rusije zapadna civilizacija, njene vrijednosti, kultura, politički sistem i ideologija (Berzins, 2014: 3-4). Uspjeh ruskog hibridnog rata u Ukrajini nametnuo je pitanje moguće primjene ovog modela u drugim dijelovima svijeta, o čemu će više biti govora u narednim poglavljima ovog rada . Berzins je identificirao osam faza hibridnog ratovanja (Berzins, 2014: 4):

2.1 Faze hibridnog djelovanja/ratovanja

Prva faza: ne-vojno asimetrično ratovanje (obuhvaća informacijske, moralne, psihološke, ideološke, diplomatske i ekonomske mjere kao dio plana za uspostavljanje povoljnog političkog, ekonomskog i vojnog okruženja).
Druga faza: Specijalne operacije koje imaju za cilj obmanuti političko i vojno vodstvo uz pomoć koordiniranih mjera koje provode diplomatski kanali, mediji i vladine i vojne organizacije fingiranim „curenjem" lažnih podataka o namjerama i planovima.
Treća faza: Intimidacija, zavaravanje, i podmićivanje vladinih dužnosnika i vojnog vodstva, kako bi ih se prisililo/potaknulo na napuštanje vlastitih položaja.
Četvrta faza: Destabilizirajuća propaganda koja izaziva nemir i nezadovoljstvo među populacijom, dodatno pojačana dolaskom ruskih militanata koji eskaliraju subverziju.
Peta faza: Uspostava „no-fly" zona iznad zemlje koju se planira napasti, postavljanje blokada, te značajna upotreba privatnih vojnih agencija u uskoj suradnju sa naoružanim jedinicama opozicije.
Šesta faza: Početak vojne akcije, kojoj prethode izvidničke akcije i zadaće subverzije. Svi tipovi, oblici, metode i snage su angažirani u provedbi ove faze, uključujući specijalne

jedinice, svemirske postrojbe, jedinice veze, diplomatske snage, obavještajne jedinice kao i aktere koji provode industrijsku špijunažu.
Sedma faza: Kombinacija ciljanih informacijskih operacija, operacija elektronskog ratovanja, operacija u svemiru, kontinuirano zastrašivanje avijacijom kombinirano s korištenjem visokopreciznog oružja.
Osma faza: Slamanje preostalih tačaka otpora i uništavanje preživjelih jedinica protivnika sprovedbom specijalnih operacija.

Teorijske analize hibridnog ratovanja nameću zaključak da je hibridni protivnik onaj protivnik koji vješto koristi napredne vojne tehnologije, a ujedno ima prilagodljivu organizacijsku strukturu koja mu dopušta brzu prilagođavanje okolnostima. Shodno tome, onome koji se želi efiasno suprotstaviti hibridnom ratovanju mora biti prioritet razviti sposobnost predviđanja i prepoznavanja kada neki izvor ugroženosti poprima hibridna obilježja. Osim Berzinsove analize toka hibridnog sukoba u osam faza, analitičari i stručnjaci sa neovisnog vojnog instituta za geopolitičke studije «Boryfsen Intel» iz Kijeva su temeljem analize dosadašnjih ratova hibridni rat podijelili u tri faze: pripremnu fazu, aktivnu fazu i završnu fazu rata (Radkovets, 2015: 27).

Prema njihovim analizama, tokom pripremne faze (koja može trajati i nekoliko godina) političko vodstvo hibridnog aktera najčešće uz pomoć sigurnosnih i obavještajnih službi vrši ideološke, političke i vojne pripreme za nadolazeći rat (Radkovets, 2015: 24). To obično obuhvata jačanje političke moći unutar vlastite države, pojačan nadzor nad svim sferama društva i života. Zatim, može se provoditi ideološko "ispiranje mozga" nad vlastitim stanovništvom kako bi se pobudili nacionalistički osjećaji i potreba za odbranom "nacionalnih vrijednosti i interesa". U pripremnoj fazi se ostvaruje određena moć nad informacijskim prostorom ciljane zemlje, te se provode i različite aktivnosti sa svrhom diskreditiranja političkog establišmenta. U ovoj fazi hibridni akter nastoji unijeti razdor i podjele među stanovništvo ciljane zemlje, obično se oslanjajući na političke, etničke i/ili religijske različitosti stanovništva.

Aktivna faza hibridnog rata podrazumijeva prikrivenu ili otvorenu agresiju hibridnog aktera na ciljanu zemlju (Radkovets, 2015: 25). Ova faza podrazumijeva izazivanje unutrašnjih ratova u ciljanoj državi temeljem političkih, socijalnih, gospodarskih, vjerskih i/ili etničkih neslaganja, podupiranje ili čak formiranje ilegalnih oružanih skupina koji se otvoreno sukobljavaju sa predstavnicima vlasti, te kreiranje paralelnih/alternativnih vladajućih struktura. U ovoj fazi može doći i do invazije, odnosno ulaska oružanih snaga hibridnog aktera u ciljanu zemlju.

U završnoj fazi hibridnog sukoba hibridni akter konsoliduje svoju poziciju u ciljanoj zemlji na način da podupire nove vladajuće političke strukture (koje su prije rata bile u opoziciji), podupire provedbu izbora i referenduma i tako usmjerava unutrašnju i vanjsku politiku.

3. Studija slučaja Bosne i Hercegovine

Na globalnom planu postoji niz pokušaja ujednačavanja praksi iz oblasti sigurnosti u virtualnom i hibridno informatičkom prostoru. Koliko neke države ovo pitanje smatraju ozbiljnim i aktuelnim govori i primjer Japana koji ima ministra za cyber sigurnost. Druge države kao što je Kina imaju zakonske okvire koji regulišu ovu oblast, a što je važnije ti zakonski okviri se često prilagođavaju novonastalim okolnostima. Pojavila se i inicijativa brojnih sigurnosnih eksperata da se na nivou UN-a donese jedan okvirni sporazum koji bi se bavio ovom problematikom. Da li će postojati volja među ključnim akterima za ovakav dokument tek ćemo da vidimo.

Razvijene države na dnevnoj osnovi prate hibridno djelovanje u cyber prostoru. Tako, prema istraživanju britanske vlade za 2019. godinu, samo u Velikoj Britaniji je zabilježeno da je preko 32 posto kompanija bilo izloženo cyber napadima ili „prodoru“ od kojih je nepoznat broj onih koji se mogu povezati sa hibridnim djelovanjem ili hibridnim ratovanjem protiv nacionalih i međunarodnih interesa Velike Britanije.

Bosna i Hercegovina je vjerojatno najkrhkija zemlja na Balkanu i plodno tlo za geopolitičke bitke između Rusije i Zapada. Njena unutrašnja politika podijeljena je trenutno između dva administrativna entiteta unutar same države (Federacija Bosne i Hercegovine i Republike Srpske), s jedne strane, i između tri zajednice (Bošnjaka, Srba, Hrvata), s druge, svaka s različitim izvorima određene eksterne podrške. Jasno je da Rusija pokušava održati zonu utjecaja u administratinom entitetu Republika Srpska, dok Zapad nije dovoljno vidljiv građanstvu u Federaciji BiH, a još manje u Republici Srpskoj. Država postaje nefunkcionalna i otporna na inicijative EU i SAD da promoviraju progres.

Političko sigurnosna situacija je dodatno zakomplicirana Izborima 2018. godine koji nisu donijeli velike političke promjene, osim što je lider secesionističkih težnji Milorad Dodik, predsjednik Republike Srpske za prethodnih osam godina, biran kao srpski član tročlanog predsjedništva države Bosne i Hercegovine. Prije glasanja 2018. godine nije bilo većeg političkog događaja koji bi intenzivirao *dihotomiju* proruskog i prosrbijanskog uticaja, ka realno nemogućoj, disoluciji Bosne i Hercegovine. Poruke prema zapadu bile su daleko manje agresivne i niže nego u Makedoniji i Srbiji. Narativni govornici u Bosni i Hercegovini više su glasni među etničkim Srbima u Republici Srpskoj, nego u Federaciji BiH, jer se poruke najčešće kanaliziraju kroz srpski interes u regiji, s posebnim naglaskom na spor s Kosovom. Republika Srpska definiše svoj politički interes prije svega kao dobru vezu sa Srbijom, bez obzira ko su političari u Beogradu i Banja Luci (administrativni centar Republike Srpske). Nakon što je izabran u predsjedništvo Bosne i Hercegovine, Dodik je obećao da će koristiti svoj srbijanski pasoš za putovanja u inostranstvo (Metodijeva, 2019: 48).

Proruski narativi dio su glavne politike u Republici Srpskoj, dijelom kao rezultat dobrih odnosa Dodika i predsjednika Vladimira Putina. Čovjek američkog državnog sekretara Madeline Albright koji je nekad opisan kao "dah svježeg zraka" danas je najbliži ruski

politički saveznik u regiji i pod američkim sankcijama[99]. On je najvjerniji i najglasniji ruski posrednik na zapadnom Balkanu. On se protivi ulasku Bosne i Hercegovine u NATO, pozivajući se na deklaraciju Republike Srpske o „vojnoj neutralnosti" potpisanu sa Rusijom. Aleksandar Vranješ, profesor na Univerzitetu u Banjoj Luci, tvrdi da anti-NATO raspoloženje ljudi u Republici Srpskoj ne bi trebalo da bude iznenađenje: "Postoji jednostavan razlog za to: NATO bombardovanje Srbije."

3.1 Rusko i srbijansko specijalno i hibridno djelovanje u Bosni i Hercegovini

Republika Srpska, okružena članicama NATO-a Hrvatskom i Crnom Gorom, ima strateški značaj za Rusiju. Rusija je Dodika otvoreno podržala u njegovim prethodnim izbornim kampanjama, uključujući izbore 2018. godine. Ruski ministar vanjskih poslova Lavrov bio je najistaknutiji strani političar koji je posjetio Bosnu i Hercegovinu, u posljednjim danima kampanje. U Banjaluci je Lavrov dobio Nagradu Republike Srpske, najviše priznanje srpskog entiteta. Podrška Rusije znači i da Rusija to ima mogućnosti suzdržavajte Dodika, ako treba, prema analitičaru Dimitaru Bečevu[100]. Naprimjer, Rusija djeluje prilično nezainteresovano da u potpunosti prihvati separatistički pogled Dodika i političke elite Republike Srpske.

Vlada Republike Srpske je 2016. godine održala neustavni referendum s blagoslovom Rusije da usvoji odvojeni nacionalni praznik. Još jedno glasanje za otcjepljenje od Bosne i Hercegovine obećano je za 2018. godinu, ali to se nije dogodilo. Ove akcije su utrle Dodikov put na američku listu sankcija i još više se pouzdale u Rusiju. Dodik je pozvao Republiku Srpsku da prizna aneksiju Krima i pozdravio Noćne vukove, prokremljinski ruski motociklistički pokret u Banjaluci 2018. U skladu s ruskim političkim interesom u regiji, Dodik potvrđuje da je opće oduševljenje EU u Bosna i Hercegovina se smanjuje i EU "propada"[101]. Budući da je najglasniji ruski zastupnik u Rusiji, on hvali Rusiju i Kinu jer su ponudili regionu prijateljstvo i ekonomsku saradnju bez vezanosti za političke uvjete i "tražeći od njega da učini bilo šta nemoguće."

Pored lojalnih političkih pristalica u zemlji, Rusija se oslanja na „geopolitičke poduzetnike" da usmjere svoje interese u Bosnu i Hercegovinu. Jedan primjer je ruski milijarder Konstantin Malofeev, nacionalista i promotor paroslavenskog pravoslavlja i ključna figura u sukobu u Ukrajini. Jedan je od stratega aneksije Krima i bio je uključen u planiranje, pripremu i finansiranje tamošnjeg separatističkog referenduma, zajedno s onim u Donjecku i Lugansku[102]. Njegove aktivnosti u istočnoj Ukrajini dovele su ga do toga da bude stavljen na listu sankcija EU . Panamski papiri koji su procurili otkrili su značajni Malofejev politički i ekonomski položaj na Zapadnom Balkanu. Poslednjih godina je posebno aktivan

[99] Maxim Edwards, "The President who wants to break his own country," The Atlantic, February, 1, 2019.
[100] Ibid
[101] Andrew MacDowall, "Bosnia's Serb Republic leader: No breakaway vote next year," Politico, June 29, 2017.
[102] Ibid

u Republici Srpskoj. 2014. godine organizovao je kontroverznu posjetu Kozaka Banjoj Luci kako bi izrazio podršku Dodiku u njegovoj izbornoj kampanji. 2015. godine Dodik je dodjelio Malofeevu (zajedno sa Putinovim savjetnikom Igor Štegolev i Leonid Reshetnikov, bivši general ruske spoljno-obaveštajne službe i direktor Ruskog instituta za strateške studije) priznaje „Njegošev orden za doprinos Republici Srpskoj“[103].

Kao i u Srbiji, proruski narativni posrednici u Bosni i Hercegovini oslanjaju se na sličan skup poruka protiv Zapada. Sve je to objavljeno u izbornoj kampanji 2018., koju je Sputnik gurnuo, ali je češće prihvaćen od strane lokalnih medija. Značajan dio ovih propagandnih priča potiče iz Srbije, gurajući prosrpska stajališta o pitanjima kojima bi oslabio identitet bosanskohercegovačke zajednice. Tako Rusija podržava lokalne aktere koji žele zadržati status quo, sve dok zemlje u regiji ne napreduju sa svojim ambicijama prema NATO-u i EU. Ipak, Rusija ne nudi suštinsku alternativu. Republika Srpska je među mjestima u regiji u kojoj preovlađuju proruski / antizapadni narativi zbog nepostojanja zajednice kritičkih glasova, uključujući akademce, novinare i grupe civilnog društva. Ni opozicija, ni mediji nisu dovoljno jaki da ih izazovu. Javni RTV servis u Banjaluci je pod političkom kontrolom i otvoreno se koristi za promicanje provladine političke agende u Republici Srpskoj. Alternativna televizija (Alternativna televizija) pokrenuta je 1996. godine kao dopisna jedinica prve višeentitetske otvorene radiodifuzne mreže koju je osnovao Ured visokog predstavnika za Bosnu i Hercegovinu i EU. Danas je to samo provladin televizijski kanal i zna se da je kontroliše sin Milorada Dodika, Igor.

Web stranica i radio emisije Sputnika dostupni su u Republici Srpskoj i Federaciji BiH. Iako nije baš popularan, njegove poruke lako prodiru u javne medije. U Republici Srpskoj sadržaj Sputnjika često preuzimaju glavni mediji. Naprimjer, novinska agencija SRNA posuđuje izvještaje Sputnika i predstavlja ih kao originalne, a kada drugi informativni portali ponovo objavljuju iste podatke, oni navode SRNA, a ne Sputnjik kao izvor. Anti-zapadni / proruski narativi popularni u su dijelovima Bosne i Hercegovine često se pojavljuju na web stranicama InfoSrpska, Krajina, Govori Srbija, Glas Srpske, Nezavisne, Srbija Danas i na mnogim drugim portalima čije vlasništvo i izvor financiranja ostaju nejasni, ponovo objavljujući jedan. priče na strani. Popularnost ovih web stranica nije toliko velika kao na televiziji ili novinama. Priča Vladimira Kovačevića, istraživačkog novinara na jednom od lokalnih televizijskih kanala, ilustrira čitav ciklus dezinformacija koje istovremeno kruže različiti narativni proxy-i. Godine 2018. napadnut je i pretučen gotovo u smrt u Banjoj Luci: „Dan nakon napada na mene, srpski provladin tabloid Informer napisao je da mi je neka američka organizacija platila 80 000 dolara za izradu moje web stranice. Uveče su se te informacije pojavile na RTRS-u i Alternativnoj televiziji “ (Metodijeva: 2019, 49). Kovačević kaže da je napad bio povezan sa njegovim radom i da sumnja u vezu sa političkim rukovodstvom Republike Srpske. Druga meta lažnih vijesti u okviru predizborne kampanje 2018. godine bili su protesti koji se u Banjoj Luci održavaju svakog dana nakon

[103] https://www.pressreader.com/bosnia-and-herzegovina/dani/20170324/282467118719365, pristupljeno 08.10.2019

ubistva mladića Davida Dragičevića u martu 2018. godine. Otac Dragičevića, ključnog organizatora Pravde za Davida, protestira, sumnja policija umešanost u ubistvo njegovog sina Demonstracije nisu bile politički pokretane, ali su imale političke efekte na Dodikovu moć koja se uzima kao zdravo za gotovo. Oni su viđeni na protestima protiv političkog statusa kvo u Republici Srpskoj. Povod je mobilizirao hiljade mladih na društvenim medijima i time postao meta lažnih Facebook profila i dezinformacija. Prema političkoj analitičarki Tanji Topić, *„Ne postoji nijedna stranka u Republici Srpskoj koja bi ikada mogla toliko ljudi motivirati da izađu na ulicu. U ovom se slučaju pojavio paradoks u vezi sa ulogom društvenih medija. S druge strane, Facebook je otvorio prostor za alternativne stavove. S druge strane, postalo je poprište rata kojim se ne predstavlja ništa*." [104] Najave o protestima lako se prenose iz internetskog prostora u glavne medije. RTRS je također često izveštavao o manjem broju demonstranata ili jednostavno nije pružio medijsku pokrivenost protestima.

3.2 Uticaj hibridnog djelovanja i ruskih narativnih posrednika

Cilj je hibridnog djelovanja produbljivanje rascjepa među tri zajednice Bosne i Hercegovine. Ruski analtički i reportažni posrednici koji su bili aktivni tokom izborne kampanje 2018. oslanjali su se na neriješeni razdor i historijske prigovore kako bi produbili polarizaciju između Srba, Bošnjaka i Hrvata u zemlji. Nema naznaka da je to imalo izravnog utjecaja na ponašanje birača, jer je takva retorika godinama normalizovana u domaćem političkom diskursu. Međutim, intervjuirani novinari i stručnjaci sa sjedištem u Sarajevu i Banjoj Luci tvrde da ova dezinformacija ima negativne efekte na bilo kakve izglede za dublju institucionalnu saradnju dva bosanskohercegovačka entiteta i stvara prostor za daljnje napetosti.

Jačanje nacionalizma i podsticanje ideje o razdvajanju Republike Srpske. Republika Srpska je 9. januara 2019. godine proslavila svoj „nacionalni" praznik, uprkos zabrani koju je Ustavni sud zabranio. Ponovno je vlada entiteta organizirala ceremoniju u Banjaluci, stvarajući svađu između bošnjačkih i bosanskih Srba. Snažnu političku podršku Rusije prosepatističkom političkom vodstvu Republike Srpske druge dvije zajednice čitaju kao prijetnju političkoj stabilnosti Bosne i Hercegovine.

Potkopavajući proevropsku i prozapadnu orijentaciju Bosne i Hercegovine. Posebni negativni efekti ruskih narativnih posrednika mogu se primijetiti u vezi s euroatlantskim integracijama. Budući da je nosilac veta u vladi zemlje, Republika Srpska prenosi poruke protiv perspektiva pristupanja Bosne i Hercegovine NATO-u. Izričita anti-NATO retorika rukovodstva Republike Srpske u velikoj meri je inspirisana prijateljstvom sa Srbijom,

[104] Iz : A.M- Interview with Tanja Topic, a political analyst, Banja Luka, October 11, 2018.u Asya Metodieva, „Russian Narrative Proxies in the Western Balkans" Policy Paper, June 2019 | No.16, GMF

doprinoseći proruskoj političkoj agendi u regionu. Kako su popularni televizijski kanali, web stranice, novine i državna novinska agencija Republike Srpske u potpunosti pod političkom kontrolom, pristup alternativnim gledištima je prilično ograničen. Vrste informacija zasnovanih na mišljenju dominiraju u pokrivanju tema poput spora Kosovo i Srbija. Intervjuirani novinari ocjenjuju ulogu ruskih narativnih hibridnih proxy-a kao štetnije za medijsku scenu u Republici Srpskoj i manje štetne u zemlji u cjelini, zbog veće izloženosti alternativnih gledišta u ostatku zemlje.

Cilj djelovanja je stvaranje imidža Rusije kao političke, vojne i ekonomske alternative Zapadu. Ruski pozitivni imidž daleko je bolje naglašen od strane ruskih narativnih posrednika u Republici Srpskoj, nego u Federaciji BiH. U tom pogledu nema veće razlike od susjedne Srbije, jer se ova slika često kanališe kroz iste medijske izvore, političke partije i pojedine političke aktere. U poluautonomnom entitetu, lokalni medijski punomoćnici uspješno su izgradili ruski imidž kao ključnog čuvara Srbije u sporu sa Kosovom kao i branitelja Republike Srpske.

Zaključak

Na nivou Bosne i Hercegovine na snazi je osam zakona koji sadrže pravnu regulativu koja tretira sigurnost na internetu, ali nemamo zaseban zakon o cyber/informacijskoj sigurnosti. Ne postoji ni državno koordinacijsko tijelo (kao što je tim za odgovor na informacijsku sigurnost na incidente (CSIRT ili CERT) radi pravovremenog koordiniranja incidenata u cyber sigurnosti. Sa druge strane Hrvatska, Crna Gora i Srbija, imaju i zakone o cyber sigurnosti, ali i državne strategije za cyber sigurnost, već duži vremenski period i razvijaju kako hibridno djelovanje tako i u određenim područjima djelomično hibridno ratovanje (i na hrizontalnom ali i vertikalnom planu). U BiH se pokušava pokrenuti to pitanje, prvenstveno u sferi odbrane od tog i takvog djelovanja, pa su u oktobru 2019. godine predstavljene Smjernice za strateški okvir cyber sigurnosti u Bosni i Hercegovini. Smjernice su izrađene pod okriljem Misije OSCE-a u Bosni i Hercegovini i uz podršku Delegacije Evropske unije i Ureda specijalnog predstavnika Evropske unije u BiH, te Ženevskog centra za demokratsku kontrolu oružanih snaga (DCAF). Ovaj korak za BiH predstavlja značajan poticaj za sve relevantne institucije da izrade svoje strategije i planove njihove realizacije zasnovane na prezentiranim smjernicama.

Iako Institucije (prvenstveno akademske), organizacije, kompanije i građani BiH, u skladu sa mogućnostima i potrebama slijede trend digitalizacije, najčešće se to dešava bez potrebnih znanja hibrdinog djelovanja ili komponenti cyber zaštite, ostavljajući tako kompletnu infrastrukturu podložnu različitim vrstama hibridnih i cyber napadima.

Studija slučaja pokazuje da su Anti-Zapad/proruski narativi našli su plodno tlo na Zapadnom Balkanu, jer je regija ključni prostor za sukob Rusije i Zapada. To se djelovanje ne pojavljuje u vakuumu, ali ih olakšavaju lokalne mreže posrednika za dezinformaciju. U razmatranoj studiji slična infrastruktura proxy-a igra ulogu u sprječavanju dezinformacija

i širenju polarizacije. Napori na dezinformaciji u regiji usmjereni su na događaje i prelaze s jednog mjesta na drugo, ovisno o lokalnom političkom kontekstu. Posljednjih mjeseci njihova se polarizirana retorika najčešće odnosila na spor između Kosova i Srbije, nakon čega su uslijedili referendum o imenu Sjeverne Makedonije i izbori u Bosni i Hercegovini. Četiri su ključne priče korištene u varijacijama u tri zemlje: NATO je agresor, EU je institucionalno i politički slaba, Sjedinjene Države nastoje stvoriti veliku Albaniju, a Rusija pouzdan partner. Ne postoji političko priznanje postojećih prijetnji dezinformacijama među političkim elitama u regiji. Oni koji ne priznaju ulogu propagandnih posrednika osjetljiviji su na njihov utjecaj. Neki dijelovi lokalne populacije više su odvojeni od glavnih medija i podložniji su proruskim / antizapadnim medijskim sadržajima od stanovništva općenito. Što je veća izloženost stanovništva neke zemlje određenom skupu medijskih narativa i dezinformacija, veće su mogućnosti da utječe na njeno društvo i političko odlučivanje (Andrei Y, Damarad V: 2018).

Hibridno djelovanje/ratovanje protiv BiH kao države je realnost, a napadi i postojeća prijetnja BiH i zahtijevaju adekvatne mjere prevencije i cyber zaštite. Od presudne je važnosti da nadležne institucije u BiH intenziviraju saradnju u oblastima edukacije, razmjene iskustava i podataka sa SAD, državama članicama EU i NATO-a, ali i da odrede, definišu i primijene u praksi strategiju, standarde, tehnike kao i da osiguraju potrebne ljudske i materijalne resurse.

Literatura:

- Andrei Yeliseyeu and Damarad Volha, (2018) Disinformation Resilience in Central and Eastern Europe, p 17. GMF
- Asya Metodieva, „Russian Narrative Proxies in the Western Balkans“ Policy Paper, June 2019 | No.16, GMF
- Berszins J. (2014). Russian New Generation Warfare: Implications for Europe. European Leadership Network. October 2014. Pristup preko http://www.europeanleadershipnetwork.org/russian-new-generation-warfare-implicationsfor-europe_2006.html
- Bugajski, Janusz (2016). Eurasian Disunion – Russia's Vulnerable Flanks. The Jamestown Foundation. Washington DC, 08/2016
- Gerasimov, V (2013). Vrijednost znanosti je u predviđanju: Novi izazovi zahtijevaju ponovno promišljanje oblika i metoda provedbe borbenih operacija. VoyennoPromyshlennyy Kurier (VPK) (Military-Industrial Courier). Pristup preko http://vpknews.ru/sites/default/files/pdf/VPK_08_476.pdf
- Horbulin, Volodymyr (2016). „Hybrid War: It is just e Beginning“. Pristup preko http://en.niss.gov.ua/public/File/englishpublic/Horbulin%20article%20eng%20%20final%20version.pdf. Autor pristupio 10/2019.
- Lind. W (1989). The Changing Face of War: Into the Fourth Generation. Marine Corps Gazette, October 1989, str. 22-26. Pristup preko http://globalguerrillas.typepad.com/lind/the-changing-face-of-war-into-the-fourthgeneration.htm
- Maxim Edwards, (2019).“The President who wants to break his own country,” The Atlantic, February, 1
- Radkovets Yuiry (2015a). Russia's Armed Agression against Ukraine: Pecularities of Preparation and Conducting New Challenges and Threats. BINTEL Geopolitical Analytics Journal, Kijev, Ukrajina, 2015
- Radkovets Yuiry (2015b). Russia's Armed Agression against Ukraine: Pecularities of Preparation and Conducting New Challenges and Threats. BINTEL Geopolitical Analytics Journal, Kijev, Ukrajina, 2015
- Radkovets, Yuriy (2015a). Today's Russia's Hybrid Policy as a Strategy for the Implementation of its National Geopolitics. Hybrid Wars as a Continuation of Hybrid Policy. BINTEL Geopolitical Analytics Journal. Special Issue. 2015., str. 4-11.
- Van Kreveld Martin, (2010) Transformacija rata, JP Službeni Glasnik i Fakultet bezbednosti, prevod -Beograd, 2010

Kriminalističke teme
Zbornik radova
Godina XIX, Broj 5, 2019.
ISSN 1512-5505

RADIKALIZAM I EKSTREMIZAM NA INTERNETU
RADICALISM AND EXTREMISM ON THE INTERNET

Pregledni naučni rad

Želimir Kešetović[105]

Apstrakt

Inspiracija za rad i problem (i) koji se radom oslovljava (ju): Internet i njegovi servisi omogućuju nasilnim ekstremistima da prošire funkcionalnosti svojih propagandnih napora izvan granica tradicionalnih mainstream medija. U mnogim zemljama vladine agencije i akademska zajednica zaključile su, na osnovu razvoja događaja u međunarodnom terorizmu, da internet igra određenu ulogu u radikalizaciji pojedinaca i njihovom učešću u ekstremističkom nasilju.

Ciljevi rada (naučni i/ili društveni): Cilj rada je analizirati kako se u literaturi o ekstremizmu i radikalizaciji priznaje se uloga Interneta u procesu individualne radikalizacije prema ekstremističkim ideologijama, mada se potpuno razumevanje ovog fenomena tek razvija. Istraživanja ovog fenomena uglavnom se sprovode putem analize sadržaja u kojem se ispituje kako ekstremističke grupe koriste.

Metodologija/Dizajn: U radu je primarno korištena tehnika iz kvalitativne istraživačke paradigme. Metodom analize sadržaja istraživat će se extremizam u procesu individualne radikalizacije i metode koje se koriste. Selekcija akademskih radova iz oblasti extremizma je urađena na način da su odabrani samo oni radovi koji u svojoj sadržini imaju historijsku i razvojnu komponentu sigurnosti i extremizma.

Ograničenja istraživanja/rada: Nedostatak naučnog diskursa i različitih postupaka te postojanje izraženog nesklada u teorijskim razmatranjima a u vezi sa interpretiranjem radikalizma i extremizma na internetu.

Rezultati/Generalni zaključak Internet i njegove servise u svojim komunikacionim i strategijama regrutacije novih sledbenika. Istraživači su razvili i Internetom posredovani model radikalizacije –RECRO sa pet faza koji pruža osnovu za razumevanje i na informacijama zasnovanu procenu o nivou uključenosti pojedinca i utire put budućem empirijskom radu. Ove mogućnosti Interneta koriste i nosioci radikalnih i ekstremističkih ideja na području Republike Srbije i Zapadnog Balkana. Istovremeno, Internet pruža i značajne mogućnosti za deradikalizaciju. U ovom preglednom radu, na osnovu analize relevatnih izvora, daće se presek stanja i aktuelni akademski nalazi o ovoj temi.

Opravdanost istraživanja/rada: Opravdanost istraživanja se ogleda u potrebi da se prizna važnost pogodnostima primjene razločitih programa borbe protiv radikalizacije i extremizma na internetu u današnje vrijeme.

Ključne reči

radikalizacija, ekstremizam, deradikalizacija, mediji, Internet

[105] Redovni profesor na Fakultetu bezbednosti Univerziteta u Beogradu, zelimir.kesetovic@gmail.com

Abstract

Internet and the services it offers, allow violent extremists to expand the functionalities of their propaganda efforts beyond the boundaries of the traditional, mainstream media. In many countries, government agencies and the academic community have concluded, based on developments in international terrorism, that the Internet plays a certain role in the radicalization of individuals and their involvement in extremist violence. The literature on extremism and radicalization recognizes the role of the Internet in the process of individual radicalization towards extremist ideologies, hoping that a complete understanding of this phenomenon is still developing. The research of this phenomenon is mainly carried out through an analysis of the content in which the extremist groups use the Internet and its services in their communication and strategies for recruiting new followers. The researchers also developed the Internet-nediated radicalization model -RECRO with five phases that provides a basis for understanding and information-based assessment of the level of individual involvement and paving the way for future empirical work.These opportunities of the Internet are also used by protagonists of radical and extremist ideas in the Republic of Serbia and in the Western Balkans. At the same time, Internet also offers significant opportunities for deradicalisation. In this review work, based on an analysis of relevant sources, state of art and current academic findings on this topic will be presented.

Key words

radicalisation, extremism, deradcalisation, media, Internet

1. Uvod – Radikalizam i ekstremizam kao istorijska konstanta

Radikalizam i ekstremizam su stalni pratioci političkog života. U posljednjih nekoliko decenija, međutim, mogu se vidjeti u političkom spektru pokreti ekstremista od krajnje ljevice prema krajnjoj desnici. Dok je anarhizam predstavljao ideološko zaleđe ekstremizma u XIX vijeku, nakon završetka Hladnog rata, parlamentarna ljevica prešla je na socijaldemokratiju i krajnja ljevica je oslabila, dok su ekstremne ljevičarske političke organizacije preuzele dio frustracija. Danas je, međutim, njihov uticaj marginalizovan, a desni ekstremizam postaje sve jači (Subotić, 2013).

Bjelodano je da se posljednjih godina svjetski politički i ideološki spektar pomaknuo udesno. Osim toga, globalni događaji sve su više zaoštreni novim valovima nasilnog ekstremizma, radikalizma i terorizma. Tako su, naprimjer, od 2010. godine izvršeni nasilni napadi širom Njemačke (u Frankfurtu, Dusseldorfu, Bonnu, Oberurselu i Berlinu), Turskoj (Istanbul, Ankara, Dijarbakir i Gaziantep), Francuskoj (Pariz, Nica i Lyon), Belgija (Bruxelles), Norveška (Oslo), Rusija (Moskva i Volgograd), Meksiko, Irak, Kina, Egipat, Pakistan, Jemen, Avganistan, Nigerija, Somalija, Sjedinjene Države, itd. Bez obzira na to jesu li ovi incidenti motivisani religioznim, etničkim ili političkim razlozima, ostaje činjenica da ideologije ekstremističkih grupa koje ih vrše veličaju vlastito postojanje i suprotstavljaju se demokratskim i liberalnim vrijednostima tolerancije, multikulturalizma i inkluzije. (CeSID, 2016)

Pratilac radikalizma i radikalnih političkih ideja je nasilni ekstremizam. Međutim, izazovi s kojima smo danas suočeni su složeniji zbog globalizacije ovog problema i njegovog prelijevanja preko nacionalnih granica. Moderni nasilni ekstremizam ima sljedeća (nova) obilježja:

- globalizacija dovodi do novih oblika povezivanja između radikalnih ekstremističkih grupa;
- moderna komunikacijska tehnologija (posebno društveni mediji) omogućava pojedincima i grupama da se lakše povežu jedni s drugima i olakšava regrutaciju novih sljedbenika,
- promjena nivoa nepredvidivosti ekstremističkog nasilja, posebno zato što se sve češće mete terorističkih napada biraju nasumično. Počinitelji također često sklapaju pakt o samoubistvima prije napada.
- Konačno, informacijama koje su slobodno dostupne na mreži olakšan je pristup smrtonosnom oružju, s tim da pojedinci i grupe imaju na raspolaganju široku lepezu oružja (uključujući oružje za masovno uništenje). (UNDP, 2016)

2. Internet i radikalizacija

Pojava interneta izmijenila je odnos između nasilnog ekstremizma i medija. Internet i mogućnosti koje nudi omogućavaju nasilnim ekstremistima da prošire funkcionalnost svojih propagandnih napora izvan granica tradicionalnih, glavnih medija. Nasilni ekstremisti svih ideoloških boja i predznaka iskoristili su mnoštvo internetskih usluga za širenje svojih ideja, povezivanje i radikalizaciju potencijalnih sljedbenika i simpatizera.

Danas postoji nebrojeno mnogo web stranica, Facebook profila, blogova ili foruma koji okupljaju različite pojedince i organizacije sa ekstremnim, kako desnim tako i lijevim, političkim stavovima. Oni u cyberspaceu, čak slobodnije nego u neposrednim kontaktima, usljed dezinhibirajućeg on-line efekta, iznose svoje stavove i uvjerenja.

Upotreba Interneta od strane nasilnih ekstremista postala je predmet sve većeg broja akademskih istraživanja, posebno kada se radi o potencijalnim funkcijama ove tehnološke inovacije u procesu radikalizacije. (Neo, 2016) Veći broj autora ukazuje na to da je povećano prisustvo nasilnih ekstremista na internetu povećalo i mogućnost da više ljudi potpadne pod uticaj radikalne ideologije (Bermingham, Conway, McInerney, O'Hare, & Smeaton, 2009; Gupta, 2011; Kruglanski, Crenshaw, Post i Victoroff , 2008).

Nasilni ekstremisti su razvili široku paletu digitalnih medija (npr. Web stranice, forume, platforme društvenih medija) kako bi ispunili svoju radikalnu agendu. Kako se njihova upotreba društvenih medija širi, to se povećavaju opseg i vrste informacija koje nasilni ekstremisti mogu dijeliti. Na mnogo načina, ovo daje nasilnim ekstremistima platformu da preuzmu kontrolu nad sadržajem svojih poruka (Conway i McInerney, 2008; General Intelligence and Security Service [AIVD]), 2012; Seib i Janbek, 2011). Slično tome, nagli

porast internetskih publikacija koje produkuju nasilni ekstremisti ukazuje na to da im je ovo sve važnije sredstvo da postignu svoje ciljeve (Lemieux, Brachman, Levitt, & Wood, 2014; Rieger, Frischich, & Bente, 2013; Rogan, 2007).

Internet je poslužio nasilnim ekstremistima kao kanal da utječu na one koji simpatiziraju njihove narative (Edwards & Gribbon, 2013; Neo, Khader, Shi, Dillon, & Ong, 2015; Torok, 2013). Naprimjer, ogroman doseg Interneta čini ga savršenim instrumentom za uspostavu internetske zajednice zajedničkog znanja, normi i interesa bez vremenskih ili geografskih ograničenja (Powers & Armstrong, 2014). Također nudi mogućnost nasilnim ekstremistima poput Abu Musabal-Zarqawia (bivši vođa Al-Qaede u Iraku) da iskoriste Internet kako bi oblikovali svjetonazore svoje publike.[106] Širenje nasilnog ekstremističkog materijala na mreži i lakoća s kojom svako može pristupiti internetskim zajednicama koje se zalažu za nasilje i pronaći radikalne materijale, nehotice su povećali kapacitet za nasilje i nasilni ekstremizam.

Kao što Shahar objašnjava, "bez interneta, radikalne grupe koje čine globalni kadar militanata iz džihada ostale bi široko raspršene i izolovane grupa ćelija koja se pozivaju na iste istorijske korijene. Internet je taj koji je globalizirao džihad pokret. Mreža globalnog džihada proizvod je revolucije u komunikacijama". (Shahar, 2007:140-141)

Prema Loo Seng Neou cijeli niz nasilnih akata poput napada studenta Roshonara Choudhryja na zastupnika u britanskom parlamentu Stephen Timmsa 2010, napada braće Tsarnaev na bostonskom maratonu 2013, napada Micheal Zehf-Bibeaua na kanadski parlament 2014 i dr., ima korijene u digitalnoj sferi budući da su njihovi izvršitelji nasile akte počinili pod uticajem ideja i ideologije koje su prethodno konzumirali na internetu (Neo, 2016:199). Na uticaj potencijalni interneta u procesu radikalizacije ukazuju i drugi autori (Conway, 2012; Lennings, Amon, Brummert, & Lennings, 2010).U analizi nedavnih trendova, Sageman (2010) napominje da je: „78% svih globalnih terorističkih napada džihadista na Zapadu u posljednjih pet godina potjecalo od domaćih autonomnih grupa bez ikakvih veza, usmjeravanja ili kontrole jezgra Al-Qaeda ili njenih saveznika “ dok Weimann primjećuje da gotovo svi napadi usamljenih vukova posljednjih godina uključuju upotrebu elektronskih društvenih medija (Weimann, 2012).

Dok, s jedne strane postoji obimna literatura[107] o upotrebi interneta od strane nasilnih ekstremista, s druge strane nema mnogo istraživačkih uvida u to kako se zapravo praktično događa internetom posredovana radikalizacija. Svakako da nema direktne uzročno posljedične veze između on-line konzumiranja radikalnih i ekstremističkih sadržaja i

[106]Prije nego što je al-Zarqawi započeo internetsku propagandnu kampanju morao je ubiti veliki broj ljudi kako bi privukao pažnju pristalica i medija. Međutim, putem mrežnih videozapisa on je uspio postići veći utjecaj i medijsku promidžbu, koristeći znatno manje resursa.

[107] Vidjeti reference na kraju teksta, pri čemu se svaki od navedenih i korišćenih članaka poziva na veliki broj izvora koji se bave ovom temom.

radikalizacije.[108] Ne postoji dovoljno razumijevanje veze između tranzicije od on-line nasilja ka nasilju u stvarnom svijetu. Iako su radikalni i nasilni sadržaji u virtuelnoj realnosti dostupni velikom broju potencijalnih korisnika, u praksi se zapravo malo njih zaista i odlučuje na nasilne akte u fizičkoj realnosti. Članovi internet zajednica koji su najglasniji i najradikalniji na mreži, ne moraju biti ti koji se i u stvarnosti uključuju u nasilje, već im online radikalizam može biti samo ventil (katarza). I obrnuto, pasivni članovi ne moraju biti najmiroljubiviji. Naprotiv. Postoji cijeli niz pitanja: koje osobine pojedinca utiču na njegovu sklonost da se putem interneta uključi u nasilni ekstremizam? Postoje li faze radikalizacije koje razlikuju mirne aktiviste od onih koji planiraju da krše zakon ili da se uključe u nasilje? Ako postoje takve razlike, kako ih mogu iskoristiti policija i obavještajne agencije za efikasniju borbu protiv nasilja? itd.

Istraživanja sugerišu da ne postoji jedinstveni put ka nasilnom ekstremizmu budući da su putevi i objašnjenja za sklonost nasilju različiti, usljed čega je konstruktivniji procesni pristup koji polazi od toga da je pojedinac kombinacija različitih dimenzija koje su kontinuirano u interakciji i transakciji sa okruženjem. Kontekst i iskustva kroz koja pojedinac prolazi oblikuju ga i utiču na njegovo uključivanje u nasilni ekstremizam. Kako pojedinci dolaze u nasilnu ekstremističku ideologiju i odluče internalizirati ta uvjerenja kako bi opravdali upotrebu nasilja? Kao takvi, ovi okviri zasnovani na fazama predstavljaju opšti slijed faza koje bi mogle dati uvid u to kako pojedinac postupno gravitira upotrebi nasilja, tj. kako usvaja radikalnu ideologiju i internalizuje njena uvjerenja i vrijednosti da bi opravdao upotrebu nasilja. U tom smislu niz autora predlaže fazni okvir u kome se pojedinac postepeno/postupno približava upotrebi nasilja. Prema Neou postoji veći broj modela koji opisuju proces radikalizacije kao što su npr. uticajni model "stepenište ka terorizmu" (Staircase to Terrorism) Fathali Moghaddama koji nalazi šest faza u ovom procesu (Moghaddam, 2005), linearni četvorofazni proces Silbera i Bhatta (2007) i dr., pri čemu svi oni posmatraju radikalizaciju kao proces koji uključuje mnogo međusobno povezanih faktora i uzroka koje treba imati u vidu u promatranju interakcije između pojedinca i vanjskih faktora (Neo, 2016;202).

Međutim svi se ovi modeli više bave radikalizacijom u fizičkoj realnosti bez posebnog uključivanja on-line elementa, odnosno virtualne realnosti gdje je potrebno posebno uzeti u obzir interakcije tokom vremena između osoba i internetsko okruženje. U tom smislu treba shvatiti na koji način Internet posreduje u procesu radikalizacije i oblikuje korisnikova ponašanja i stavove - tj. razumijevanje iskustva pojedinca na mreži i načina na koji on koristi internet u procesu radikalizacije.

U pokušaju da ovo objasni Saifudeen (2014) je razvio „Model orbitalnih puteva cyber ekstremizma" (Cyber Extremism Orbital Pathways Model) naglašavajući važnost

[108] Teorija potkožne igle koja je pokušala objasniti vezu direktnu uzročno posljedičnu vezu između medija i nasilja po principu gledam nasilje postajem nasilan, odavno je napuštena. Osim toga većina radikaliziralnih pojedinaca dolazi u dodir sa ekstremističkom ideologijom kroz offline socijalizaciju prije nego što bude dalje indoktrinirana online.

razumijevanja jedinstvenih atributa Interneta i ukazujući na široku raznolikost i dostupnost zajednica kontrakulture koje Internet pruža. Drugim riječima, umjesto da se uloga Interneta preusmjerava na ulogu facilitatora, potrebno je objasniti kako internetske komunikacije između različitih entiteta zapravo doprinose procesu radikalizacije.

Weimann i von Knop (2008) u nastojanju da shvate kako se pojedinac uključuje u internetske nasilne ekstremističke narative predlažu petofazni model: faza pretraživanja (pojedinci pokazuju interes i motivaciju za traženje radikalnih web stranica); faza zavođenja (pojedinac je izložen radikalnoj ideologiji nakon što je posjetio određene web stranice); faza privlačnosti (pojedincu postaje privlačna radikalna ideologija i počinje posjećivati još radikalnije web stranice); faza uvjeravanja/ubjeđivanja (pojedinac postaje aktivni član mrežne zajednice); i operativna faza (pojedinac se uključuje u operativne aktivnosti internetske zajednice i / ili nasilne ekstremističke grupe). Iako nedovoljno razvijen i pretežno deskriptivan ovaj model predstavlja korisnu polaznu tačku za konceptualizaciju i agregaciju faktora koji pojedincu mogu pružiti podršku i uključenje u nasilni ekstremizam na mreži budući da nudi koristan način da se organizuju koncepti, mehanizmi i procesi koji mogu biti uključeni u radikalizaciju posredovanu internetom i razumijevanje ponašanja aktera u virtuelnom okruženju.

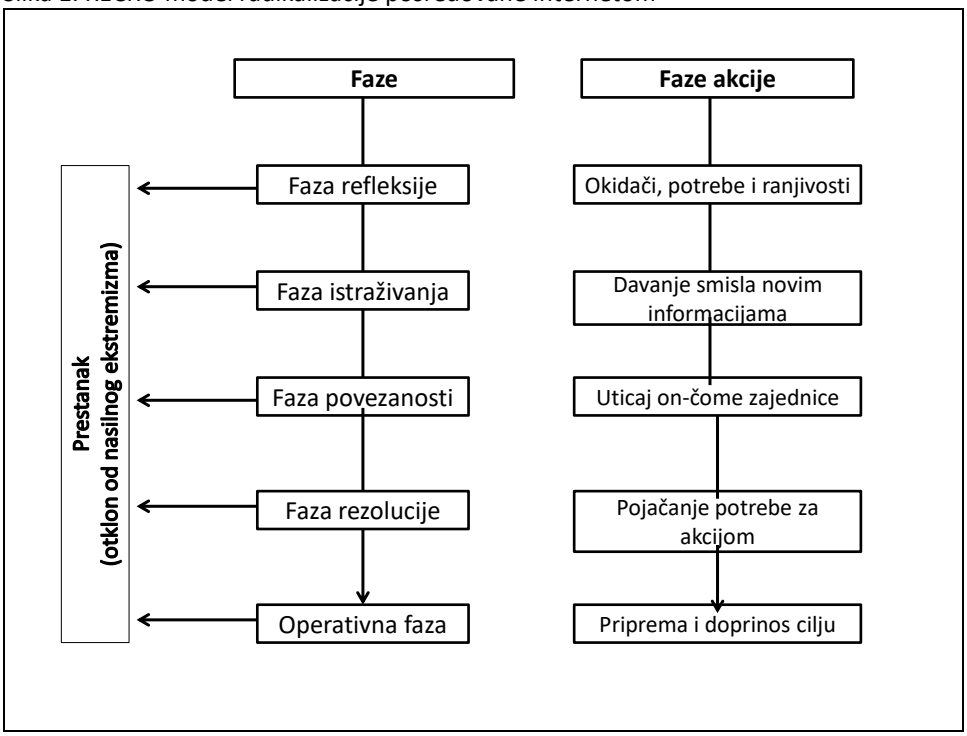
On-line radikalizacijom posebno se bavio Loo Seng Noon iz Centra za bihejvioralne nauke Ministarstva unutrašnjih poslova Singapura koji u istraživanju polazi od radne definicije on-line radikalizacije određujući je kao "proces u kome se pojedinacu šalju ideološke poruke i sistem vjerovanja koji podstiče otklon od većinskih (mainstream) vjerovanja ka ekstemnim pogledima, pre svega korišćenjem online medija kao što su Facebook, Twitter i YouTube.

On predlaže RECRO (Reflection, Exploration, Connection, Resolution, Operational) model internetom posredovane radikalizacije sa pet faza:

- Faza refleksije detaljno opisuje okidače, potrebe i ranjivosti koje pojedinac može imati, a koji povećavaju prijemčivost prema alternativnim sistemima vjerovanja
- Faza istraživanja detaljno opisuje period u kojem pojedinac počinje da ima razumijevanje za informacije koje su na internetu postavili nasilni ekstremisti
- Faza povezanosti detaljno objašnjava uticaj istomišljenika i internetske zajednice na novi svjetonazor pojedinca
- Faza rezolucije detaljno opisuje razdoblje u kojem pojedinac dobija zamah da prevede svoja radikalna uvjerenja u djelovanje; i
- Operativna faza detaljno opisuje razdoblje u kojem je pojedinac spreman počiniti nasilje kako bi ostvario radikalne ciljeve na mreži i/ili van nje (Neo, 2016).

Ovaj model se može i grafički predstaviti

Slika 1. RECRO model radikalizacije posredovane Internetom



Izvor: Neo, 2016:205

Kako navodi sam autor ovaj model

- predstavlja osnovu za razumijevanje i informiranje procjene o stepenu uključenosti pojedinca;
- osvjetljava kako Internet utiče na načine na koje se pojedinac može povezati i zbližiti sa istomišljenicima;
- Identifikuje lične, kognitivne i emocionalne transformacije koje se mogu dogoditi dok pojedinci internaliziraju nove vrijednosti i uvjerenja; i
- otvara put budućim empirijskim istraživanjima (Neo, 2016).

3. Radikalizam i ekstremizam u Republici Srbiji

Zapadni Balkan se više od decenije smatrao regijom koja se polako oporavlja od sukoba devedesetih i koja se nalazi na putu konsolidacije mira i stabilnosti. Međutim, lanac ozbiljnih sigurnosnih incidenata pokazao je da je ova regija i dalje ranjiva. Stalna ekonomska kriza, umor od proširenja EU i NATO-a, pogoršanje odnosa zapad-Rusija i neviđeni priliv izbjeglica jačaju krajnju desničarsku mobilizaciju u cijeloj regiji. (Austrijska nacionalna akademija odbrane, 2015)

Pojava ekstremno desničarskih ideologija u Srbiji rezultat je strukturalnih promjena nakon razgradnje socijalističke države. Pored ekonomske krize, krize identiteta i krize predstavničke demokratije, kao opštih faktora koji doprinose afirmaciji ultradesničkih stranaka i grupacija, što je još snažnije uticalo na Srbiju kao tranzicijsku državu, nego na razvijene zapadne demokratije, ekstremna desnica u Srbija je ojačana nekim, uslovno rečeno, lokalnim specifičnostima. Najvažnije su: raspad SFRJ i nasljeđe etničkih sukoba; istorijski revizionizam i anti-antifašizam; odnos države i Srpske pravoslavne crkve (SPC); te slabe institucije i nepostojanje vladavine zakona.[109]

Dublji strukturni uzroci ekstremizma u Srbiji mogu se pratiti najmanje dvije stotine godina unazad. Sociolog Đokica Jovanović smatra da postoje duboko ukorijenjena uvjerenja, ideje, navike, sklonosti i sjećanja koja je srpski narod stvorio o sebi i drugim narodima koji su sačuvani u kolektivnom nesvjesnom i koja predstavljaju gotovo nepremostive prepreke modernizaciji srpskog društva. To su na prvom mjestu: tradicionalizam (anti-modernizam), autoritarni mentalitet, predrasude i stereotipi, anti-intelektualizam, nedostatak političke kulture i jezički obrasci (ratnički jezik, obojen političkim značenjima) (Jovanović, 2017).

Od početka 1990-tih desničarski ekstremizam prisutan je u političkom životu Srbije. Dok su tokom ratova u bivšoj SFRJ ultradesničarske grupe djelovale prvenstveno kao paravojne formacije, današnje desničarske organizacije, u promijenjenim okolnostima, nastavljaju širenje nacionalne, rasne i vjerske mržnje i sudjeluju u brojnim nasilnim incidentima. Iako nije destruktivan kao devedesetih, nacionalizam u Srbiji i dalje je prisutan u svim sferama društvenog života - od spoljne politike, preko obrazovanja i kulture, do porodičnih odnosa. Takva društveno-politička klima pogoduje nastanku i jačanju ekstremno desničarskih organizacija. Savremeni desničarski ekstremizam u Srbiji dijeli osnovne karakteristike nove evropske ultradesnice, ali ima i svoje specifičnosti: normalizaciju nacionalizma, porast anti-antifašizma, ispitivanje sekularizma države i deficit vladavine zakona, koji predstavljaju, prije svega, posljedice društveno-političkih i ratnih događaja devedesetih godina prošlog vijeka u bivšoj SFRJ (Stakić, 2013).

U Srbiji postoji nekoliko ekstremnih desničarskih grupa i pokreta kao što su Srbski Obraz, Nacionalni stroj, SNP Naši, 1389, Zavetnici itd. Elementi ideologije ovih organizacija - ekstremni nacionalizam, veličanje ratnih zločinaca, opsednutost ugroženošću nacije, antimodernost, mržnja prema manjinama, kult nacionalnog jedinstva, militarizam, ideje bliske pravoslavnoj teokratiji itd. - jasno govore u prilog fašističkoj prirodi tih organizacija. Oni su prisutni ne samo u fizičkom, društvenom i političkom prostoru, već i u virtuelnom prostoru Srbije.[110]

[109]Više u Stakić, 2013.
[110]O tome više u Jelinčić i Ilić, 2013.

Pored verbalnog nasilja (govor mržnje), otvorenih prijetnji istraživačkim novinarima, nacionalistički i rasistički napadi na sportskim terenima, paljenje zastava i simbola stranih država, lijepljenje uličnih plakata sa spiskovima „antisrpskih“ medija i nevladinih organizacija, pretnje silom u TV emisijama predstavnicima "nepatriotskih" i "izdajničkih" nevladinih organizacija itd., članovi ovih ekstremnih grupa učestvovali su i u brojnim nasilnim akcijama i demonstracijama kao što je paljenje džamije u Beogradu tokom anti-albanskih demonstracija 2004. godine, demonstracija nakon proglašenja nezavisnosti Kosova kada je 2008. godine zapaljena ambasada SAD i upotrebe nasilja radi sprečavanja gej parada u Beogradu. Čak su i atentat na francuskog navijača Bricea Tatona prije utakmice sa Partizanom 2009. godine počinili fudbalski huligani, čiji je sistem vrijednosti blizak ekstremističkim političkim grupama. Dveri, parlamentarna politička stranka s konzervativnim i nacionalističkim svjetonazorom koja se snažno protivi javnoj promociji stavova seksualnih manjina i članstvu u EU-u, također je povezana sa korištenjem fizičkog nasilja nad novinarima, kao i u parlamentu Srbije.

U Srbiji postoje i ljevičarske ekstremne grupe, ali njihov utjecaj je marginalan, jer imaju mnogo manje aktivista i kapaciteta za obavljanje bilo kakvih značajnih akcija. Ekstremna ljevica je više omladinska subkultura nego organizovani društveni pokret (Ilić, 2013). Praktično su zabilježena samo dva incidenta manjih razmjera iza kojih stoje pripadnici ekstremne ljevice.[111]

Također, postoje ekstremističke organizacije nacionalnih manjina kao što su mađarski pokret Šezdeset i četiri županije/Hatvannégy Vármegye Ifjúsági Mozgalom i neke strukture usko povezane s mađarskom strankom Jobbik. Osim toga, postoje bošnjačke organizacije koje se zalažu za nezavisnost Sandžaka i grupe sljedbenika vehabijskog učenja. U Sandžaku je bilo nekoliko aktivnosti za koje su sljedbenici vehabizma bili odgovorni: na planini Ninaja pronađen je veliki broj komada oružja, dok su pripadnici ovog pokreta optuženi za pokušaj bombaškog napada na diplomatska konzularna predstavništva u Beogradu, posebno na ambasadu SAD-a.[112]

Kao što napominje Miša Đurković, ekstremističke grupe u Srbiji ne ostavljaju utisak originalnih i autentičnih pokreta, već odražavaju ideologije i pokrete koji postoje u drugim zemljama (Đurković, 2013).

---

[111]Bacanje Molotovljevog koktela na grčku ambasadu 2009. godine od strane Anarcho-Unionističke inicijative i pokušaj blokiranja rada Filozofskog fakulteta u Beogradu od strane Plenuma studenata 2011. (Đurković, 2013)

[112]Vehabisti se uglavnom fokusiraju na regrutovanje mladih, između 19 i 27 godina, lošeg finansijskog stanja, učestalih porodičnih problema i nižeg obrazovanja. Indoktrinacija vehabijskim idejama uglavnom se provodi u privatnim objektima (mesdžidima) koji su iznajmljeni ili u vlasništvu vehabijskih pristalica, kao i u određenim vjerskim zgradama (džamije) s vehabijskim propovjednicima. Najvažniji nalaz jednog istraživanja je da je značajan procenat mladih u Sandžaku potencijalno ili čak znanto otvoren za islamski ekstremizam. Čak petina ispitanika smatra da je opravdano braniti svoju religiju nasiljem (Ilić, 2016).

4. Ekstremizam i radikalizam su cyberspaceu Srbije

Za razliku od situacije u razvijenim zapadnim zemljama u srpskoj akademskoj zajednici je relativno malo istraživanja ekstermizma i radikalizma na Internetu. Još uvijek se traže odgovarajući metodološki pristupi ovakvoj vrsti istraživanja budući da su ona skopčana sa čitavnim nizom problema tehničke, prave, etičke i dr. prirode. Jedna od rijetkih monografija odnosno zbornika radova na ovu temu je studija/knjiga *Politički ekstremizam u cyber prostoru Srbije* nastala u saradnji i uz podršku Fondacije za otvoreno društvo i objavljena 2013. godine.

Kad je riječ o srpskoj krajnjoj desnici u cyber prostoru posebno su prepoznatljivi Obraz (https://www.obraz.rs/) i, inače zabranjeni, Nacionalni stroj dok je njihov vođa Goran Davidović Firer izuzetno aktivan na Twitteru. Stormfront kao glavne neprijatelje na svom forumu navodi Rome, Albance, crnce Hrvate, gejeve te pojedince iz političkog života Srbije. Rasizam, mržnja prema drugom i drugačijem, podrška Zlatnoj zori u Grčkoj, protivljenje antifašizmu neka su od obilježja ovih organizacija. Po nekim mišljenjima Srpski narodni pokret Naši (https://nasisrbija.org/) sa sjedištem u Aranđelovcu je najznačajnija i najorganizovanija desničarska organizacija u Srbiji (Bakić, 2013). I u cyberspaceu ovo je jedna od najaktivnijih i najuticajnijih organizacija, inače u ideološkoj i finansijskoj vezi sa Sveruskim narodnim frontom Ruske Federacije i Međunarodnim Evroazijskim pokretom. U vitruelnoj stvarnosti manje je prisutan Srpski narodni pokret 1389 (http://www.1389.org.rs/), dok su nešto aktivniji Srpski sabor Zavetnici (http://zavetnici.rs/)i Srbska akcija (https://akcija.org/) koja kombinuje neonacistički ideološki stav sa klerofašističkim sadržajima. Svi srpski desničari se zalažu za tradicionalne vrijednosti, a protiv su Evropske unije i parlamentarizma.

Vitruelne zajednice krajnjih desničara su svojevrsne "institucije socijalizacije" posredstvom kojih se usvajaju jezik, ideologija, teme, obrasci ponašanja i poželjni stavovi kao osnova desničarskog radikalizovanja pojedinaca u cilju njihovog pratičnog djelovanja u budućnosti.

Radikalna ljevica je gotovo neprimjetna na internetu u Srbiji. Na sajtu Saveza komunističke omladine Jugoslavije (SKOJ- http://www.skoj.org.rs/o-skoj/) navodi se da je omladinska revolucionarna marksističko-lenjinistička organizacija koja djeluje kao omladina Nove komunističke partije Jugoslavije (NKPJ) a okuplja radničku, seosku, studentsku i srednjoškolsku omladinu. Aktivnosti na ovom sajtu (postovi i odgovori na njih) su malobrojne. Slično je i sa Anarho sindikalističkom inicijativom (https://inicijativa.org/) koja osim web sajta ima i svoj Facebook profil na kome je kao političke neprijatelje označila gazde, političare, Petra II Krađorđevića. Dražu Mihajlovića, Zorana Đinđića, kapitalizam, ministarstvo obrazovanja, medija i državu. Na ovim sajtovima su rijetki pozivi na akciju. Twitter Studentskih borbi je okrenut "staleškim" problemima studenata (Bolonjski proces, univerzitetske vlasti, profesori) sa lijevih pozicija. Najveći doprinos širenju lijevih ideja preko svog Twittera daje organizacija

Marx21 a predmet kritike su kapitalizam, NATO, imperijalizam, bogataši, fašizam, nacionalističke organizacije, privredne i političke elite (https://marks21.info/).

Prema Đurkoviću pored navedenih političkih aktera u užem smislu u cyber prostoru i blogosferi Srbije prisutni su i posebno aktivne i

- navijačke grupe sa posebnom potkulturom i bliskim vezama sa mafijom, policijom i političarima,
- ekstremističke organizacije manjina,
- te pojedinci sa ekstremističkim stavovima poput Petra Lukovića i Nenada Prokića (Đurkovič, 2013).

5. (Ne)mougćnost deradikalizacije

U formalno pravnom smislu postojanje ekstremno desničarskih organizacija u Srbiji nije izričito zabranjeno, ali mnoge aktivnosti koje su karakteristične za rad ovih organizacija zabranjene su Ustavom i zakonom. Srbija posjeduje pravnu i normativnu osnovu za suprotstavljanje ekstremističkim nasilnim radnjama. Ustav zabranjuje svako podsticanje na rasnu, nacionalnu, vjersku ili drugu nejednakost, mržnju i netrpeljivost, dok je diskriminacija zabranjena međunarodnim konvencijama koje je potpisala Srbija (Međunarodni sporazum o građanskim i političkim pravima, Evropska konvencija o ljudskim pravima itd.) i domaćim zakonskim propisima akata, (Zakon o javnom informisanju, kao i Zakon o zabrani diskriminacije[113]). Osim toga, u Krivičnom zakoniku postoji čitav niz krivičnih dijela koja mogu biti rezultat desničarskog ekstremizma ili su povezani sa desničarskim ekstremizmom.

Međutim, problem leži u sudskoj i političkoj praksi koju karakterišu dugi sudski postupci, odlaganje sudskih rasprava zbog nedostupnosti optuženih, neprimjerivanje odredbi o zabrani ovih organizacija u slučajevima kršenja zakona od strane Ustavnog[114] i redovnih sudova, nejednaka i nedosljedna kaznena politika, vrlo blaga politika kažnjavanja [115] (kvalificirajući određena djela kao ona za koja je predviđena blaža kazna i izricanje novčane

[113]Ovaj zakon usvojen 2009. godine prvi je sveobuhvatni zakon protiv diskriminacije u Srbiji. Nacrt ovog zakona povučen je iz skupštinske procedure na zahtjev Srpske pravoslavne crkve i drugih tradicionalnih vjerskih zajednica koje su bile protiv nekih njegovih članova koji regulišu slobodu vjeroispovijesti i zabranjuju diskriminaciju na osnovu seksualne orijentacije (u izvornom tekstu također diskriminacija je predviđena osnova rodnog identiteta - što je u konačnoj verziji izostavljeno).

[114]Ustavni sud je u junu 2012. godine donio odluku o zabrani klerikalističke organizacije Obraz i na taj način napravio korak u pozitivnom smjeru. Država je, barem deklarativno, pokazala da fašističke organizacije nisu legitimni politički subjekti i da njihovo postojanje i djelovanje ne mogu biti opravdani građanskim slobodama. Međutim, već krajem 2012. Ustavni sud je odbio zahtjev tužilaštva za zabranu rada organizacija SNP 1389 i SNP Naši i tako učinio nekoliko koraka unazad. Takva odluka Ustavnog suda predstavlja podsticaj svim ekstremno desničarskim organizacijama i potvrdu njihove političke legitimnosti (Stakić, 2013).

[115]Kada se analizira praksa srpskog pravosudnog sistema u poslednjih dvadeset godina, primjetan je izostanak krivičnog gonjenja za većinu zločina sa ekstremističkim elementima (Subotić, 2013).

kazne ispod zakonskog minimuma). Apelacioni sud često vraća predmete na ponovno suđenje, što između ostalog ukazuje na to da niži sudovi ne posvećuju dovoljno pažnje tim slučajevima i što obično rezultira značajnim smanjenjem kazni. Različite presude u vrlo sličnim slučajevima su u korelaciji sa promjenom političke vlasti i dokaz u prilog tezi da pravosuđe u Srbiji nije nezavisno od izvršne vlasti.

Odnos Srbije prema desničarskom ekstremizmu bio je pragmatičan i tolerantan od početka devedesetih do danas; dok je Milošević koristio ekstremno desne grupe kao jedno od sredstava svoje ratne politike, vladajući režimi od 2000. godine do danas nazivali su ih legitimnim faktorima političkog života, što je nesumnjivo doprinijelo jačanju desničarskog ekstremizma u Srbiji. (Petakov, 2009). Posljednjih nekoliko godina neofašisti, ekstremni desničari i drugi ekstremisti ušli su u državne institucije bez ikakvih problema, iako, za sada, samo kao gosti.[116]U Uslovima kada neki političari odbijaju da se ograde od ekstremnih ideologija i sistema vrijednosti i izbjegavaju da otvoreno osude poruke i postupke ekstremističkih organizacija, relativiziraju i izjednačavaju ultradesničarske organizacije i neke NVO, otvoreno koketiraju sa navijačima i drugim ekstremnim grupama, te kada nedostaje stigmatizacija dolazi praktično do nekakve vrste (nenamjerne?) legitimizacije ovih organizacija. Izjave predstavnika države u kojima su desničari okarakterizirani kao marginalne "budale" neminovno dovode do relativizacije i banalizacije problema. Povezanost desničarskih stranaka s tim organizacijama očita je u njihovoj podršci i ideološkoj bliskosti (odnos prema Kosovu, podrška secesiji Republike Srpske i bliskost sa SPC. (Biserko, 2014: 8)

Zaključak

Internet predstavlja novu moćnu političku alternativnu arenu za organizovanje ekstremističkih pokreta sa političke margine. Politički ekstremisti ga koriste za širenje svoje ideologije regrutaciju novih članova i propagiranje svojih aktivnosti, ali i za mobilizaciju članstva i prikupljanje sredstava za ekstremističke organizacije. Naročito u uslovima kontrole štampanih i elektronskih medija internet pruža mogućnosti za promovisanje lijevih i desnih sadržaja koji su neprihvatljivi nosiocima vlasti i kontrolorima javnog mnjenja.

Odnos ekstremizma i novih informaciono komunikacionih tehnologija još je uvijek predmet istraživanja, a brzi i intenzivan razvoj ove oblasti utiče i na brzo zastarijevanje znanja i aktuelnosti ostvarenih uvida.

Zastupnici radikalnih političkih ideja i ekstremnih shvatanja, posebno desničari, aktivni su i u cyber prostoru Srbije. Iako je prema podacima Zavoda za statistiku još uvjek ni polovica stanovnistva Srbije nije prisutna na internetu nikako ne treba zanemariti

[116]Matica srpska u jesen 2017. na zahtjev Ministarstva informisanja morala je objasniti predavanje njemačkog ekstremno-desničarskog intelektualca Geca Kubiceka (Pegida). Krajnje desni zapadni političari Jim Dowson i Nick Griffin bili su gosti u Uredu za Kosovo i Metohiju.

opasnost prisustva i potencijalnog uticaja ekstremnih političkih ideja, naročito na mlade ljude. Ovo utoliko prije što čitav niz društvenih i političkih faktora u današnjoj Srbiji upravo pogoduje radikalizaciji tako da ove ideje mogu naići na plodno tlo i pogodovati i pojavi nasilnog ekstremizma pa i terorizma.

Upravo stoga potrebna je stalna budnost organa i službi sigurnosti, ali i posvećivanje veće pažnje ovoj temi u akademskim istraživanjima.

Literatura

1. Austrian National Defence Academy (2015) Violent Extremism in the Western Balkans, 31st RSSEE SG WORKSHOP - Belgrade, Serbia 27 – 29 September 2015
2. Bermingham, A., Conway, M., McInerney, L., O'Hare, N., & Smeaton, A. F. (2009). Combining social network analysis and sentiment analysis to explore the potential for online radicalisation. Paper presentedat Advances in Social Networks Analysis and Mining, Athens, Greece. doi:10.1109/ASONAM.2009.31
3. Biserko S. (2014). "Ekstremizam: nastavak državnog projekta" u Ekstremizam: kako prepoznati društveno zlo, Beograd:Helsinški odbor za ljudska prava u Srbiji
4. Centar za slobodne izbore i demokratiju (CeSID), (2016), Pokretači radikalizma i nasilnog ekstremizma među mladima u Srbiji – rezultati istraživanja, Beograd:CeSID
5. Conway, M. (2012). Introduction: terrorism and contemporary mediascapes – reanimating research on media and terrorism. Critical Studies on Terrorism, 5 (3), 445-453.
6. Conway, M., & McInerney, L. (2008). Jihadi video & auto-radicalisation: Evidence from an exploratory YouTube study. Intelligence and Security Informatics, 5376, 108–118.
7. Đurković, M. (2013) "Metodološki i teorijski okvir za razumevanje izvora i razvoja ekstremizma u Srbiji" u Jelinčić, J. i Ilić, S. (Ur.) Politički ekstremizam u sajber prostoru Srbije, Zrenjanin:Centar za razvoj civilnog društva
8. Edwards, C., & Gribbon, L. (2013). Pathways to violent extremism in the digital era. The RUSI Journal, 158 (5), 40–47. doi:10.1080/03071847.2013.847714
9. General Intelligence and Security Service (AIVD). (2012). Jihadism on the web: A breeding ground for jihad in the modern age. The Hague: Algemene Inlichtingen en Veiligheidsdienst
10. Gupta, D. K. (2011). Waves of international terrorism: An exploration of the process by which ideas flood the world. In J. E. Rosenfeld (Ed.), Terrorism, identity and legitimacy: The four waves theory and political violence (pp. 30–43). New York, NY: Routledge.
11. Ilić, V. (2013) "Viđenje poželjnog načina organizacije političkog života" uJelinčić, J. i Ilić, S. (Ur.) Politički ekstremizam u sajber prostoru Srbije, Zrenjanin:Centar za razvoj civilnog društva
12. Ilić, V. (2016) Stavovi mladih u Sandžaku – koliko su mladi otvoreni prema islamskom ekstremizmu. Beograd:Helsinški odbor za ljudska prava u Srbiji
13. Jelinčić, J. i Ilić, S. (Ur.) (2013) Politički ekstremizam u sajber prostoru Srbije, Zrenjanin:Centar za razvoj civilnog društva
14. Jovanović, Đ. (2017) Prilagođavanje: Srbija i moderna, Beograd:Dan Graf
15. Khader, M., Neo, S.L., Ong, G., Mingyi, E.T. and Chin, J. (2016). Combating Violent Extremism and Radicalization in the Digital Era, Hershey PA:Information Science Reference (an imprint of IGI Global)
16. Kruglanski, A. W., Crenshaw, M., Post, J. M., & Victoroff, J. (2008). What should this fight be called? Metaphors of counterterrorism and their implications.

Psychological Science in the Public Interest, 8 (3), 97–133. doi:10.1111/j.1539-6053.2008.00035.x PMID:26161891
17. Lennings, C. J., Amon, K. L., Brummert, H., & Lennings, N. J. (2010). Grooming for terror: The internet and young people. Psychiatry, Psychology and Law, 17 (3), 424–437. doi:10.1080/13218710903566979
18. Lemieux, A. F., Brachman, J. M., Levitt, J., & Wood, J. (2014). Inspire Magazine: A Critical Analysis of its Significance and Potential Impact Through the Lens of the Information, Motivation, and Behavioral Skills Model. Terrorism and Political Violence, 26 (2), 354–371. doi:10.1080/09546553.2013.828604
19. Moghaddam, F. M. (2005). The staircase to terrorism: A psychological exploration. The American Psychologist, 60 (2), 161–169. doi:10.1037/0003-066X.60.2.161 PMID:15740448
20. Neo, S., L. (2016). "An Internet-Mediated Pathway for Online Radicalisation:RECRO", in Khader,M. et al (Eds) Combating Violent Extremism and Radicalization in the Digital Era, Hershey PA:Information Science Reference (an imprint of IGI Global)
21. Neo, L. S., Khader, M., Shi, P., Dillon, L., & Ong, G. (2015). Extremist cyber footprints: A guide to understanding and countering online extremism. Singapore: Home Team Behavioural Sciences Centre
22. Petakov, Z. (2009) „Neonacističke, fašističke i ekstremno desničarske organizacije u Srbiji danas"u Klarić, Ž. & Atanacković, P. (ed.) Mapiranje desnog ekstremizma, Novi Sad: Cenzura, str. 42-54.
23. Powers, S., & Armstrong, M. (2014). Conceptualising radicalisation in a market for loyalties. In C. K. Winkler & C. E. Dauber (Eds.), Visual propaganda and extremism in the online environment (pp. 165–192). Carlisle, PA: Strategic Studies Institute and U.S. Army War College Press
24. Rieger, D., Frischich, L., & Bente, G. (2013). Propaganda 2.0 Psychological effects of right-wing and Islamic extremist internet videos. German Federal Criminal Police Office
25. Rogan, H. (2007). Al-Qaeda's online media strategies: From Abu Reuter to Irhabi 007. Norway: Norwegian Defence Research Establishment (FFI).
26. Saifudeen, O. A. (2014). The cyber extremism orbital pathways model. Singapore: S. Rajaratnam School of International Studies
27. Sageman, M. (2010). Confronting Al-Qaeda: Understanding the threat in Afghanistan. Perspectives onTerrorism, 3 (4), 4–25
28. Shahar, Y. (2007). The internet as a tool for intelligence and counter-terrorism. In B. Ganor, K. vonKnop, & C. Duarte (Eds.), Hypermedia seduction for terrorist recruiting (pp. 140–153). Washington,DC: IOS Press
29. Seib, P., & Janbek, D. M. (2011). Global terrorism and new media: The post-Al Qaeda generation. New York, NY: Routledge
30. Silber, M. D., & Bhatt, A. (2007). Radicalization in the West: The Home Grown Threat. New York, NY:New York Police Department
31. Stakić, I. (2013). "Odnos Srbije prema ekstremno desničarskim organizacijama", Beograd: Beogradski centar za bezbednosnu politiku

32. Subotić, M. (2013) "Ekstremističke tendencije kao prepreka u (pre)oblikovanju političkog identiteta Srbije", Kultura polisa, vol. 10, br. 21, str. 163-181.
33. Torok, R. (2013). Developing an explanatory model for the process of online radicalisation and terrorism. Security Informatics, 2 (1), 1–10. doi:10.1186/2190-8532-2-6
34. UNDP (2016) Preventing Violent Extremism through Promoting Inclusive Development, Tolerance and Respect for Diversity, Global meeting, 14-16 March, 201 Oslo, Norway
35. Weimann, G. (2012). Lone wolves in cyberspace. Journal of Terrorism Research, 3 (2), 75–90. doi:10.15664/jtr.405
36. Weimann, G., & von Knop, K. (2008). Applying the notion of noise to countering online terrorism.Studies in Conflict and Terrorism, 31 (10), 883–902. doi:10.1080/10576100802342601

Kriminalističke teme
Zbornik radova
Godina XIX, Broj 5, 2019.
ISSN 1512-5505

MEĐUNARODNO PRAVO I CYBER SIGURNOST
INTERNATIONAL LAW AND CYBER SECURITY

Pregledni naučni rad

Prof. dr. Sakib Softić[117]

Sažetak

Inspiracija za rad i problem (i) koji se radom oslovljava (ju): Cyber napadi predstavljaju novu sigurnosnu prijetnju koja se pojavila u dvadeset prvom vijeku. Ova sigurnosna prijetnja stavlja nove izazove pred pojedine države i međunarodnu zajednicu u cjelini. Sigurnosna prijetnja može dolaziti od drugih država ili od nedržavnih aktera.
Ciljevi rada (naučni i/ili društveni): Autor se u ovom tekstu bavi pitanjima koja se tiču primjene pravila međunarodnog prava odnosno prava oružanih sukoba na suzbijanje ove prijetnje.
Metodologija/Dizajn: Prvo se nastoji objasniti i definisati pojam međunarodnog prava cyber sigurnosti, zatim se analizira pitanje odnosa države prema cyber napadima i pravo države da upotrijebi silu radi suzbijanja cyber napada i na kraju se analizira pitanje da li se *cyber* napad može smatrati kao napad koji povlači pravo na individualnu i kolektivnu samoodbranu u smislu Povelje UN. I pod kojim uslovima.
Ograničenja istraživanja/rada: Rad je pregledni i pravno-teorijske prirode.
Rezultati/Nalazi: Pravo država na samoodbranu nije samo pasivno pravo države da čeka da se napad zaista i desi i da šteta bude pričinjena. Država ima pravo na aktivnu samoodbranu koja se između ostalog manifestuje i kao pravo na anticipativnu samoodbranu. Država, također, ima pravo na proporcionalne kontramjere.
Generalni zaključak: Pravo država na samoodbranu postoji i u slučaju napada počinjenog od nedržavnih aktera.
Opravdanost istraživanja/rada: Ovaj članak daje odgovor na složena međunarodnopravna pitanja vezana za ovu sigurnosnu prijetnju što svakako doprinosi boljem razumijevanju ovog pitanja i predstavlja doprinos razvoju nauke međunarodnog prava u ovoj materiji.

Ključne riječi

sigurnosna prijetnja, pravo oružanih sukoba, cyber sigurnost, upotreba sile, pravo države na samoodbranu

Abstract

Reason for writing and research problem (s): Cyber attacks constitute a new security threat in the twenty-first century. This security threat put new known and unknown challenges to the international community in the whole. The security threat may come from other states or from non-state actors.

[117] FKKSS, Univerzitet u Sarajevu

Aims of the paper (scientific and/or social): In this article the author deals with issues related to the application of the rules of international law and the right of armed conflict to counteract this kind of threats.
Methodology/Design: At first the author endeavor to explain and define the concept of international cyber security law, then analyzes the question of the state's relationship to cyber-attacks and the right of the state to use force to counter cyber-attacks, and finally analyzes whether cyber-attack can be considered as an act that entitles rights to individual and collective self-defense within the meaning of the UN Charter. And under what conditions.
Research/Paper limitation: This is a review paper and legal theory.
Results/Findings: The right to self-defense is not just a passive right of the state to wait for to be attacted. And that the damage be done. The state has the right to active self-defense, which also manifests itself as the right to anticipatory self-defense. The state is also entitled to proportional countermeasures.
General Conclusion: The right to self-defense also exists in the case of attacks committed by non-state actors.
Research/Paper Validity: This article givs answers to complex international legal issues related to this security threat, which certainly contributes to a better understanding of this issue and represents a contribution to the development of international law science in this matter.

Keywords
security threat, the right of the armed conflict, cyber security, use of force, the right of the state to self-defense.

1. Uvod

Cyber napadi predstavljaju novu sigurnosnu prijetnju sa kojom se države suočavaju početkom dvadeset prvog vijeka. *Cyber* napadi mogu po svojoj težini biti ekvivalentni konvencionalnim napadima sa kojima su države bile suočene u svojoj ranijoj historiji. Mogu proizvesti iste ili čak štetnije posljedice za državu i njene stanovnike nego konvencionalni napadi. Stoga se postavlja pitanje primjenjivosti međunarodnog prava odnosno prava oružanih sukoba i međunarodnog humanitarnog prava na situacije uzrokovane *Cybe*r napadima.

Pošto se radi o novoj pojavi nužno je utvrditi nova ili potvrditi primjenu postojećih pravila međunarodnog prava na *cyber* napade. O ovim pitanjima još uvijek ne postoji puna saglasnost među državama kao ni među pravnim piscima. Kao što je poznato međunarodno pravo je proizvod međudržavnih odnosa i kreira se putem međunarodnih ugovora i međunarodnih običaja. Problem je u tome što ne postoje međunarodni ugovori koji se direktno bave *cyber* napadima.[118] Također ni međunarodno običajno pravo u ovoj materiji

[118] Konvencija Vijeća Evrope iz 2001. godine donesena je radi sprečavanja djela koja narušavaju povjerljivost, integritet i dostupnost kompjuterskih sistema, mreža i podataka, kao i sprečavanje zloupotrebe tih sistema, mreža i podataka, osiguravajući usvajanje ovlasti dovoljnih da bi se omogućila efikasna borba protiv tih

nije dovoljno razvijeno. Jer se radi o novoj pojavi. Pitanje postojanja međunarodnopravnih normi primjenjivih na *cyber* napade postavilo se naročito nakon hakerskih napada u prvoj deceniji ovog vijeka. Što je ovu vrstu napada stavilo u fokus pažnje savremenih država i međunarodne zajednice u cjelini. Neke države kao naprimjer Kanada, Velika Britanija i SAD-e su usvojile određene dokumente kao reakciju na ovu vrstu prijetnji. [119] Također je ovo pitanje dospjelo na dnevni red Ujedinjenih nacija koje su potvrdile da je međunarodno pravo i to naročito onaj dio koji je sadržan u Povelji UN primjenjiv i na Cyber napade.[120] Neke međunarodne organizacije su nastojale utvrditi pravila međunarodnog prava primjenjiva na oružane sukobe.[121] Većina pravnih pisaca je shvatanja da se međunarodno pravo primjenjuje i na Cyber prostor.[122] Mada su neki mišljenja da je primjena međunarodnog prava na Cyber sigurnost u krizi.[123]

Da bi se uopšte postavilo pitanje primjenjivosti međunarodnog pravo na *Cyber* napade potrebno je da oni imaju određenu težinu. Prema mišljenju Međunarodnog suda pravde pravo oružanih sukoba se primjenjuje na ,,bilo koju upotrebu sile, bez obzira na upotrijebljeno oružje''.[124] Ali 'upotrijebljena sila'' mora proizvesti posljedice relevantne za međunarodno pravo.

Međunarodno pravo sadrži dvije grupe odredaba primjenjivih na ove situacije. Prva se odnosi na *jus ad bellum* odnosno na pravo pribjegavanja upotrebi sile. Druga grupa *jus in bell*o se primjenjuje kad je rat već otpočeo i tiče se primjene pravila međunarodnog

krivičnih djela, olakšavajući njihovo otkrivanje, istragu i gonjenje, kako na unutrašnjem tako i na međunarodnom nivou, i predviđajući materijalne odredbe u cilju brže i povjerljivije međunarodne saradnje. Vidi uvod: Convention on Cybercrime 185 CETS (opened for signature 23 November 2001, entered into force 1 July 2004).

[119] Ministarstvo odbrane SAD je 2011. godine izdalo Strategiju za djelovanje u cyber prostoru označavajući cyber napade kao sigurnosnu prijetnju. Strategija je nekoliko puta dopunjena.

[120] Vidi: U.N. Secretary-General, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, ¶ 19, U.N. GAOR, 68th Sess., U.N. Doc. A/68/150 (June 24, 2013).

[121] NATO suradnički centar za izvrsnost u Cyber odbrani sa sjedištem u Talinu, izdao je 2013. godine ''Talin manuel o međunarodnom pravu koje se primjenjuje na cyber ratovanje. Priručnik (*manuel*) je dopunjen 2017. godine i predstavlja najpotpuniju kompilaciju međunarodnog prava primjenjivog na ovu oblast. Sačinjen je od strane istaknutih neovisnih međunarodnih pravnika iz dvadeset pet zemalja. U daljem tekstu: *Talin manuel*. Vidi: https://ccdcoe.org/research/tallinn-manual/.

122 Vidi npr. Gary D. Brown: International law Apllies to Cyber Warfare! Now What. 355 BROWN (DO NOT DELETE) 4/11/2017 7:52 PM. https://www.swlaw.edu/sites/default/files/2017-08/355%20International%20Law%20Applies%20to%20Cyber%20Warfare-Brown.pdf 20.09.2019.; MIRANDA GRANGE: CYBER WARFARE AND THE LAW OF ARMED CONFLICT LAWS 533: LAW OF ARMED CONFLICT, RESEARCH PAPER. Faculty of Law Wictoria 2014. https://core.ac.uk/download/pdf/41339676.pdf . 20.09.2019.

123 Vidi: Kubo Mačák: Is the International Law of Cyber Security in Crisis? 2016 8th International Conference on Cyber Conflict. 127-139.

124 INTERNATIONAL COURT OF JUSTICE REPORTS OF JUDGMENTS, ADVISORY OPINIONS AND ORDERS LEGALITY OF THE THREAT OR USE OF NUCLEAR WEAPONS ADVISORY OPINION OF 8 JULY 1996. U daljem tekstu: Nuclear Weapons Advisory Opinions, para. 39.

ratnog prava, prava oružanih sukoba i međunarodnog humanitarnog prava na konkretnu situaciju.[125]

Naročiti problem za primjenu pravila međunarodnog prava na *cyber* napade uzrokovani su karakterom ''internetske mreže'' koja otežava otkrivanje i identifikovanje napadača. Nesporno je da države nastoje prikriti činjenicu da su one izvršilac *cyber* napad. To im olakšava mogućnost angažovanja anonimnih pojedinaca i grupa koje će izvršiti *cyber* napad. Nakon čega se brišu svi tragovi koji bi mogli dovesti u vezu državu napadača sa izvršenim napadom.

Pošto je pitanje primjenjivosti odredaba međunarodnog prava na *cyber* napade nova tema to je o njoj bilo vrlo malo riječi. Stoga je namjera autora da doprinese razvoju ovog dijela međunarodnog prava i da istraži i analizira primjenjivost nekih od postojećih instituta međunarodnog prava na *cyber* napade.

2. Pojam Međunarodnog prava cyber sigurnosti

Međunarodno pravo *cyber* sigurnosti je novi pojam u međunarodnom pravu. Služi nam da identifikujemo one dijelove međunarodnog prava koji se bave neprijateljskom upotrebom *Cyber* prostora. I ako je međunarodno pravo *cybe*r sigurnosti novi pojam u međunarodnom pravu on ne znači stvaranje neke nove grane međunarodnog prava.[126] Ne stvaraju se novi instituti međunarodnog prava. Ovdje se više radi o specifičnostima primjene postojećih instituta na novu situaciju.

Međunarodno pravo uspostavlja odgovornost država za međunarodne protivpravne akte počinjene od njenih državnih organa kao i nekih nedržavnih aktera čiji su akti pod određenim okolnostima pripisivi državi.[127] Po međunarodnom pravu države mogu biti odgovorne za *cyber* operacije svojih državnih organa i nedržavnih aktera koji joj se mogu pripisati.

Ovdje se radi o neprijateljskim *cyber* napadima takve težine da aktiviraju primjenu pravila međunarodnog prava koja zabranjuju upotrebu sile protiv drugih nezavisnih država. Ili spadaju u napade takvog intenziteta da povlače primjenu glave VII Povelje UN koja

125 Vidi: Michael N Smitt, ''Attack'' as a Term of Art in International law: The Cyber Operations Context. 2012 4thInternational Conferenc on Cyber Conflict. (283-293).

[126] Ovaj pojam je više deskriptivan i obuhvata pojmove suverenosti, jurisdikcije i odgovornosti država ukoliko se ovi bave međunarodnim pravom rata i međunarodnim pravom u ratu. Vidi: Talin manuel o međunarodnom pravu koje se primjenjuje na *cyber* ratovanje. General editor Michael N Schmitt. Cambridge University Press 2017. str. 24

[127]United Nations A/RES/56/83 from 28 January 2002. Responsibility of States for internationally wrongful acts. http://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf. Pristupio *16*.09.2019.

predviđa pravo država na individualnu ili kolektivnu samoodbranu kao i upotrebu sile od strane Savjeta sigurnosti UN u cilju suzbijanja (*cyber*) napada.

Povelja UN zabranjuje nezakonitu upotrebu sile u odnosima između država koristeći pri tome dva pojma značajna za našu temu.

Prvi je ''upotreba sile'' protiv druge države.

Opća zabrane rata temelji se na odredbi člana 2. stav 4. Povelje UN: "Svi članovi će se u svojim međunarodnim odnosima uzdržavati od prijetnje silom ili od upotrebe sile protiv teritorijalnog integriteta ili političke nezavisnosti ma koje države, ili koja bi na ma koji drugi način bila u suprotnosti sa ciljevima Ujedinjenih nacija."

Ova zabrana upotrebe sile prihvaćena je kao međunarodno običajno pravo i čak kao *ius cogens* norma kako je to potvrđeno u presudi Međunarodnog suda u Hagu u predmetu *Nikaragva* protiv SAD.[128]

Drugi upotrijebljeni izraz je ''agresija''. Član 39. Povelje daje ovlaštenje Savjetu sigurnosti da procjenjuje da li se radi o prijetnji miru, povredi mira ili aktu agresije. Ujedinjene nacije su svojom rezolucijom 3314 (XXIX) iz 1974. godine definsale agresiju kao:

''...upotreba oružane sile od strane neke države protiv suvereniteta, teritorijalne cjelovitosti ili političke nezavisnosti neke druge države ili upotrebu oružane sile koja je na bilo koji drugi način nespojiva s Poveljom Ujedinjenih nacija...''.

Povelja UN ne definiše napad. Ali to čini drugi opšteprihvaćeni međunarodnopravni dokument. Dopunski protokol I iz 1977. godine na Ženevske konvencije iz 1949. godine. Članom 49 Protokola I napad se definiše kao ''akti nasilja protiv protivnika, bilo da su ofanzivni ili defanzivni''.

Protokol I se primjenjuju na sve napade, bez obzira na kojoj se teritoriji preduzimaju, uključujući nacionalnu teritoriju koja pripada strani u sukobu, ali koja je pod kontrolom protivničke strane. Također, Protokol I se primjenjuje na kopneno, zračno ili pomorsko ratovanje koje može pogoditi civilno stanovništvo, pojedine civile ili civilne objekte na kopnu.[129]

Da bi cyber napadi predstavljali napade u smislu člana 49. Dopunskog protokola I moraju uzrokovati fizičku destrukciju ili štetne povrede kao i druge vrste oružja: konvencionalno,

---

[128] Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Merits, Judgement, ICT Reports 1986, p 14, para 190.
[129] Vidi: Michael N Smitt, ''Attack'' as a Term of Art in International law: The Cyber Operations Context. 2012 4thInternational Conferenc on Cyber Conflict. (283-293).

nuklearno, hemijsko i biološko.[130] Zapaženo je nekoliko pristupa u analizi da li neki cyber napad predstavlja napad u smislu međunarodnog prava.

Prvi je pristup zasnovan na učinku. Da bi se radilo o napadu zahtijeva se da *cyber* napad uzrokuje iste posljedice kao i druge vrste napada. Drugi je pristup zasnovan na cilju. Ukoliko je napad usmjeren protiv bilo čega što se zove kritična infrastruktura onda napad zadovoljava kriterije koje postavlja međunarodno pravo. Pristup koji uključuje upotrijebljena sredsta za napad je odbačen kao neprimjenjiv na ovu vrstu napada.[131]

Međunarodno pravo oružanih sukoba primjenjuje se i na *cyber* operacije kao i na druge operacije preduzete tokom oružanog sukoba. Tako prema *Talin manuelu* ,,*Cyber* operacije izvršene u kontekstu oružanog sukoba podliježu pravu oružanih sukoba''.[132] Pravo oružanih sukoba primjenjuje se na *cyber* operacije bez obzira da li se radi o međunarodnom ili unutrašnjem oružanom sukobu.[133]

S druge strane pravo oružanih sukoba se ne primjenjuje na aktivnosti privatnih korporacija koje nisu povezane sa oružanim sukobima.[134] Za *cyber* oružane sukobe ključna su pitanja: mjesto sa kojeg su *cyber* operacije pokrenute, lokacija gdje su smješteni uređaji za *cyber* operacije i mjesto na koje su usmjerene *cyber* operacije. Također, sa ovim pitanjima povezana su i pravila o neutralnosti koja nenamjerno mogu biti povrijeđena ovom vrstom operacija.

''Međunarodni oružani sukob postoji kadgod postoje neprijateljstva koja mogu uključiti ili biti ograničena na *cyber* operacije, koji se odvijaju između dvije ili više država.''[135] Dok ''Nemeđunarodni oružani sukob postoji kadgod postoji produženo oružano nasilje, koje može uključiti ili biti ograničeno na *cyber* operacije, koji se odvijaju između vladinih oružanih snaga i snaga jedne ili više oružanih grupa, ili između takvih grupa. Sukobljavanja moraju dostići minimalni stepen intenziteta i strane uključene u sukob moraju pokazati minimalni stepen organizacije''.[136]

Pravo cyber oružanih sukoba se ne odnosi samo na pitanja njegove primjene *jus ad bellum* nego i na *jus in bello*. *Talin manuel* reguliše pitanje krivične odgovornosti komandanata i nadređenih za ratne zločine nastale kao posljedica naredbe da se izvrše *cyber*

---

[130] Vidi: Mateusz Piatkowski, The Definition of the Armed Conflict in the Condition of Cyber Warfera, Polish politikal Science Yearbook vol. 46 (2017) pp. 271 – 280.
[131] Vidi: Mateusz Piatkowski, The Definition of the Armed Conflict in the Condition of Cyber Warfera, Polish politikal Science Yearbook vol. 46 (2017) pp 275.
[132] Član 20 *Talin manuela*.
[133] Vidi članove 22 i 23 *Talin manuela*.
[134] Vidi *Talin manuel* o međunarodnom pravu koje se primjenjuje na *cyber* ratovanje. General editor Michael N Schmitt. Cambridge University Press 2017. str. 69.
[135] Član 22 *Talin manuel*-a.
[136] Član 23 *Talin manuel-a*.

operacije koje predstavljaju ratni zločin. Također, komandant i nadređeni su odgovorni za nepreduzimanje mjera da se takvi zločini spriječe odnosno da se počinioci kazne.[137]

3. Država i cyber napadi

Osnovno je pravilo da država može na temelju svoje suverenosti vršiti kontrolu nad *cyber* infrastrukturom i aktivnostima unutar svoje teritorije.[138]

Ovo pravo proizlazi iz koncepta suverenosti kako je utvrđen međunarodnim pravom. Suverenost podrazumijeva vršenje efektivne vlasti nad teritorijom i stanovništvom. ''*Država ne mora imati bilo kakav poseban oblik vlasti, ali tu mora postojati neka vlast koja vrši funkcije vlade i biti sposobna da predstavlja entitet u međunarodnim odnosima*.''[139]

U predmetu: Ostrva Aland (*Aaland Islands*) imenovan je *Međunarodnog odbora pravnika sa zadatkom da* istraži status ostrva povodom pitanja vremena uspostave Finske republike. Pitanje je postavljeno radi utvrđivanju odgovornosti za nerede koji su nastupili tokom ruske revolucije i državnog osamostaljenja Finske. Odbor je sačinio Izvještaj u kome je iznio *stav o pravnim aspektima pitanja Alandskih ostrva.* U Izvještaju se o sticanju suverenosti navodi:

''*To se sigurno nije desilo dok nije stvorena stabilna politička organizacija, i dok javna vlast nije postala dovoljno jaka da se učvrsti na državnom teritoriju bez pomoći stranih trupa*.''[140]

Maks Huber je u predmetu *Palmas Island* istakao:

''*Suverenost između država znači nezavisnost. Nezavisnost u odnosu na dio zemljine površine je pravo da se na tom dijelu, uz isključenje svake druge države, vrše državne funkcije. Razvoj države kao nacionalne organizacije tokom nekoliko posljednjih vjekova, i kao prirodna posljedica, razvoj međunarodnog prava, utemeljili su ovaj princip isključive nadležnosti države u odnosu na njenu vlastitu teritoriju na takav način da predstavlja tačku razdvajanja u rješavanju većine pitanja koji se tiču međunarodnih odnosa*.''[141]

Postoje dvije posljedice suverenosti države nad *cyber* infrastrukturom. Prva je da je *cyber* infrastruktura podvrgnuta pravnoj i regulatornoj kontroli države. I druga je da državni

---

[137] Član 24. Talinnmanuel-a.
[138] *Talin manuel* str. 25.
[139] Carter/Trimble/Bradley. *(2003) International Law*, forth edition. New York: Aspen Publisher. Str. 433.
[140] L.N.O.J., Special Supp. No. 3., p.3 (1920). Harris (2004) Cases and Materials on International Law, sixth edition. London: Thomson, Sweet§Maxwell. Str. 100-101; Shaw, N. M. (2008) International Law, sixth edition, Cambridge: Cambridge University Press. Str.200-201.
[141] Island of Palmas Case. RIAA II 829, at 838. Cit. Prema Malanczuk, P. (1997) Akehurst's modern introduction to International Law, seventh revised edition, London and New York: Routledge. Str. 109-10.

suverenitet štiti takvu infrastrukturu.[142] *Cyber* napad od strane jedne države usmjeren protiv *cyber* infrastrukture druge države predstavlja povredu njene suverenosti.[143]

Svaka država ima pravo da uređuje svoj pravni poredak i radi toga da uređuje prava i obaveze svih pravnih subjekata koji se nalaze na njenoj teritoriji. U isto vrijeme država ne može izvršavati bilo kakav akt vlasti na teritoriji koja pripada nekoj drugoj državi. Ova prava proizlaze iz prava jurisdikcije.

Jurisdikcija je usko povezana sa suverenošću jer predstavlja primjenu državne vlasti kojom nastaju, prestaju ili se mijenjaju prava i obaveze pravnih subjekata na područjima na kojima država ima teritorijalni suverenitet.

Talin manuel u članu 2. potvrđuje jurisdikciju država u odnosu na *cyber* infrastrukturu:

,,Bez prejudiciranja primjene međunarodnih obaveza država može ostvarivati vlastitu jurisdikciju:

a) Nad osobama angažovanim u *cyber* aktivnostima na njenoj teritoriji,
b) Nad *cyber* infrastrukturom koja se nalazi na njenoj teritoriji, i
c) Ekstrateritorijalno, u skladu sa međunarodnim pravom.''

Da bi država bila odgovorna za počinjenje *cyber* napada kao međunarodnog protivpravnog djela ponašanje (napadi) mora biti pripisivo toj državi. Generalno pravilo je da samo ponašanje državnih organa ili njenih agenata[144] može biti pripisivo državi.

Član 4. Pravila o odgovornosti država za međunarodna protivpravna djela pobliže određuje koji su to organi države čije ponašanje povlači odgovornost države. [145]

"1. *Ponašanje bilo kojeg državnog organa će se smatrati aktom države prema međunarodnom pravu, bilo da organ vrši zakonodavnu, izvršnu, sudsku ili kakvu god drugu funkciju, bez obzira koju poziciju ima u državnoj organizaciji i bez obzira da li ima karakter organa centralne vlade ili vlade teritorijalne jedinice države. 2. Organ uključuje lice ili subjekt koji ima status u skladu sa domaćim pravom države*.''

Država odgovara također, i za lica ili subjekte koji faktički postupaju kao organi države, čak i ukoliko nisu tako klasificirani po unutrašnjem pravu države. Akti osoba ili subjekata

---

[142] *Talin manuel*. str. 25.
[143] Vidi Talin manuel. str. 25 -27.
[144] Osobe ili entiteti koji djeluju po uputstvima, ili su poticani ili kontrolisani od strane države odnosno njenih organa.
[145]United Nations A/RES/56/83 from 28 January 2002. Responsibility of States for internationally wrongful acts. http://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf. Pristupio *16*.09.2019.

koji nisu državni organi, ali su po unutrašnjem pravu ovlašteni da vrše elemente javne vlasti, smatrat će se kao akti države ako u konkretnom primjeru osoba ili subjekt postupa u tom kapacitetu.[146]

Pravila pokrivaju i relativno nove fenomene kao što su paradržavni organi i privatizirane državne korporacije. Čak i privatne osobe i subjekti mogu biti obuhvaćeni ako su po domaćem pravu ovlašteni da izvršavaju državne funkcije kao što su izvršavanje državnih propisa o izvršavanju kazne lišenja slobode, što je slučaj u nekim državama.

Međunarodno protivpravno djelo države postoji kad je ponašanje države, koje može biti činjenje ili propuštanje: '' (a) *pripisivo državi po međunarodnom pravu; i (b) predstavlja povredu neke međunarodne obaveze države*.''[147]

Ukoliko je neko djelo protivpravno djelo po međunarodnom pravu, njegova protivpravnost se ne može isključiti njegovom karakterizacijom kao dopuštenog djela pravilima unutrašnjeg pravnog poretka. Karakterizacija jednog akta države kao protivpravnog po međunarodnom pravu vrši se prema kriterijima ustanovljenim u međunarodnom pravu (član 3. Pravila).

4. Upotreba sile od strane država radi suzbijanja *cyber* napada

Kao što je već rečeno član 2. tačka 4. Povelje zabranjuje svaku upotrebu sile i propisuje da će se svi članovi UN u svojim međunarodnim odnosima uzdržavati od prijetnje silom ili od upotrebe sile protiv teritorijalnog integriteta ili političke nezavisnosti druge države, ili koja bi na ma koji drugi način bila u suprotnosti sa ciljevima Ujedinjenih nacija**.**

Povelja Ujedinjenih nacija je centralizovala kontrolu upotrebe sila u rukama Savjeta sigurnosti UN. Samo Savjet sigurnosti ima pravo da utvrdi *''postojanje prijetnje miru, povrede mira ili agresije*" (Član 39. Povelje UN).

Izraz ''zabrana upotrebe sile'' upotrijebljen u članu 2. stav 4. Povelje UN nije definisan. Također, postojanje prijetnje miru, povreda mira i akt agresije, izrazi upotrijebljeni u članu 39. Povelje UN nemaju preciznu definiciju. To daje široke mogućnosti Savjetu sigurnosti prilikom odlučivanja da li postoji situacija iz člana 39. Povelje, ili se pak radi o nekoj

[146] United Nations A/RES/56/83 from 28 January 2002. Responsibility of States for internationally wrongful acts. Articl 5.http://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf. Pristupio *16*.09.2019.
[147] United Nations A/RES/56/83 from 28 January 2002. Responsibility of States for internationally wrongful acts. Articl 2.http://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf. Pristupio *16*.09.2019.

drugoj situaciji. Član 51. Povelje UN daje državama pravo na individualnu i kolektivnu samoodbranu u slučaju oružanog napada.

Međunarodni sud pravde je u predmetu *Nikaraqua* naveo da se član 2. tačka 4. i član 51. Povelje primjenjuju na ,,bilo koju upotrebu sile, bez obzira na upotrijebljeno oružje''.[148]

Prema članu 10. *Talin Manuela* ''*Cyber* operacije koje predstavljaju prijetnju ili upotrebu sile protiv teritorijalnog integriteta ili političke nezavisnosti bilo koje države, ili koja je na bilo koji drugi način nespojiva sa ciljevima UN, je nezakonita.''[149]

Ne postoji jedan autoritativan međunarodni dokument koji definiše prijetnju silom i upotrebu sile.

Član 11. *Talin Manuela* definiše upotrebu sile u *cyber* prostoru navodeći da : ,,*Cyber* operacije predstavljaju upotrebu sile kad se njen obim i posljedice uporedivi sa ne-*Cyber* operacijama uzdižu do nivoa upotrebe sile.''

Ovdje se naglašavaju obim i posljedice kao kvantitativni i kvalitativni faktor za definisanje upotrebe sile.

Međunarodni sud pravde u predmetu *Nikaraqua* razlikuje najozbiljnije oblike upotrebe sile koji predstavljaju oružane napade od manje ozbiljnih oblika.[150] Ovakav stav Suda implicira da se svaka nezakonita upotreba sile određenog obima koja je uzrokovala određene posljedice može kvalifikovati kao oružani napad.

Prilikom procjene da li neku situaciju kvalifikovati kao oružani napad države uzimaju u obzir određene faktore: ozbiljnost, neposrednost, direktnost, invazivnost, mjerljivost posljedica, vojni karakter, uključenost države i pretpostavljena legalnost.[151]

Član 12. *Talin Manuela* definiše *cyber* prijetnju na sljedeći način: ''*Cyber* operacija, ili prijetnja *cyber* operacijom, predstavlja nezakonitu prijetnju silom, koja bi ukoliko bi bila provedena, predstavljala nezakonitu upotrebu sile.''

Član 13. *Talin Manuela* potvrđuje pravo na samoodbranu protiv oružanog napada. ''Država protiv koje je usmjerena *cyber* operacija koja se uzdiže do nivoa oružanog

[148] Nuclear Weapons Advisory Opinion, para. 39.
[149] *Talin manuel* o međunarodnom pravu koje se primjenjuje na *cyber* ratovanje. General editor Michael N Schmitt. Cambridge University Press 2017. str. 45.
[150] Nuclear Weapons Advisory Opinion, para. 191.
[151] Vidi: *Talin manuel* o međunarodnom pravu koje se primjenjuje na *cyber* ratovanje. General editor Michael N Schmitt. Cambridge University Press 2017. str. 49 – 52.

napada može vršiti vlastito urođeno pravo na samoodbranu. Da li jedna *cyber* operacija predstavlja oružani napad zavisi od obima i posljedica.''

5. Pravo država na samoodbranu od oružanog napada

Kao što smo vidjeli član 13. *Talin Manuela* slijedi pravila opšteg međunarodnog prava u pogledu prava država na samoodbranu protiv *cyber* napada.

Član 51. Povelje Ujedinjenih nacija koji predstavlja izvor prava na samoodbranu glasi:

*"*Ništa u ovoj Povelji ne ograničava urođeno pravo na individualnu i kolektivnu samoodbranu u slučaju oružanog napada protiv neke članice Ujedinjenih nacija, dok Savjet sigurnosti ne preduzme mjere potrebne za održavanje međunarodnog mira i sigurnosti. O mjerama koje preduzmu članice pri vršenju tog prava na samoodbranu, odmah će se obavijestiti Savjet sigurnosti, i one neće ni na koji način dovesti u pitanje ovlašćenje i obavezu Savjeta sigurnosti da, na osnovu ove Povelje, preduzme u svakom trenutku korak koji smatra nužnim radi održanja ili uspostavljanja međunarodnog mira i sigurnosti.*"*

Da bi se utvrdilo tačno značenje ovog člana potrebno ga je razmotriti u kontekstu Povelje UN kao i u odnosu prema međunarodnom običajnom pravu. U kontekstu Povelje UN potrebno je prije svega posmatrati ga u vezi sa članom 2. (4) koji obavezuje sve članove UN-a da se u svojim odnosima uzdrže od prijetnji silom ili upotrebe sile protiv teritorijalnog integriteta ili političke nezavisnosti ma koje države, ili koja bi na ma koji drugi način bila u suprotnosti sa ciljevima Ujedinjenih nacija.

Oružani napad treba biti usmjeren protiv teritorijalnog integriteta ili političke nezavisnosti. Takav oružani napad dopušta izuzetak od opće zabrane upotrebe sile prema Povelji, i daje pravo svakoj državi da pribjegne samoodbrani.

Postoje situacije koje su očigledne i koje državama bez ikakve sumnje daju opravdanje za samoodbranu.

U predmetu *Nicaraqua* Međunarodni sud pravde je koristio definiciju agresije (član 3. g)[152] da bi definisao značenje pojma oružani napad u međunarodnom pravu. Oružani napad mora obuhvatati ne samo upotrebu regularnih oružanih snaga nego i ''slanje od države ili u ime države oružanih bandi, grupa, iregularaca ili plaćenika, koji vrše akte oružanog nasilja protiv druge države takve težine da znače stvarni oružani napad, ili njeno

[152] United Nations General Assembly Resolution 3314 (XXIX). Definition of Aggression. Dostupno na: http://jurist.law.pitt.edu/3314.htm,

bitno učešće u njemu. Ali Sud ne smatra da se pojam oružani napad proteže na pomoć pobunjenicima u formi nabavke oružja ili logističku ili drugu podršku.[153]''

Nakon terorističkog napada od 11. septembra 2001. godine, rezolucijom 1368. od 12. septembra 2001.[154]godine, teroristički napad je označen kao prijetnja međunarodnom miru i sigurnosti u smislu poglavlja VII Povelje UN.

Pravo na država na samoodbranu proteže se i na odbranu od cyber napada. ''Međunarodna grupa eksperata jednoglasno je zaključila da neke cyber operacije mogu biti dovoljno ozbiljne da opravdaju njihovo klasifikovanje kao 'oružani napad' unutar značenja Povelje.[155] Što onda povlači pravo države na samoodbranu u skladu sa Poveljom UN. Ovaj zaključak je u skladu sa mišljenjem Međunarodnog suda pravde datom u predmetu *O zakonitosti upotrebe nuklearnog oružja* gdje se navodi da se: ,,Ove odredbe ne odnose na određeno oružje. One se primjenjuju na bilo koju upotrebu sile, bez obzira na upotrijebljeno oružje''.[156]

Pravo na samoodbranu od *cyber* napada obuhvata i upotrebu dopuštenih kontramjera čiji je cilj da potakne državu povreditelja da prestane sa kršenjem međunarodnopravnih obaveza i da počne poštovati svoje međunarodne obaveze.[157] Pravo na kontramjere traje dok postoji nezakanito ponašanje. Sa prestankom kršenja međunarodnih obaveza prestaje i pravo na kontramjere. Kontramjere moraju biti nužne i proporcionalne te su vremenski ograničene.

Talin Manuel u članu 9. potvrđuje pravo države na kontramjere:

''Država povrijeđena međunarodnim protivpravnim djelom može, protiv odgovorne države, pribjeći proporcionalnim kontramjerama, uključujući i *cyber* kontramjere.''

[153] Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Merits, Judgement, ICT Reports 1986, p 14, para 195.
[154] Resolution S/RES/1368 (2001), Dostupno na: http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N01/533/82/PDF/N0153382.pdf?OpenElement, 21.12.2010.
[155] *Talin manuel* o međunarodnom pravu koje se primjenjuje na *cyber* ratovanje. General editor Michael N Schmitt. Cambridge University Press 2017. str. 54.
[156] Nuclear Weapons Advisory Opinion, para. 39. https://www.icj-cij.org/files/case-related/95/095-19960708-ADV-01-00-EN.pdf. 1.9.2019.
[157] Vidi čl.49. Draft articlies. United Nations A/RES/56/83 from 28 January 2002. Responsibility of States for internationally wrongful acts. http://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf. Pristupio *16*.09.2019.

6. Preduvjeti za postojanje prava na samoodbranu

U pravnoj literaturi je skoro jednoglasno prihvaćeno da je za ostvarenje prava na samoodbranu neophodno ispunjenje uvjeta: neophodnosti (nužde) i proporcionalnosti.

Međunarodni sud pravde u predmetu *Nikaragva* ističe da član 51. "ne sadrži neko specifično pravilo kojim bi samoodbrana garantovala samo mjere koje su proprcionalne oružanom napadu i potrebne da se njima odgovori, pravilo dobro ustanovljeno u međunarodnom običajnom pravu."[158]

Pravila nužde i proporcionalnosti su pravila međunarodnog običajnog prava i njihov sadržaj zavisi od okolnosti svakog konkretnog slučaja. Da li su ti uvjeti ispunjeni cijene prvo, država koja se nađe u situaciji koja zahtijeva pribjegavanje samoodbrani, a zatim i međunarodna zajednica. "Svaka nacija je slobodna u svako vrijeme bez obzira na odredbe ugovora da se brani i jedini sudija u tome šta znači pravo samoodbrane i nužde i šta oni obuhvataju."[159]

Stanje nužde postoji kad je država u odgovoru na oružani napad prinuđena da upotrijebi svoje oružane snage pošto nema drugih sredstava da bi zaštitila neko svoje pravo.

"Običajno pravo o samoodbrani uključuje pretpostavku da upotrijebljena sila mora biti proporcionalna prijetnji."[160] *Proporcionalnost* se mora cijeniti sa potrebnom mjerom fleksibilnosti, jer nema proporcionalnosti ukoliko na povrede granice malog obima država odgovori neproporcionalnim sredstvima, posebno što napadi malog intenziteta često mogu biti proizvod greške ili pogrešno shvaćenog naređenja od nižih komandi.

Talin Manuel propisuje u članu 14. da: ''Upotreba sile koja uključuje *cyber* operacije poduzeta od strane države u ostvarivanju njenog prava na samoodbranu mora biti nužna i proporcionalna.''

U vezi sa pravom na samoodbranu postavlja se pitanje da li je ona moguća i prije nego što se stvarni napad desi. Ovo pitanje je posebno značajno za zemlje koje posjeduju nuklearno oružje odnosno koje bi mogle biti objektom njegovog udara, ali i za druge s obzirom da od prve upotrebe oružja možda zavisi i ishod rata.

Član 51. Povelje, dopušta samoodbranu samo u slučaju postojećeg oružanog napada. U pogledu prava preventivne samoodbrane mišljenja su podijeljena. Dok jedni smatraju da

---

[158] Dinstein, Y. (1994). op. cit. str. 202, nota 124; Vidi također: Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Merits, Judgement, ICT Reports 1986 .
[159] Brownlie, I. (2003). Ibid., str. 237, nota 4.
[160] Ibid., str. 261.

ne postoji pravo na preventivni rat odnosno anticipatornu samoodbranu, većina pravnih pisaca smatra da međunarodno običajno pravo dopušta ovakvu samoobranu.

Prema *Westlaku*:

"Država se može braniti preventivnim sredstvima ako je po njenoj savjesnoj prosudbi to neophodno protiv napada druge države, prijetnji od napada ili pripremanja ili drugog postupanja iz koga se namjera napada može razumno zaključiti."[161]

Prema *Westlaku*:

"Država se može braniti preventivnim sredstvima ako je po njenoj savjesnoj prosudbi to neophodno protiv napada druge države, prijetnji od napada ili pripremanja ili drugog postupanja iz koga se namjera napada može razumno zaključiti."[162]

Izrael je 1967. godine, izvršio preventivni napad na svoje arapske susjede zbog blokade luke Elijat i zaključenja vojnog pakta između Egipta i Jordana. Značajno je da Ujedinjene nacije u raspravama koje su nakon toga uslijedile nisu osudile ovaj izraelski napad i način ostvarenja samoodbrane. Međunarodni sud u predmetu Nikaragva nije se bavio pitanjem neposredne prijetnje oružanim napadom, pošto ovo pitanje pred njega nije ni stavljeno.

Talin Manuel u članu 15. propisuje: ''Pravo na upotrebu sile u samoodbrani ako se desi cyber oružani napad ili napad neposredno predstoji.''

Sa predhodnim pitanjem povezano je i pitanje da li država može upotrijebiti silu da zaštiti svoje državljane i imovinu u inozemstvu? Do donošenja Povelje UN-a ovo pitanje je bilo van svake sumnje. Stav međunarodnog običajnog prava bio je da države mogu braniti svoje državljane odnosno osobe koje su podlijegale njenoj jurisdikciji kao i imovinu bez obzira gdje se ona nalazila. Ukoliko se oni nalaze na teritoriji odnosne države nije bilo nužno da se primjenjuju odbrambene mjere. Ali ako se oni nalaze na teritoriji druge države, međunarodno običajno pravo je dopuštalo primjenu mjera samoodbrane i na takvoj teritoriji.

Ukoliko posmatramo ovo pitanje u smislu člana 51. Povelje, uočljivo je da on ne dopušta pravo samoodbrane radi zaštite državljana i imovine u inozemstvu. I pored toga većina pravnih pisaca stoji na stanovištu da međunarodno običajno pravo dopušta ovaj vid samoobrane. Što je još značajnije savremena praksa pokazuje da ono još uvijek egzistira u međunarodnim odnosima. Oni koji podržavaju ovo pravo kao uvjet njegovu primjenu

[161] Ibid., str. 257, nota 5.
[162] Ibid., str. 257, nota 5.

vezuju za državljanstvo osoba kao i neposrednu opasnost koja prijeti životima ili imovini. Tako je američki predstavnik na Konferenciji u Havani 1928. godine izjavio:

"Šta da radimo kad vlada padne i u opasnosti su životi američkih građana?... Sada je to princip međunarodnog prava da u takvim slučajevima država ima puno opravdanje da preduzme akciju - ja bih to nazvao uplitanje privremenog karaktera zbog ciljeva zaštite života i imovine državljana.."[163]

Ovo pitanje je isticano posljednih godina u nekolicini primjera. Poznata je američko-belgijska akcija spašavanja talaca u Kongu 1964. godine. "Najpoznatiji incident, međutim, bio je spašavanje talaca od Izraela koje su držali Palestinci i drugi teroristi na *Entebbe*, slijedeći oteti avion francuske kompanije. Debata u Savjetu sigurnosti u ovom slučaju bila je bez zaključaka. Neke države podržavale su izraelski stav da je to bilo zakonito djelovanje u zaštiti njenih državljana u inostranstvu, gdje je lokalna država pomagala otmičarima. Drugi su prihvatili stav da je Izrael počinio agresiju protiv Ugande ili koristio prekomjernu silu."[164]

,,SAD-e su izvršile bombaški napad na Libiju 15. aprila 1986. godine koji je posljedica navodne libijske uključenosti u napad na američke službenike u zapadnom Berlinu. Ovo je pravdano od SAD-a kao akt samoodbrane."[165]

"Britanski ministar vanjskih poslova je zaključio 28. juna 1993. godine da:

'Sila može biti primijenjena u samoodbrani protiv prijetnji nečijim državljanima ako (a) je tu dobar dokaz da bi napadnuti cilj nastavio da se drugdje koristi podrškom druge države u terorističkim napadima protiv nečijih državljana, (b) ako nema drugog efikasnog načina da se preduprijede neposredni dalji napadi na nečije državljene, i (c) ako je upotrijebljena sila proporcionalna prijetnji.'"[166]

Član 51. Povelje UN-a, navodi između ostalog da je pravo na kolektivnu samoodbranu prirođeno pravo svake države. Ova ideja se dalje razvija u članu 52. gdje stoji da (ova) Povelja ničim ne isključuje postojanje regionalnih sporazuma ili ustanova čija je svrha bavljenje pitanjima koja se tiču održanja međunarodnog mira i sigurnosti i koja su podesna da budu predmet regionalne akcije, pod uvjetima da su ti sporazumi i ustanove i njihovo djelovanje u skladu sa ciljevima i načelima Ujedinjenih nacija.

---

[163] Bowett, D. W. (1958). Ibid., str. 99 - 100, nota 1.
[164] Shaw, N. M. (1997). International Law. Cambridge: University Press. str. 792, nota 84, 85. i 86.
[165] Ibid., str. 793. nota 90.
[166] Ibid., str. 793. nota 92.; "Prema Waldoku uvjeti za primjenu sile za zaštitu državljana u inostranstvu su: (1) Neposredna prijetnja štete državljanima, (2) Propust ili nesposobnost na strani teritorijalnog suverena da ih zaštiti, (3) Mjere zaštite su strogo ograničene na objekat koji se štiti od povrede." Dinstein, Y. (1994). Ibid., str. 226. nota 51.

Talin Manuel propisuje: ''Pravo na samoodbranu može se ostvarivati kolektivno. Kolektivna samoodbrana protiv *cyber* operacija znači da oružani napad može biti izvršen na zahtjev države žrtve i u okviru zahtjeva.''[167]

7. Samodbrana protiv terorizma

Kao odgovor na teroristički napad od 11. septembra Sjedinjene Američke Države pokrenule su vojnu kampanju protiv Avganistana poznatu kao Operacija trajne slobode (engl. *Operation Enduring Freedom*)[168] 7. oktobra 2001. godine. Prilikom informisanja Savjeta sigurnosti o poduzetim akcijama SAD su tvrdile da postupaju u samoodbrani. Velika Britanija se također pozvala na individualnu i kolektivnu samoodbranu. Uprkos ranijim dilemama po pitanju prava na samoodbranu protiv proteklih terorističkih napada, ove akcije naišle su na opštu podršku. Rezolucija Savjeta sigurnosti 1368 od 12. septembra 2001. godine, izričito je priznala pravo na samoodbranu protiv terorizma. Kasnija Rezolucija 1373 od 14. novembra 2001. godine,[169] također se poziva na individualno i kolektivno pravo na samoodbranu.

Ovdje se očito radi o proširenju tradicionalnog modela prava država na samoodbranu kako je to propisano Poveljom UN. Ali pošto se radi o opštoj podršci pravu na samoodbranu u slučaju terorističkog napada na djelu je reinterpretacija odredaba Povelje stvaranjem instant međunarodnog običaja koji to dopušta.

''Sada je očigledno prihvaćeno da je teroristički napad na državnu teritoriju od nedržavnih počinitelja, oružani napad koji opravdava odgovor protiv države koja pruža utočište odgovornim.''[170] Povodom ovog napada NATO se po prvi put pozvao na član 5. osnivačkog ugovora koji propisuje da će se napad na jednu državu članicu smatrati napadom na sve njih.

Sjedinjene Američke Države i Velika Britanija smatraju da imaju pravo i na anticipatornu i preventivnu samoodbranu protiv terorizma. Ovo pravo je prihvaćeno od velikog broja država ali samo u odnosu na terorističku prijetnju ali ne i izvan toga. Ali i u tom pogledu uslov je da Savjet sigurnosti svojom rezolucijom utvrdi postojanje terorističke prijetnje.

Talin Manuel u članu 36. propisuje: ''*Cyber* napadi ili prijetnja cyber napadima, čiji je primarni cilj teror među civilnim stanovništvom, su zabranjeni.'' Na ovaj način *Talin Manuel*

---

[167] Talin manuel, član 16.
[168] Operation Enduring Freedom , Dostupno na: http://www.history.army.mil/brochures/Afghanistan/Operation%20Enduring%20Freedom.htm, 23.12.2010.
[169] Security Council Resolution S/RES/1373 (2001), Dostupno na: http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N01/557/43/PDF/N0155743.pdf?OpenElement, 23.12.2010.
[170] Gray, C. The use of force and the international legal order. U Evans. M. D. (ed.). (2003). International Law. Oxford: University Press. str. 604.

prepoznaje *cyber* napade kao teroristički akt i kao terorističku prijetnju na koju se primjenjuju ista pravila kao na bili koju drugu terorističku prijetnju.

8. Zaključak

Cyber napadi su po svojoj sadržini vrsta oružanih sukoba. Primjena prava oružanih sukoba ne zavisi od klasifikacije oružanog sukoba niti od vrste vojnih operacija i korištenih metoda ratovanja. Stoga *cyber* operacije mogu same, bez prisustva drugih vrsta operacija značiti i međunarodni i nemeđunarodni oružani sukob.

Pravo oružanih sukoba se primjenjuje na sve aktivnosti poduzeta tokom trajanja oružanog sukoba i na sve posljedice nastale na teritoriji država koje su uključene u oružani sukob ne ograničavajući se samo na prostor gdje se vrše vojne operacije.

Da bi *cyber* napadi predstavljali napade relevantne za pravo oružanih sukoba moraju biti takve težine i uzrokovati fizičku destrukciju ili štetne povrede kao i druge vrste oružja: konvencionalno, nuklearno, hemijsko i biološko. Odnosno, potrebno je da cyber napad uzrokuje iste posljedice kao i druge vrste napada ili da je napad usmjeren protiv bilo čega što se zove kritična infrastruktura.

Cyber napadi podliježu primjeni pravila *jus ad bellum* koja se odnose na pravo države na upotrebu sile u cilju realizacije svoje nacionalne politike. Također podliježu primjeni pravila *jus in bello* kojima se reguliše način vođenja oružanih sukoba.

Za primjenu prava oružanih sukoba na *cyber* ratovanje nisu neophodni neki novi izvori prava. Na *cyber* napade se primjenjuju postojeći pravni izvori: međunarodni ugovori, međunarodni običaji i opća pravna načela.

Sve suverene države su na osnovu prava na jurisdikciju ovlaštene vršiti kontrolu nad *cyber* infrastrukturom i *cyber* aktivnostima unutar svoje teritorije.

Posljedice suverenosti države nad cyber infrastrukturom su da je *cyber* infrastruktura podvrgnuta pravnoj i regulatornoj kontroli odnosne države i da državni suverenitet štiti takvu infrastrukturu.

Cyber napad ili ozbiljna prijetnja cyber napadom od strane jedne države usmjeren protiv *cyber* infrastrukture druge države predstavlja povredu njene suverenosti što povlači odgovornost države za međunarodne protivpravne akte. Generalno pravilo je da samo ponašanje državnih organa ili njenih agenata može biti pripisivo državi.

Država koja je meta cyber napada ima pravo na samoodbranu u skladu sa Poveljom UN uz obavezu poštovanja prava nužde i proporcionalnosti.

U vezi sa preventivnim pravom na samoodbranu mišljenja su podijeljena. Ali ipak prevladava stav o njenoj opravdanosti i zakonitosti.

Literatura:

Knjige i članci:

1. Akehurst's modern introduction to International Law, seventh revised edition, 1997. London and New York: Routledge.
2. Brownlie, J: International Law and the use Force by States, Oxford University Press 1963.
3. Bowett, D. W.: Self - Defence in International Law, Manchester University Press, 1958.
4. Carter/Trimble/Bradley. *(2003) International Law*, forth edition. New York: Aspen Publisher. Dinstein, Y.: War, Agression and Self -Defence, Cambridge University Press, 1994.
5. Harris (2004) Cases and Materials on International Law, sixth edition. London: Thomson, Sweet§Maxwell.
6. Mateusz Piatkowski, The Definition of the Armed Conflict in the Condition of Cyber Warfera, Polish politikal Science Yearbook vol. 46 (2017) pp. 271 – 280.
7. Michael N Smitt, ''Attack'' as a Term of Art in International law: The Cyber Operations Context. 2012 4thInternational Conferenc on Cyber Conflict. (283-293).
8. Softić, S. (2012). *MEĐUNARODNO PRAVO.* Sarajevo: DES doo - Sarajevo.
9. Shaw, N. M. (2008) International Law, sixth edition, Cambridge: Cambridge University Press.

Drugi izvori:

1. Talin manuel o međunarodnom pravu koje se primjenjuje na *cyber* ratovanje. General editor Michael N Schmitt. Cambridge University Press 2017.
2. International Court Of Justice Reports Of Judgments, Advisory Opinions And Orders Legality Of The Threat Or Use Of Nuclear Weapons Advisory Opinion Of 8 July 1996.
3. United Nations A/RES/56/83 from 28 January 2002. Responsibility of States for internationally wrongful acts. http://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf.
4. Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Merits, Judgement, ICT Reports 1986.
5. Convention on Cybercrime 185 CETS (opened for signature 23 November 2001, entered into force 1 July 2004).

Kriminalističke teme
Zbornik radova
Godina XIX, Broj 5, 2019.
ISSN 1512-5505

CYBER TERORIZAM
CYBER TERRORISM

Pregledni naučni rad

Enes Bezdrob, MA[171]

Sažetak

Inspiracija za rad i problem (i) koji se radom oslovljava (ju): U prvom dijelu radu se problematizira način kreiranja teoretskog okvira za analiziranje fenomena „cyber terorizma". U drugom dijelu rada se analizira fenomen „virtualnog genija". Ova pojava je specifičan produkt posredne komunikacije dostupne na društvenim mrežama. U trećem dijelu rada autor raspravlja o otpornosti društvenih grupa na indoktrinaciju koja se odvija u cyber prostoru.

Ciljevi rada (naučni i/ili društveni): Upravo je cyber prostor, svojom specifičnošću dozvolio izranjanje genijalaca koji na izgled imaju puno veće znanje od osoba sa kojima dolazimo u dodir u direktnoj svakodnevnoj komunikaciji. U ovom radu se raspravlja i o vrstama poruka koje se nastoje odaslati i steći naklonost ili, kao forma specijalnog rata, izazvati strah u određenoj društvenoj zajednici.

Metodologija/Dizajn: U radu je korištena analiza sadržaja relevantne literature.

Ograničenja istraživanja/rada: Rad je pregledni naučni.

Rezultati/Nalazi: Gotovo da ne postoji strukturirana društvena zajednica koja nije na neki način upoznata sa materijalnim i intelektualnim resursima i potencijalima njenih članova, sa prednostima i nedostacima socijalizacije unutar grupe. Upravo ovdje je šansa za preventivno djelovanje i sprečavanje eventualnih cyber podstrekača da pronađu stvarne izvršioce terorističkih akata.

Generalni zaključak: Ključno je naglasiti da postoji potreba razumijevanja onih koji regrutiraju izvršioce terorističkih akata, njihovih motiva, metoda djelovanja i prepoznavanja potencijalnih istomišljenika. Poseban naglasak se stavlja na profil podstrekača koji iskorištava slabosti eventualnog izvršioca predstavljajući se kao njegov istomišljenik i ohrabruje odnosnog na poduzimanje nasilnih aktivnosti na osnovu činjenica i pojava koje sam izvršilac smatra da treba ispraviti u njegovom okruženju.

Opravdanost istraživanja/rada: Poseban problem nastaje pri pokušaju da se ovaj fenomen promatra izdvojeno od ostalih negativnih oblika društvenosti. Naravno, autor prepoznaje specifičan, tehnološki, uvjet koji bi, na prvu, ukazivao da se radi o posebnom obliku terorizma. Međutim, evolucija društvene dinamike ne mijenja posljedicu djelovanja onih koji se bave terorizmom. Važan aspekt zamjene teza je i u činjenici da su u propagiranje ove nove „naučne discipline" snažno uključeni i mediji ne praveći razliku između nauke i naučne fantastike koju „učenjaci" željni slave namjerno izostavljaju.

[171] Vijeće ministara BiH, Odjel za sigurnost

Ključne riječi
Terorizam, Internet, sigurnost, cyber prostor, specijalni rat

Abstract
Reason for writing and research problem (s): In the first part of the paper, the way theoretical frame for the analysis of the "cyber terrorism" phenomenon was created, is problematized. The second part of the paper analyses the "virtual genius" phenomenon. This appearance is a specific product of indirect communication available on social networks. In the third part of the paper the author discuss the resilience of social groups to indoctrination that occurs in cyber space.
Aims of the paper (scientific and/or social): It is cyber space, with its specificity, that allows the emerging of geniuses who, at first glance, have a larger knowledge then people; we come in contact in everyday communications. This part also deals with the types of messages that are conveyed in order to gain favor or, as a form of special war, cause fear in a specific social community.
Methodology/Design: Paper is a review paper.
Research/Paper limitation: This paper employed content analysis of relevant literature.
Results/Findings: A structured social community, not familiar with the material and intellectual resources and potential of its members, together with the advantages and disadvantages of socialization inside of the group, almost does not exist. Right here is the chance for prevention and the stopping of potential cyber persuaders to find actual executors of terrorist acts.
General Conclusion: It is crucial to emphasize that a need exists to understand those who recruit the executors of terrorist acts, their motives, methods, and the way they recognize potential supporters. A special emphasis is put to the profile of the persuader who uses the weaknesses of potential executors appearing as a like-minded individual and encouraging him to conduct violent activities based on the facts and appearances that the executor himself believes need fixing in his surroundings.
Research/Paper Validity: A particular problem occurs when trying to view this phenomenon separately from other negative social forms. Of course, the author recognizes a specific, technological, environment that would, at first, point out that it is a special form of terrorism. However, the evolution of social dynamics does not change the consequence of the activities those who engaged in terrorism. An important aspect of this scientific error is in the fact that media are strongly involved in the propagation of this new "scientific discipline" without making a difference between science and science fiction which is deliberately left out by fame craving "scholars".

Keywords
Terrorism, internet, security, cyber space, special war

Uvod

Na samom početku je potrebno uspostaviti određeni logički okvir analize razmatrane teme. Da li je nužno pri raspravi o cyber terorizmu „izmišljati" kompleksne teorije i metodološke zahvate ili je moguć jednostavniji pristup kako sa aspekta teorije tako i metodologije? Prema mom shvatanju ne radi se o novom fenomenu niti o novoj nauci. Specifična tehnološka dimenzija, na prvu, ostavlja dojam da se radi o novom fenomenu ali i o

potrebi stvaranja nove nauke koja će moći ponuditi rješenja problema kojim cyber terorizam opterećuje društva širom svijeta (Weimann, G., 2004: 4). Mnogi od nesporazuma nastaju iz želje naučnika da zasnuju novu nauku, da budu pioniri u nekoj novoj oblasti, ili su u pitanju neki drugi egoistični razlozi. Bez obzira na manipuliranje pojmovnim određenjima cyber terorizam ne izlazi izvan, već uspostavljenog teoretskog okvira (Babić, V., 2009: 171). Rasprava o terorizmu je daleko od zaokružene, niz je neslaganja među naučnicima o uzročno-posljedičnim vezama terorizma i društvene dinamike, ali ni u kom slučaju to ne znači da postojeći teoretsko-metodološki okvir nije dostatan u analiziranju cyber terorizma (Beggs, C., 2010: 14).

Važno je istaći da definicije terorizma, koje je moguće naći u literaturi, dolaze iz različitih teoretskih krugova, što je u neku ruku dovelo do definicijske zamagljenosti i otežalo ogoljenje fenomena. Ovdje se nećemo baviti definicijama, već ćemo se fokusirati na jedan aksiom i to da je terorizam uvijek politički motiviran. Bez obzira na ideološku obojenost grupa ili pojedinaca koji izvode terorističke napade, uvijek je prisutan politički motiv (Kovačević, G. 2015: 110). O svim ostalim elementima terorizma, na koje se ukazuje u različitim definicijama, moguće je raspravljati osim o političkom motivu. Dakle, o kojem god obliku terorizma da se radi, kada ogolimo politički motiv možemo se efikasno boriti protiv njega. Mnogi autori se neće složiti sa ovom konstatacijom, jer su navodili druge motive kao razloge za terorizam. Međutim, svi motivi koliko god izgledali udaljeni od politike, podvrgnuti su, u svakom konkretnom slučaju, procesu politizacije i tek tada su postali motivi terorizma. Kao primjer možemo uzeti religijski fundamentalizam, koji je prema velikom broju naučnika ideološka matrica, u mnogo slučajeva, terorističkih organizacija i grupa. Posebno se ovdje ističe islamski fundamentalizam. Problem je u činjenici da se ovdje zanemaruje proces politizacije a u prvi plan se stavlja religija. Međutim, religijski fundamentalizam je politička ideologija i religija mu je samo u imenu i ako bismo ga ogolili vidjeli bismo da se radi o klasičnom obliku fašizma (Kovačević, G. 2013: 238).

Terorizam se uvijek javlja u uvjetima gdje određena grupa ili pojedinac ne mogu legitimnim i legalnim političkim mehanizmima postići željene političke promjene. Izvori nemogućnosti postizanja željenih političkih promjena mogu biti različiti: od toga da je percipirani neprijatelj nasilan u nastojanju da zadrži stečene pozicije društvene moći, do toga da grupa koja želi te promjene nema podršku većinske zajednice (Held, D. 1999: 200).

Da bih bio što precizniji potrebno je objasniti suštinu političkog u terorizmu. Svako društvo, uokvireno u nacionalnoj državi, profilira se i bivstvuje posredstvom niza političkih institucija i mehanizama koji, u većoj ili manjoj mjeri, su odraz volje tog društva. Što je veća usklađenost volje i postojećih institucija i mehanizama to je manje prostora za nezadovoljstvo. Obrnuto, postoji prostor za oživljavanje političkih aspiracija usmjerenih na drugačije usklađivanje. Naravno, i ovdje postoji granica. Ako je neusklađenost velikog obima onda će doći do pokušaja usklađivanja drugim političkim sredstvima, a ne terorizmom (Abazović, M. 2012: 52 - 54). Važno je istaći da terorizam je nasilno političko sredstvo ali samo u mirnodopskim uvjetima. U uvjetima rata, napad na bilo koju neprijateljsku metu je legitiman, posebno ako će to rezultirati strahom u neprijateljskim redovima. Iz

prethodne konstatacije je jasno da je niz aktivnosti u historiji čovječanstva pogrešno okarakteriziran kao terorizam. Neko djelovanje nazvati terorizmom može samo akter koji u datom momentu raspolaže mogućnošću da određuje šta jeste a šta nije istina. Dakle, onaj ko je u poziciji moći raspolaže mogućnošću da imenuje neku aktivnost kako mu u tom trenutku odgovara i da protiv nosilaca te aktivnosti primjenjuje različite mehanizme represije iz arsenala koji mu je na raspolaganju, ovisno od njegove sposobnosti da društvenoj zajednici legitimira primjenu tim mjera (Ibid.). Poseban problem u razumijevanju terorizma nastaje iz konvergencije neznanja predstavnika vlasti i medija, gdje „povika na vuka" može otići u nedogled dok se ne utvrdi činjenično stanje. Ovo se posebno lako dešava kada je u pitanju dobro reklamirana pojava kao što je terorizam. Medijski momentum koji postoji u slučaju terorizma nastoji se iskoristiti i za „reklamiranje" cyber terorizma, posebno ukazujući na fantastične mogućnosti koje su na raspolaganju cyber teroristima. Mi, kao naučnici, moramo razlikovati naučnu fantastiku od nauke. Moramo društvu objasniti šta jeste moguće a šta nije. Na kraju mnogo je teoretski mogućih aktivnosti koje nisu praktično sprovodive.

Cyber prostor i terorizam

Cyber prostor ili okruženje je, također, jedan od onih fenomena koji se atribuira mogućnostima i sposobnostima preko mjere. Naravno, to jeste prostor, u pravom smislu, materijalizirane globalizacije. Po našem mišljenju mjesto dijaloga različitih kulturoloških krugova; mjesto postavljanja informacija, podataka, obavještenja u različitim formama i za različitu publiku; mjesto pružanja raznih usluga; mjesto obrazovanja; mjesto dijaloga, polemike, reklamiranja, propagande, vrbovanja, prevara i tako dalje (Chu, S. C., Lien, C. H., Cao, Y. 2018.). Međutim, potrebno je istaći da je niz sistema različite namjene dostupno u cyber prostoru kojima upravljaju direktno ljudi ili neki oblik vještačke inteligencije. Iako izgleda da su mogućnosti bezgranične ovaj prostor je upravljan određenim zakonitostima, čije zaobilaženje ili zloupotreba privlače pažnju i aktiviraju mehanizme zaštite (Bara, D. 2015: 130). Ovdje ću se fokusirati na jednu specifičnost komunikacije unutar cyber prostora koja pojedincima ili grupama otvara mogućnost da šire svoje „ideje", poruke, prijetnje, da vrbuju istomišljenike, da traže podršku za svoje „projekte" i sl. Vrlo je važno razumjeti u kojem su obimu pojedinci pa i čitave zajednice opterećeni svakodnevnim rutinama čijim izvršavanjem obezbjeđuju vlastitu egzistenciju i funkcioniranje društvene grupe u kojoj psihički i fizički egzistiraju (Weimann, G. 2019: 115). Radi se o uhodanim bihevioralnim obrascima koji konzumiraju vrijeme pojedincima ili grupama, ostavljajući im malo prostora za bilo kakvo kritičko promišljanje o nekim predočenim problemima (Guegan, J. 2019: 192). Kritičko promišljanje podrazumijeva upoznavanje sa historijom „problema", argumentima svih zainteresiranih strana i donošenje suda u na osnovu stavljanja sebe u odnosnu situaciju. Pregršt novih informacija uvijek otežava historijski uklon, pa mnogi od njega i odustaju zarad svježih informacija. Upravo zbog poteškoća koje su povezane sa prethodnim postupkom pojedinci ili grupe su, u većoj ili manjoj mjeri, skloni da prihvate tuđu „analizu" problema koja im ima više logike u odnosu na njihove životne uvjete i provedu određene aktivnosti iz preporuka „analize" (Lehti, L., Kallio, J. 2017: 60). Ovdje je potencijalno prostor za cyber terorizam gdje ne postoje fizičke barijere, poput granica, za okupljanje simpatizera i istomišljenika, pa i aktivnih članova koji

su spremni poduzimati aktivnosti na planu realizacije određenih ideja ili djelatnosti za koje drže da će riješiti specifičan problem (Karapanos, E., Teixeira, P., Gouveia, R. 2016: 889). Iako se radi o virtualnoj zajednici uvijek moramo imati na umu da su stvarni ljudi iza tih virtualnih osoba, koji mogu svojim djelovanjem proizvesti željene efekte (Sudweeks, F. 2001: 71). Potrebno je napomenuti još jednu ljudsku osobinu, kada govorimo o virtualnim identitetima, kojima se pojedinci predstavljaju u cyber okruženju moramo skrenuti pažnju na jedan posebno, za analiziranje terorizma, važan aspekt. Dakle, većina ljudi koji su prisutni u cyber prostoru susreli su se sa virtualnim genijem. Radi se o osobama koje u komunikaciji raspolažu znanjima i informacijama, mnogo većeg obima, od onoga koje bismo susreli u realnom životu kod bilo koje osobe. Obzirom da je komuniciranje u cyber okruženju modelirano na način da oponaša ono koje se dešava i u realnom svijetu, često se previdi činjenica da ljudi koji se pojavljuju u ulozi virtualnog genija (Jang-Jaccard, J. 2014: 981) mogu biti profesionalci čija je dnevna rutina upravo iskorištavanje identificirane nekritičnosti šire publike. Znanja i informacije kojima ovi ljudi raspolažu ne moraju, i u većini slučajeva nisu, njihova, već ona koja su dostupna u samom cyber prostoru a odnosne osobe znaju kako u što kraćem vremenu pristupiti takvim znanjima i plasirati ih (Chen, J. 2014: 902). Upravo brzina iznošenja informacija je ona koja stvara privid direktne komunikacije i stvara privid da se radi o stvarnom autoritetu u nekoj oblasti (Gordon, S. 2002: 640). Jednom kada se identificira publika koja će prihvatiti poruke i identificirati se sa sadržajem, otvara se prostor za djelovanje bilo da se radi o pozitivnih ili negativnim aktivnostima. U tom trenutku publika, koja je sve do tada bila relativno pasivna, postaje protagonista dobro kreiranog scenarija (Marwick, A. E., Boyd, D. 2011: 129). Važno je naglasiti da su teroristi samo jedni od negativaca koji koriste ovakav model stjecanja resursa za ostvarivanje svojih ciljeva (Choo, K-K. R. 2011: 722). Nedoumice postoje oko toga koliko je ovaj pristup funkcionalan, ali je u svakom slučaju mnogo jeftiniji od istog ovog pristupa koji bi se provodio u realnom životu (Huang, L. 2011: 732). Međutim, zadnji pokazatelji, posebno vezano za napade u EU, dovode do zaključka da je efikasnost neupitna.

Kao što sam već ranije napomenuo cyber prostor je i zamišljen kao virtualna replika stvarnosti i da bi se to postiglo niz je mehanizama kojima se prikupljaju podaci o subjektima koji operiraju u odnosnom prostoru (Stanfield, D., Beddoe, L., Ballantyne, N., Lowe, S., Renata, N. 2017: 45). Veoma sofisticirane naučne metode su primijenjene da bi stvarna osoba prihvatila i svoj virtualni identitet kao nedjeljiv od njegove ličnosti. Različite statističke, bihevioralne, psihološke, sociološke analize osiguravaju „istinitost" virtualne stvarnosti . Dakle, postojanje mehanizama koji u realnom vremenu prikupljaju podatke o svakom korisniku i stvaraju procjene o njegovim budućim obrascima ponašanja su sastavni dio sistema na kojima je uspostavljen cyber prostor. Podaci koji se dobiju na ovaj način mogu biti zloupotrebljeni od strane, u našem slučaju, terorista za „nagovaranje" osoba da urade nešto što bez sistematskog i ciljanog uvjeravanja ne bi uradili (Wise, J. B., O'Byrne, W. I. 2015: 404). Ne radi se o prostom nagovaranju, jer većina ljudi instinktivno prepoznaje takvu vrstu komuniciranja kao negativnu i stvara otpor prema njoj. Nagovaranje u ovom smislu postoji kao zagovaranje određenog ponašanja i projiciranje vlastitog motiva kao zajedničkog cilja, što rijetko nailazi na bilo kakav otpor od strane onih koji su meta ovakvih indoktrinacija (Huang-Horowitz, N. C., Freberg, K. 2016: 200). Zagovaranje podrazumijeva i poseban identitet zagovaratelja. U jednom slučaju zagovaratelj ne krije

svoj politički motiv i poziciju zbog kojih traži „pomoć" jer slušaoci mogu da se identificiraju sa njegovim statusom i razlozima za djelovanje posebno ako se poziva na organske ideje kao što su religija, rasa, etnička pripadnost itd. (Gunduz, U. 2017: 87). Sa druge strane kada je u pitanju publika koju nije moguće pridobiti na osnovu organskih ideja, zagovaratelj će se identificirati sa tom publikom oponašanjem njih samih i izražavajući zabrinutost za probleme u njihovom društvu pozivajući ih na akciju za promjene (Davis, J. L., Jurgenson, N. 2014: 479). U zadnjem slučaju pravi politički motiv je maskiran drugim političkim motivom koji se nalazi kod ciljane grupe. Grupa ili pojedinac može poduzimati terorističke aktivnosti iz razloga koji nemaju veze sa razlozima onoga koji ih potiče na djelovanje. U ovom slučaju je bitna posljedica, bez obzira što politički motiv ostaje skriven.

Cyber prostor je samo sredstvo i mjesto dogovora za izvođenje terorističkih napada, tako da se opet vraćamo na početak i tvrdnju da cyber terorizam nije poseban oblik terorizma. Važnost ovog pojma je medijski kreirana a sve ono što se pripisuje kao mogućnost cyber prostora se zasniva na identificiranim nezadovoljstvima pojedinaca i grupa koje egzistiraju u realnom društvu (Leeds-Hurwitz, W. 2009: 892).

Djelovanje u cyber prostoru je moguće nadzirati i identificirati nosioce negativnih aktivnosti. Specijalizirani sistemi i obučeni kadrovi itekako su prisutni u cyber prostoru i aktivno rade na otkrivanju nezakonitih aktivnosti i onesposobljavanju njihovih nosioca terorizma (Beggs, C. 2010: 57).

Dodatno, svaka država vodi određene baze podataka o svojim građanima i raspolaže nizom podataka o njihovim sposobnostima. Pored toga, svaka država, identificira i analizira sigurnosne probleme i rizike koji su prisutni unutar njenih granica (Abazović, M. 2012: 15). Naučnim pristupom je svakako moguće provoditi društvene projekte koji će kreirati svijest u društvu o mogućim načinima vrbovanja i iskorištavanja pripadnika društvene zajednice. Država treba da ima jasnu predstavu o zadovoljstvu građana načinom alociranja društvenih resursa i radi aktivno na povećanju tog zadovoljstva što će svakako imati pozitivan efekt u smanjenju mogućnosti vrbovanja pripadnika vlastitog društva od strane terorista u postizanju nekih njihovih političkih ciljeva, ali će doprinijeti općoj otpornosti zajednice na bilo koju vrstu negativne indoktrinacije koja bi za posljedicu mogla imati ljudske žrtve i materijalnu štetu (Christensen, T. 2019: 19). Ovakvo stanje je ideal, ne postoji društvo u kojem su svi njegovi članovi zadovoljni, pa se mora aktivno raditi kako na otkrivanju, kako, onih koji potiču na terorizam, tako i onih koji bi mogli biti izvođači terorističkih aktivnosti. Kontinuirane naučne analize i istraživanja u oblasti terorizma su jedan od ključnih mehanizama ove borbe, ali pored toga i izgradnja institucija koje će voditi računa o subjektima koji su identificirani kao potencijalni izvršioci terorističkih aktivnosti. Svako društvo ima dovoljno kapaciteta da se zaštiti od terorizma samo je pitanje da li postoji svijest i volja kod nosioca političkih funkcija da se aktivno posvete izgradnji sigurnog društva i zajednice uspostavljene na povjerenju, poštovanju ljudskih prava, neosporivim kolektivnim identitetima i jakom i efikasnom socijalnom modelu.

Mogućnosti vs nemogućnosti

Nauka, ni u kom slučaju, ne smije biti pod utjecajem bilo kakvih argumenata koji nisu produkt primjene naučne metodologije. Ovo je posebno važno kada govorimo o političkim utjecajima pod koje često potpadaju naučnici. Drugo, naučnici svojim radom moraju ponuditi odgovore kojima se objašnjava problem i nude konkretna rješenja. Nije nauka samo u identificiranju prijetnji i rizika nego u iznalaženju efikasnog odgovora, tek tu dolazi do izražaja stvarna priroda nauke. Novo doba, ovo temeljeno na tehnologiji dalo je zamaha mašti ljudi koji nauku poznaju posredno, a ustvari se ne bave naukom direktno. To su oni ljudi koji logiciraju određene scenarije a da ih naučno ne potvrđuju. Svjedoci smo niza takvih zahvata, posebno u filmskoj industriji gdje je urađeno mnogo na stvaranju kulta ličnosti hakera koji su svemoćni i raspolažu znanjima koja se mogu zloupotrijebiti i svijet dovesti do propasti. Kao što smo već ranije rekli, važno je da naučnici prave razliku između naučne fantastike i nauke. Ne zaboravimo da je i cyber okruženje produkt nauke i zakonitosti koje je vrlo teško zaobići, bez obzira na uvriježeno mišljenje.

Sistemi koji su esencijalni za funkcioniranje društava ili sistemi čije uništenje ili zaustavljanje bi izazvalo teške posljedice su zaštićeni od bilo koje vrste cyber napada. Tehnologija koja je potrebna da bi ugrozila ovakve sisteme je preskupa i pod striktnim nadzorom vlada država koje bi mogle biti meta takvog napada. Sa druge strane stručnjaci koji posjeduju znanja za izvođenje ovakvih napada su također poznati. Specifična znanja o načinu funkcioniranja ovih sistema poznata su ograničenom broju ljudi, a sami ti ljudi su također, poznati agencijama za provedbu zakona ili agencijama za drugu namjenu. Dakle, mit je haker koji sa laptopom upada u obrambeni sistem npr. SAD. U slučaju da se desi neka situacija sličnog obima, izvršioci se vrlo brzo mogu otkriti i to sa aspekta potrebne tehnologije za takvu aktivnost ili fizičkog pristupa sistemu. U odnosnom slučaju vrbovana je osoba koja ima pristup i znanje, a nije u pitanju poseban fenomen terorizma. Zašto bi osoba pristala da sabotira sistem koji osigurava funkcioniranje nekog društva, iako joj je društvo dalo povjerenje da upravlja tim sistemom, je pitanje za drugu vrstu analize. Društva kroz svoje mehanizme socijalizacije i usvajanja pozitivnih normi od strane pojedinaca i grupa trebaju stvarati svijest o društvenim vrijednostima koje svi pripadnici tog društva percipiraju kao pozitivne. Bez ovakvog pristupa uvijek postoji prostor za nezadovoljstvo, pa čak i kod pojedinaca koji upravljaju veoma osjetljivim sistemima. Dakle, postoji prostor za manipulaciju od treće osobe kojoj u danom trenutku odgovara da je određeno društvo pogođeno posljedicama krize.

Zaključak

Fenomen cyber terorizma je više propaganda nego je stvarna pojava u pitanju. Postoje specifičnosti koje ostavljaju prostora da se govori o posebnom pojavnom obliku, ali stvaranje nove nauke je bespotrebno. Sa aspekta nauke, jasno je da, treba uvažiti interdisciplinarnost u borbi protiv zloupotrebe tehnoloških dostignuća ali isto tako neizostavan je i zahvat društvenih nauka u zaokruživanju strategije suprotstavljanja ovom načinu pripremanja terorističkih napada. Mnogo je informacija u cyber okruženju koje na neki

način mogu biti iskorištene u planiranju napada, identificiranju izvršioca, potrebnih resursa za određene aktivnosti itd. Međutim, nadzorom takvih informacija i identificiranjem osoba koje se interesiraju za specifične resurse i tehnologije iskoristive za izazivanje štete u nekom društvu aktivno se mogu spriječiti nedozvoljene aktivnosti. Ne smije se zaboraviti da terorizam ima političku pozadinu, koja ne mora biti u interakciji između lokalnih aktera, već zainteresirana strana dolazi iz druge države i terorizam koristi za postizanje svojih vanjsko-političkih ciljeva.

I na kraju opet se vraćam na tvrdnju da kada otkrijemo politički motiv u određenoj terorističkoj aktivnosti u mogućnosti smo da formuliramo adekvatan odgovor i aktiviramo efikasne mehanizme zaštite određene zajednice koja je meta takvih aktivnosti.

Literatura

1. Ashforth, B. E., Schinoff, B. S., Rogers, K. M. (2016). "I identify with her," "I identify with him": Unpacking the dynamics of personal identification in organizations. Academy of Management Review, 41.
2. Babić, Vladica (2009). Kompjuterski kriminal, Sarajevo: Rabic.
3. Bara, Danijel (2015). Uloga cyber-osiguranja u upravljanju i prijenosu rizika cyber- sigurnosti, Opatija: ZBORNIK RADOVA S MEĐUNARODNE ZNANSTVENO-STRUČNE KONFERENCIJE Dani hrvatskog osiguranja.
4. Beggs, Charles (2010). Safeguarding Infrastructure Assets from Cyber-terrorism, London: Lambert Academic Publishing.
5. Chen, Jinjun (2014). Special Issue: Dependable and Secure Computing, Journal of Computer and System Sciences vol. 80, London: Elsevier.
6. Choo, Kim-Kwang Raymond (2011). The cyber threat landscape: Challenges and future research directions, Computers & Security, Volume 30, Issue 8, London: Elsevier
7. Christensen, Tom (2019). Organizing for Societal Security and Crisis Management: Governance Capacity and Legitimacy, London: Springer.
8. Chu, S. C., Lien, C. H., Cao, Y. (2018). Electronic word-of-mouth (eWOM) on WeChat: Examining the influence of sense of belonging, need for self-enhancement, and consumer engagement on Chinese travellers' eWOM. International Journal of Advertising.
9. Davis, J. L., Jurgenson, N. (2014). Context collapse: Theorizing context collusions and collisions. Information, Communication & Society, 17.
10. Gordon, Sarah (2002). Cyberterrorism?, Computers & Security, Volume 21, Issue 7, London: Elsevier.
11. Guegan, Jerome (2019). (Social) Identity and Creativity in Virtual Settings: Review of Processes and Research Agenda, The Palgrave Handbook of Social Creativity Research. London: Pelgrave.
12. Gunduz, U. (2017). The effect of social media on identity construction. Mediterranean Journal of Social Sciences, 8 (5).
13. Held, David (1999). Global Transformations: Politics, Economics and Culture: Cambridge: Polity Press.
14. Huang, Lin (2011). Masquerade detection using profile hidden Markov models, Computers & Security, Volume 30, Issue 8, London: Elsevier.
15. Huang-Horowitz, N. C., Freberg, K. (2016). Bridging organizational identity and reputation messages online: A conceptual model. Corporate Communications: An International Journal, 21.
16. Jang-Jaccard, Julian (2014). A survey of emerging threats in cybersecurity, Journal of Computer and System Sciences vol. 80, London: Elsevier.
17. Jin, Y., Liu, B. F., Austin, L. L. (2014). Examining the role of social media in effective crisis management: The effects of crisis origin, information form, and source on publics' crisis responses. Communication Research, 41.

18. Karapanos, E., Teixeira, P., Gouveia, R. (2016). Need fulfillment and experiences on social media: A case on Facebook and WhatsApp. Computers in Human Behavior, 55, 888-897.
19. Kovačević, G., Smajić, M., Ahić, J., Korajlić, N. (2013). Novi koncept razumijevanja odnosa sigurnosti i politike, Policija i sigurnost, godina 22. broj 2/2013. MUP HR, Hrvatska, str. 236 – 248.
20. Kovačević, G., Alispahić, B., Korajlić, N. (2015). Nastanak i razvoj krize u 21. solјeću, Veleučilište Velika Gorica – Zbornik radova, Hrvatska, str. 103 – 113.
21. Leeds-Hurwitz, W. (2009). Social construction of reality. In Littlejohn, S., Foss, K. (Eds.), Encyclopedia of communication theory. Thousand Oaks, CA: SAGE.
22. Lehti, L., Kallio, J. (2017). Participation in an online social policy discussion: Arguments in focus. Discourse, Context & Media, 19.
23. Marwick, A. E., Boyd, D. (2011). I tweet honestly, I tweet passionately: Twitter users, context collapse, and the imagined audience. New Media & Society, 13.
24. Stanfield, D., Beddoe, L., Ballantyne, N., Lowe, S., Renata, N. (2017). Critical conversations: Social workers' perceptions of the use of a closed Facebook group as a participatory professional space. Aotearoa New Zealand Social Work, 29 (3).
25. Sudweeks, Fay (2001). Culture, Technology, Communication - Towards an Intercultural Global Village, New York: Sunny Press.
26. Weimann, Gabriel (2004). Cyberterrorism: How Real is the Threat?, Special Report, United States Institute of Peace.
27. Weimann, Gabriel (2019). The Influentials: People Who Influence People, New York: Sunny Press.
28. Wise, J. B., O'Byrne, W. I. (2015). Social scholars: Educators' digital identity construction in open, online learning environments. Literacy Research: Theory, Method, and Practice, 64.

Kriminalističke teme
Zbornik radova
Godina XIX, Broj 5, 2019.
ISSN 1512-5505

CYBER TERORIZAM KAO NOVI OBLIK RATOVANJA: SEKUNDARNA ANALIZA SLUČAJA „STUXNET“ I TEORETSKI OKVIRI CYBER TERORIZMA

CYBER TERRORISM AS NEW WAY OF WARFARE: SECONDARY CASE ANALYSIS OF “STUXNET” AND THEORETICAL APPROACH TO CYBER TERRORISM

Stručni rad

Emir Muhić[172]

SAŽETAK

Inspiracija za rad i problem (i) koji se radom oslovljava (ju): Dolaskom u novu eru rapidnog razvoja informacionih sistema i tehnologija i neokolonijalnih težnji i borbe za resurse dolazi do evolucije terorizma koji poprima nove nenasilne ali jednako ubilačke oblike. Napadi i diverzije na informacione sisteme vlada ili nuklearnih istraživačkih centara (primjer Irana) predstavljaju novi oblik ratovanja koji zamjenjuje konvencionalno oružje i seli se iz prirodnog u digitalno okruženje. Novi frontovi pomjeraju granice društvene etičnosti i otvaraju vrata novim malicoznim oblicima ljudskog ponašanja.

Ciljevi rada (naučni i/ili društveni): Rad pruža uvid u oblike i načine gerilske i paravojne borbe protiv uspostavljenih državnih i nacionalnih sistema. Rat protiv teorizma nije dobijen, on je promijenio samo formu, ali je suština ostala ista te kao takav još uvijek predstavlja značajnu prijetnju društvu. Rezultati mogu poslužiti kao smjernice i uvidi u događanja u skorijoj budućnosti koja će postati tehnološki naprednija, samim time i ranjivija.

Metodologija/Dizajn: Istraživanje je deskriptivno te će predstavljati sekundarnu analizu i pregled događaja koji su klasifikovani kao rad obavještajnih agencija i pojedinaca u domeni elektronskog ratovanja i uspostavljanja političkih pritisaka na druge regionalne i globalne aktere.

Ograničenja istraživanja/rada: Sam terorizam predstavlja dinamičnu kategoriju čiji se elementi kreću na političkom spektru od borbe za slobodu do opravdanog preventivnog napada. Jasna i tačna klasifikacija svakog od događaja ima notu favorizovanja i osuđivanja aktera što može ući u domen političke korektnosti i nacionalne favorizacije određenih subjekata. Rad predstavlja hipotetički okvir događaja koji se mogu desiti, ali nisu uslovljeni niti direktno vezani za trenutnu političku klimu.

Rezultati/Nalazi: Rezultati prezentirani u radu predstavljaju predviđanje budućih događaja koji nastaju kao rezultat anarhije cyber prostora i međusobnog obavještajnog rata državnih i paradržavnih aktera u borbi za dominaciju nad globalnom politikom. Multipolaritet i neravnomjerna raspodjela snaga i moći bilo državnih ili paradržavnih

[172] Student FKKSS, emirmuhic@fkn.unsa.ba

aktera predstavlja značajnu opasnost za narušavanje krhkog mira i relativne sigurnosti zemalja prvog svijeta koje kao kolonizatori porobljavaju ostatak zemaljske kugle sigurni da neće doći do retribucije.
Generalni zaključak: Ranjivost cyber prostora omogućava različitim akterima da djeluju protiv nacionalnih i državnih sistema kao primarnih meta koje omogućavaju brz i efikasan povrat informacija o uspješnosti napada. Pritisci nastali od strane terorističkih organizacija i njihovog obavještajnog sistema na države ili vlade imaju poguban karakter jer se u pitanje dovodi nacionalni opstanak. Promijenjen je samo front djelovanja, od postavljanja bombi u tržne centre u postavljanje virusa i malware programa u nuklearna postrojenja, hidrocentrale i finansijske sisteme.
Opravdanost istraživanja/rada: Radom su prikazani mogući elementi i načini izvršenja terorističkih aktivnosti koji mijenjaju modus operandi i prelaze na društveno i nacionalno opasnije akte poput rušenja berzi, diverzija električne mreže, uništenja nuklearnih reaktora i pristupa tajnim informacijama na primjeru napada na iranska nuklearna postrojenja.

Ključne riječi
cyber napadi, cyber terorizam, rat, teroristička organizacije, zastrašivanje

ABSTRACT
Reason for writing and research problem (s): New age of rapid evolution of information systems and technology and neocolonial aspirations and struggle for resources leads to the evolution of terroirsm that takes new form, non-violent but equally deadly. Attacks and diversions in government information systems or nuclear research centers (eg Iran) represent a new form of warfare that replaces conventional weapons and moves from a natural to a digital environment. New fronts are pushing the boundaries of social ethics and opening the door to new malicious forms of human behavior.
Aims of the paper (scientific and/or social): The paper provides insights into new ways of guerrilla and paramilitary struggle against established state and national systems, the war against terrorism was not won, it changed only form but the essence remained same, and as even more represents a significant threat society. The results can serve as guidelines and insights into what will happen in the near future, which will become more technologicaly advanced, but in same time more vulnerable.
Methodology/Design: The research is descriptive and will present a secondary analysis of events that are classified as a work of intelligence agencys and subjects in the domain of electronic warfare and the establishment of political pressures on other regional and global actors.
Research/Paper limitation: Terrorism itself represents a dynamic category of all elements that move on the political spectrum from struggle for freedom to a justified preventive attack. The clear and accurate classification of each individual act has favoritizations and judgments of actors that can enter into the domain of political correctness and national favoritisation of certain subjects. The paper presents a hypothetical framework of acts that can happen but are not conditioned or directly related to the current political climate.
Results/Findings: The results presented in the paper shows future events that can arise as a result of the anarchy of cyber space and the mutual intelligence wars of the state and paramilitary actors in the struggle for domination of global politics. Multipolarity and uneven distribution of power of state or parastatal actors, poses a significant risk

of disturbing the fragile peace and relative security of the countries of the first world, which, as colonizers, enslaved the rest of the world while not anticipating retribution.
General Conclusion: The vulnerability of cyber space allows different actors to act against national and state systems as primary targets that enable fast and efficient return of informations on the success of the attack. The pressures incurred by terrorist organizations and their intelligence systems on hostage states or governments have a devastating character because national survival is in question. Only weapons have been changed, from planting bombs at shopping malls to setting up viruses and malware programs to nuclear plants, hydroelectric power stations and financial systems.
Research/Paper Validity: The paper presents possible elements and ways of committing terrorist acts that change modus operandi and switch to socially and nationally dangerous acts such as destroying stock exchanges, electricity diversion, destruction of nuclear reactors and access to classified information shown as example on Iranians nuclear plants.

Keywords
cyber attacks, cyber terrorism, war, terrorist organizations, intimidation

1. UVOD

Terorizam u novom milenijumu je svakodnevno prisutan, te u jednu ruku postaje svakodnevnica. Teroristički napadi postaju novi način izražavanja političkih stavova i vrijednosti svih ekstremnih skupina, lijevih i desnih, religioznih i kriminalnih. Za vrijeme hladnog rata i bipolariteta svijet je strahovao od napada ICBM-ovima sa nuklearnim bojevim glavama. Novo, cyber doba je zamijenilo barbarske i „prljave" nuklearne projektile sa dosta sofisticiranijim i perfidnijim načinima borbe u kojima je napadač anoniman, djeluje bez emocija i za novčanu naknadu.

Cyber kao pojam se pojavljuje ekspanzijom kompjutera i označava kompjuterske mreže ili virtuelni prostor. Dominacija cyber prostora u novom milenijumu je označila početak nove silikonske ere, ere čiji frontovi se ne nalaze u poljima, ravnicama ili šumama, nego u novom neopipljivom i metafizičkom svijetu- svijetu 0 i 1.

Prema definiciji FBI-a terorizam se definiše kao nezakonita upotreba sile ili nasilja nad osobama ili vlasništvom, kako bi se zastrašila ili na nešto prinudila vlast, civilno stanovništvo ili neki njihovi segmenti radi postizanja političkih ili socijalnih ciljeva (Coady & O´Keefe, 2004). Način zastrašivanja u novom dobu je putem virusa i malware programa koji vrše pritisak na određene dijelove društva kako bi ih potčinili i nametnuli svoju volju. Prema Šmitu (1983) terorizam je metod ponovljenih akcija, nasilja koji podstiče uznemirenost; koriste ga polutajni pojedinci, grupe ili državni činioci, zbog idiosinkrazijskih, kriminalnih ili političkih razloga, gdje nasuprot atentatu neposredni ciljevi nasilja nisu i glavni ciljevi. Tomaševski (1983) navodi da se pod pojmom terorizma obuhvataju različiti akti nasilja i ugrožavanja ljudskih prava i ljudskih života, kao i javnih, odnosno zajedničkih, individualnih dobara. Shodno tome, nasilje i prijetnje po ljudski život pronalaze svoje

mjesto i u cyber domeni, koja uticajem na određene bitne objekte i faktore društva ugrožava živote ljudi.

Kada govorimo o novoj eri terorizma i razvoju informacionih tehnologija moramo pomenuti ekstenzivnu evoluciju interneta te razvoj industrijskih kapaciteta i kritične infrastrukture širom svijeta. Internet kao čudo 20. stoljeća je sada poprimio novi oblik, oblik svakodnevnice kako u privatnom tako i u javnom sektoru, a ubrzani razvoj tehnologija i industrije uporedo prati i razvoj interneta. Korelacija između intrerneta i kritične infrastrukture zasniva se na stvaranju, prijemu i protoku informacija koja je neophodna za funkcionisanje kritične infrastrukture koja koristi kompjuterske sisteme spojene na internet (Catrantzos, 2009). Osjetljivost podataka i ranjivost samog sistema kojeg koriste subjekti kritične infrastrukture predstavljaju ključni faktor zaštite od cyber napada od strane terorističkih organizacija. Evolucija terorističkih organizacija u domenu elektronskog ratovanja predstavlja značajnu prijetnju nacionalnoj sigurnosti bilo koje države i nacije. Sama kritična infrastruktura predstavlja stvar nacionalne i javne sigurnosti i ekonomske stabilnosti koja proizilazi iz njenog funkcionisanja. Krah u domenu kritične infrastrukture predstavlja značajnu pogubnost za samu državu i uspostavlja hijerarhijsku strukturu između države i terorističke organizacije koja je izvela napad i stvara stanje opće panike koja je multiplicirana prestankom rada elemenata kritične infrastrukture. Loša prevencija i zaštita kritične infrastrukture od malicioznih antisocijalnih elemenata može prouzrokovati novi elektronski 11. septembar gdje bi cyber napadom posebni elementi industrije ili infrastruktura bili neutralizovani i uništeni, a društvom bi zavladao strah, histerija i panika. Slučaj iz Irana 2010. godine i moć Stuxnet virusa, ali i drugih malicioznih programa predstavlja sve bližu i bližu budućnost za svijet koji je potresen stalnim ratovima i krizama koje su vjerovatna uvertira za treći svjetski rat između azijskih, evropskih i američkih aktera koji su u trenutnom trgovinskom i ekonomskom ratu potpomognuti industrijskom špijunažom.

Cyber terorizam kao novo moćno oružje u rukama svjetskih aktera predstavlja novi oblik političke prinude i oblik proxy ratovanja. Nekonvencionalni oblici ratovanja predstavljaju efikasniji način vođenja borbe između suprostavljenih strana. Ekonomski, cyber ili drugi vidovi ratovanja omogućavaju zaraćenim stranama da prikažu prividno stanje mira i spriječe socijalne kolapse dok se iza kulisa odigravaju presudne bitke za opstanak nacija i država.

2. Analiza Stuxnet napada na iranska nuklearna postrojenja

Proxy ratovi vođeni između Irana i ostatka pro-zapadno orjentiranih država koje su stale uz SAD su kulminirali slučajom Stuxnet. Malware koji je pogodio iranska nuklearna postrojenja je otovorio vrata novog fronta koji za razliku od konvencionalnog ratovanja ne koristi „primitivnu tehniku" poput tenkova, aviona i pješadije nego kompjuterske kodove. Specijalno dizajnirani programi omogućavaju napadaču da elektronskim putem izvršava napade na kritičnu infrastrukturu udaljenu hiljadama kilometara i obezbjeđenu svim mogućim fizičkim oblicima zaštite. To se upravo i desilo iranskom postrojenju u Natanzu koje

je bilo „žrtva" takovog jednog programa nazvanog Stuxnet koji usporio iranski nuklearni program i odgodio planove za obogaćivanje uranijuma namjenjenog za vojne svrhe.

2.1. Novi cyber front

Tokom 2010. godine, po prvi put iranski inžinjeri su otkrili da su uzroci stalnih kvarova i uništenja centrifuga za obogaćivanje uranijuma rezultat kompjuterskog koda, odnosno uzrok je bio malware zvani Stuxnet. Udar na kritičnu infrastrukturu poput nuklearnih postrojenja za obogaćivanje uranijuma, elektrana ili berzi je rezultat nedovoljne zaštite i propusta u samim sistemima sigurnosti i nadzora. Propusti vezani za sistem sigurnosti iranskih postrojenja su omogućili odlaganje iranskih planova za obogaćivanje uranijuma, ne značajno, ali ipak ranjivost kritične infrastrukture je još uvijek na izrazito visokom nivou. Kritična infrastruktura u ovom slučaju je postala žrtva zlonamjernih programa koji su iskoristili dizajnerske propuste postrojenja i sigurnosne propuste koji se tiču ljudstva što direktno implicira na moć novog cyber oružja koje je u mogućnosti da djeluje bilo gdje bilo kada i nanese značajnu štetu. Žrtve ovakvih malicioznih programa mogu postati bilo koji elementi kritične infrastrukture poput termo/hidro elektrana, bankovnih sistema, telekomunikacijskih sistema, saobraćajnih sistema i mnogih drugih elemenata koji su neophodni za svakodnevno i sigurno funkcionisanje društva i prekidi u radu kritične infrastrukture bi imali značajan udar na svakodnevni život građana (US Department of Homeland Security, 2019).

2.2. Arhitektura postrojenja

Kada govorimo o industrijskim postrojenjima pažnju trebamo obratiti na sami dizajn i funkcionisanje postrojenja kroz *Industrial Control System* (ICS). ICS predstavlja kombinaciju kontrolnih komponenti koje usklađeno djeluju u ostvarivanju industrijskog zadatka (Stouffer, Pillitteri, Lightman, Abrams, & Hahn, 2014). Kontrolne komponente od kojih se ICS sastoji su hardwareske i softwareske komponente, odnosno fizički elektronski uređaji i programi koji kontrolišu rad elektronskih uređaja. Uloga ICS-a u kritičnoj infrastrukturi je reguliranje struje, vode, otpadnog materijala, hemikalija, transporta materija etc (Stouffer i sur. , 2014).

U slučaju iranskih postrojenja vektor napada se sastojao iz dva dijela, kompleksnog i jednostavnog, kompleksni napad je imao za zadatak povećanje pritiska u centrifugama za obogaćenje uranijuma, dok je jednostavniji napad za zadatak imao povećanje brzine rotacije samih centrifuga (Langer, 2013). Iz navedenog zaključujemo da je Stuxnet imao dva zadataka usklađena u uništavanju centrifuga, ali na dva različita načina što možemo protumačiti kao failsafe mehanizam, ukoliko jedan napad zakaže, drugi ostaje da dovrši posao što je strategija za novi napad ukoliko bi prvi bio otkriven i zaustavljen.

Jedan od faktora uspješnosti izvršenja napada je bila i upotreba zastarjele tehnologije koju je Iran koristio u nuklearnim postrojenjima, naime upotrijebljena tehnologija datira

iz 60-ih i ranih 70-ih godina 20. vijeka koju je Iran kupio od pakistanskog nuklearnog trgovca Abdul Kadir Khana (Langer, 2013). Jedna od značajki tog zastarjelog sistema je uporeba kaskada, odnosno grupiranja centrifuga, 984 centrifuge su bile raspoređene u 6 kaskada odnosno 164 centrifuge po kaskadi (Langer, 2013). Cilj Stuxnetovog napada je bio automatska upotreba Cascade Protection System-a (CPS) koji je djelovao na dva nivoa, centrifugalnom i kaskadnom. Centrifugalni se sastojao od tri ventila za odvajanje koji su se nalazili na svakoj centrifugi, a njihova svrha je izolacija centrifuge koja ima određene probleme dok ostale rade nesmetano (Langer, 2013). Prilikom zastoja više centrifuga UF6 (Uranium hexafluoride) i stvaranja visokog pritiska prilikom čega UF6 prelazi u čvrsto stanje i oštećuje centrifugu, da bi izbjegli negativne posljedice, iranski inžinjeri su ugradili ispušne ventile čime se vrši kompenzacija za visok pritisak u centrifugama (Langer, 2013).

2.3. Modus operandi Stuxneta

Nakon što je izvršena infekcija preko mobilne memorije (USB) Stuxnet preuzeo potpunu kontrolu, a legitimna kontrola od strane inžinjera i sistema se obavljala samo koliko je to Stuxnet dozvoljavao, a u periodu mirovanja malware je dozvoljavao funkcionisanje i input i output signala inžinjera i sistema. Malware je replicirao funkciju kontrolnog operativnog sistema koji je regularno obavljao zadane funkcije, ali je isključen prilikom infekcije. Malware je obavljao funkciju *man-in-the-middle*, odnosno, kada su input i output signali slati od periferne memorije i nazad, ali preko napadnog koda koji je bio pozicioniran u „sredini". Nakon što je aktivirana napadačka sekvenca, malware preuzima kontrolu nad ispušnim ventilima te mjeri proces inputa signala 21 sekundu koju kasnije pušta u konstantu petlju prilikom napada čime prikriva prave input vrijednosti koje se očitavaju u kontrolnoj sobi, a output signali legitimne automatske kontrole nemaju efekta jer su blokirani (Langer, 2013).

2.3.1. Prva faza napada

Prilikom početka prvog procesa napada izolacijski ventili za prve i posljednje dvije faze obogaćenja se zatvaraju čime dolazi do blokade produkta, a UF6 gas se širi po zahvaćenim kaskadama. Preostale centrifuge se izoliraju osim onih koje su u fazi punjenja, te se pritisak u neizoliranim centrifugama povećava što je uzrokovano blokiranjem ispušnih ventila. Napad se okončava kada napadač odluči da je to dovoljno, te se prelazi na drugu fazu.

2.3.2. Druga faza napada

Druga faza napada za cilj ima uništenje rotora centrifuga. Nova verzija virusa koja je infiltrirana na sistem preko USB-a imala je direktni utjecaj na centralni drajverski sistem (CDS). Stuxnet je postao ažuriran novim zakrpama za MS Windows propuste ali i digitalnim certifikatima koji su omogućili legitimno predstavljanje virusa kao drajverskog

softwarea kojeg je nova verzija operativnog sistema Windows prihvatila (Langer, 2013). Propusti koje je virus pronašao odnose se na kontrolu nad centrifugalnim rotorima koji postaju ranjivi prilikom prevelikog ubrzanja. Napadi u drugoj fazi mijenjali su brzinu rotora IR-1 centrifuga sa 63,000 RPM (rotations per minute) na 84,000 RPM u periodu od 15 čime su prouzrokovana određena minorna oštećenja. Kako navodi Langer (To Kill a Centrifuge, 2013) nakon toga isprobana je nova taktika naglog zaustavljanja centrifuga koje su sa 84,000 RPM spuštane na 120 RPM, nakon čega su se ponovno ubrzavale u periodu od 50 minuta pa ponovno zaustavljale što bi proizvodilo značajnija oštećenja. Zbog određenih sistema zaštite ovakvi radikalni manevri od strane Stuxneta su bili zaustavljeni automatski i načinjena šteta nije bila katastrofalna, ali je ipak odgodila završetak programa.

2.4. Razlozi ranjivosti sistema

Kako navodi Lendvay (2016), uslovi koji su trebali postojati da bi program djelovao se odnosi na tri ključna elementa ranjivosti stema, a to su: insajderska prijetnja (Stuxnet je dizajniran tako da ga je potrebno ručno spojiti na računar da bi došlo do infekcije), propusti u sigurnosnoj mreži čime je omogućena infekcija programskih logičkih kontrola i nedostatak jasnih i legitimnih cyber mjera odbrane. Ranjivost iranskih nuklearnih postrojenja se nalazi u velikom broju sabotera i insajdera koji su spremni da iz zbog nekih nepoznatih razloga zaustave razvoj nuklearnog programa. Kritična infrastruktura posjeduje element ranjivosti uzrokovan od strane insajderske prijetnje i loše kontrole i nadzora nad zaposlenim.

U slučaju iranskog postrojenja Natanz, ljudski faktor je odigrao značajnu ulogu, kontrolni sistem nije bio spojen na internet ili neku eksternu vezu, ali je ipak došlo do infekcije koja se jedino mogla desiti manualnim ubacivanjem virusa uz pomoć USB-a. Nadzor nad zaposlenicima i mogućim saboterima je ključni faktor koji je mogao da prevenira infekciju i zaustavi napad, ali nedostatak nadzora i kontrole u slučaju kritične infrastrukture ima pogubne posljedice koje se odražavaju u ekonomskim, proizvodnim i ljudskim resursima. Rudimentarnost cyber sistema zaštite kritične infrastrukture koji je trebao djelovati agresivno prema virusu je zakazao i zahtijeva konstantna unapređenja u tom polju kako bi se proces infekcije zaustavio i stavio pod kontrolu čime bi ostatak ICS-a mogao nesmetano obavljati svoje funkcije.

3. Kritična infrastruktura u cyber prostoru i terorizam

Vanredne situacije predstavljaju jedno od stalnih i učestalih situacija koje u svakom trenutku mogu da pogode kritičnu infrastrukturu te reakcija subjekata na takva stanja mora biti momentalna bilo da se radi o fizičkom ili cyber ugrožavanju te postojanje zaštite je imperativ za opstanak. Zaštita kritične infrastrukture je definisana kao strategija, politika i spremnost da se zaštiti, spriječi, a kada je potrebno i odgovori na napade na ove ključne infrastrukture i sredstva (Lewis, 2006). Kritična infrastruktura obuhvata pojedine

institucije javnog i privatnog sektora, kanale distribucije te mreže osoba i informacija koje garantuju nesmetan i kontinuiran protok ljudi, roba, servisa, usluga, što je ključno za stabilnost ekonomskog i bezbjednosnog sistema zemlje i ima direktan uticaj na nacionalnu bezbjednost, nacionalnu ekonomiju, javno zdravlje, sigurnost stanovništva i efikasnost djelovanja vlasti (Garaplija, 2018).

Simbioza KI i terorizma je od velikog značaja za nacionalnu sigurnost. Konvencionalni oblici terorističkih napada koji odnose desetine i stotine žrtava se ne mogu mjeriti sa novim cyber oblicima napada na KI gdje uspješan napad ostavlja desetine ili stotine hiljada ljudi bez pitke vode, električne energije ili dolazi do zagađenja okoliša hemijskim, nuklearnim ili drugim otpadom te uništenja finansijskog sistema države. Politički cilj koji nosi teroristički akt ogleda se u strahu i pritiscima koji nastaju ugrožavanjem KI čime dolazi do multiplikacije straha kod građana i domaća vlada se stavlja u nepovoljan položaj iz dva razloga - nemogućnost adekvatnog odgovora na napad i pucanje socijalne kohezije. Društveni nemiri potaknuti terorističkim napadima konvencionalnim sredstvima se ne mogu mjeriti sa cyber napadima iz razloga slabe detekcije istih te povjerljivosti informacija koje dolaze iz KI. U slučaju da dođe do defekata u radu KI, te se isti plasiraju kao tehnička greška u radu postrojenja, javno priznanje organizacije koja je izvela napad bi znatno oslabilo povjerenje između države i građana zbog faktora tajnosti od strane državnih tijela koja su pokušala zataškati slučaj. Nesigurnost i nepovjerenje građana bi značajno doprinijelo terorističkim organizacijama u njihovoj integraciji u javnu sferu života kroz sijanje straha čime bi postali de facto gospodari života i smrti, te oni koji formiraju socijalnu sliku društva. Takav jedan napad bi sigurno izazvao lančanu reakciju drugih napada i pojavu sabotera i insajdera koji bi pokušali da postanu pripadnici jedne takve organizacije. Socijalno isključeni pojedinci predstavljaju najbolji materijal za regrutovanje te oni kao *lone wolf* napadači bi žrtvovali i vlastiti život zarad višeg cilja.

Kada govorimo o kritičnoj infrastrukturi, istu definišemo kao infrastrukturu značajnu za određenu zajednicu, čije oštećenje ili gubitak vodi do gubitka isporuke neke usluge koje su prijeko neophodne za normalno funkcionisanje društva. U grupu kritične infrastrukture ubrajaju se telekomunikacije, elektroprivreda, skladištenje i prenos plina i nafte, bankarstvo i finansije, transport, vodosnabdjevanje, hitna služba (uključujući medicinske, policijske, vatrogasne i spasilačke službe) i druge institucije (Garaplija, 2018).

Napadi na kritičnu infrastrukturu mogu biti fizički, upotrebom određenih sredstava sile ili prinude na proizvodni proces ili virtuelni, cyber napad. I jedna i druga vrsta napada zahtijeva i ljudski angažman i djelovanje. Prilikom fizičkog i cyber napada ili ugrožavanja kritične infrastrukture, ljudski faktor igra značajnu ulogu koja se odražava kroz sabotažu, infiltriranje i djelovanje insajdera predstavlja ključni faktor uspješnosti stvaljanja van pogona infrastrukturu. Sabotažu ključnih elemenata infrastrukture obavljaju infiltratori i insajderi. Kada je riječ o infiltratorima, tada govorimo o osobama koje kao članovi neprijateljske organizacije ulaze u redove institucije i kao radnici stječu određena saznanja o ranjivostima sistema i na taj način pokušavaju da ostvare vlastiti cilj (Catrantzos, 2009). Insajderi kao osobe na visokoj hijerarhijskoj poziciji unutar institucije poznaju sve

nedostatke sistema zaštite i ključnih elemenata infrastrukture, ali ih je teže kontrolirati zbog određenih psiholoških faktora poput egocentrizma, te kod njih ne postoji lojalnost određenoj frakciji, ali i shodno tome postoji visoka šansa da planovi budu otkriveni namjerno ili njihovom nepažnjom (Catrantzos, 2009). Kao jedan od primjera insajderske prijetnje imamo cyber napad virusa Stuxnet na iranska nuklearna postrojenja u Natanzu gdje je sam virus ubačen u sistem preko USB-a, te za takvo djelovanje i pristup kontrolnom sistemu je potrebna osoba koja se nalazi visoko na hijerarhijskoj poziciji, koja posjeduje pristup svim nivoima infrastrukture bez stvaranja sumnje drugih zaposlenika.

Uloga insajdera i sabotera kao pripadnika terorističkih skupina ili kao *lone wolf* počinitelja je jedna od bitnijih sigurnosnih pitanja zaštite KI. Osobe koje imaju pristup kontrolnim tačkama i sistemima uz pomoć malicioznih programa i virusa nanose značajne štete radu KI, ali i nacionalnoj sigurnosti, te se stvara klima nepovjerenja između države i naroda.

3.1. Ranjivost kritične infrastrukture

Modernizacija industrije, ostvarena kroz globalizaciju i međunarodnu saradnju, predstavlja dobrobit za razvoj kritične infrastrukture, te se ostvaruje velika nacionalna dobrobit kroz isto, ali se pojavljuju i određeni izazovi i prijetnje u domenu sistema sigurnosti. Nacionalna ekonomska stabilnost i sigurnost ovisi o shvatanju ozbiljnosti internih i eksternih prijetnji na nivou cyber prostora. Udar na industrijski kontrolni sistem određene kritične infrastrukture predstavlja i udar na ekonomski sistem jedne države, što znači da onemogućavanje rada i proizvodnje ostvaruje posljedice i na samu ekonomsku i sigurnosnu situaciju u državi.

Uloga ICS-a u sistemu rada kritične infrastrukture je od visokog značaja, jer u samoj osnovi ICS predstavlja mozak čitave operacije proizvodnje i napad na mozak predstavlja i napad na cjelokupnu kritičnu infrastrukturu koja u tom slučaju prestaje sa proizvodnjom ili dolazi do nepoželjnih posljedica izazvanih od strane malicioznih virusa.

Napadni vektori cyber prijetnji na ICS se odražavaju u dva nivoa, prvi se odnosi na ometanje sistema komunikacija i dijeljenja informacija, a drugi na neovlaštene instrukcije, komande i spuštanje/podizanje alarmantnog praga za pojedine opasne situacije (Stouffer i sur., 2014). Neovlaštene radnje za posljedicu imaju oštećenje, onemogućenje ili gašenje opreme, oštećenje okoline ili ugrožavanje ljudskih života (Stouffer i sur., 2014). Kao primjer imamo centrifuge nuklearnog postrojenja u Nantzu koje su na osnovu neovlaštenih komandi Stuxneta rapidno ubrzavale ili usporavale rotacije ili povećavale pritisak unutar centrifuga čime dolazi do oštećenja istih. Simbioza kritične infrastrukture i ICS-a je izvršena umrežavanjem IT komponenata u postojeći sistem koji je zamjenio fizičku (ljudsku) kontrolu nad određenim mehanizmima i procesima koji se uz pomoć ICS-a obavljaju automatski samo uz ljudski vizuelni nadzor. Integrisanjem ICS-a sa mrežnim sistemima i online servisima stvara veću dostupnost samog sistema eksternim prijetnjama.

Kako navode Borau i Badita (2008) postoje 4 faktora koja doprinose eskalciji modernih prijetnji za ICS:

1. Široka upotreba standardizirane tehnologije sa poznatim ranjivostima,
2. Mrežno spajanje ICS-a sa drugim mrežama,
3. Nesigurna upotreba sistema daljinske kontrole,
4. Široka distribucija tehničkih karakterisitika o ICS-u preko interneta.

Na osnovu modernih prijetnji i jačanja cyber napada i malicioznih radnji, način zaštite kritične infrastrukture je postojanje zatvorenog sistema koji je fizički i cyber odvojen od realnog svijeta što bi kao krajnji cilj imalo stvaranje određenih problema. Problem odvojenosti sistema KI od realnog svijeta i umrežavanja na internet je nepostojanje ili nedovoljan protok informacija. Informacije koje nastaju komunikacijom sa drugim centrima KI i subjektima na terenu kao i informacije koje su potrebne za daljinsko upravljanje su neophodne za rad, te načini zaštite cyber prostora moraju da se prilagode uvjetima u kojim postoje.

Postojanje adekvatnih cyber timova je jedan od imperativa zaštite i opstanka KI u cyber prostoru, upotreba neobrazovanog i neadekvatnog kadra u sistemu zaštite od vanjskih i unutarnjih prijetnji je jedan od otvorenih puteva za narušavanje integriteta KI, ali i društva koje ovisi o njima.

3.2. Cyber zaštita kritične infrastrukture

Kada se govori o zaštiti KI, isto se odnosi u većini slučajeva na fizičku zaštitu postrojenja uz upotrebu ljudstva i tehničkih sredstava da se osigura kontinuiran rad i otklone svi uljezi. Ono šta ja specifično za KI je to što je ista ranjivija u cyber sferi, te su štete prouzročene virusima i malwareima značajnije od fizičke štete. Šteta nastala primjenom sile je lokalizovana i izolirana te teško da u potpunosti zaustavi rad postrojenja. Također, fizička zaštita od uljeza posjeduje i preventivni vid, odnosno zastrašivanje uljeza i sabotera, dok je cyber zaštita apstraktna i nevidljiva. Sama apstraktnost i fizičko nepostojanje cyber zaštite je poziv za mnoge da pokušaju izvršiti određenu vrstu napada na KI. Postupanje pod premisom da KI nije dovoljno zaštićena u cyber sferi i da ne postoje adekvatne sigurnosne mjere može uveliko uticati na učestalost napada. U slučaju da ne postoji adekvatna cyber zaštita, da rukovodstvo štedi na zapošljavanju IT stručnjaka i kupovini nove opreme, KI postaje meta za sve one koji posjeduju dovoljno saznanja o unutarnjim propustima. Osoblje koje nema dovoljno obrazovanja u sferi cyber zaštite je daleko od optimalnog i zadovoljavajućeg stanja za preživljavanje i opstanak KI pod cyber napadima. Nesposobno osoblje također predstavlja značajnu ranjivost za samu KI koja će prvim napadom biti onesposobljena i time dolazi do ugrožavanja i prestanka normalnog funkcionisanja korisnika usluga. Kao primjer toga imamo cyber napade iz 2015. godine na električnu mrežu Ukrajine kad je bez struje ostalo 225,000 korisnika ili kada je 2016. ransomware napao US Medstar te prisilio 10 bolnica da rade bez elektronskih kartona

pacijenata i email sistema (Gallagher, 2016). U 2017. godini Wells Fargo je potvrdio postojanje DoS (denial-of-service) napada koji je 4 dana onemogućio sve online usluge (Pagliery, 2016). Cyber napadi poput onog u Ukrajni ili napada na US Medstar značajno utječu na kvalitetu života korisnika usluga, dok napadi na institucije poput Wells Fargo zadaju i značajan udarac samom finansijskom sistemu institucije, pružanja usluga, ali i postoji direktan udar na krajnjeg korisnika usluga - običnog građanina u vidu straha i nepovjerenja prema instituciji.

Kontrola fizičkih procesa može biti veoma osjetljiva na vremenska zakašnjenja (lag) koja onemogućava enkripciju ili druge sigurnosne mehanizme te kao primjer je vremenski odgovor sigurnosnih sistema u nuklearnim postrojenjima (She & Jiang, 2011). Software koji se koristi za obavljanje industrijskih procesa (ICS) je često zastario, te su njegove ranjivosti poznate napadačima, te softwarske zakrpe ne mogu biti momentalno izvršene zbog verifikacijskih procesa koje moraju biti dovršene kako bi se osiguralo da su sve kontrole nad sigurnosnim funkcijama netaknute ili će sigurnosni update uvesti nove rizike u operacije fizičkih procesa. (Babu, Ijyas, Muneer, & Varghese, 2017).

Cyber sigurnosna zaštite koje se razvijaju i postavljaju mogu ublažiti ranjivosti i prijetnje cyber-fizičkim sistemima (CPS). Odbrambeni mehanizmi kao firewall-i, antivirusni programi i sistemi prepoznavanja uljeza se implementiraju i unapređuju kako bi se onemogućio neodobreni pristutp (Nicholson, Webber, Dyer, Patel, & Janicke, 2012). Implementacija mamaca omogućava odvraćanje uljeza od pravih sistema (Disso, Jones, & Bailey, 2013). Mamci kao vid odbrane i skretanja napada su adekvatno rješenje sve dok napadač ne otkrije prevaru i usmjeri sve svoje snage na pravi sistem. Primitivni i naivni vidovi zaštite poput mamaca i slabih antivirusnih programa ne predstavljaju značajnu prepreku za cyber teroriste koji posjeduju dosta više znanja i materijalno-tehničkih sredstava za izvršenje napada.

4. Cyber terorizam i kritična infrastruktura

Kao što smo već mogli da vidimo u radu, cyber terorizam i kritična infrastruktura su u parazitskoj vezi, cyber terorizam ne bi mogao da postoji bez kritične infrastrukture koju bi iskoristio i napao, ali bez cyber terorizma kritična infrastruktura bi bila opet podložna konvencionalnim oblicima napada i opasnosti poput samoubilačkih ili bombaških napada, frontalnih napada određenih ćelija terorističkih skupina i slično. Specifičnost cyber terorizma se zasniva na podršci od stranih država i vlada koje dolaze u povoljan položaj napadom na određenu kritičnu infrastrukturu u stranoj državi (Metropuolos & Platt, 2019). Prije svega moramo postaviti pitanje koja je razlika između cyber napada i konvencionalnih oblika terorističkih djela (upotreba vatrenog ili hladnog oružja, eksplozivnih ili hemijskih sredstava)? Zašto je jedan oblik napada efikasniji od drugog i koji se ciljevi ostvaruju jednom ili drugom vrstom napada? Efikasnost i razlika između konvencionalnog i nekonvencionalnog terorističkog napada može se ogledati u nanesenoj materijalnoj šteti, izazvanom strahu i ostvarenom političkom cilju.

4.1. Proxy ratovanje

Proxy ratovi trenutno postaju novi trend vođenja globalne politike te u suštini predstavljaju indirektno učestvovanje treće strane u konfliktu koja za cilj ima nametanje vlasitih ciljeva i strategija (Rauta, 2017). Uloga državnih aktera u proxy ratovanju je značajna za izazivanje sabotaža, odnosno terorističkih napada koji služe za destabilizaciju određenih dijelova društva. U vrijeme razvijene elektronike i elektronskog poslovanja, „hakerski poduhvati" brisanje ili izmjene na raznim sajtovima, ubacivanje raznih virusa u računare itd. je sabotaža velikih dimenzija (Alispahić, 2011). Blokada određenih sradržaja na internetu, napadi na uslužne sisteme, bankarski sektor ili berze može da izazove negativne posljedice za ekonomske sisteme neke države što se direktno odražva na sve korisnike tih usluga, te na taj način izaziva socijalne nemire i strah. Cyber terorizam za razliku od konvencionalnih oblika ne upotrebljava standardna sredstva poput oružja i eksploziva za ostvarivanje cilja. Kako Alispahić (2011) navodi, „sabotaže ove vrste ostaju tajne" – niti jedna država ili institucija ne želi priznati da je bila žrtva nekog napada čime bi se kompromitirao njen status. Konvencionalnom oružju upotrijebljenom u napadu veoma lahko se može ući u trag, te se na taj način otkriti odakle oružje potiče, počinitelja, a samim time i nalogodavca, stoga takvi zastarjeli oblici napada više nisu adekvatni za postizanje određenih ciljeva. Teroristčke skupine veoma često imaju političku pozadinu i idejni tvorci takvih organizacija su dio obavještajno-sigurnosnog aparata države iz koje skupina potiče ili neke druge države koja je u „bliskom" odnosu sa državom porijeka terorističke skupine, a samim time je u cilju istim da ostanu neotkriveni. Kao takve, terorističke skupine sa direktnom vladinom pomoći mogu doći u posjed nekonvencionalnog cyber oružja kao što je Stuxnet ili sličan program koji će služiti za ostvarivanje traženih ciljeva.

4.2 Cyber terorizam

Za razliku od „primitivnih" fizičkih i brutalnih terorističkih napada, cyber terorzam ima drugačiju doktrinu i relativno „čišći" modus operandi. Cyber napadi se mogu izvršiti iz bilo kojeg dijela svijeta, potpuno anonimno i efikasno, te ne postoji mogućnost da se izvršitelji zarobe ili predaju, te da se na taj način otkrije stvarna politička pozadina i nalogodavac. Otkrivanje počinitelja cyber terorizma predstavlja komplikovan zadatak, te su izrazito visoke šanse da se počinitelji nikada ne otkriju. Primarni razlog je visoka sofisticiranost i sposobnost počinitelja da vješto sakriju tragove čime se napadi teško predviđaju, otkrivaju i sprečavaju.

Kao pretpostavku možemo imati da su cyber teroristi u najvećem slučaju vrsta paraobavještajnih službi, službi koje usko surađuju sa legitimnim državnim obavještajnim agencijama te primaju direktne naredbe od državnog vrha. U primjeru Irana, uloga državnih aktera i međunarodnih odnosa je od velikog značaja za postojanje i funkcionisanje cyber terorizma. Ono što bi izazvalo osudu međunarodne zajednice poput konvencionalnog terorističkog napada na nuklearna postrojenja, bilo je skriveno u cyber napadu. Cyber (teroristički) napadi koji su usmjereni na kritičnu infrastrukturu dosta su pogubniji kada se govori o nanesenoj šteti koja se mjeri u ljudskim životima, izgubljenoj infrastrukturi,

vremenu i finansijskim sredstvima koja su izgubljena prestankom rada infrastrukture te sredstava koja su neophodna da bi se kritična infrastruktura ponovo reparirala i stavila u pogon. Prednost takvih terorističkih cyber napada na kritičnu infrastrukturu se odražava i u tajnovitosti napada i često sama žrtva i ne zna da je bila meta napada te sami napad može biti karakterisan kao nesretan slučaj ili nepažnja prilikom rukovanja sistemima za kontrolu, ali se može pojaviti i određena organizacija koja će preuzeti krivnju kako bi se „skinula" odgovornost sa očiglednog napadača-državnog aktera. Tajnovitost takvih operacija je cilj uspješnosti u održavanju relativno dobrih odnosa sa susjednim državama i vladama, ali je i u cilju da napad ostane neprimjećen i klasifikovan kao sistemska greška čime se otklanja sumnja na neke od neprijateljski raspoloženih aktera koji bi imali koristi od takih cyber napada.

U slučaju iranskih nuklearnih postrojenja za obogaćivanje uranijuma, Iranci nisu ni bili svjesni da su žrtve cyber napada, a ne slučajnih sistemskih grešaka koje su prouzrokovale disfunkcionalnost centrifuga. Iz primjera vidimo da je bilo potrebno dugo vremena da bi se otkrili pravi uzroci kvarenja centrifuga, ali nije oktriven počinitelj ili nalogodavac, te se samo može nagađati ko stoji iza takvog napada. Efikasnost napada ogleda se u vremenu koji je potrebno da se isti otkrije te šteti koju je isti nanio. Iako šteta može biti minorna, psihološki efekat nad žrtvom (društvom) je dosta značajniji, te stvara ogromne doze nepovjerenja i paranoje unutar same napadnute strukture. Paranoja je u poptpunosti opravdana, svako može postati žrtva cyber terorista.

5. Zaključak

Kritična infrastruktura predstavlja glavnu metu novih oblika terorizma, odnosno, cyber terorizam kao svoju primarnu žrtvu ima sve oblike infrastrukture čije uništenje ili prestanak rada predstavlja opasnost po ljudski život. Primjer centra za obogaćivanje uranijuma u Iranu je jedan od niza cyber napada koji su u početku bili okarakterisani kao sistemska greška ili propust zaposlenika da bi se kasnije ispostavilo da je u pitanju sofisticirani cyber napad. Povezanost kritične infrastrukture sa „vanjskim" svijetom, odnosno internetom, predstavlja prvi i početni korak da ista postane kompromitovana i da se na taj način ostvare uvjeti za izvršenje terorističkog napada. Terorizam kao bolest pronalazi nove načine prilagođavanja okolini, te niti jedna sfera društvenog života nije sigurna od istih. Evolucija terorizma je tek započela. Nadmetanje internacionalnih aktera za dominacijom nad određenim sektorima povlači za sobom i inovacije koje su potrebne za ostvarivanje ciljeva. Cyber terorizam je novus u toj igri te u budućnosti možemo očekivati njegovu evoluciju. Ovisnost o tehnologiji pospješuje viktimizaciju kako običnog puka tako i državnih i nacionalnih sektora i oblasti te pruža plodno tlo za sijanje straha i nemira. Društvo u cjelini postaje nesigurno i zastrašeno „divljanjem" cyber terorista i disidenata, a razlog tome su vulnerabilnost ekonomije, industrije i sigurnosnog sistema koja proizilazi iz dostupnosti i povezanosti istih u cyber prostoru. Napadi na berze utiču direktno na finansijsko stanje društva, uništenje ili zaustavljanje proizvodnih kapaciteta industrije je povezano sa neprilikama ekonomske prirode i nastanka abnormalnosti u društvu, dok pad sigurnosnog sistema države karakteriše isti kao „nesposoban" te u konačnici epidemija

straha i socijalnih nemira je prirodan slijed događaja. Cyber terorizam predstavlja novu eru terora i straha protiv koje se čovječanstvo mora boriti.

6. Literatura

A) Knjige

- Alispahić, B. (2011). Sabotaža. In B. Alispahić, Osnovi metodike rada obavještajno-sigurnosnih službi (p. 117). Sarajevo: Šahinpašić.
- Garaplija, E. (2018). Proces identifikacije, analize i evaluacije rizika kritične infrastrukture u vanrednim situacijama. Sarajevo: Institut za zaštitu od požara i eksplozije.
- Lewis, T. G. (2006). Critical Infrastructure Protection in Homeland Security-Defending a Networking Nation. New Jersey: Wiley-Interscience
- Tony Coady, Michael O´Keefe (2004). Terorizam i pravednost. T. Coady M. O' Keefee, Terorizam i pravednost. Zagreb.
- Primorac, I. (2002). Državni terorizam i protuterorizm. In I. Primorac, Državni terorizam i protuterorizm (p. 62).
- Schmidt, A. (1983). Political Terrorism. In A. P. Schmidt, Polical Terrorism. Amsterdam.
- Tomaševski, K. (1983). Terorizam u suvremenom svijetu. In K. Tomaševski, Izazov terorizma. Beograd.

B) Članci

- Gallagher, S. (2016, april 7). Maryland hospital: Ransomware success wasn't IT Department's fault. Dotupno na: https://arstechnica.com/security/2016/04/maryland-hospital-group-denies-ignored-warnings-allowed-ransomwareattack/, pristupljeno 21.06.2019
- Langer, R. (2013). To Kill a Centrifuge. A Technical Analysis of What Stuxnet's Creators Tried to Achieve. Hamburg: The Langner Group. Preuzeto sa: https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf Pristupljeno: 20.06.2019
- Metropuolos, E., & Platt, J. S. (2019). Global Cyber Terrorism Incidents on the Rise. Dostupno: https://www.mmc.com/insights/publications/2018/nov/global-cyber-terrorism-incidents-on-the-rise.html, Pristupljeno 13.07.2019
- Pagliery, J. (2016, maj 27). Global banking system under attack: What you need to know. Dostupno na: http://money.cnn.com/2016/05/27/technology/swift-bank-hack/ , Pristupljeno: 11.06.2019
- US Department of Homeland Security. (2019, maj 22). CISA. Retrieved from Supporting Policy and Doctrine: https://www.dhs.gov/cisa/supporting-policy-and-doctrine , Pristupljeno 22.06.2019

C) Dokumenti i izvještaji

- Babu, B., Ijyas, T., Muneer, P., & Varghese, J. (2017). Security issues in SCADA based industrial control systems. 2nd International Conference on Anti-Cyber Crimes (ICACC), (pp. 46-51). Abha, Saudi Arabia. Dostupno na: https://ieeexplore.ieee.org/document/7905261, preuzeto 21.06.2019.
- Boaru, G., & Badita, G.-I. (2008). Critical Infrastructure Protection Challenges and Efforts to Secure Control Systems. In B. G.-I. Boaru Gheorghe. Romania. Dostupno na: http://www.codrm.eu/conferences/2008/ProQuestDocuments-2008.pdf, Preuzeto: 15.06.2019
- Catrantzos, N. (2009). No Dark Corners: Defending Against Insider Threats to Critical Infrastructure. Monterey, California: Naval Postgraduate School. Dostupno na: https://calhoun.nps.edu/handle/10945/4656 , Preuzeto 17.06
- Disso, J. P., Jones, K., & Bailey, S. (2013). A plausible solution to SCADA security honeypot systems. 2013 Eighth International national Conference on Broadband and Wireless Computing, Communication and Applications (pp. (pp. 443–448)), New York . Preuzeto sa https://ieeexplore.ieee.org/document/6690926, DOI: 10.1109/BWCCA.2013.77
- Lendvay, R. L. (2016). Shadows Of Stuxnet: Recommendations For U.S. Policy On Critical Infrastructure Cyber Defense Derived From The Stuxnet Attack. Monterey, California: Naval Postgraduate School. Preuzeto sa: https://www.hsdl.org/?view&did=792239
- National Counterintelligence and Security Center. (2018). Foreign Economic Espionage in Cyberspace. Office of the National Intelligence. Dostupno na: https://www.dni.gov/files/NCSC/documents/news/20180724-economic-espionage-pub.pdf, Pristupljeno:17.07.2019
- Nicholson, A., Webber, S., Dyer, S., Patel, T., & Janicke, H. (2012). SCADA security in the light of cyber-warfare. Computers & Security, 31, 418–436. Dostupno na: https://www.researchgate.net/publication/257006726_SCADA_security_in_the_light_of_Cyber-Warfare , Pristupljeno 12.06.2019
- Rauta, V. (2017). Proxy Wars and the Contemporary Security Environment. In P. Macmillan, The Palgrave Handbook of Security, Risk and Intelligence (pp. 99-115). Basingstoke, UK: Palgrave Macmillan,dostupno na: https://www.researchgate.net/publication/318249920_Proxy_Wars_and_the_Contemporary_Security_Environment, pristupljeno: 04.08.2019
- She, J., & Jiang, J. (2011). On the speed of response of an FPGA based shutdown system in CANDU nuclear power plants. Nuclear Engineering and Design, 241, 2280–2287. Dostupno na https://www.researchgate.net/publication/232372822_On_the_speed_of_response_of_an_FPGA-based_shutdown_system_in_CANDU_nuclear_power_plants , pristupljeno: 07.07.2019

- Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M., & Hahn, A. (2014). Guide to Industrial Control Systems Security. Gaithersburg, MD: National Institute of Standards and Technology. Dostupno na: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf , Pristupljeno: 01.08.2019

Kriminalističke teme
Zbornik radova
Godina XIX, Broj 5, 2019.
ISSN 1512-5505

Panel 4

„DIGITALNE“ GENERACIJE: DJECA, MLADI I PSIHOLOGIJA

Kriminalističke teme
Zbornik radova
Godina XIX, Broj 5, 2019.
ISSN 1512-5505

VIKTIMIZACIJA STUDENATA U SAJBER PROSTORU: ISKUSTVA IZ SRBIJE[173]

STUDENTS' EXPERIENCE IN CYBERSPACE: EXPERIENCES FROM SERBIA

Izvorni naučni rad

Mr Ljiljana Stevković[174]
Popović Milica[175]
Doc. dr Kovačević Milica[176]

Sažetak

Inspiracija za rad i problem koji se radom oslovljava: Život savremenog čoveka nezamisliv je bez sredstava savremene tehnologije. Pored nespornih prednosti života u eri digitalizacije, sajber prostor predstavlja ujedno i veoma rizičnu sferu mogućih zloupotreba, manipulacija i različitih oblika viktimizacije. Mladi, kao najbrojniji korisnici sredstava informacione tehnologije u najvećem su riziku kako od njihove zloupotrebe, tako i od viktimizacije u sajber prostoru.

Ciljevi rada (naučni i/ili društveni): Rad ima za cilj predstavljanje dela rezultata istraživanja viktimizacije studenata Univerziteta u Beogradu. Dobijeni rezultati mogu poslužiti kao dobra osnova za identifikovanje negativnih iskustava studenata u sajber prostoru, te osmišljavanje preventivnih strategija u cilju edukovanja studenata i eliminacije njihove sajber viktmizacije.

Metodologija/dizajn: Istraživanje je eksplorativnog karaktera, realizovano primenom kvantitativne metodologije**,** na uzorku od 338 studenata svih nivoa studija na fakultetima iz svih naučnih oblasti Univerziteta u Beogradu.

Ograničenja istraživanja/rada: Ograničenja istraživanja proizilaze iz ograničenje primenjenih tehnika za prikupljanje podataka. Iako nesumnjivo korisne za saznavanje tamne brojke kriminaliteta, anketa o viktimizaciji i sa samoprijavljivanjem nasilja imaju svojih nedostataka, a koji se ogledaju u nespremnosti priznavanja viktimizacije i nasilnog ponašanja, kao i subjektivnosti ispitanika ("greške" u pamćenju, različito percipiranje pitanja od strane različitih ispitanika i sl.)

Rezultati/Nalazi: Rezultati pokazuju da je većina ispitanika doživela neki oblik sajber viktimizacije, te da se u većini slučajeva radi se o višestrukoj viktimizaciji učinjenoj od

[173] Rad je nastao kao rezultat rada autorki na projektu br. 179044 Razvoj metodologije evidentiranja kriminaliteta kao osnova kreiranja efikasnih mera za njegovo suzbijanje, koji finansira Ministarstvo prosvete, nauke i tehnološkog razvoja Republike Srbije, a implementira Fakultet za specijalnu edukaciju i rehabilitaciju. Rukovoditeljka projekta je prof. dr Vesna Nikolić Ristanović.

[174] Fakultet za specijalnu edukaciju i rehabilitaciju, Univerzitet u Beogradu, Viktimološko društvo Srbije, stevkoviclj@gmail.com

[175] doktorand, milicap1986@gmail.com

[176] Fakultet za specijalnu edukaciju i rehabilitaciju, Univerzitet u Beogradu, bucak80@gmail.com

strane nepoznatih osoba. Takođe, ispitanici prijavljuju i viktimizaciju partnerskim nasiljem u sajber prostoru koje se najčešće ogleda u primeni različitih kontrolnih taktika. Istraživanjem je utvrđena povezanost između viktimizacije u realnom životu i sajber prostoru, sa posebnim akcentnom na prediktorskom efektu iskustva nasilne viktimizacije.

Generalni zaključak: Može se zaključiti da su studenti u visokom riziku od sajber viktimizacije različitim pojavnim oblicima, pri čemu su najzastupljeniji oni oblici koji se tretiraju kao teža krivična dela. To ukazuje na potrebu za realizacijom obuhvatnijih istraživanja na uzorku ove kategorije mladih i osmišljavanja njima prilagođenih preventivnih strategija u cilju sprečavanja kako njihove viktimizacije, tako i ispoljavanja kriminalnih ponašanja u sajber prostoru.

Ključne reči

sajber prostor, viktimizacija, studenti, istražvanje, Srbija.

Summary

The inspiration for the paper and the problem that the paper addresses: The life of a modern man is unthinkable without the use of modern technology. Additionally to the undeniable advantages of life in the digitalization era, cyberspace also represents a very risky domain of possible abuse, manipulation and various types of victimization. Young people, as the largest users of information technology assets, are at the highest risk of their misuse and victimization in cyberspace

Aims of the paper (scientific and/or social): This paper aims at presenting a part of research findings which relate to the experiences of victimization of Belgrade University students in cyberspace. The results obtained can serve as a good basis for identifying characteristics of negative experiences of students in cyberspace, and planning preventive strategies aiming to eliminate students' cyber victimization.

Methodology/Design: The research is exploratory in nature, implemented using a quantitative methodology, on a sample of 338 students of all levels of study at faculties from all scientific fields of the University of Belgrade.

Research/paper limitations: The limitations of the research comes from the limitations of the techniques used for data collection. Although undoubtedly, useful for finding out the dark crime figures, victimization surveys and self-report surveys have their limitations, which are reflected in the unwillingness of the respondents to admit victimization and violent behaviour, as well as the subjectivity of the respondents ("mistakes" in memory, different perception of questions by different respondents etc.).

Results/Findings: The results show that more than half of the respondents had the experience of victimization in cyberspace during the studies. Mostly, it was multiple victimization committed by unknown perpetrators. Additionally, respondents reported a cyber IPV victimization, mostly manifested in a form of different control tactics. Correlation between victimization in real life and cyberspace, with particular emphasis on the experience of violent victimization, was also found.

General conclusion: It can be concluded that students are at high risk of different forms of cyber-victimization, with the most prevalent those forms than can be treated as serious crimes. This indicates the need for more comprehensive research on a sample of this category of young people and the development of preventive strategies adjusted to them in order to prevent their victimization and the perpetration of criminal

behaviour in cyberspace as well.

Keywords
cyberspace, victimization, students, research, Serbia.

Uvod

Savremeni svet nezamisliv je bez brojnih blagodeti brzog tehničko-tehnološkog razvoja, među kojima svakako značajno mesto zauzimaju informaciono-komunikacione tehnologije. Danas je gotovo postala praksa da deca i mladi od najranijeg uzrasta poseduju ili bar imaju pristup mobilnim telefonima, tabletima i računarima, pa samim tim i internetu. Za mnoge adolescente savremena tehnologija ima važnu ulogu u njihovom svakodnevnom životu, kroz svakodnevnu upotrebu mobilnih telefona i interneta (Wright, 2015), što potvrđuju i nalazi istraživanja Smith i saradnika (2008), koji su pokazali da je još 2006. godine u Ujedinjenom Kraljevstvu 51% dece uzrasta od 10 godina i 91% dece na uzrastu od 12 godina posedovalo mobilni telefon. Među studentskom populacijom digitalna tehnologija je, pored upotrebno u privatne svrhe, postala i neizostavni resurs za usvajanje novih i proširivanje postojećih znanja tokom studiranja. Uprkos brojnih blagodeti, kao što je to slučaj i u većini drugih oblasti društvenog napretka, moderna tehničko-tehnološka revolucija praćena je i negativnim efektima, među kojima se poslednjih godina govori o različitim oblicima sajber viktimizacije.

Već dugo se u literaturi raspravlja o vršnjačkom nasilju, njegovom obimu, karakteristikama, pojavnim oblicima, faktorima koji na njega utiču, kao i posledicama. Danas se polje interesovanja u ovom domenu širi i na viktimizaciju u sajber prostoru, pri čemu fokus ostaje na mladima školskog uzrasta, što svodi sajber viktimizaciju na „novu" manifestaciju tradicionalnog vršnjačkog nasilja. U tom kontekstu su i shvatanja sajber viktimizacije kao namernog akta agresije usmerenog ka manje moćnom vršnjaku upotrebom elektronskih sredstava poput tekstualnih ili e-mail poruka. Iako oba oblika viktimizacije imaju brojne istovetne posledice, poput anksioznosti, agresije i problema u domenu škole i školskog postignuća, brojni su aspekti u kojima se sajber viktimizacija razlikuje od tradicionalnog vršnjačkog nasilja. Jedan od njih svakako je anonimnost, što smanjuje rizik za učinioca da bude otkriven i sankcionisan, a istovremeno utiče na povećanje straha i osećanje bespomoćnosti kod žrtve sajber vršnjačkog nasilja. Takođe, jedna od bitnih razlika jeste i pristup žrtvi, što neki autori, poput Tennant i sar. (2015) tumače kao mogućnost učestalijih kontakata, imajući u vidu da se sajber viktimizacija može dešavati u bilo koje doba dana i ne zahteva kontakte licem u lice, pri čemu su mogućnosti, odnosno, sredstva izvršenja, a samim tim i povređivanja žrtve, sve dostupnija i brojnija (Kowalski i sar., 2014; Tennant i sar., 2015).

Kada je u pitanju sajber viktimizacija problemi nastaju već pri samom pokušaju definisanja i određenja koja ponašanja obuhvata. Često se o sajber viktimizaciji u širem smislu govori kao o „namernom, štetnom činu primenom elektronskih sredstava kao što su

tekstualne i e-mail poruke i sadržaji websajt-ova" (Ryan i Curwen, 2013: 1; Snakenborg, Van Acker i Gable, 2011: 89). Uže definicije pod sajber viktimizacijom podrazumevaju „voljno i ponovljeno nanošenje ponovljenog zla primenom kompjutera, mobilnih telefona i drugih elektronskih uređaja" (Patchin i Hinduja, 2006), odnosno, „agresivni, nameran čin grupe ili pojedinca korišćenjem elektronskih formi kontakta, ponovljeno tokom vremena i upereno ka žrtvi koja se ne može samostalno odbraniti" (Smith i sar., 2008: 376).

Teškoće definisanja pojma sajber viktimizacije proizilaze iz njenih različitih oblika i mogućnosti odigravanja na različitim „mestima" u sajber porstoru, ali i konstantnog usavršavanja tehnologije, odnosno, potencijalnih sredstava izvršenja. Tako Langos (2012) pravi razliku između *direktne* (privatna komunikacija, na primer, putem tekstualnih poruka) i *indirektne* sajber viktimizacije (u javnom prostoru, poput, na primer, komentara na društvenim mrežama) (Langos, 2012). Sa istraživačkog aspekta posebno je značajna taksonomiju tipova viktimizacije u sajber prostoru koju je kreirao Willard (2007), a koja uključuje: a) *rasplamsavanje* (eng. flaming) - online svađa; b) *uznemiravanje* - ponovljeno slanje poruka uvredljivog sadržaja određenoj osobi; c) *izleti i varanje* (eng. outing and tickery) - pridobijanje nečijih ličnih podataka i njihova elektronska distribucija drugima bez saglasnosti vlasnika; d) *isključivanje* - na primer, blokiranje određene osobe na listi prijatelja, u pričaonici, grupi; d) *impersonacija* - predstavljanje kao žrtva i negativna elektronska komunikacija ili deljenje neadekvatnih informacija sa drugima u ime žrtve; e) *sajber proganjanje* - primena elektronske komunikacije u cilju proganjanja druge osobe slanjem ponovljene preteće neželjene komuniakcije); f) *seksting* - distribucija slika druge osobe sa seksualnom konotacijom bez njenog pristanka (Willard, 2007: 265-267; Kowalski, 2014: 1074).

Sa druge strane, autori poput Corcoran, Mc Guckin i Prentice (2015) ukazuju kako oslanjanje na shvatanja tradicionalnog bulinga u definisanju pojma sajber viktimizacije, što je slučaj u većini definicija, onemogućava uvažavanje brojnih razlika između ova dva oblika. Tako, naglasak na nameri da se nanese zlo u drugi plan stavlja samo iskustvo žrtve (i nenamerni akt može može rezultirati posledicama po žrtvu), dok poistovećivanje sa bulingom sajber viktimizaciju stavlja isključivo u vršnjački kontekst. Imajući to u vidu, Corcoran i saradnici predlažu korišćenje termina *agresija u sajber prostoru*, pod kojim podrazumevaju „svako ponašanje koje podrazumeva primenu informaciono-komunikacione tehnologije, koje je namereno da povredi određenu osobu a koje ciljana osoba želi da izbegne" (Corcoran, Mc Guckin i Prentice, 2015: 253).

Za razliku od pomenutih pristupa definisanju sajber viktimizacije u kojima je fokus na ponašanju učinilaca i posledicama koje takvo ponašanje proizvodi, u kriminološkoj i psihološkoj literaturi dominiraju definicije u kojima je akcenat na procesu viktimizacije, odnosno iskustvima žrtve i prema kojima sajber viktimizacija podrazumena ponižavanje i uznemiravanje od strane drugih osoba putem digitalne tehnologije (Ferdon i Hertz, 2007; Kowalski i Limber, 2007; Topcu, Erdur-Baker i Aydin, 2008; Wolak, Mitchell i Finkelhor, 2007; Ybarra, Diener-West i Leaf, 2007). Tako shvaćena, sajber viktimizacije

podrazumeva disbalans moći između učinioca i žrtve, koji posebno proizilazi iz načina izvršenja, mogućnosti anonimnog, kontinuiranog povređivanja žrtve koja posledice može da trpi i dugo nakon konkretnog postupka učinioca (na primer, dugo nakon što je neovlašćeno online distribuirao fotografije žrtve, ili dugo nakon što je neko o žrtvi online širio laži) (Grigg, 2010).

Predmet ovog rada jeste viktimološki aspekt viktimizacije u sajber prostoru, sa posebnim akcentom na populaciji studenata. U radu je prikazan deo rezultata istraživanja koje je imalo za cilj ispitivanje rasprostranjenosti, karakteristika i faktora koji su u vezi sa viktimizacijom i izvršenjem nasilja u sajber prostoru među studentskom populacijom. Shodno tome, cilj ovog rada je predstavljanje dela rezultata istraživanja koji se odnose na rasprostranjenost i karakteristike viktimizacije u realnom životu i sajber viktimizacije, njihovu povezanost i eventualni prediktorski efekta viktimizacije u realnom životu na izloženost sajber viktimizaciji. Za potrebe ovog rada prihvaćeno je šire viktimološko određenje pojma sajber viktimizacije i modifikovana Willard - ova tipologija pojavnih oblika sajber viktimizacije.

Rezultati prethodnih istraživanja sajber viktimizacije u populaciji studenata

Podaci o rasprostranjenosti i karakteristikama sajber viktimizacije među studentima su retki, imajući u vidu da se mali broj autora i istraživanja bavio ispitivanjem ove pojave u populaciji studenata (npr, Finn, 2004; Walker, Sockman i Koehn, 2011; Avais i sar., 2014; Crosslin i Crosslin, 2014). Prva istraživanja sajber viktimizacije bila su fokusirana na utvrđivanje prevalence, i to primarno na uzorku dece i adolescenata. I danas, većina istraživanja fokusira se na decu i mlade osnovnoškolskog i srednjoškolskog uzrasta, pri čemu se podaci o prevalenci sajber viktimizacije u ovoj kategoriji mladih znatno razlikuju. Tako neki autori iznose podatak da je čak 72% adolescenata uzrasta 12-17 godina bilo izloženo bar jednom incidentu sajber viktimizacije (Juvonen i Gross, 2008). Interesantno je da je zastupljenost sajber viktimizacije među učenicima u odnosu na pol relativno slična (oko 29% devojčica i 23% dečaka), osim u situacijama kada se radi o viktimizaciji sajber seksualnim uznemiravanjem i nasiljem, kojoj je izloženo oko 15% devojčica i 7% dečaka (Zweig i sar., 2013).

Prevalenca sajber viktimizacije među studentskom populaciju varija između 8,6% i 43,3% (Crosslin i Crosslin, 2014; Finn, 2004; Hinduja i Patchin, 2010; Schenk i Fremouw, 2012). Jedna od prvih studija realizovanih na uzorku studenata pokazala je da je prevalenca sajber viktimizacije studenata putem e-mail ili tekstualnih poruku između 10% i 15% (Finn, 2004). Walker, Sockman i Koehn (2011) su utvrdili da je 56% studenata iz njihovog uzorka bilo izloženo napadima preko Facebook-a. Slično, studija realizovana na populaciji studenata u Turskoj, ukazuje da je 55,3% ispitanika bar jednom doživelo iskustvo viktimizacije u sajber prostoru (Dilmac, 2009). Slični nalazi dobijeni su i u studiji sprovedenoj u Pakistanu na prigodnom uzorku od 100 studenata (50 ispitanika i 50 ispitanica) uzrasta između 18 i 24 godine. Ovo istraživanje je pokazalo da trećina ispitanika dozvoljava prijateljima korišćenje ličnih podataka i šifri, te da iako više od polovine njih koristi online

mere bezbednosti (filtriranje, blokiranje, zaključavanje ličnih podataka, albuma i slično), čak 39% nije upoznato sa istima ili ih ne praktikuje. Da su mladi iz ovog istraživanja izloženi riziku od sajber viktimizacije potvrđuje i podatak da više od dve trećine njih deli lične podatke u sajber prostoru, poput adrese i broja telefona, od kojih svega 23% iste deli samo sa poznatim osobama, a ostali i sa nepoznatima (Avais i sar., 2014). Kada je u pitanju iskustvo viktimizacije, 37% ispitanika prijavljuje da je nekada bilo hakovano u online prostoru, dok 23% ima osećaj da su iskusili sajber proganjanje, 29% prijavljuje viktimizaciju lažnim predstavljanjem (impersonacija), a 59% je imalo iskustvo sa širenjem laži ili kleveta u online prostoru. Primanje poruka nasilnog sadržaja prijavljuje 40% ispitanika, dok čak 60% njih ima iskustvo sa upućivanjem uvredljivih reči (*flaming words*) kako putem e-maila i u privatnim komunikacijama, tako i na javnim mrežama. Iskustvo sa menjanjem slika bez odobrenja imalo je 36% ispitanika, pri čemu je tek svaki četvrti ispitanik svoju viktimizaciju prijavio bilo kome, pa makar i administratorima društvene mreže, poput Facebook-a i Twitter-a (Avais i sar., 2014).

Istraživanje realizovano na uzorku od 543 studenata medicinskog fakulteta Univerziteta u Murciji (Španija) ukazalo je na povezanost između sajber i tradicionalnog bulinga. Naime, više od polovine studenata bilo je izloženo zlokobnom zadirkivanju u sajber prostoru (52,7%), oko dve trećine (62,2%) je bilo izloženo tradicionalnom bulingu u istom periodu, dok je 40,7% njih bilo žrtva oba oblika bulinga. Uočene su razlike u zavisnosti od pola ispitanika, u smislu da su studentkinje znatno češće bile žrtve sajber bulinga, a studenti tradicionalnog bulinga. Kao rizični faktori sajber bulinga izdvojeni su ekonomski problemi, dok je prisustvo porodičnih konflikta rizični faktor i za tradicionalne i za sajber oblike viktimizacije (Sánchez i sar., 2016).

Pojedina istraživanja, pored utvrđivanja prevalence i karakteristika sajber viktimizacije, bila su fokusirana i na utvrđivanje korelata sajber viktimizacije. Kao najvažniji korelati izdvajaju se učestalo korišćenje interneta i društvenih mreža, uključenost u sajber buling u adolescenciji (bilo u ulozi žrtve ili nasilnika), nisko samopouzdanje i nisko samopoštovanje (Balakrishnan, 2015; Bossler, i Holt, 2010; Hemphill i Heerde, 2014; Ngo i Paternoster, 2011).

Među različitim autorima ne postoji saglasnost u pogledu toga da li su sajber viktimizaciji više izložene osobe muškog ili ženskog pola. Shodno tome, istraživanje realizovano primenom ankete sa samoprijavljivanjem i ankete o viktimizaciji na uzorku od 267 studenata psihologije u Sjedinjenim Američkim Državama (u nastavku: SAD) nije utvrdilo povezanost između pola i sajber viktimizacije, odnosno pokazalo je da je sajber viktimizacija gotovo podjednako zastupljena kod ispitanika oba pola (Tennant, 2015). Sa druge strane, neka istraživanja ukazuju na postojanje razlika u sajber viktimizaciji između osoba muškog i ženskog pola. Tako Ortega i saradnici (2012) navode da žene češće prijavljuju iskustvo viktimizacije na internetu i upotrebom mobilnih telefona, dok drugi autori ističu da su muškarci češće izloženi pretećim tekstutalnim porukama u kojima je pretnja usmerena na telesni integritet (pretnja fizičkim nasiljem), dok su žene više izložene porukama u kojima se preti napadom na njihovu reputaciju, što je u skladu sa rodnim razlikama

kada su u pitanju tradicionalni oblici viktimizacije (muškarci su češće uključeni u fizičko a žene u emocioanlno nasilje) (Ortega, 2012; Tennant, 2015).

Partnersko nasilje u svakodnevnom životu je rasprostranjen, ozbiljan društveni problem koji pogađa alarmantan broj odraslih osoba globalno. Razvojem tehnologije mogućnosti partnera da demonstrira moć nad partnerkom (i obrnuto) su znatno proširene. Zato i ne iznenađuju podaci istraživanja koji ukazuju da je čak 93% studenata bilo izloženo blažim oblicima sajber partnerskog nasilja, poput vređanja i psovanja, dok 13 % njih prijavljuje ozbiljnije oblike poput pretnji, javnog ponižavanja i slično, pri čemu se ukazuje na povezanost partnerskog nasilja u realnom životu i sajber prostoru (Watkins, Maldonado i DiLillo, 2016; Marganski i Melander, 2018). Istraživanje realizovano primenom online ankete na uzorku od 397 ispitanika starijih od 18 godina u SAD, koji su u trenutku anketiranja bili minimalno 6 meseci u partnerskoj vezi (241 ispitanica i 154 ispitanika), pokazalo je da postoji povezanost između partnerskog nasilja u realnom životu i sajber prostoru, kao i visoka korelacija između viktimizacije i samoprijavljivanja nasilnog ponašanja u sajber prostoru, što, prema autorima, ukazuje na dvosmernost sajber partnerskog nasilja (Watkins, Maldonado i DiLillo., 2016).

Predmet interesovanja istraživača, prvenstveno u SAD, bilo je i sajber proganjanje. Savremene tehnologije se često koriste za praćenje, kontrolu ili uznemiravanje partnera. Shodno tome, studija realizovana u SAD ukazala je na vezu između proganjanja u stvarnom životu i sajber prostoru, dok neki autori, imajući u vidu rapidnu evoluciju tehnologija, upozoravaju na trend povećanja stope viktimizacije sajber proganjanjem (Fraser i sar., 2010, prema Woodlock, 2017). Pri tome, istraživanja ukazuju na podjednaku izloženost studenata oba pola viktimizaciji sajber proganjanjem (Burke i sar., 2011). Istraživanje sajber partnerskog nasilja realizovano primenom fokus grupnog intervjua na uzorku od 39 studenata koledža pokazalo je da postoji visok stepen (zlo)upotrebe informaciono-komunikacionih tehnologija u cilju kontrole partnera - praćenje aktivnosti, uznemiravanje porukama, zastrašivanje (Merlander, 2010). Upravo zahvaljujući savremenoj tehnologiji učinilac ima mogućnost da održi kontrolu, uznemirava i zlostavlja žrtvu čak i u javnom prostoru i bez potrebe da su na istoj lokaciji (Merlander, 2010). Kada je u pitanju seksualno uznemiravanje i seksualno nasilje u sajber prostoru, istraživanja pokazuju da je više od 10% tinejdžera doživelo da njen/njegov partner deli njihove privatne fotografije bez odobrenja, dok je 20% njih dobijalo poruke sa pozivima za uključivanje u neželjene seksualne aktivnosti (Picard, 2007 prema Woodlock, 2017).

Woodlock i sar. (2017) realizovali su SmartSafe studiju u cilju ispitivanja uticaja mobilnih tehnologija (pre svega mobilnih, 'pametnih' telefona koji imaju pristup internetu, GPS i video) na proganjanje žrtava nasilja u porodici. Istraživanje je realizovano na uzorku stručnih radnika u oblasti zaštite žrtava porodičnog nasilja u Viktoriji i žrtava porodičnog nasilja. Utvrđeno je da su žrtve najčešće proganjane tekstualnim porukama, pri čemu se ukazuje i na verovatnoću da žena koja je izložena partnerskom nasilju u sajber prostoru bude žrtva drugih oblika nasilja od strane istog partnera - više od 80% ispitanica je

doživelo i emocionalno nasilje, 58% seksualno, 39% psihičko nasilje dok je 37% prijavilo ekonomsko nasilje.

Govoreći o posledicima viktimizacije u sajber prostoru, većina autora fokus stavlja na učenike osnovnih i srednjih škola. Kao najčešće posledice navode se negativna osećanja i emocije poput sramote, tuge, usamljenosti, depresije, anksioznosti, straha, kao i uticaj na samopouzdanje (javno poniženje), uticaj na reputaciju i samopoštovanje, osećanje odbačenosti. Kada su u pitanju posledice koje se javljaju kod studenata žrtava sajber viktimizacije pominju se poremećaji ishrane, suicidalne misli i depresija, kao i anksizonost, fobije, pa i paranoične ideje i misli (Almenayes, 2017; Cowie, 2013; Schenk i Fremouw, 2012; Tennant, 2015). Kada su u pitanju anksioznost i depresija, utvrđena je povratna veza, u smislu da anksioznost i depresija povećavaju rizik od sajber viktimizacije među studentima (Kokkinos, Antoniadou, Markos, 2014). Istraživanja pokazuju da između 35% - 43% žrtava sajber viktimizacije ne prijavljuje posledice, što ne znači da posledice nisu prisutne već pre može da ukazuje na nespremnost žrtve svoja iskustva u sajber prostoru percipira kao nasilje, ili pak na nepostojanje svesti o posledicama (Hinduja i Patchin, 2008). Kao jedna od ozbiljnih posledica pominje se i samopovređivanje i rizik od suicida, koji se posebno javljaju u situaciji kada su deca žrtve sajber bulinga.

Sajber viktimizacija studenata Univerziteta u Beogradu

Metodologija istraživanja

U radu je prikazan deo rezultata istraživanja realizovanog u periodu između septembra 2018. i juna 2019. godine među studenatima različitog nivoa i vrste studija Univerziteta u Beogradu. Istraživanje je imalo za cilj ispitivanje rasprostranjenosti, karakteristika i faktora koji su u vezi sa viktimizacijom i vršenjem nasilja u sajber prostoru među studentskom populacijom. Realizovano je primenom kvantitativne metodologije, kombinacija tzv. „papir-olovka" i online tehnike prikupljanja podataka. Uzorak su činili studenti različitog nivoa i vrsta studija Univerziteta u Beogradu. Iako je, po svojoj strukturi, uzorak neprobabilistički - namerni, prilikom uzorkovanja ispoštovane su određene karakteristike teorije verovatnoće. Naime, deo ispitanika, koji su popunjavali anketu metodom „papir-olovka", izabran je slučajnim putem (studenti koji su u tom periodu pohađali fakultet i pristali na učešće), dok su ispitanici koji su anketu popunjavali online birani snowboling metodom. S obzirom na okolnost da su ciljnu populaciju činili studenti, kao i da, prema podacima napred pomenutih istraživanja, veći deo ove populacije ima pristup društvenim mrežama i online prostoru, da je polna struktura ujednačena u odnosu na populaciju[177], uzorak dosta dobro odražava realne karakteristike ispitivane populacije te se može smatrati reprezentativnim.

[177] Prema podacima Republičkog zavoda za statistiku RS, ukupan broj studenata Beogradskog univerziteta u 2019. godini iznosi 98808, od čega 61,1% čine osobe ženskog pola.

Kao istraživački instrument korišćena je posebno formulisana anketa koja se sastojala iz pet delova. Prvi deo ankete činili su osnovni sociodemografski podaci (pol, uzrast, nivo studija, grupacija nauka), dok se drugi deo ankete odnosio na iskustva viktimizacije različitim oblicima nasilja u realnom životu (podeljeno na kategorije psihološko, fizičko - lakši i teži oblici, seksualno uznemiravanje i seksualno nasilje, pri čemu su u okviru svake kateogirije postojala pitanja o učiniocu konkretnog oblika nasilja). Treći deo ankete činio je set pitanja o korišćenju sredstava informaciono-komunikacione tehnologije, dok su poslednja dva dela činile anketa o viktimizaciji (iskustvu viktimizacije u sajber prostoru, pri čemu su u radu prikazani rezultati dobijem primenom ovog dela ankete) i anketa sa samoprijavljivanjem nasilja u sajber prostoru, respektivno. Polazna osnova za dizajniranje instrumenta bila je Cyber Victim and Bullying Scale, koju su razvili Çetin, Yaman i Peker (2011).

Za potrebe istraživanja, sajber nasilje je operacionalizovano kao svako ponižavanje, uznemiravanje ili na bilo koji drugi način ugrožavanje spokojstva ličnosti osobe koja je izložena takvim postupcima, od strane drugih osoba, primenom digitalne tehnologije, a koje podrazumeva disbalans moći između učinioca i žrtve (posebno kada je u pitanju sajber partnersko nasilje) koji proizilazi iz načina izvršenja, mogućnosti anonimnog pristupa žrtvi kao i pristupa u bilo koje vreme bez potrebe za kontaktima licem u lice, a koje može dovesti do posledica po blagostanje žrtve i dugo nakon konkretnog postupka. Prilikom definisanja pojavnih oblika, odnosno, konstruisanja konkretnih pitanja, korišćena je Wilardova (2007) taksonomija (navedena u prethodnom delu rada) pri čemu je, kao posebna kategorija, ispitivano sajber partnersko nasilje.

Za potrebe obrade podataka korišćen je kompjuterski program *Statistical Pacage for Social Sciences* (SPSS). Podaci su analizirani primenom deskriptivne statistike, Pearson korelacije i binarne logističke regresije.

Tabela 1. Karakteristike uzorka

Pol	Broj	Procenat
M	109	32,2
Ž	229	67,8
Uzrast	Broj	Procenat
19-22	220	65,1
23-25	86	25,4
26-30	20	5,9
31-40	9	2,7
> 40	3	0,9
Nivo studija	Broj	Procenat
OAS	234	69,2
OSS	65	19,2
MAS	30	8,9

DAS	9	2,7
Grupacija nauka	Broj	Procenat
Prirodno-matematičke	60	17,8
Društveno-humanističke	192	56,8
Medicinske	48	14,2
Tehničko-tehnološke	38	11,2

OAS - osnovne akademske studije; OSS - osnovne strukovne studije;
MAS - master akademske studije; DAS - doktorske akademske studije

Ukupan uzorak obuhvatio je 338 studenata, od čega su dve trećine ispitanice (67,8%), dok su ispitanici muškog pola zastupljeni u manjem procentu (32,2%). Najzastupljeniji su ispitanici uzrasta od 19-22 godine (65,1%), a najmanje ispitanici uzrasta 30-40 godina (2,7%) i stariji od 40 godina (0,9%) (Tabela 1). Struktura uzorka prema nivou studija pokazuje da su više od dve trećine uzorka činili studenti osnovnih akademskih studija (69,2%), zatim osnovnih strukovnih studija (19,2%), dok su znatno manje zastupljeni studenti master akademskih (8,9%) i doktorskih studija (2,7%). Posmatrano prema vrsti studija, odnosno grupaciji nauka kojoj pripada visokoškolska ustanova na kojoj studiraju, više od polovine ispitanika su studenti društveno-humanističkih nauka (56,8%), zatim slede studenti prirodno-matematičkih (17,8%), medicinskih (14,2%) i tehničko-tehnoloških nauka (11,2%).

Rezultati istraživanja viktimizacije studenata u sajber prostoru

Iskustvo viktimizacija u realnom životu i komunikacione tehnologije

Da je savremena tehnologija široko raspostranjena među studentskom populacijom potvrđuju naši podaci, s obzirom da su se samo dva ispitanika (0,6%) izjasnila da ne koriste pametni telefon i jedan ispitanik (0,3%) da ne koristi kompjuter, dok svi ispitanici koriste e-mail. Slično tome, svi ispitanici imaju aktivan nalog na bar jednoj društvenoj mreži, dok velika većina njih ima naloge na više mreža (327; 96,7%). Kada je u pitanju dužina vremena koje ispitanici provode na društvenim prežama, za trećinu njih (35,2%) to je vremenski okvir između jednog i dva sata, 32,4% njih na društvenim mrežama provodi između dva i četiri sata dnevno, dok gotovo svaki peti ispitanik (19,7%) više od četiri sata u toku dana odvaja za aktivnosti na društvenim mrežama. Boravak na društvenim mrežama, sam po sebi, ne mora biti rizičan ukoliko korisnik preduzima mere zaštite i vodi računa sa kim je kontaktu i koje lične informacije čini javno dostupnim. Pa tako, više od dve trećine naših ispitanika (69,5%) kao prijatelje na društvenim mrežama prihvata samo osobe koje poznaje u realnom životu, dok 30,5% njih prihvata sve zahteve za prijateljstvo, bez obzira da li se radi o poznatoj osobi ili ne. Takođe, nešto više od polovine ispitanika (59,2%), ne ostavlja lične podatke na društvenim mrežama. Reklo bi se da je ohrabrujuće to što većina ispitanika (87%) smatra da je dovoljno informisano o rizicima korišćenja društvenih mreža, ali podaci o prevalenci sajber viktimizacije do kojih smo došli to demantuju.

Istraživanjem je utvrđeno da je gotovo polovina studenata obuhvaćenih uzorkom (158; 46,7%) tokom života bilo izloženo bar jednom obliku viktimizacije u realnom životu i u većini slučajeva u pitanju je bila višestruka viktimizacija i reviktimizacija. Posmatrano prema pojedinačnim oblicima viktimizacije, najviše je zastupljena viktimizacija psihološkim nasiljem, kojoj je bilo izloženo 75,7% ispitanika oba pola, potom viktimizacija seksualnim uznemiravanje (52,4%), kao i krađom i fizičkim nasiljem, kojima je bio izložen podjednak procenat studenata iz uzorka (po 46,7%) ispitanika. Viktimizaciji seksualnim nasiljem (u smislu silovanja) bio je izložen skoro svaki deseti ispitanik (31; 9,2%). Posmatrano prema polu, nešto više su studentkinje (49,8%) bile izložene viktimizaciji u realnom životu nego studenti (40,4%). Interesantno je da su ispitanici oba pola gotovo podjednako, ili su pak ispitanici muškog pola nešto češće bili izloženi nasilnoj viktimizaciji u svakodnevnom životu. Naime, psihološkom nasilju bilo je izloženo 76,9% ispitanica i 83,4% ispitanika, fizičkom nasilju 46,3% ispitanica i 47,7% ispitanika, dok je podjednak procenat (9,2%) ispitanika oba pola doživeo seksualno nasilje (21 ispitanica i 10 ispitanika).

Kada su u pitanju učinioci, u slučajevima viktimizacije nasiljem u realnom životu većinom se radilo o više različitih osoba. Naime, kod polovine ispitanika (50%) koji su iskusili psihološko nasilje, radi o više od jednog učinioca. U ostalim slučajevima, učinilac je bio prijatelj (22,3%), nepoznata osoba (21,5%), partner (5,1%) i roditelj (1,2%). Situacija je drugačija kada je u pitanju viktimizacija fizičkim nasiljem, gde se u nešto više od petine slučajevi radi o više učinilaca (22,8%). U ostalim slučajevima, prema ispitanicima ovaj oblik nasilja najčešće su primenjivali roditelji (32,4%), prijatelji (18,4%), partner (12,7%), nepoznata osoba (7%) ili neka druga poznata osoba (5,1%). U slučajevima seksualnog nasilja, prema 3,2 % studenata iz uzorka ovaj oblik nasilja primenilo je više učinilaca. Silovanje u partnerskim odnosima zastupljeno je u 64,5% slučajeva seksualnog nasilja (20 ispitanika). U petini slučajeva (19,4%) učinilac je prijatelj, dok se u 9,7% slučajeva viktimizacije seksualnim nasiljem radi o nepoznatoj osobi. Jedna ispitanica je bila žrtva incesta, odnosno učinilac je bio član porodice.

Karakteristike sajber viktimizacija studenata

Analizom podataka je utvrđeno da su studenti iz uzorka znatno više bili izloženi viktimizaciji u sajber prostoru nego u realnom životu, što nije iznenađujuće ako se imaju u vidu rizici i mogućnosti za anonimna delovanja koje sa sobom nosi savremena tehnologija, kao i činjenica da su svi ispitanici korisnici društvenih mreža, pri čemu gotovo svi imaju nalog na više društvenih mreža. U skladu sa tim, većina ispitanika, čak njih 310 (91,7%), doživelo je bar jedan oblik viktimizacije u sajber prostoru. Najviše su zastupljeni napadi slanjem virusom zaraženih sadržaja (55,9%), potom sajber proganjanje (51,8%) i sajber vređanje (49,7%) (Tabela 2).

Interesantno je primetiti da je gotovo polovina ispitanika bila izložena različitim oblicima seksualnog uznemiravanja, bilo tako što su dobijali neželjene poruke ili komentare na društvenim mrežama sa seksualnom konotacijom (46,4%) ili su dobijali neželjene fotografije i video sadržaje pornografskog karaktera (36,7%). U oko dve trećine slučajeva

prisutno je i seksualno nasilje u sajber prostoru koje se manifestovalo u neželjenom dobijanju fotografija na kojima je pošiljalac nag ili je u eksplicitnim pozama (37,9%), kao i u upornom dobijanju zahteva za slanjem ličnih fotografija na kojima je ispitanik/ispitanica nag ili u eksplicitnim pozama (28,7%) (Tabela 2).

Posebno je zabrinjavajuće što je gotovo polovina ispitanika bila izložena nekom obliku partnerskog nasilja u sajber prostoru, bilo tako što bi bivši ili sadašnji partner neovlašćeno čitao poruke ili ulazio na profil na društvenim mrežama (45,6%), kontrolisao sve aktivnosti u sajber prostoru, poput proveravanja istorije pregleda i slično (43,5%) ili pratio svaki korak ispitanika upotrebom aplikacije za lociranje (29,3%) (Tabela 2). Ostalim oblicima viktimizacije u sajber prostoru bila je izloženo oko trećine ispitanika (Tabela 2).

Tabela 2. Zastupljenost različitih oblika viktimizacije u sajber prostoru

Oblici viktimizacije u sajber prostoru	Broj	Procenat
Ružni komentari	82	24,3
Vređanje	168	49,7
Pretnje	73	21,6
Hakovanje	86	25,4
Slanje poruka/komentari bez znanja i odobrenja	50	14,8
Sajber proganjanje	175	51,8
Objavljivanje/distribucija fotografija bez odobrenja	50	14,8
Menjanje fotografija bez odobrenja - „Maskarada”	15	4,4
Komunikacija na prevaru	98	29,0
Objavljivanje/distribucija ličnih podataka bez odobrenja	33	9,8
Diskriminacija	71	21,0
Isključivanje iz grupe	45	31,3
Slanje virusom zaraženih sadržaja	189	55,9
Slanje poruka sa seksualnom konotacijom	157	46,4
Slanje fotografija/video sadržaja sa seksualnom konotacijom	124	36,7
Zahtev za slanje ličnih fotografija sa seksualnom konotacijom	97	28,7
Slanje ličnih fotografija sa seksualnom konotacijom	128	37,9
Praćenje lokacije od strane partnera	99	29,3
Kontrola poruka/društvenih mreža od strane partnera	154	45,6
Proveravanje aktivnosti na društvenim mrežama od strane partnera	147	43,5

Posmatrano prema polu, većina ispitanika oba pola iskusila je bar jedan oblik nasilja u sajber prostoru (92,1% ispitanica, odnosno 90,8% ispitanika). Interesantno je da su ispitanici češće navodili da su bili izloženi različitim oblicima partnerskog nasilja u sajber prostoru u odnosu na ispitanice - 31,2% ispitanika naspram 28,4% ispitanica bilo je izloženo neovlašćenom čitanju poruka ili ulasku na profil na društvenim mrežama; 50,5% ispitanika i 43,2% ispitanica je doživelo da im partner/ka kontroliše sve aktivnosti na internetu, dok je praćenju svakog koraka upotrebom aplikacije za lociranje bilo izloženo 46,8% ispitanika i 41,9% ispitanica. Međutim, te razlike se nisu pokazale statistički značajnim.

Nešto manje od trećine studenata iz uzorka (30,9%) koji su bili izloženi nekom obliku viktimizacije u sajber prostoru doživelo je i posledice zbog toga, među kojima dominiraju anksioznost, strah, gubitak poverenja u ljude, osećanje nesigurnosti, sramota i kajanje.

Kada su u pitanju učinioci, generalno posmatrano dominiraju nepoznate osobe, što potvrđuje tezu o anonimnosti kao jednoj od prednosti sajber viktimizacije sa apsketa onih koji viktimiziraju druge. U skladu sa tim, kod seksualnog uznemiravanja i seksualnog nasilja u sajber prostoru, za razliku od viktimizacije u realnom životu, znatno više su zastupljeni nepoznati učinioci, a nije zanemarljiv ni broj ispitanika koji prijavljuje više od jednog učinioca. Nepoznat učinilac dominira i u drugim oblicima sajber viktimizacije poput hakovanja, komunikacije na prevaru (pretvaranjem da je neko drugi), slanja virusa i sajber proganjanja (Tabela 3).

Neovlašćeno objavljivanje ili distribucija ličnih podataka, neovlašćeno menjanje ili uređivanje fotografija, isključivanje iz online pričaonice ili društvene grupe su oblici sajber viktimizacije u kojima je učinilac u više od polovine slučajeva poznat ispitanicima. Slično tome, poznata osoba kao učinilac se javlja u nešto manje od polovine slučajeva i u slučajevima izloženosti neovlašćenom objavljivanju ili distribucija fotografija u sajber prostoru, slanju poruka ili komentara drugim ljudima bez odobrenja kao i ružnim komentarima ili širenju laži o ispitaniku u sajber prostoru (Tabela 3).

Tabela 3. Učinioci nasilja u sajber prostoru

Oblici viktimizacije u sajber prostoru	**NU**		**PU**		**P**		**VU**		**Ukupno (n)**
	n	**%**	**N**	**%**	**n**	**%**	**n**	**%**	
Ružni komentari	21	25,6	35	42,7	6	7,3	20	24,4	82
Vređanje	54	32,1	59	35,1	12	7,1	43	25,6	168
Pretnje	25	34,2	17	23,3	12	16,4	19	26,0	73
Hakovanje	54	62,8	18	20,9	10	11,6	4	4,7	86
Slanje poruka/komentari bez znanja	20	40,0	23	46,0	6	12,0	1	2,0	50
Sajber proganjanje	91	52.0	37	21.1	14	8.0	33	18.9	175
Objavljivanje/distribucija fotografija bez odobrenja	21	42.0	24	48.0	1	2.0	4	8.0	50

Menjanje fotografija bez odobrenja	4	26.7	9	60.0	2	13.3	-	-	15
Komunikacija na prevaru	61	62,2	21	21,4	6	6,1	10	10,2	98
Objavljivanje/distribucija ličnih podataka bez odobrenja	7	21,2	21	61,6	-	-	5	15,2	33
Diskriminacija	28	39,4	26	36,6	4	5,6	13	18,3	71
Isključivanje iz grupe	18	40,0	24	53,3	-	-	3	6,7	45
Slanje virusa	117	61,9	27	14,3	-	-	45	23,8	189
Slanje poruka sa seksualnom konotacijom	90	57,3	20	12,7	7	4,5	40	25,5	157
Slanje fotografija/video sadržaja pornografske sadržine	84	67,7	18	14,5	5	4,0	17	13,7	124
Zahtev za slanje ličnih fotografija sa seksualnom konotacijom	49	50,5	14	14,4	10	10,3	24	24,7	97
Slanje ličnih fotografija sa seksualnom konotacijom	85	66,4	14	10,9	5	3,9	24	18,8	128

NU- nepoznat učinilac; PU- poznat učinilac; P-učnilac partner; VU- više učinilaca; Uk- ukupno

Uprkos tome što je znatna većina ispitanika bila izložena nekom obliku viktiimizacije u sajber prostoru, gotovo polovina njih (46,3%), to svoje iskustvo nisu podelili ni sa kim, odnosno nikome se nisu obratili za pomoć i podršku. Među onima koji su svoje iskustvo podelili sa nekim, najviše ih je pomoć i podršku potražilo od druga ili drugarice (52,4%), dok je njih 42,2% svoje iskustvo podelilo sa više osoba, a 3% sa članovima porodice. Ohrabrujuće je to što je 70,1% ispitanika dobilo podršku od koje su se osećali sigurnije. Sa druge strane, ostali ispitanici koji su se nekome obratili za pomoć i podršku doživeli su negativne reakcije, poput minimiziranja značaja onoga što im se dogodilo u sajber prostoru (14, 8,5%), ignorisanja, okrivljavanja i ubedjivanja da prijave policiji iako oni to ne žele (po jedan ispitanik), dok je 19,5% njih doživelo više od jedne neprijatne reakcije.

Viktimizacija u realnom životu kao faktor viktimizacije u sajber prostoru

Za potrebe rada, a u skladu sa rezultatima prethodnih istraživanja, iskustvo viktimizacije u realnom životu posmatrano je kao faktor sajber viktimizacije. Primenom Pearson korelacije analizirana je povezanost između ova dva oblika viktimizacije studenata. Rezultati

su prikazani u Tabeli 4, gde se može videti da veliki broj prediktorskih varijabli korelira sa kriterijumskim varijablama, većinom na nivou slabe korelacije.[178]

Svi oblici nasilja u realnom životu umereno koreliraju sa pojedinim oblicima sajber viktimizacije, poput pretnji i vređanja u sajber prostoru i sajber seksualnog uznemiravanja i seksualnog nasilja. Pri tome, najjača povezanost uočava se upravo između seksualnog uznemiravanja u realnom životu i seksualnog uznemiravanja u sajber prostoru (r=.41) (Tabela 4).

[178] Kao kriterijum veličine korelacije, odnosno jačine veze uzimamo: mala (slaba): r=0,10-0,29; srednja: r=0,30 - 0,49; velika (jaka): r = 0,50-1. Više o tome videti u: Cohen (1988, s. 79-81).

Tabela 4**.** Korelacije različitih oblika viktimizacije u realnom životu i sajber prostoru

	1	**2**	**3**	**4**	**5**	**6**
1	-					
2	.20**	-				
3	.16**	.25**	-			
4	.16**	.09	.05	-		
5	.16**	.20**	.19**	.10	-	
6	.19**	.08	.16**	.10	.25*	-
Ružni komentari	.11*	.13*	.20**	.05	.21**	.26**
Vređanje u sajber prostoru	**.30****	.16**	.24**	.15**	.24**	**.33****
Pretnje u sajber prostoru	.23**	.22**	**.33****	.04	**.35****	.27**
Hakovanje	.11*	.13*	.12*	.09	.14*	.18**
Slanje poruka/komentari bez zananja	.04	-.02	.10	-.01	.08	.06
Sajber proganjanje	.13*	0.9	.14**	.07	.11*	**.37****
Objavljivanje/distribucija fotografija bez odobrenja	.10	.03	.10	-.04	.08	.08
Menjanje fotografija bez odobrenja	.02	.05	.08	-.06	.09	.15**
Komunikacija na prevaru	.07	.10	.16**	.00	.08	.20**
Objavljivanje/distribucija ličnih podataka bez odobrenja	..12*	.27**	.14*	.05	.15**	.17**
Diskriminacija	.21**	.03	.14*	.07	.18**	.20**
Isključivanje iz grupe	.08	.03	.06	.03	.08	.15**
Slanje virusa	.08	.04	.05	.01	.04	.18**
Slanje poruka sa seksualnom konotacijom	.22**	.15**	.20**	.13**	.13*	**.41****
Slanje fotografija/video sadržaja pornografske sadržine	.26**	.14**	.20**	.05	.15*	**.34****
Zahtev za slanje ličnih fotografija sa seksualnom konotacijom	.19**	.06	.23**	-.00	.10	**.32****
Slanje ličnih fotografija sa seksualnom konotacijom	.23**	.11*	.17**	.16**	.12*	**.33****
Praćenje lokacije od strane partnera	.09	.10	.18**	.05	.23**	.26**
Kontrola poruka/društvenih mreža od strane partnera	.13*	.06	.10	.15**	.13*	.18**
Proveravanje aktivnosti na društvenim mrežama od strane partnera	.12*	.06	.15**	.16**	.16**	.19**

***p<.001, **p.01, *p<.05

1- psihološko nasilje u realnom životu; 2 - fizičko nasilje u realnom životu; 3 - seksualno nasilje u realnom životu; 4 - krađe; 5 - pretnje u realnom životu; 6 - seksualno uznemiravanje u realnom životu.

Prediktori viktimizacije u sajber prostoru

Pored postojanja povezanosti, analizom se nastojalo utvrditi i da li iskustvo viktimizacije u realnom životu ima prediktorski efekat na viktimizaciju u sajber prostoru. Kako bi se to postiglo prediktorske i kriterijumske varijable su dihotomizovane i

primenjena je binarna logistička regresija.[179] Kao prediktorske varijable testirani su ispitivani oblici viktimizacije u realnom životu. Rezultati regresione analize prikazani su u tabelama 5 i 6.

Regresionom analizom dobijeno je pet statistički značajnih logističkih regresionih modela za tzv. opštu sajber viktimizaciju - izloženost vređanju u sajber prostoru kao oblik sajber viktimizacije (χ^2 (8)=23,50; p<0,01; Nagelkerke R^2=0,172; PAC=71,8), izloženost pretnjama pretnjama u sajber prostoru (χ^2 (8)=37,93; p<0,001; Nagelkerke R^2=0,270; PAC=76,8); neovlašćeno menjanje ličnih fotografija sa seksualnom konotacijom (χ^2 (8)=80,71; p<0,001; Nagelkerke R^2=0,372; PAC=92.7); izloženost krađi fotografija koje su potom neovlašćeno online distribuirane - (χ^2 (8)=16,82; p<0,01, Nagelkerke R^2=0,243; PAC=85,9) i sajber diskriminacija (χ^2 (8)=25,26; p<0,01; Nagelkerke R^2=0,282; PAC=71,8).

Kao što se može videti u Tabeli 5, viktimizacija nasiljem u realnom životu znatno povećava verovatnoću, ili bolje da kažemo rizik, da će ispitanici biti izloženi nekom od ovih pet oblika opšte sajber viktimizacije. Konkretnije, studenti koji su u nekom trenutku u životu bili primorani na neželjeni seksualni odnos imaju 5,07 puta veću verovatnoću da će doživeti vređanje u sajber prostoru, poput društvenih mreža, prilikom elektronske komunikacije i slično. Slično, iskustvo viktimizacije seksualnim nasiljem u realnom životu 3,66 puta povećava verovatnoću da će studenti biti izloženi pretnjama u sajber prostoru, dok iskustvo seksualnog uznemiravanja u svakodnevnom životu 2,25 puta povećava verovatnoću da će studenti biti izloženi sajber viktimizaciji koja se ogleda u tome da neko menja njihove fotografije tako što, na primer, lice ispitanice „prikači" na telo druge ženske osobe koja je na fotografiju u eksplicitnoj pozi ili naga, a potom tako izmenjenu fotografiju dalje distribuira online tako što će, na primer, otvoriti nalog na društvenoj mreži sa tako izmenjenom slikom i identitetom ispitanice koja je žrtva takvog ponašanja (Tabela 5). Predikciji izloženosti pretnjama u sajber prostoru značajno doprinosi i izloženost pretnjama u realnom životu, mada sa manjom verovatnoćom nego viktimizacija seksualnim nasiljem. Kada je u pitanju krađa i online distribuiranje ličnih fotografija, regresionom analizom je utvrđeno da izloženost fizičkom nasilju u nekom trenutku u životu više od tri puta povećava (Exp. (B)=3,37) verovatnoću da će student/studentkinja biti i žrtva ovog oblika sajber viktimizacije, dok iskustvo psihološkog nasilja u ofline životu gotovo četiri puta (Exp. (B)=3,89) povećava verovatnoću da će studenti biti izloženi nekom obliku diskriminacije u sajber prostoru, bilo po osnovu pola, seksualnog opredeljenja, porekla ili etničke pripadnosti (Tabela 6).

[179] Za binarnu logističku regresiju smo se opredelile s obzirom da su kao kriterijmske, odnosno zavisne varijable u ovom istraživanju korištene kategorijalne varijable. Poznato je da logistička regresija omogućava ispitivanje modela predikcije kategorijskih ishoda za dve ili više kategorija.

Tabela 5. Prediktori opšte sajber viktimizacije

Prediktor	B	S.E.	Wald	df	p	Količnik verovatnoće	95% interval poverenja za količnik verovatnoće	
							DG	GG
Izloženost vređanju u sajber prostoru								
Seksualno nasilje	1,62	0,78	4,32	1	0,002	5,07	1,09	23,40
Izloženost pretnjama u sajber prostoru								
Pretnje fizičkim nasiljem	0,38	0,12	9,58	1	0,002	1,46	1,15	1,85
Seksualno nasilje	1,30	0,51	6,44	1	0,011	3,66	1,34	9,98
Menjanje fotografija bez odobrenja (sa seksualnom konotacijom)								
Seksualno uznemiravanje	0,81	0,33	6,06	1	0,014	2,25	1,18	4,28
Krađa i online objavljivanje/distribucija ličnih fotografija								
Fizičko nasilje	1,21	0,52	5,45	1	0,020	3,37	1,22	9,32
Sajber diskriminacija zbog izgleda, porekla/pripadnosti, seksualnog opredeljenja								
Psihičko nasilje	1,36	0,65	4,40	1	0,036	3,89	1,09	13,89

B - nestandardizovani regresioni koeficijent; Wald - Voldov statistik; DG - donja granica za 95% interval poveranja za količnik verovatnoće; GG - gornja granica za 95% interval poveranja za količnik verovatnoće

Regresionom analizom dobijena su i dva statistički značajna logistička regresiona modela za sajber seksualnu viktimizacija - ponavljano primanje neželjenih pornografskih fotografija ili video sadržaja (χ^2 (8)=25,35; p<0,01; Nagelkerke R^2=0,298; PAC=52,5) i dobijanje zahteva za slanje ličnih fotografija sa seksualnom konotacijom (bez garderobe, u eksplicitnim pozama ili fotografije genitalne regije) (χ^2 (8)=18,69; p<0,05, Nagelkerke R^2=0,243; PAC=61,6) (Tabela 5). U oba slučaja kao prediktor izdvojeno je iskustvo viktimizacije psihološkim nasiljem u realnom životu, koje kod studenata nešto više od tri puta

povećava verovatnoću da će u nekom periodu života biti žrtve jednog od ova dva oblika sajber viktimizacije seksualnim nasiljem (Tabela 5).

Tabela 5. Prediktori sajber viktimizacije seksualnim nasiljem

Prediktor	**B**	**S.E.**	**Wald**	**df**	**p**	**Količnik verovatnoće**	**95% interval poverenja za količnik verovatnoće**	
							DG	GG
Slanje pornografskih fotografija ili video sadržaja								
Psihološko nasilje	1,11	0,47	5,65	1	0,017	3,03	1,21	7,55
Zahtev za slanje ličnih fotografija sa seksualnom konotacijom								
Psihološko nasilje	1,19	0,51	5,45	1	0,020	3,27	1,21	8,84

B - nestandardizovani regresioni koeficijent; Wald - Voldov statistik; DG - donja granica za 95% interval poveranja za količnik verovatnoće; GG - gornja granica za 95% interval poveranja za količnik verovatnoće

Diskusija i zaključci

Relativno je malo istraživanja koja su se bavila ispitivanjem sajber viktimizacije u populaciji studenata, budući da su istraživanja uglavnom usmerena na ispitivanje karakteristika ovog oblika viktimizacije među učenicima osnovnih i srednjih škola, a da se sa istraživanjima na populaciji studenata počelo tek nešto pre jedne decenije. Aktuelno istraživanje pokazuje veoma visoku stopu izloženosti studenata sajber viktimizaciji, imajući u vidu da više od 90% ispitanika prijavljuje da je iskusilo bar jedan od oblika sajber viktimizacije. Ovako visok procenat sajber viktimizacije u populaciji studenata nije dobijen u prethodnim studijama koje su se bavile ovom problematikom, a čiji nalazi ukazuju da je između 8,6% i 55,3% studenata doživelo neki oblik nasilja u sajber prostoru (Dilmac, 2009; Crosslin i Crosslin, 2014; Finn, 2004; Hinduja i Patchin, 2010; Schenk i Fremouw, 2012). Ovo neslaganje sa ranijim studijama bi se moglo objasniti vremenskom distancom između istraživanja, rapidnim napredovanjem savremene informaciono-komunikacione tehnologije, kao i porastom broja korisnika.

Podaci o izloženosti studenata različitim oblicima seksualnog uznemiravanja i seksualnog nasilja su zabrinjavajući, imajući u vidu da je jedna trećina (a kod pojedinih oblika i gotovo jedna polovina) bar jednom iskusila ovaj oblik sajber viktimizacije, što je znatno više u odnosu na nalaze dosadašnjih istraživanja (Picard, 2007 prema Woodlock, 2017). Ipak, treba naglasiti da se radi o istraživanjima koja su usmerena na populaciju učenika osnovnih i srednjih škola. Ovaj nalaz jasno ukazuje na potrebu diferencijacije sajber nasilja od drugih oblika bulinga, kao i na neophodnost realizacije obimnijih i detaljnijih istraživanja

ove pojave u populaciji studenata, s obzirom na specifičnosti ovog perioda u životu mladih ljudi, a posebno imajući u vidu dobijenu visoku korelaciju između seksualnog uznemiravanja u realnom životu i seksualnog uznemiravanja i nasilja u sajber prostoru.

Istraživanja je pokazalo i veliku zastupljenost sajber partnerskog nasilja, što je u skladu sa drugim studijama (Marganski i Merlander, 2015; Woodlock, 2017). Takođe, utvrđena je povezanost između viktimizacije partnerskim nasiljem u realnom životu i sajber partnerskog nasilja. Ovakvi nalazi potvrđuju teze pojedinih autora da informaciono-komunikacione tehnologije olakšavaju pristup žrtvi, što se posebno odnosi na žrtve intimnog partnerskog nasilja (Merlander, 2010).

Utvrđeno je da je više od polovine ispitanika doživelo sajber proganjanje, što je više nego u drugim istraživanjima (Avais i sar., 2014). Naši rezultati ukazuju na opravdanost tvrdnje nekih autora o povećanju trenda viktimizacije sajber proganjanjem usled evolucije savremenih tehnologija (Fraser i sar., 2010, prema Woodlock, 2017). Pored toga, sajber proganjanje se pokazalo povezanim sa iskustvom seksualnog uznemiravanja u realnom životu, kao i sa iskustvom viktimizacije seksualnim i psihičkim nasiljem u realnom životu, što, takođe, može da implicira da tehnologija olakšava pristup i mogućnosti povređivanja žrtve, te da uz njenu primenu kontinuitet viktimizacije poprima još teži oblik.

Kao i u većini dosadašnjih istraživanja, aktuelno istraživanje nije utvrdilo povezanost između pola i viktimizacije u sajber prostoru (Almenayes, 2017), budući da su studenti oba pola podjednako izloženi različitim oblicima sajber vitimizacije. Pri tome, muškarci češće prijavljuju sajber partnersko nasilje u odnosu na žene, što se možda može tumačiti većim osećanjem sigurnosti i moći koje tehnologija pruža, te žena ima veću slobodu da vrši nasilje kada je fizički odvojena od partnera. Pored toga, treba imati u vidu mogućnost o bidirektivnosti partnerskog nasilja, na šta ukazuju Watkins, Maldonado i DiLillo, 2016). Ova pretpostavka čeka svoju potvrdu u naknadnim analizama podataka.

Kada su u pitanju posledice sajber viktimizacije, nešto manje od trećine studenata iz uzorka prijavljuje da je iskusilo iste, dok se nešto više od polovine obratilo nekome za pomoć i podršku. Interesantno je da je procenat studenata koji prijavljuju posledice sajber viktimizacije manji nego u drugim studijama (Hinduja i Patchin, 2008), što nužno ne podrazumeva izostanak istih već može ukazivati na prisustvo potiskivanja kao mehanizma odbrane ili na nespremnost žrtve da o govori o svom iskustvu. Obraćanje drugima, posebno ljudima iz okruženja, svakako jeste jedan od načina prevazilaženja negativnih emocija vezanih za pretrpljenu viktimizaciju, a prema nekim autorima čak i najbolji (Schenk i Fremouw, 2012). Međutim, zabrinjavajuće je što je nešto manje od trećine ispitanika koji su se obratili za pomoć nekome iz okruženja, doživelo negativnu reakciju, poput minimiziranja njihovog iskustva i omalovažavanja, što ukazuje na potrebu podizanja svesti javnosti o ozbiljnosti sajber viktimizacije i njenih posledica.

Veoma značajni nalazi dobijeni su regresionom analizom jer ukazuju da iskustvo nasilne viktimizacije u realnom životu višestruko povećava rizik viktimizacije u sajber prostoru. Ovaj nalaz je u skladu sa nalazima drugih istraživanja na populaciji mladih (Kowalski, Morgan i Limber, 2012), pri čemu se rizik objašnjava okolnošću da se nasilje iz škole često prenosi i u virtuelni prostor. Sa aspekta aktuelnog istraživanja može se zaključiti da je dobijeni nalaz u skladu sa dosadašnjim viktimološkim saznanjima, prema kojima je primarna viktimizacija (nasilna viktimizacija u realnom životu) snažan prediktor ponovljene viktimizacije, odnosno reviktimizacije (sajber viktimizacije). Pri tome, priroda utvrđenih odnosa bi trebala biti detaljnije ispitana.

Ograničenja istraživanja

Aktuelno istraživanje je eksplorativnog karaktera i svakako ima svoje ograničenja, prvenstveno u metodološkom smislu. Prvo ograničenje se odnosi na ograničenost uzorka samo na studente Univerziteta u Beogradu, i u vezi sa tim, na potrebu ispitivanja iskustava sajber viktimizacije i na populaciji studenata koji studiraju i na preostalim univerzitetima u Srbiji. Jasno, i sama istraživačka tehnika ima svoja ograničenja. Poznato je da su anketa o viktimizaciji i anketa sa samoprijavljivanjem delinkventnog ponašanja dragocene tehnike za saznavanje tamne brojke kriminaliteta, posebno u kombinaciji sa zvaničnim statističkim podacima. Međutim, one imaju i svoje nedostatke, a koji proizilaze iz nepreciznosti (imajući u vidu pitanje reprezentativnosti uzorka), dobrovoljnosti priznavanja viktimizacije i nasilnog ponašanja, kao i subjektivnosti ispitanika (tzv. 'greške' u pamćenju ispitanika, različita shvatanja pitanja od strane različitih ispitanika i slično) (KonstatinovićVilić, Nikolić-Ristanović, Kostić, 2009). Takođe, i online anketiranje ima svoja ograničenja, poput ograničene reprezentativnosti, autoselekcije i mogućnosti lažnog predstavljanja ispitanika (Galešić, 2005).

Nalazi našeg istraživanja jasno ukazuju na potrebu ozbiljnijeg društvenog bavljenja problematikom sajber viktimizacije u ovoj populaciji mladih. Pre svega, potrebna su dodatna istraživanja koja bi ispitala efekte različitih sociodemografskih varijabli poput socioekonomskog statusa, prisustva direktnog ili indirektnog nasilja u porodici, reviktimizacije nasiljem u realnom životu i sajber prostoru i slično, i to na većem uzorku studenata iz različitih gradova u Srbiji. Jasno je da se karakteristike sajber viktimizacije utvrđene istraživanjima u populaciji učenika osnovnih i srednjih škola ne mogu u potpunosti primeniti i na populaciju studenata, pri čemu, za razliku od školskih sredina, u kojima se sve veća pažnja poklanja različitim oblicima nasilja i njihovoj generalnoj i specijalnoj prevenciji, slični društveni resursi, kada su u pitanju studenti, ograničeni su, a najčešće i potpuno odsutni. Stoga, pored bavljenja ovom problematikom sa istraživačkog i teorijskog aspekta, potrebna je i šira društvena strategija usmerena na širenje svesti mladih u visokoškolskim ustanovama o sajber viktimizaciji, kao i osmišljavanje konkretnih programa pomoći i podrške u cilju prevazilaženja negativnih posledica iskustva sajber viktimizacije.

Literatura

1. Almenayes, J. (2017). The relationship between cyberbullying victimization and depression: The moderating effects of gender and age. *Social Networking*, 6, 215-223.
2. Avais, M. A., Wassan, A. A., Narejo, H. i Khan, J. A. (2014). Awareness regarding cyber victimization among students of University of Sindh, Jamshoro. *International Journal of Asian Social Science*, 4 (5), 632-641.
3. Balakrishnan, V. (2015). Cyberbullying among young adults in Malaysia: The roles of gender, age and Internet frequency. *Computers in Human Behavior*, 46, 149–157.
4. Bossler, A. M. i Holt, T. J. (2010). The effect of self-control on victimization in the cyberworld. *Journal of Crime Justice*, 28 (3), 227–236.
5. Burke, S., Wallen, M., Vail-Smith, K. i Knox, D. (2011). Using technology to control intimate partners: An exploratory study of college undergraduates. *Computers in Human Behavior*, 27, 1162-1167.
6. Çetin, B., Yaman, E. i Perker, A. (2011). Cyber victim and bullying scale: A study of validity and reliability. *Computers & Education*, 57, 2261-2271.
7. Corcoran, L., Mc Guckin, C. i Prentice, G. (2015). Cyberbullying or cyber aggression?: A review of existing definitions of cyber-based peer-to-peer aggression. *Societies*, 5, 245-255.
8. Cohen, J. W. (1988) *Statistical power analysis for the behavioral sciences* (2nd ed.). Hillsdale: Lawrence Erlbaum Associates.
9. Cowie, H. (2013). Cyberbullying and its impact on young people's emotional health and well-being. *Psychiatrist*, 37, 167–170.
10. Crosslin, K. L. i Crosslin, M. B. (2014). Cyberbullying at a Texas university—A mixed-methods approach to examining online aggression. *Texas Public Health Journal*, 66 (3), 26–31.
11. Dilmac, B. (2009). Psychological needs as a predictor of cyber bullying: A preliminary report on college students. *Educational Sciences: Theory and Practice*, 9, 1307–1325.
12. Ferdon, C. D. i Hertz, M. F. (2007). Electronic media, violence, and adolescents. An emerging public health problem. *Journal of Adolescent Health*, 41, s1–s5.
13. Finn, J. (2004). A survey of online harassment at a university campus. *Journal of Interpersonal Violence*, 19 (4), str. 468–483.
14. Galešić, M. (2005). Anketna istraživanja putem interneta: Mogući izvor pogrešaka. *Društvena istraživanja- Časopis za opća društvena pitanja*. 14 (1-2), 297-320.
15. Grigg, D. W. (2010). Cyber-aggression: Definition and concept of cyberbullying. *Australian Journal of Guidance and Counseling*, 20 (2), 143–156.
16. Hinduja, S. i Patchin, J. (2008). Cyberbullying: an exploratory analysis of factors related to offending and victimization. *Deviant Behaviour*, 29, 129-156.
17. Hinduja, S. i Patchin, J. W. (2010). Bullying, cyberbullying, and suicide. *Archives of Suicide Research*, 14 (3), 206–221.

18. Hemphill, S. A. i Heerde, J. A. (2014). Adolescent predictors of young adult cyberbullying perpetration and victimization among Australian youth. *Journal of Adolescent Health*, 55 (4), 580–587.
19. Kokkinos, C. M., Antoniadou, N. i Markos, A. (2014). Cyber-bullying: An investigation of the psychological profile of university student participants. *Journal of Applied Developmental Psychology*, 35 (3), 204–214.
20. Nikolić-Ristanović, V., Konstatinović Vilić, S. (2018). *Kriminologija*. Beograd: Prometej.
21. Kowalski, R. M. i Limber, S. P. (2012). Psychological, physical, and academic correlates of cyberbullying and traditional bullying. *Journal of Adolescent Health*, 53 (1 supl), s13–s20.
22. Kowalski, R., Giumetti, G., Schroeder, A. i Lattanner, M. (2014). Bullying in the digital age: A critical review and meta-analysis of cyberbullying research among youth. *Psychological Bulletin*, 140 (4), str. 1073-1137.
23. Langos, C. (2012). Cyberbullying: The challenge to define. *Cyberpsychology, Behavior and Social Networking*, 15, 285–289.
24. Marganski, A. i Merlander, L. (2018*).* Intimate partner violence victimization in the cyber and real world: Examining the extent of cyber aggression experiences and its association with in-person dating violence. *Journal of Interpersonal Violence*, 33 (7), 1071-1095.
25. Merlander, L. (2010). College students' perceptions of intimate partner cyber harassment. *Cyberpsychology, Beohavior and Social Networking*, 13 (3), 263-268.
26. Ngo, F. T. i Paternoster, R. (2011). Cybercrime victimization: An examination of individual and situational level factors. *International Journal of Cyber Criminology*, 5 (1), 773–793.
27. Ortega, R., Elipe, P., Mora-Merchan, M., Genta, M. L., Brighi, A., Guarini, A., Smith, P., Thompson, F. i Tippett, N. (2012). The emotional impact of bullying and cyberbullying on victims: A European cross national sample. *Aggressive Behavior*, 38, 342–356.
28. Patchin, J. W. i Hinduja, S. (2006). Bullies move beyond the schoolyard: a preliminary look at cyberbulling. *Youth Violence and Juvenile Justice*, 4 (2),148-169.
29. Ryan, K. i Curwen, T. (2013). Cyber-victimized students: Incidence, impact, and intervention. *SAGE Open*, 1-7.
30. Sánchez, F. C., Romero, M. F., Navarro-Zaragoza, J., Ruiz-Cabello, A. L., Oriali Rodriges, F. i Maldonado, A. L. (2016). Prevalence and patterns of traditional bullying victimization and cyber-teasing among college population in Spain. *BMC Public Health*, 16-176.
31. Schank, A. i Fremouw, J. (2012). Prevalence, psychological impact, and coping of cyberbully victims among college students. *Journal of School Violence*, 11 (1), 21-37.
32. Smith, P., Mahdavi, J., Carvalho, M., Fisher, S., Russel, S. i Tippett, N. (2008). Cyberbullying: Its nature and impact in secondary school pupils. *Journal of Child Psychology and Psychiatry*, 49 (4), 376–385.

33. Snakenborg, J., Van Acker, R. i Gable, R. A. (2011). Cyberbullying: Prevention and intervention to protect our children and youth. *Preventing School Failure: Alternative Education for Children and Youth*, 55 (2), 88-95.
34. Tennant, J., Demaray, M., Coyle, S. i Malecki, C. (2015). The dangers of the web: Cybervictimization, depression, and social support in college students. *Computers in Human Behaviour*, 50, 348-357.
35. Topcu, C., Erdur-Baker, O. i Capa, A. Y. (2008). Examination of cyber-bullying experiences among Turkish students from different school types. *CyberPsychology & Behavior*, 11 (3), 644–648.
36. Walker, C., Sockman, B. i Koehn, S. (2011). An exploratory study of cyberbullying with undergraduate university students. *Tech Trends*, 55 (2), 31–38.
37. Watkins, L., Maldonado, R. i DiLillo, D. (2016). The cyber aggression in relationships scale: A new multidimensional measure of technology-based intimate partner aggression. *SAGE Open*, 1-19.
38. Willard, N. E. (2007). *Cyberbullying and cyberthreats: Responding to the challenge of online social aggression, threats, and distress*. Champaign, IL, US: Research Press.
39. Woodlock, D. (2017). The Abuse of Technology in Domestic Violence and Stalking. *Violence against Women*. 23 (5), 584-602.
40. Wolak, J., Mitchell, K. i Finkelhor, D. (2007). Does online harassment constitute bullying? An exploration of online harassment by known peers and online-only contacts. *Journal of Adolescent Health*, 41, 51–58.
41. Wright, M. F. (2015). Cyber victimization and adjustment difficulties: The mediation of Chinese and American adolescents' digital technology usage. *Cyberpsychology: Journal of Psychological Research on Cyberspace,* 9 (1), article no. 7.
42. Ybarra, M. L., Diener-West, M. i Leaf, P. J. (2007). Examining the overlap in internet harassment and school bullying: Implications for school intervention. *Journal of Adolescent Health*, 41, str. 42–50.
43. Juvonen, J. i Gross, E. F. (2008). Extending the school grounds? Bullying experiences in cyberspace. *Journal of School Health*, 78, 496-505.
44. Zweig, J. M., Dank, M., Lachman, P. i Yahner, J. (2013). *Technology, teen dating violence and abuse, and bullying*. Washington: Urban Institute Justice Policy Center.
45. Republički zavod za statistiku RS (2019). Visoko obrazovanje (2018/2019). Beograd: Republički zavod za statistiku RS.

Kriminalističke teme
Zbornik radova
Godina XIX, Broj 5, 2019.
ISSN 1512-5505

ULOGA PSIHOLOGIJE U UNAPREĐENJU CYBER SIGURNOSTI
THE ROLE OF PSYCHOLOGY IN ENHANCING CYBERSECURITY

Pregledni naučni rad

Doc. dr. Elvira Čekić[180]

SAŽETAK

Inspiracija za rad i problem (i) koji se radom oslovljava (ju):
Online okruženje je značajan činilac svakodnevnog ponašanja i aktivnosti pojedinaca i organizacija u savremenom ljudskom društvu. Pojava naglašenog posredovanja u komunikaciji povećava rizike i razvija negativna iskustva sa kojima se susreću korisnici, posebno mladi. U tom smislu online okruženje značajno doprinosi pojavi kriminalnog i nasilnog ponašanja (npr. uznemiravanje, seksualno iskorištavanje, prevare, hakovanje). Stoga je veoma bitna uloga psihologije u unapređenju cyber sigurnosti.
Ciljevi rada (naučni i /ili društveni):
Naučni cilj ovog istraživanja je da ostvari saznanje o uzročno-posljedičnom odnosu pojava online komunikacije i devijantnih, uključujući i kriminalne oblike ponašanja.
Društveni cilj je da istraživanja svojim rezultatima doprinesu razumijevanju ljudskog ponašanja u virtualnom prostoru, pri čemu psihologija istražuje i proučava promjene u ponašanju na individualnom i kolektivnom nivou.
Metodologija/Dizajn:
U istraživanju metodološki pristup je zasnovan na shvatanjima savremene socijalne psihologije.
Ograničenja istraživanja/rada:
Imajući u vidu da informatički stručnjaci i psiholozi sve više zajedno djeluju u oblasti interakcije pojedinca sa računarom, cyber psihologija značajnije je polje istraživanja. Ipak, zagovornici i stručnjaci u oblasti cyber psihologije i dalje se suočavaju sa problemima multidisciplinarnosti i transdisciplinarnosti (npr. Kibernetika-računari). Naučnici iz različitih disciplina gledaju na iste pojave sa različitih perspektiva, te se ponekad njihovo shvatanje i jezik razlikuje toliko da je teško postići optimalnu i prihvatljivu saglasnost.
Rezultati/Nalazi:
Na osnovu dosadašnjih rezultata istraživanja i proučavanja naučno-saznajnog fonda, evidentan je zabrinjavajući porast cyber kriminala u svijetu, što potvrđuje i činjenica da je nešto manje od oko 2/3 populacije postalo žrtva nekog od oblika cyber kriminala.
Generalni zaključak:

180 doktor psiholoških nauka, docent na Fakultetu za kriminalistiku, kriminologiju i sigurnosne studije, Univerziteta u Sarajevu. Izvodi nastavu iz više naučnih disciplina iz oblasti psiholoških nauka - Psihologija, Forenzička psihologija, Psihologija kriminaliteta, Psihologija ličnosti i Socijalna psihologija. e-mail: ecekic@fkn.unsa.ba

Razumijevanjem uticaja savremenih tehnologija na ljudsko ponašanje u virtualnom prostoru psihologija je utvrdila značajne promjene u ponašanju na individualnom i kolektivnom nivou.
Opravdanost istraživanja/rada:
Uloga Cyber psihologije je značajno polje istraživanja, koje se bavi psihološkim uticajima i implikacijama kompjuterskih i online tehnologija na pojavu raznih i raznovrsnih oblika devijantnog ponašanja.

Ključne riječi
cyber psihologija, cyber sigurnost, online ponašanje, cyber kriminal, viktimizacija, ljudski faktor

ABSTRACT
Inspiration behind the paper and the issue (s) it addresses:
The online environment is a significant factor which takes part in the daily behavior and activities of individuals and organizations in the modern human society. The emergence of online communication increases risks and develops experiences of negative encounters among users, especially young people. In this regard, the online environment significantly contributes to a serious emergence of criminal and violent behavior (eg harrasment, sexual exploitation, fraud, hacking). Therefore, the role of psychology in enhancing cybersecurity is very important.
Rresearch objectives (scientific and/or social):
The scientific aim of this research is to examine the causal link between online communication and deviant, including criminal forms of behavior.
The social aim of the results of this reseach is to contribute to the understanding of human behavior in a virtual space, whereby psychology explores and studies the changes in behavior at the individual and collective levels.
Methodology/Design:
The methodological approach in this research is based on perceptions of contemporary social psychology.
Limitations of the research/paper:
Given the fact that information technology experts and psychologists increased their mutual cooperation in the field of interaction of individuals with computers, however, cyberpsychology is a more significant field of research. Nevertheless, advocates and experts in cyberpsychology continue to face issues regarding multidisciplinarity and transdisciplinarity (eg. cybernetics-computers). Scientists from different disciplines look at the same phenomena from different perspectives, and sometimes their understanding and language differs in a way that it is difficult to achieve an optimal and acceptable consent.
Results/Findings:
On the basis of results from previous research and of studying scientific and cognitive information, there is an alarming rise in cybercrime in the world, as confirmed by the fact that something under 2/3 of the population has become the victim of some type of cybercrime.
General conclusion:
Through understanding the influence of modern technologies on human behavior in the virtual space, psychology identified significant changes in behavior at individual and collective levels.
Justification of the research/paper:

The role of cyberpsychology is a significant field of research addressing the psychological impacts and implications of computer and online technologies on the emergence of various and diverse forms of deviant behavior.

Key words
cyberpsychology, cybersecurity, online behavior, cyber crime, victimization, human factor

UVOD

Naslov – odredbe naslova teme nas obavezuju na istraživanje (u ovom slučaju dominantno teorijsko sa činiocima empirijskog uvida i saznanja) psihologije, odnosno posebno socijalne psihologije u procesu unapređenja i razvoja sistema personalne, ali i institucionalne zaštite od cyber kriminala.

U samom pristupu proučavanja identifikovanog problema suočavamo se s određenim problemima, kao što su pripadnost teme nauci – naučnoj disciplini, problem sigurnosti i bezbjednosti, problemima ljudskog i društvenog ponašanja, koji uključuju činioce individualne i društvene svijesti i društvene i pojedinačne volje kao bitnih komponenti ljudskog i društvenog ponašanja, itd.

Da bi govorili o sigurnosti i bezbjednosti svakako treba poći od činjenice ugrožavanja ljudi i ljudskih zajednica, njihove imovine i svojine, te u tom smislu problem sigurnosti, odnosno sigurnost je prema svim važećim savremenim relevantnim društvenim teoretičarima i teorijama jedna od osnovnih, primarnih ljudskih, društvenih potreba. Čovjek i ljudsko društvo se ostvaruju u mnoštvu sfera u ljudskom i društvenom i u svakoj od tih sfera života čovjek i društvo teže za sigurnošću. To ispoljavanje težnje za sigurnošću i društvenom bezbjednošću se mora posmatrati u dva osnovna vida: pasivna i aktivna sigurnost. Ukoliko se radi o sigurnosnoj situaciji u kojoj subjekti – ljudi i njihova imovina i svojina nisu ugroženi od prirodnih sila ili društvenih subjekata, onda bi takvu situaciju smatrali pasivnom bezbjednošću, jer je ona zaštićena angažovanjem nekih trećih subjekata. U savremenom društvu, u većini slučajeva, obični građani su uživaoci pasivne bezbjednosti – sigurnosti. Dok se proces aktivne bezbjednosti – sigurnosti ostvaruje preko države i njenih sistema ili/i međunarodnih sistema bezbjednosti.

Priroda i čovjek su istovremeno izvor i predmet ugrožavanja i sigurnosti i ugroženosti. Stoga savremeno društvo poznaje situacije sa zaštićenim i nezaštićenim dijelom prirode i zaštićenim i posebno zaštićenim dijelom ljudi – ljudskog društva. Mi se u radu ne bavimo ugrožavanjem prirode i prirodom kao nosiocem ugrožavanja, već čovjekom koji svojim ponašanjem i djelanjem ugrožava druge ljude – pojedince, društvene grupe, ljudske zajednice, organizacije i institucije društva. Razumijevajući ljudsko ponašanje u virtuelnom prostoru, u kome je ljudski faktor „najslabija karika sigurnosti u cyber (virtuelnom) prostoru“, pri čemu je 70% ukupne populacije u svijetu imalo pristup internetu do 2017“, psihologija na više načina („podizanje javne svijesti o rizicima cyber sigurnosti u cilju

prilagođavanja percepcije ljudi i, posljedično, njihovog ponašanja prema privatnosti"; „razumijevanje uticaja cyber kriminala na ponašanje žrtava u procesu viktimizacije" i dr.) može utvrditi promjene u ponašanju na individualnom i kolektivnom nivou, pri čemu, istražujući ljudsku prirodu, ona ima ključnu ulogu u ublažavanju tog rizika (Wederhold, 2014).

Psihologija je složena nauka o ponašanju ljudi i drugih živih bića, koja otkriva i razumije unutrašnje razloge i spoljne poticaje, iz fizičkog socijalnog i online okruženja, na određena ponašanja. Nije naš zadatak da se u kontekstu obrade predmetnog konglomerata problema bavimo problemom definicije predmeta psihologije i njene klasifikacije, ali to ćemo učiniti u mjeri u kojoj se ukazuje na ulogu i značaj psihologije (korpusa psiholoških nauka) koja obuhvata ukupnu psihologiju ljudi. Pritom, treba imati u vidu da su oblasti društvenih i psiholoških nauka neodvojivi, međusobno povezani i prožeti i da su u bliskom odnosu sa prirodnim naukama, naročito sa prirodnim naukama koje se bave živom prirodom.

Ljudsko saznanje je tvorevina ljudskog uma i ljudskog djelanja, to znači ljudske psihe i ljudskog organizma u kome postoje organi neophodni za odgovarajuće opažanje i percepciju, promišljanje i zaključivanje. Ustvari, to je ljudski mozak i živčani sistem.

U okviru psihologije postoji veliki broj psihologijskih grana i disciplina. Jedna od njih je i Socijalna psihologija, za koju Zvonarević (1976) tvrdi da je to "grana psihologije koja proučava psihološke aspekte pojava i socijalne aspekte psiholoških pojava".

U Psihologijskom rječniku na str. 449-450, se kaže da je socijalna psihologija "grana ili disciplina psihologije … Kao opći predmet socijalne psihologije određuje se socijalna psihologija čovjeka, njegov socijalni razvoj, socijalno ponašanje, društveni život ljudi ili uzajamno djelovanje …"

U samom središtu socijalne psihologije je **pojava socijalnog uticaja**, te se socijalna psihologija definira kao znanstvena disciplina **koja proučava kako stvarna ili zamišljena prisutnost drugih ljudi utiče na naše misli, osjećaje i ponašanje** (bold. E. Č.) (Allport, 1985; Aronson et al., 2005).

Odredbe citirane definicije najbliže i najpreciznije ukazuju na predmet socijalne psihologije, koja je od posebnog značaja u ostvarivanjima ljudskog i društvenog ponašanja, djelanja i njihovim društvenim interakcijama. Dakle, u sticanju i praktikovanju – primjeni (sa)znanja pored ljudskih čula kao organa i nagona neophodan je um. A izučavanje uma se svodi na proučavanje mozga (kao organa) i nervnog sistema i ponašanja u raznim sistemima i raznim situacijama. Sposobnosti (obdarenost, afinitet, itd.) uma su različiti a izvori razlika nepoznati, osim za jedan faktor koji nazivamo obrazovanje i vaspitanje ili kako ga upravo naziva socijalna psihologija "socijalizacija" (Termiz, 2013).

Prema tome, značaj i uloga psihologije, odnosno socijalne psihologije se ogleda u formiranju i razvoju ličnosti individue (izgradnja socijalizovane ličnosti) i formiranju društveno prihvatljivih modela ponašanja u procesima ljudskih i društvenih interakcija i raznih oblika i načina društvenih komunikacija, uključujući i online komunikacije, kao bitan činilac njihove personalne, ali i grupne, institucionalne i organizacijske sigurnosti kao brane jednom od razvijenih savremenih oblika kriminala, kao što je cyber kriminal.

1. Definicija pojma sigurnost

Ne postoji univerzalno prihvaćena definicija cyber sigurnosti. Riječ, pojam, termin cyber sigurnost je složenica i ona se sastoji od pojma – termina "cyber" i "sigurnost", pri čemu je "cyber" prefiks i označava virtuelni prostor i odnosi se na elektronske komunikacione mreže i virtuelnu stvarnost (Oxford, 2014; Craigen et al., 2014). On je kao takav nastao od pojma "kibernetika", koji se odnosi na "polje kontrole i teorije komunikacije, bilo to među mašinama ili životinjama" (Wiener, 1948; Craigen et al., 2014). Kao virtuelni prostor bio je namijenjen i osmišljen kao okruženje za informacije" (Singer & Friedman, 2013), a „danas je proširena procjena cyber prostora". Tako, npr. Public Safety Canada (2010) definiše cyber prostor kao "elektronski svijet koji su stvarali međusobno povezane mreže informacijske tehnologije i informacije na tim mrežama". On „predstavlja globalno dobro u kome ljudi zajedno razmjenjuju ideje, usluge i prijateljstvo" (ukoliko nije to dobro zloupotrebljeno). "Cyber prostor nije statičan, već je dinamičan, evoluirajući, višerazinski ekosistem fizičke infrastrukture, softvera, propisa, ideja, inovacija i interakcija pod uticajem sve veće populacije saradnika, koji predstavlja spektar ljudskih namjera (Deibert & Rohozinski, 2010).

Pojam sigurnost teško je definirati u opštem smislu. Rasprave o sigurnosti, prema nekim autorima „nužno uključuju i nastoje razumjeti ko sekuritizira, o kojim pitanjima (prijetnjama), za koga (referentni objekt), zašto, s kojim rezultatima i pod kojim uslovima (Buzan, Waever i De Wilde, 1998). Može se govoriti o različitim oblicima sigurnosti (ljudskih osobina, fizičke sigurnosti, emocionalne sigurnosti, psihološke sigurnosti, sigurnosti informacijskih sistema, itd). Značenje termina sigurnosti je zasnovano na opažanju, mišljenju, znanju, osjećaju, vjerovanju, uvjerenju, sistemu vrijednosti, emocijama i personalnoj perspektivi.

Imajući u vidu polaznu, prethodno navedenu definiciju pojma sigurnosti, koja je vezana za situaciju pojedinca i njegovu koncepciju sigurnosti (aktuelno i perspektivno odsustvo lične ugroženosti, kao osnov za izvedeni pojam cyber sigurnosti), zapažamo da se ni teoretičari cyber sigurnosti nisu usaglasili, a time ni ponudili jednu, u osnovi, opšteprihvatljivu definiciju.

Prema dostupnoj savremenoj literaturi prisutne su sljedeće definicije cyber sigurnosti:

(1) "Cyber sigurnost uglavnom obuhvata odbrambene metode koje se koriste za otkrivanje i sprječavanje potencijalnih uljeza" (Kemmerer, 2003; Craigen et al., 2014);

(2) "Cyber sigurnost podrazumijeva zaštitu informatičkih mreža i informacija koje iste sadrže od prodora i od zlonamjernog oštećenja" (Lewis, 2006; Craigen et al., 2014);

(3) "Cyber sigurnost uključuje smanjenje rizika od zlonamjernog napada na softwer, kompjutere i mreže. To uključuje alate koji se koriste za otkrivanje pravila, zaustavljanje virusa, blokiranje zlonamjernog pristupa, provođenje provjere autentičnosti, omogućavanje šifrovanih komunikacija, itd." (Amoroso, 2006; Craigen et al., 2014);

(4) "Cyber sigurnost je skup instrumenata, politika, sigurnosnih koncepata, sigurnosnih mjera, smjernica, pristupa upravljanja rizicima, radnji, obuke, najboljih praksi, osiguranja tehnologija koje se mogu koristiti za zaštitu od cyber okruženja i organizacije i korisnikovih resursa" (ITU, 2009; Craigen et al., 2014);

(5) "Sposobnost zaštite ili odbrane upotrebe cyber-prostora od cyber-napada" (CNSS, 2010; Craigen et al., 2014);

(6) "Tehnologija, procesi, prakse i mjere za odgovor i ublažavanje koje su dizajnirane da zaštite mreže, računare, programe i podatke od napada, oštećenja ili neovlaštenog pristupa, kako bi se osigurala povjerljivost, integritet i dostupnost" (Public Safety Canada, 2014; Craigen et al., 2014);

(7) "Umijeće osiguranja postojanja i kontinuiteta informacijskog društva određene nacije, garantirajući i štiteći, u virtuelnom prostoru, informacije, imovinu i kritičnu infrastrukturu" (Canongia & Mandarino, 2014; Craigen et al., 2014);

(8) "Stanje zaštite od kriminalne ili neovlaštene upotrebe elektronskih podataka, ili mjere poduzete da se to postigne" (Oxford University Press, 2014; Craigen et al., 2014);

(9) "Aktivnost ili proces, sposobnost ili stanje prema kojem su informacioni i komunikacioni sistem i informacije sadržane u njemu zaštićene od i/ili zaštićene od oštećenja, neovlaštene upotrebe ili modifikacije ili eksploatacije" (DHS, 2014; Craigen et al., 2014);

Iz citiranih definicija cyber sigurnosti uočavamo njihove bitne odredbe: zaštite od kriminalne ili neovlaštene upotrebe podataka u procesu info-tehnologija u cyber prostoru, čime se faktički aktuelno i/ili potencijalno subjekti – ljudi kao pojedinci, grupe, ljudske zajednice i institucije ugroženi i čime se ugrožava njihov ljudski integritet, imovina i svojina.

To zahtijeva da se kompjuterska sigurnost fokusira na osiguranje tehnologije – sistema i komunikacijske infrastrukture, koja sadrži podatke i programe. Bitna komponenta informaciono – komunikacijskih tehnologija i sistema su ljudi, sigurnosno-bezbjednosna kultura i bezbjednosna politika i ponašanje subjekata, čije su bitne komponente svijest i volja u čemu, pored ostalog, psihologija, odnosno socijalna psihologija ima naglašeno značajnu ulogu.

2. Cyber kriminal

Odredbe naslova teme zahtijevaju da određenu pažnju posvetimo cyber kriminalu. Cyber kriminal se razlikuje od tradicionalnog ili klasičnog kriminala koji može biti počinjen na jednom određenom geografskom području. Cyber kriminal „se može počiniti na internetu i često nije jasno povezan sa geografskom lokacijom" (Wall, 2017; Jahankhani et al., 2014). Identifikaciju lokacije sa karakterističnim elementima kriminala gotovo je nemoguće utvrditi u cyber kriminalu.

U slučaju cyber kriminala prostorna karakteristika napadača se ne može ili je teže istu utvrditi, jer tzv. kompjuterski ili internet kriminal je "anti-prostorni". Stoga i jeste zadatak kriminologije razumijevanje motivacije kriminalaca analizom socijalnih karakteristika kriminalaca i njihovih prostornih lokacija. Pored kriminologije, u procesu razlikovanja sitnog lopova od profesionalnog kriminalnog hakera značajnu ulogu ima jasno utvrđena metodologija, koja treba obezbijediti pouzdanu vezu sa kompjuterskom forenzikom i psihologijom, koja će omogućiti otkrivanje i identifikaciju profila cyber kriminala i omogućiti razumijevanje njihovog ponašanja (Hemraj et al., 2012).

Prethodno navedenim se dovoljno jasno ukazuje na potrebu razlikovanja novih oblika od klasičnog kriminala, krivičnih djela koja su usmjerena na IT i počinjene putem IT (informacionih tehnologija) kao što su npr. hakiranje, prevare putem interneta (Holt, T., & Bossler, A., 2014; McGuire, M., & Dowling, 2013; Leukfeldt, 2017). Krivična djela počinjena putem interneta, kao što su: hakovanje, kreiranje borneta, zarazivanje kompjutera malwareom (zlonamjernim programima) su povezani sa tradicionalnim oblicima kriminala, – krivična djela prevare, prijetnje i uhođenja, a ponekad spadaju u obje kategorije kriminala – klasični i cyber kriminal.

Nesumnjivo je naglašen značaj cyber sigurnosti u savremenom društvu u kojem tzv. tehničkim napadima i nedopuštenim pristupima nosioci cyber kriminala dolaze do informacija od kojih imaju veliku korist. Informacije o kadrovskim registrima, kreditnim informacijama, poslovnim i drugim tajnama, šiframa, virtuelnom novcu, stanju na računu, itd. se prodaju, pa čak i više od jednom. Kriminalno pribavljene informacije se mogu koristiti za ucjenu i prodaju ukradenih informacija žrtvi (kao što je to naprimjer slučaj u kriminalu sa automobilima u klasičnom kriminalu) (Tikkanen, 2017).

Osnovne metode u cyber kriminalu su ubjeđivanje i manipulacija koja se koristi i u sprezi s ubjeđivanjem. Vještinom ubjeđivanja se obezbjeđuje dobra volja pojedinca i njegova spremnost da se pomogne. Dakle, ubjeđivanje je usmjereno na emociju žrtve. Manipulacija ima za cilj da preoblikuje percepcije druge osobe o nečemu, a njena svrha je da se ta osoba drži pod kontrolom (Hadnagy, Ch., & Ekman, P., 2014).

3. Cyber psihologija i ljudski faktori

Pojam cyber psihologija su utvrdili istraživači sredinom 1990-ih godina koji su proučavali online ponašanje. Imajući u vidu činjenicu da stručnjaci iz oblasti informatike i psiholozi „sve više djeluju u oblasti interakcije pojedinca sa računarom“, cyber psihologija je postala značajnije polje istraživanja (Widman, 2018).

Cyber psihologija je subdisciplina psihologije, koja proučava psihološke uticaje i implikacije kompjuterskih i online tehnologija, koje se odvijaju unutar virtuelnog, odnosno cyber prostora putem korištenja tehnologije (Attrill, 2016; Kaye, 2016; Widman, 2018).

Jedan od aspekata istraživanja i naučnog proučavanja je uticaj online okruženja na ponašanje i aktivnosti pojedinaca, ljudskih zajednica, institucija i organizacija. Ta posredovanost u komunikaciji (korištenje interneta) doprinosi povećanju rizika u manifestacijama raznih oblika devijantnih i kriminalnih ponašanja kao što su: uznemiravanje, seksualno iskorištavanje, prevare, hakovanje, zarazu malware-om, itd. (Bryce, 2015).

Da bi razumjeli online viktimizaciju i njeno prisustvo u kriminalnom ponašanju neophodno je poznavati bitne karakteristike online komunikacije a koje su vezane za pristup i pristupačnost savremenim IT, uslugama i aplikacijama koje predstavljaju sastavni dio digitalnog okruženja. Poznavanje bitnih karakteristika online interakcije je značajno zbog njihovog uticaja na ponašanje subjekata – ljudi, a koji aktuelno i potencijalno mogu doprinijeti kriminalnom ponašanju i viktimizaciji. U osnovne karakteristike online komunikacije mogu se svrstati: anonimnost, dezinhibicija, otkrivanje ličnih informacija, hiper intimnost, obmana, deindividualizacija, itd. (Bryce, 2015).

Nesumnjivo je da postoji visok nivo korelacije između online informacije i offline okruženja, u manifestaciji raznih oblika devijantnog i kriminalnog ponašanja i online ponašanja koja izlažu pojedinca riziku od viktimizacije. U online komunikacijama pojedinci dijele informacije koje se tiču njihovog identiteta, emocija, potreba, želja, namjera, aktivnosti, očekivanja, itd. Ta podjela značajnih personalnih informacija sa drugim, najčešće nepoznatim, u ovoj vrsti, visokorizičnih komunikacija se može koristiti u svrhe uznemiravanja, proganjanja, prevare, kompromitacije do hakiranja računara u bankama. Dakle, takva ponašanja u online komunikacijama doprinose narušavanju i/ili ugrožavanju tzv. cyber sigurnosti.

Rezultati savremenih istraživanja su, pored ostalog, utvrditi psihološku ranjivost pojedinaca kao posljedicu niskog stepena samopouzdanja, socijalne anksioznosti, depresije, te njihove socijalne situacije koju odlikuje haotična porodična situacija izazvana roditeljskim sukobima, razvodom braka i slično.

Polazeći od prethodno navedenog nameće se logično pitanje – a ko su to žrtve cyber kriminala, koji je to broj – kvalitet žrtava i obim krivičnih djela cyber kriminala? Istraživači cyber kriminala su otkrili postojanje značajne povezanosti između osobina ličnosti podložne napadima ove vrste kriminala, kao i vezu između podložnosti napadima socijalnog inžinjeringa i ključnih faktora ličnosti. Socijalni inžinjering se smatra upotrebom

manipulacije, uvjeravanja i utjecaja napadača kako bi se dobile osjetljive informacije ili kako bi se dobio pristup ograničenim područjima (Uebelacker and Quiel, 2014; Hadlington, 2017). Oni su predstavili teorijski okvir kojim ukazuju na direktnu povezanost između određenih osobina ličnosti (John and Srivastava, 1999; Hadlington, 2017) i osjetljivosti na socijalni inžinjering. Autori ukazuju na to da pojedinci koji posjeduju osobine kao što su: impulsivnost, ekstraverzija, otvorenost prema iskustvu i prihvatljivost su podložni napadima socijalnog inžinjeringa, dok su savjesnost, suglasnost, kritički odnos prema iskustvu i veća svijest o informatičkoj sigurnosti značajni mehanizmi cyber sigurnosti (McCormac, et al., 2016; Hadlington, 2017).

U istraživanju ljudskog i društvenog ponašanja jedna od osobina ličnosti koja se tiče sigurnosti informacija je impulsivnost koja se definiše kao "potreba da se djeluje spontano bez razmišljanja o djelovanju i njegovim posljedicama (Coutlee et al., 2014, Hadlington, 2017). Istraživanja su pokazala da oni pojedinci koji imaju viši nivo impulsivnosti su izloženi većem riziku od onih sa nižim nivoom impulsivnosti (Coutlee et al., 2014; McCoul i Haslam, 2001; Zuckerman i Kuhlman, 2000; Hadlington, 2017). Isto tako, konstatuje Coutlee et al., (2014) da je impulsivnost osobina – komponenta velikog broja kliničkih stanja kao što su ADHD, granični poremećaji ličnosti i poremećaj impulsivne kontrole. Zavisnost od interneta se može uvrstiti u patološke poremećaje (Griffiths, 1998. i 2000; Young, 1998; Hadlington, 2017), ali je potrebno razlikovati zavisnost od interneta od zloupotrebe interneta. Međutim, Stanton (2002) tvrdi "da je zloupotreba interneta na radnom mjestu prirodni nastavak aktivnosti vezanih za ovisnost o internetu". Ali je nesumnjivo da zlupotreba interneta povećava mogućnosti sigurnosti unutar organizacije (Pee et al., 2008; Weatherbee, 2010; Hadlington, 2017) njegovo neetičko korištenje na radnom mjestu doprinosi razvoju cyber kriminala koji uključuje aspekte intelektualnog vlasništva, distribuciju uvredljivog materijala i piraterije na internetu (Chen et al., 2008; Hadlington, 2017).

U tom smislu obrazovanje o informacijskoj sigurnosti mora uključiti efikasne i pouzdane identifikacije u elektronskim komunikacijama polazeći od individualne svijesti subjekata, aspekata njihove ličnosti i sigurnosno – bezbjednosne kulture. Tehnički rizici u cyber sigurnosti se mogu odgovarajućim rješenjima umanjiti, ali ranjivost u ponašanju ostaje permanentno i trajno prisutan problem. Posredovane komunikacije utiču na individualna i grupna ponašanja koja se mogu iskoristiti (zloupotrijebiti) od strane drugih za asocijalna i/ili kriminalna ponašanja. Stoga je posebna uloga i značaj psihologije na razvijanju svijesti o potencijalnim rizicima tzv. ranjivostima i formiranju i projektovanju prihvatljivih modela socijalnog ponašanja koji uključuju dovoljno pouzdane i djelotvorne bihevioralne mjere u zaštiti personalne privatne sigurnosti, ali i sigurnosti organizacije, institucije do online okruženja kome pripadaju.

Zaključak

Od postanka ljudskog društva brojni su i raznovrsni oblici ugrožavanja sigurnosti – bezbjednosti društva i države, a jedan od osnovnih oblika i načina ugrožavanja je kriminalitet. Kriminalitet se u savremenom društvu, pored klasičnih oblika, manifestuje u novim i savremenim oblicima. Savremeni oblik kriminaliteta je cyber kriminal u virtuelnom prostoru, koji je jedna od njegovih specifičnosti, ali i savremene IT (informacione tehnologije) kao savremeno sredstvo njegovog (iz)vršenja, što otežava proces identifikacije, kako njegovih nosilaca, tako i primarnih i tzv. sekundarnih žrtava ovog oblika kriminala. Nesumnjivo da je ljudski faktor najosjetljivija karika u sistemu sigurnosti – bezbjednosti u cyber (virtuelnom) prostoru.

Psihologija i njene naučne discipline kao što su: forenzička, penološka, inžinjerijska, socijalna psihologija, psihologija kriminaliteta, cyber psihologija, itd., u procesu istraživanja, čovjeka i njegove ljudske prirode, u primjeni stečenih naučnih saznanja u nauci i svim sferama ljudskog i društvenog života imaju bitnu ulogu u prevenciji rizika i ublažavanja posljedica viktimizacije. U tom smislu psihologija ima posebnu ulogu i značaj u izgrađivanju ličnosti i formiranju pozitivnih osobina ličnosti, razvijanju individualne i društvene svijesti o personalnim, grupnim i institucionalnim rizicima od cyber kriminala, potrebi određenih (sa)znanja o elektronskim komunikacionim mrežama i komunikacijama u savremenom društvu, sigurnosno – bezbjednosnoj kulturi i formiranju i razvijanju društveno prihvatljivih modela ponašanja u online komunikacijama kao bitnim faktorima unapređenja cyber sigurnosti u virtuelnom prostoru.

Literatura

- Allport, G. W. (1985). The historical background of social psychology. In G. Lindzey & E. Aronson (Eds.), The handbook of social psychology (3rd ed., Vol.1, pp.1-46). New York. McGraw-Hill.
- Amoroso, E. (2006). Cyber Security. New Jersey: Silicon Press.
- Aronson, E., Wilson, T. D., Akert R. M. (2005), Socijalna psihologija, Nakladnik, Zagreb: Mate.
- Attrill, A. (2015). Cyberpsychology. Oxford University Press; 1 edition.
- Bryce, J. (2015). Cyberpsychology and Human Factors, Engineering and Technology, Cyberspace Research Unit, School of Psychology, University of Central Lancashire, Preston.
- Buzan, B., Waever, O., & De Wilde, J. (1998). Security: A New Framework for Analysis. Boulder, CO: Lynne Rienner Publishers.
- Canongia, C., & Mandarino, R. (2014). The New Challenge of the Information Society. In Crisis Management: Concepts, Methodologies, Tools and Aplications: 60-80. Hershey, PA:IGI Global.
- Chen, J.V., Chen, C.C., Yang, H.-H., (2008). An empirical avaluation of key factors contributing to internet abuse in the workplace. Ind.Manage. Data Syst. 108 (1), 87-106.
- CNSS. (2010). National Information Assurance Glossary: Committee on National Security Systems (CNSS) Instruction No. 4009
- Coutlee, C.G., Politzer, C.S., Hoyle, R.H., Huettel, S., (2014). An abbreviated impulsiveness scale constructed through confirmatory factor analysis of the Barratt Impulsiveness Scale Version I 1. Arch. Sci. Psychol. 2, 1-12.
- Craigen, D., Diakun - Thibault N., Purse R., (2014). Defining Cybersecurity, Technology Innovation Management Review, 4 (10):13-21.
- Deibert , R., & Rohozinski, R. (2010). Liberation vs. Control: The Future of Cyberspace. Journal of Democracy, 21 (4): 43-57.
- DHS. (2014). A Glossary of Common Cybersecurity Terminology. National Intiative for Cybersecurity Careers and Studies: Department of Homeland Security. October 1, 2014:
- Griffiths, M. (1998). Internet addiction: does really exist? In Gackenbach, J. (Ed.), Psychology and the Internet: Intrapersonal, Interpersonal and Transpersonal Implications. Academic Press, San Diego, CA, pp.61-75.
- Griffiths, M. (2000). Internet addiction: time to be taken seriously? Addict. Res 8 (5), 413.
- Hadlington, L. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. Heliyon 3, Elsevier Ltd.
- Hadnagy Ch., Eckman, P. (2014). Unmasking the Social Engineer: The Human Element of Security, 1st Edition, Indianapolis Wiley.
- Holt, T.J., Bossler, A.M. (2014). An assessment of the current state of cybercrime scholarship. Deviant Behavior, 35 (1), 20-40.

- ITU. (2009). Overview of Sybersecurity. Recommendation ITU-T X.1205. Geneva: International Telecommunication Union (ITU).
- Jahankhani, H., Al-Nemrat, A., Hosseinian-Far, A. (2014). Cyber crime Classification and Characteristics. In book: Cyber Crime and Cyber Terrorism Investigator's Handbook, Chapter:12, Elsevier Science, pp.149-164.
- John, O.P., Srivastava, S., (1999). Big Five Inventory (BFI). Handbook of Personality: Theory and Research 2, 102-138.
- Kaye, L. K. (2016). Book Review: An Introduction to Cyberpsychology. Cyberpsychology, Behavior, and Social Networking, 19 (4), 294-294.
- Kemmerer, R. A. (2003). Cybersecurity. Proceedings of the 25th IEEE International Conference of Software Engineering: 705-715.
- Leukfeldt, R. (2017). Research Agenda: The human factor in Cybercrime and Cybersecurity. Eleven International Publishing, Netherlands.
- Lewis, J. A. (2006). Cybersecurity and Critical Infrastructure Protection. Washington, DC: Center for Strategic and International Studies.
- McGuire, M., Dowling, S. (2013). Chapter 1: Cyber-dependent crimes Cyber crime: A review of the evidence (Home Office Research Report 75 ed., pp. 4-34).
- McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., Pattinson, M. (2016). Individual differences and Information Security Awareness. Comput. Human. Behav. 69, 151-156.
- McCoul, M.D., Haslam, M. (2001). Predicting high risk sexual behaviour in heterosexual and homosexual man: the roles of impulsivity and sensation seeking. Pers. Individ. Dif. 31 (8), 1303-1310.
- Oxford University Press. (2014). Oxford Online Dictionary. Oxford: Oxford University Press. October 1.
- Pee, W.G., Woon, I.M.Y., Kankanhalli, A. (2008). Explaining non work related computing in the work place: A comparison of alternative models. Inform. Manage. 45, 120-130.
- Petz, B. (ur.), Furlan, I., Kljajić, S., Kolesarić, V., Krizmanić, M., Szabo, S., Šverko, B., (2005). Psihologijski rječnik, Naklada Slap, Jastrebarsko, Zagreb.
- Public Safety Canada. (2010). Canadas Cyber Security Strategy. Ottawa: Public Safety Canada, Government of Canada.
- Public Safety Canada. (2014). Terminology Bulletin 281: Emergency Management Vocabulary. Ottawa: Translation Bureau, Government of Canada.
- Saini, H., Rao, Y. Sh., Panda, T.C. (2012). Cyber-Crimes and their Impacts: A Review, International Journal of Engineering Research and Applications (IJERA),Vol. 2, Issue 2, pp. 202-209.
- Singer, P.W., & Friedman, A. (2013). Cybercecurity and Cyberwar: What Everyone Needs to Know. New York: Oxford University Press.
- Stanton, J. (2002). Company Profile of the Frequent Internet User. Communications of the ACM 45 (1), 55-59.
- Termiz, Dž. (2013), Kritika teorije, Amos Graf, Sarajevo.

- Tikkanen, T. (2017). Human behavior from Cyber Security perspective, Master's Thesis, School of Technology, Master's Degree Programme in Information and Communications Technology, Cyber Security.
- Uebelacker, S., Quiel, S. (2014). The Social Engineering Personality Framework. Workshop on Socio-Technical Aspects in Security and Trust, 24-30.
- Wall, D. (2017). Hunting, Shooting and Phishing: New Cybercrime Challenges for Cybercanadians in the 21st Century. The ECCLES Centre for American Studies.
- Wederhold, B. (2014), The role of Psychology in Enhancing Cybersecurity, Cyberpsychology, Behavior and Social Networking, Volume 17, Number 2.
- Weatherbee, T.G. (2010). Counterproductive use of technology at work: Information and communications technologies and cyberdeviancy. Hum. Resource Manage. R 20 (1), 35-44.
- Widman, J. (2018). The Emergence of Cyberpsychology. Cyberpsychology: Journal of Psychosocial Research on Cyberspace.Vol.
- Wiener, N. (1948). CYBERNETICS or control and communication in the animal and the machine. second edition, The MIT. Press, Cambridge, Massachusetts.
- Young, K.S. (1998). Internet addiction: The emergence of a new clinical disorder. Cyberpsycholog. Behav. 1 (3), 237-244.
- Zuckerman, M., Kuhlman, D.M. (2000). Personality and risk-taking: common biosocial factors. J. Personal. 68 (6), 999.
- Zvonarević, M. (1978), Socijalna psihologija, Školska knjiga, Zagreb.

Kriminalističke teme
Zbornik radova
Godina XIX, Broj 5, 2019.
ISSN 1512-5505

Panel 5

DIGITALNA SIGURNOST U UMREŽENOM SVIJETU: FORENZIKA I TEHNIKA

Kriminalističke teme
Zbornik radova
Godina XIX, Broj 5, 2019.
ISSN 1512-5505

POSTUPCI KRIPTOGRAFIJE I NJIHOVA ULOGA
CRYPTOGRAPHY PROCEDURES AND THEIR ROLE

Pregledni naučni rad

Prof. dr. Jasmin Ahić
Kenan Hodžić, MA[181]

SAŽETAK

Inspiracija za rad i problem (i) koji se radom oslovljava (ju): Tehničko-tehnološki razvoj omogućava i pogoduje unapređivanju i inoviranju novih komunikacijskih kanala. U domenu kritičnih ljudskih djelatnosti osnovno je pitanje na koji način zaštititi čovjeka od savremenih prijetnji kojima je izložen. U raspoloživoj akademskoj literaturi ne postoji dovoljno informacija o metodama koje proučavaju skrivanje informacija što spada u skupinu postupaka kriptografije.

Ciljevi rada (naučni i/ili društveni): Cilj rada je analizirati historijsku ulogu kriptografije, ukazati na razloge njene pojave, primjenu i važnost u cilju unapređenja sigurnosti i zaštite ljudi u cjelini. Svakako da je popunjavanje praznina u dostupnoj građi iz ove oblasti dopunski cilj rada, uzimajući u obzir da će se u radu na sistematičan i jedinstven način zaokružiti zapaženo stanje.

Metodologija/Dizajn: U radu je primarno korištena tehnika iz kvalitativne istraživačke paradigme. Metodom analize sadržaja istraživat će se kriptografski sistemi i metode koje se koriste. Selekcija akademskih radova iz oblasti kriptografije je urađena na način da su odabrani samo oni radovi koji u svojoj sadržini imaju historijsku i razvojnu komponentu sigurnosti i kriptografije.

Ograničenja istraživanja/rada: Nedostatak naučnog diskursa i postojanje izraženog nesklada u teorijskim razmatranjima a u vezi sa interpretiranjem kripto postupaka.

Rezultati/Generalni zaključak: Rezultati se odnose na prikaz i klasifikaciju sistema i metoda kriptografije.

Opravdanost istraživanja/rada: Opravdanost istraživanja se ogleda u potrebi da se prizna važnost pogodnostima primjene kriptografije u današnje vrijeme.

Ključne riječi

historija kriptografije, kriptografija, područja primjene, kriptografske metode

ABSTRACT

Reason for writing and research problem (s)

Technical-technological development enables the improvement and innovation of new communication channels. In the field of critical human activities, the basic question is

[181] Fakultet za kriminalistiku, kriminologiju i sigurnosne studije Univerziteta u Sarajevu

how to protect a man from the modern threats he is exposed to. In the available academic literature, there is incomplete information about methods for analyzing hidden information and which belong under the category of cryptography.
Aims of the paper (scientific or social)
The aim of the paper is to analyze the historical role of cryptography, to indicate the reasons for its appearance, application, and importance in order to improve the safety and protection of people and society as a whole. Filling the gaps in the available material from this field is a supplementary goal of work, as it will work in a systematic and unique way to encircle the observed situation.
Methodology/ Design
The paper uses primarily the technique from a qualitative research paradigm. The method of content analysis will explore the cryptographic systems and methods. The selection of academic papers in the field of cryptography was done in a way that only works that have a history and development component of security and cryptography are selected.
Research/ Paperlimitation
Lack of scientific discourse and the existence of a pronounced disparity in theoretical considerations, regarding the interpretation of crypto operations.
General Conclusion
The results refer to the display and classification of systems and methods of cryptography.
Research/ Paper Validity
The justification of the research is reflected in the need to recognize the importance of the benefits of applying cryptography today.

Keywords
history of cryptography, cryptography, application areas, cryptographic methods

UVOD

Prema osnovnom modelu komunikacije pošiljatelj šalje poruku primatelju koja do njega putuje komunikacijskim kanalom, istu tumači na svoj način i koristi u svom vlastitom interesu ili potrebi. Temeljni proces komunikacije je stvaranje odnosa, odnosno stvaranje raznovrsnih socijalnih interakcija, dok je središnji element komunikacije upravo interakcija koja pomaže da se prihvaćene informacije interpretiraju prema namjeni i želji pošiljatelja (Rouse i Rouse, 2005).

"Poriv za otkrivanje tajni duboko je protkan kroz ljudsku narav; čak i krajnje neradoznali um uzbuđuje misao da bi mogao saznati nešto što je drugima uskraćeno."
John Chadwick

Svakako da današnji informacijsko-komunikacijski sistemi izuzetno smanjuju značaj prostornog i vremenskog faktora i time, možemo pretpostaviti, donose velike uštede uz povećanje efikasnosti informacijskih aktivnosti. Povećanje efikasnosti informacijskih aktivnosti donosi nove mogućnosti proširenja pristupa informacijskim sadržajima, kvalitetnije provođenje svih aktivnosti neposredno vezanih za korištenje informacijskih sadržaja.

Prema Reardonu (1998) šest je temeljnih karakteristika ljudske komunikacije koje uključuju sljedeće: 1. Ljudi komuniciraju iz mnoštva različitih razloga; 2. Komuniciranje rezultira namjeravanim, ali i nenamjeravanim učincima; 3. Komunikacija je obično obostrana; 4. Komuniciranje uključuje najmanje dvije osobe, koje jedna na drugu utječu u nejednakoj mjeri; 5. Komunikacija se dogodila i onda kada nije bila uspješna; 6. Komuniciranje uključuje upotrebu simbola.

Ljudi su od davnina željeli neometano i sigurno komunicirati,[182] s tim što su istovremeno bili svjesni da njihove poruke često putuju nesigurnim komunikacijskim kanalima kojima može pristupiti i treća osoba koja će vidjeti poruku iako joj nije namijenjena. Shodno tome, raste prijetnja da se otkriju važne informacije od kojih se očekuje da nas vode i da nam pomažu u pronalaženju alternativa i prijedloga, odnosno da reduciraju negativne efekte određenih problemskih situacija.

Uvijek aktuelna opasnost da bi neprijatelj mogao doći do informacije, potaknula je razvoj šifri i kodova. Zbog toga su naprimjer, mnoge zemlje počele osnivati odjele i institute za analizu i primjenu šifriranja. Kao rezultat pojave ovih aktivnosti, na neprijateljskim stranama istovremeno su započele mjere i aktivnosti za analizu kriptiranih sadržaja i razbijanje primijenjenih šifrarskih sistema kako bi se došlo do tih vrijednih informacija. Svaka je šifra snažna sve dok se ne otkrije njen ključ, te ista postaje beskorisna i mora se napraviti nova te tako sve u krug (Posavec, 2018). Kako su se kroz stoljeća promijenili načini prenošenja poruka, osnovni problem zapravo je ostao isti, a to je kako onemogućiti onoga tko može nadzirati komunikacijski kanal, kojim se prenosi poruka, da dozna njezin sadržaj. Načinima rješavanja ovog problema bavi se naučna disciplina koja se naziva *kriptografija*. Njezine su potencijale koristili vladari, ratnici, diplomate, uhode, mistici, kabalisti, alkemičari, nekromanti, policajci, ljubavnici, tragači za zakopanim blagom, naučnici, industrijalci, umjetnici i ljudi željni intelektualnih izazova. Ona je štitila državne, vojne, vjerske ali i privatne tajne.

Tokom posljednjih dvadeset godina akademska istraživanja o kriptografiji su doživjela veliku ekspanziju. U tom pravcu, autori ovog rada su postavili za cilj da ponude kratki historijski pregled i da ukažu na značaj kriptografije do danas, naročito obraćajući pažnju na određene pristupe razumijevanju savremenih postupaka koji se koriste u moderno doba. Naša zamisao i cilj će biti u cjelosti ostvaren ako barem u minimalnoj mjeri ojača svijest javnosti o važnostima korištenja sigurnih, zaštićenih i neometanih komunikacijskih usluga.

[182] Herodot u *Historijama* daje hroniku sukoba između Grčke i Perzije u 5. st. pr. Kr. i navodi da se već u tom razdoblju Grčka branila umijećem tajnog pisanja (Majić, 2015).

1. RAZLOZI NASTANKA KRIPTOGRAFIJE

Kako ćemo se u ovom radu baviti temama za koje je potrebno osnovno znanje, na samom početku ćemo ponuditi i obrazložiti osnovne elemente kategorijalno-pojmovnog aparata. Uzimajući u obzir da ljudi međusobno komuniciraju putem poruka važno je odrediti šta su poruke. Prema Reardonu (1998) sve poruke se sastoje od nizova simbola. Simboli su riječi, geste, slike, zvukovi ili pokreti, stoga što se ljudi više ili manje slažu u pogledu objekata, zbivanja ili osjećaja na koje se ti simboli odnose. Za potrebe izrade ovog rada, poruke ćemo razmatrati u kontekstu pisane komunikacije.

Prema Baueru (2002) kriptologija je starija više hiljada godina, i njen razvoj usko je vezan za razvoj matematike. Danas predstavlja interdisciplinarnu nauku koja obuhvata sve od matematike, statistike, logike, lingvistike, pa sve do elektromehanike, računarstva i umjetne inteligencije koje su više izražene danas nego u prošlosti. Ključ[183] je u kriptologiji naziv za informaciju koja onome koji tu informaciju posjeduje otkriva kojim je postupkom originalna poruka sakrivena, što mu omogućuje otkrivanje poruke. Kriptologija je u velikoj mjeri osnova za zaštitu informacija i cyber sigurnost.

Potreba za sakrivanjem poruka prisutna je otkako je ljudski rod iselio iz pećina, počeo živjeti u skupinama i odlučio ozbiljno shvatiti civilizacijsku ideju. Kako su postojale različite grupe ili plemena, pojavila se i ideja da, u cilju opstanka, moraju raditi jedni protiv drugih i raširiti se, zajedno s nasiljem, manipulacijama gomile i tajnošću. Načelno se razlikuju dva oblika skrivanja poruka u pisanoj komunikaciji. Naime, steganografija (grč. στεγανός, pokriven i γράφειν, pisati) pretpostavlja skrivanje same poruke, a kriptografija (grč. κρυπτός, skriven i γράφειν, pisati) skriveno, tajno pisanje, odnosno oblikovanje tajne, šifrirane poruke koja će biti razumljiva samo pošiljatelju i primatelju (Pawlan, 1998). Poruku koju pošiljatelj želi poslati primatelju zvat ćemo otvorenim tekst (engl. *plaintext*). To može biti tekst na bilo kojem jeziku, numerički iskazan tekst ili nešto drugo. Pošiljatelj transformira otvoreni tekst pomoću unaprijed dogovorenog ključa (engl. *key*). Taj postupak zove se šifriranje, a dobiveni rezultat zove se šifrat (engl. *ciphertext*) ili kriptogram.

Ponekad nije dovoljno samo zadržati tajnost sadržaja poruke, što čini kriptografija, nego treba sakriti i samo postojanje poruke. Tehnika kojom se skriva poruka zove se steganografija. Moderna steganografija, koja koristi prednosti digitalne tehnologije, najčešće podrazumijeva skrivanje tajne poruke unutar neke multimedijske datoteke, npr. slike, audio ili video datoteke. Multimedijske datoteke u pravilu sadrže neupotrijebljene ili nevažne podatkovne prostore koje različite steganografske tehnike koriste tako da ih

[183] Ključ također može biti i predmet koji je kao takav nositelj informacije o metodi zakrivanja poruke. U antičkoj Grčkoj poruke su bile ispisane na životinjskoj koži ili platnu koje bi se potom omotalo oko štapa tačno određene visine i debljine. Taj štap predstavljao je ključ - ako bi se poruka na platnu ili koži omotala oko bilo kojeg drugog štapa, bila bi nečitljiva. U tom smislu, predmet je bio ključ.

popune s tajnim informacijama. Takve datoteke se potom mogu razmjenjivati bez da itko bude svjestan prave svrhe dotične komunikacije (CARNet, 2006).

Kako navodi Posavec, steganografija se primjenjivala u mnogo različitih oblika. Vojskovođe su znali obrijati glasniku glavu i na nju napisati poruku, te su pričekali da kosa ponovno naraste, a zatim poslali glasnika na odredište. Kinezi su poruke pisali na tankoj svili, koju bi potom smotali u kuglicu zvanu *„la wan"* i obavili voskom, a zatim bi ju glasnik sakrio u odjeću ili jednostavno progutao. Jedan od načina skrivanja poruke je bila i upotreba nevidljive tinte iz biljaka ili organskih tekućina, koja je nevidljiva kad se osuši, ali pri zagrijavanju postane smeđa. Sve metode tajnog komuniciranja bile su jako opasne jer ih se lako moglo otkriti. Prednost kriptografije je što neprijatelj ne može saznati sadržaj čak ni uhvaćene poruke (2018). Zbog toga se, uz steganografiju, počinje razvijati kriptografija koja se dijeli na klasičnu i modernu.

Međutim, da bismo razumjeli razlike između klasične i moderne kriptografije, moramo shvatiti osnovnu supstancu obje. The Concise Oxford Dictionary (2006) kriptografiju definira kao umjetnost pisanja ili rješavanja šifara. Ova bi definicija mogla biti historijski tačna, ali ne obuhvata suštinu moderne kriptografije. Prvo, fokusira se isključivo na probleme tajne komunikacije. O tome govori činjenica da definicija određuje „šifre", dok je drugdje definirana kao „sistem unaprijed dogovorenih simbola, koji se posebno koriste za osiguravanje tajnosti u prenošenju poruka". Do 20. stoljeća stvaranje dobrih šifara ili probijanje postojećih oslanjalo se na kreativnost i lične vještine. Prema Bagiću (2018) ogromne su razlike između rane klasične i moderne kriptografije s obzirom na tehnike i metode šifriranja, ali i s obzirom na komplesnost kriptograma ili šifrata. Krajem 20. stoljeća kriptografija se radikalno promenila. Polje kriptografije sada obuhvata mnogo više od elemenata tajne komunikacija, uključujući autentifikaciju poruka, digitalni potpis, protokole za razmjenu tajnih ključeva, protokole za provjeru autentičnosti, elektronske aukcije i digitalni novac (Katz i Lindell, 2007), što sve zajednički opet ne zatvara krug. Kriptografija je prešla iz umjetničke forme koja se striktno bavila tajnom komunikacija za vojsku do nauke koja pomaže u osiguranju sistema za sve ljude širom svijeta. To u velikoj mjeri znači da je postala središnja tema informatike i informacijske sigurnosti.

Generalno posmatrano, a uključujući trendove koje nameće tehničko-tehnološki razvoj, pored rizika da sadržaj poruka bude razotkriven, paralelno je rasla potreba za zadržavanjem tajnosti. To dovodi do osmišljavanja metoda kojima bi poruka na svom putovanju od pošiljatelja do primatelja došla bez da je itko s treće strane primijeti i preuzme. Tako su se vremenom osmišljavali alati za pisanje, načini prikrivanja pisma, načini pisanja, materijali za pisanje i druge tehnike. Usmjeravalo se na fizičko prikrivanje poruke. Jednom otkriveno postojanje poruke je razotkrilo i cijeli njezin sadržaj. Nije bilo dovoljno sakriti samo fizički zapis, ukazala se potreba ka orijentisanju i na značenje sadržaja samog zapisa. Kako su smišljane metode za očuvanjem tajnosti zapisa, tako su neprestano traženi i načini probijanja, odnosno dešifriranja istih.

2. SEGMENTI HISTORIJSKOG RAZVOJA

Dugo godina je kriptografija bila ekskluzivna vojna domena. Američka agencija za nacionalnu sigurnost (NSA) i agencije iz bivšeg Sovjetskog Saveza, Engleske, Francuske, Izraela i sl., potrošili su milijarde dolara u vrlo ozbiljnu igru osiguranja sopstvene komunikacije i razotkrivanja tuđe. Privatno pojedinci[184], sa daleko manje stručnosti i budžeta, nisu mogli zaštititi vlastitu privatnost od ovih vlada (Schneier, 1996). Mehanizmi zaštite u pravilu bi trebali biti pouzdani i jednostavni za korisnike. Da li je to uvijek bio slučaj, nastojat ćemo u nastavku prikazati kroz pregled određenih najznačajnijih historijskih razvojnih perioda ove izuzetne discipline.

Već 1900. godine prije Krista, u današnjem Egiptu korišteni su hijeroglifi na nestandardan način, vjerojatno kako bi sakrili značenje od onih koji nisu znali značenje (Whitman i Mattord, 2005). Rana kriptografija bavila se isključivo pretvaranjem poruka u nečitljive grupe simbola, brojeva i/ili slika radi zaštite sadržaja same poruke tokom prenošenja poruke s jednog mjesta na drugo.

Metode, koje su se najčešće tokom historije koristile za šifriranje poruka, bile su zamjena (supstitucija[185]) i premještanje (transpozicija[186]) osnovnih elemenata teksta (slova, blokova slova, bitova). Kombinaciju ovih metoda susrećemo i danas u najmodernijim simetričnim kriptosistemima. Asimetrični kriptosistemi s javnim ključem pojavili su se tek 70-tih godina 20. stoljeća. Kod njih se za šifriranje koriste funkcije koje su "jednosmjerne" i to znači da funkcija za šifriranje može biti javna, dok samo funkcija za dešifriranje mora biti tajna. U konstrukciji jednosmjernih funkcija koriste se "teški" matematički problemi, kao što su faktorizacija velikih prirodnih brojeva, te logaritmiranje u konačnim grupama (Dujella i Maretić, 2007).

U transpozicijskim[187] šiframa slova ishodišne poruke ili otvorenog teksta mijenjaju redoslijed pojavljivanja, ali zadržavaju svoj identitet. Što je poruka opsežnija, raste i broj

---

[184] Krug korisnika kriptografije uključuje i kriminalce. Vrijeme prohibicije u SAD-u pogodovalo je usponu kriptografije u službi kriminalnog miljea. Od tada, pa do danas u FBI-u postoji jedinica za kriptoanalizu (skr. CRRU) koja se bavi razbijanjem šifri koje koriste kriminalci.

[185] U sistemu supstitucije, kratki tekstovi poruke su sistematski zamijenjeni drugim znakovima. Nakon zamjene, redoslijed temeljnog konteksta je nepromijenjen, ali isti znakovi nisu više prisutni. U najjednostavnijim sistemima zamjene, zamjena je dosljedna; dati znak otvorenog teksta uvijek prima isti zamjenski znak. Sigurniji sistemi mijenjaju zamjene tako da imaju određene ekvivalente koji se mijenjaju svaki put kada se isti znak šifrira.

[186] U sistemu transponiranja, simboli otvorenog teksta se sistemski preuređuju. Nakon prenošenja poruke, isti su znakovi još uvijek prisutni, ali redoslijed slova je promijenjen.

[187] Transpozicijsko šifriranje je klica kriptografije. Naime na njezinu početku stoji skital, prvo poznato kriptografsko pomagalo. Radi se o tehnici tajne komunikacije za koju su bila potrebna dva drvena štapa jednake duljine i debljine, tj. dva skitala – jedan bi posjedovao pošiljatelj, a drugi primatelj poruke. Pošiljatelj bi oko štapa namotao vrpcu od pergamenta ili kože i na nju okomito napisao poruku. Kada bi se vrpcu odmotalo, kriptogram bi bio zgotovljen – na njoj se mogao vidjeti samo niz naizgled nepovezanih slova. Ako je

potencijalnih kombinacija njezinih dijelova. Tako primjerice rečenica od 30 slova omogućuje više od 50 milijardi kombinacija (Lunde 2010).

Kod supstitucijskih šifri slova otvorenoga teksta mijenjaju identitet, tj. bivaju zamijenjena drugim slovima ili znakovima, ali zadržavaju redoslijed pojavljivanja. Najstarija, a možda i najglasovitija supstitucijska šifra je ona koju je Julije Cezar koristio u Galskom ratu. Upotrijebljena je zamisao o prebacivanju slova na dogovoreni broj i tako je napisana poruka. Tada bi primatelj preusmjerio slova na isti broj i jednostavno dešifrirao poruku (Taylor, 2002). Cezarova šifra nazvana je monoalfabetskom šifrom. Budući da se temelji na jednostavnom pomaku, kombinacija je onoliko koliko i slova abecede. To je vrlo malen broj i takvu je šifru relativno lako dešifrirati. Međutim, monoalfabetska šifra može se oblikovati i određenim pomacima koji neće poštovati abecedni redoslijed slova, što do vrtoglavih granica uvećava broj potencijalnih kombinacija.

U nastavku, kako u arapskom svijetu dolazi do revolucije u području matematike, paralelno se izučava i razvija kriptologija. Arapski matematičari prikupili su veliku količinu znanja iz antičkih grčkih polisa i iskoristili ga za napredak civilizacije.[188] Teorija i praksa kriptoanalize tako je započela razvijanjem frekvencijske metode**,** koja se temeljila na proučavanju frekvencijskog pojavljivanja riječi, znakova ili simbola u tekstu (Wrickson, 1998). Matematičar, astrolog, psiholog i meteorolog Al–Kindi pojašnjava da se enkriptirana poruka na poznatom jeziku razrješuje tako da se potraži neki drugi otvoreni tekst na istom jeziku dovoljno dug da se može utvrditi učestalost pojavljivanja pojedinih slova (Bagić, 2018).

Frekvencijska analiza je ponudila jedinstven, nadasve dragocjen alat svima koji su nastojali proniknuti u smisao monoalfabetskih tajnih poruka. Ona se zasniva na tezi da je učestalost pojavljivanja važan element identiteta svakog slova te da nam upravo jednom utvrđeni identiteti omogućuju prepoznavanje tih slova, čak i kada su skriveni drugim znakovima. U daljnjem razvoju frekvencijske analize, uz istraživanje mogućih veza između podjednako učestalih slova i kriptografskih simbola, uspoređivale su se i relacije između podjednako učestalih dvoslova ili troslova u jeziku poruke i dvočlanih ili tročlanih dijelova šifrata. Frekvencijska analiza je podstakla kriptografe da traže druge i drukčije, tj. sigurnije načine šifriranja.

Cezarova šifra predstavljala je jedan od najpoznatijih postupaka kriptografije. Kasnije, istaknutiji postupci su sistemi koje je osmislio Leon B. Alberti, Blaise de Vigener i Gilbert Vernam.

---

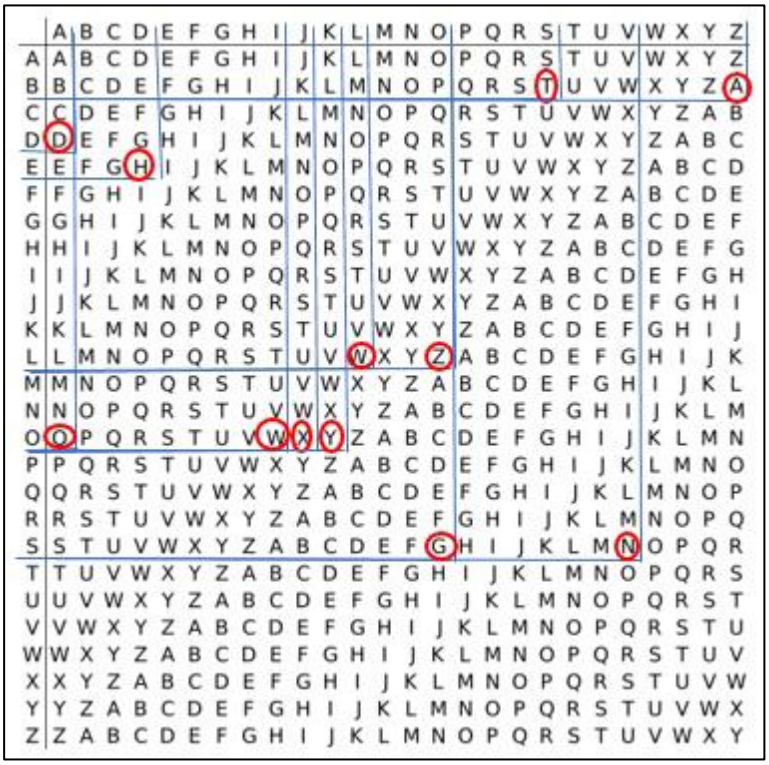
vrpca bila kožna, glasnik ju je mogao okrenuti naopako i opasati se njome. Kada bi poruka došla primatelju, on bi je namotao na svoj skital i pročitao (Bagić, 2018).

[188] Za razliku od Grka koji su se do tada bavili isključivo kriptografijom (npr. Spartanci, metodom korištenja platna omotanog oko štapa), Arapi su prvi krenuli razvijati kriptoanalizu.

Leon Battista Alberti umjesto monoalfabetske zamjene predlaže polialfabetski[189] sistem s dvije šifrarne abecede koje će oblikovati šifrat nedostupan frekvencijskoj analizi. Njegov se šifrirni brojčanik sastoji od dva diska, nepokretnog vanjskog (stabilis) na kojem je ispisana latinska abeceda bez slova H, K, J i Y te brojevi od 1 do 4, i pokretnog unutrašnjeg (mobilis) na kojemu su ispisana slova abecede prema slučajnom rasporedu i znak &. Poruka se enkriptira čas prema jednoj, čas prema drugoj abecedi, što rezultira time da isto slovo iz otvorenog teksta može biti zamijenjeno različitim slovima u šifratu. Mowry naglašava da sagovornici moraju imati identične diskove, a prije komuniciranja trebaju dogovoriti indeksno slovo u pokretnom unutrašnjem krugu (2014). Alberti je doprinio razvoju polialfabetičke supstitucije. Njegova metoda bila je upotreba dva bakrena diska koji se međusobno uklapaju. Svaka je na sebi imala upisanu abecedu. Nakon svakih nekoliko riječi, diskovi su rotirani kako bi promijenili logiku šifriranja, čime je ograničena upotreba frekvencijske analize za pucanje šifre (Cohen, 1990). Albertijev šifrarnik je nastao kao modifikacija, odnosno usavršeni postupak Cezarove šifre.

Slijedom razvoja kriptografskih postupaka, Bagić (2018) ističe da je francuski diplomat Blaise de Vigenére tokom službovanja u Italiji pomno proučio Albertieve spise, te oblikovao snažan kriptosistem koji se služi s 26 šifrarnih abeceda. Snaga ovog postupka je u činjenici da se ona služi ne jednom ili dvjema šifriranim abecedama, nego poruku enkriptira pomoću 26 abeceda, tačnije za svako slovo jednom. Prema istom autoru, punih 300 godina se vjerovalo da je kao takav posve siguran, toliko da je prozvan i neprobojnom šifrom (fr. *le chiffre indéchiffrable*). Vigenéreov kvadrat funkcionira tako da kriptograf odredi ključnu riječ (npr. SLOBODA) koja će, budući da je sedmoslovna, povezati sedam šifrarnih abeceda koje naizmjenično sudjeluju u šifriranju poruke. Škrobo (2017) u svom radu slikovito navodi da ključ pokazuje koji redak (počinje slovom iz ključa) treba upotrijebiti za šifriranje, a zatim se slovo spaja sa slovima obične abecede ispisane iznad stupca. Stoga bi početna poruka: „VOJSKADOLAZI“ nakon šifriranja glasila „NZXTYDHGWOAW“.

[189] Šifra koja jedno slovo otvorenog teksta mijenja sa više slova šifriranog teksta.



Slika 1: Vigenéreov kvadrat u kombinaciji s ključem SLOBODE (Škrobo, 2017).

Gilbert Vernam, inženjer američke kompanije Telephone & Telegraph (AT&T) radio je na poboljšanju šifre, stvarajući šifru Vernam-Vigenere 1918. godine. Njegov rad doveo je do jednokratne pločice, koja ključnu riječ koristi samo jednom, a pokazalo se da je gotovo neraskidiva (Rubin, 2008). U vrijeme Vernamovog rada, sve poruke koje se prenose preko AT&T-ovog teleprinter sistema bile su kodirane u *Baudot Code*[190], binarnom kodu u kojem kombinacija znakova i razmaka predstavlja slovo, broj ili drugi simbol (Britannica, 2020). Vernam je predložio način uvođenja izjednačavanja istom brzinom koji je smanjen suvišnim brojem simbola poruke, čime je zaštitio komunikaciju od kriptoanalitičkog napada. Uvidjelo se da se periodičnost (kao i informacije o frekvenciji i intersimbolna povezanost), na koju su se oslanjale ranije metode dešifriranja različitih Vigenèreovih sistema, može eliminirati ako se slučajna serija znakova i razmaka (tekući ključ) pomiješa s

[190] U digitalnoj telegrafiji (teleprinter, telex) standardni 5-bitni kod obično se koristi za predstavljanje znaka (slovo, broj ili interpunkcijski znak), poznat kao Baudot kod. Zvanični naziv za najnoviji telegrafski standard je ITA2 (Međunarodna telegrafska abeceda br. 2). Nadjačao ga je ASCII 1963. godine, ali i danas ga koriste amateri. Najčešći 'Baudot' kod poznat je i kao Murray kod, ili kao Baudot-Murray kôd. Standard ITA2 široko se koristi kod povijesnih šifrarskih strojeva (CryptoMuseum, 2020).

porukom tokom šifriranje da bi se dobilo ono što je poznato kao šifra niza[191] (engl. *stream cypher).*

Međutim, postojala je jedna ozbiljna slabost u Vernamovom sistemu. Zahtijevao je jedan simbol ključa za svaki simbol poruke, što je značilo da će korisnici morati unaprijed razmijeniti suviše veliki ključ, što praktično znači da su morali sigurno razmijeniti ključ ravnomjerne dužine poruke koju će na kraju poslati. Sam ključ sastojao se od probušene papirne vrpce koja se mogla automatski čitati dok su simboli upisani na tastaturi teleteksta i šifrirani za prijenos (Britannica, 2020).

Upravo je telegraf omogućio ogroman napredak u području kriptologije i kriptografije. Telegraf predstavlja uređaj za prenos kodiranih poruka. Prema Pađenu (2018) prenos skrivenih poruka postao je lakši i telegraf je omogućio nastanak elektromehaničkih enkripcijskih uređaja koji bi se koristili složenijim algoritmima za šifriranje ili dešifriranje poruka, a vrhunac ovog otkrića manifestirat će se za vrijeme Drugog svjetskog rata, izumima kao što su Enigma, SIGABA i mnogi drugi. U svojim počecima, telegraf je zahtijevao vezu između dva uređaja kako bi komunikacija bila moguća, no izumom radija omogućena je bežična komunikacija korištenjem električnih signala koje su uređaji mogli odašiljati.

Prijenos skrivenih poruka postao je lakši nego u početku, kada je trebala postojati fizička veza između dva telegrafska centra. No, loša strana je bila ta da su radio-signalu mogli pristupiti i oni koji nisu učestvovali u komunikaciji između dva operatera. Tako je došlo do potrebe za sve jačim kontramjerama koje bi spriječile pokušaje kriptoanalize presretanih radio-poruka. Ovakve novosti potaknule su na razmišljanje i donošenje novih pretpostavki o tome kako bi se kriptografija trebala shvatiti, razvijati, i na kraju krajeva koristiti. Pađen (2018) navodi da je jedan od tih teoretičara bio i Auguste Kerckhoffs, koji je u djelu "*La Cryptographie Militaire*" (fr. "Vojna kriptografija") napisao da:

a) šifrat u praksi mora biti neprobojan;
b) kriptosistem mora biti prikladan za komuniciranje;
c) ključ mora biti lako pamtljiv i lako promjenjiv;
d) šifrat mora biti moguće prenijeti telegrafom;
e) aparat za šifriranje mora biti lako prenosiv;
f) kriptografski stroj mora biti jednostavan za rukovanje.

Pored telegrafa, za revoluciju u području kriptografije u proteklom stoljeću zaslužna su upravo velika ratna zbivanja, gdje su brojni elektromehanički izumi korišteni često kao sredstvo za ostvarenje ratnog cilja i svrhe, a predstavljali su već sintezu određenih gore spomenutih realizacija različitih teorija i postupaka.

[191] Šifra kojom se šifrira čitav niz podataka.

Puno razumijevanje doprinosa kriptografije ali i same obavještajne djelatnosti uključuje mnoge događaje tokom prve polovine 20. stoljeća. Prema Tayloru (2010) uloga britanskih obavještajnih službi u ulasku Amerike u Prvi svjetski rat zbog afere sa Zimmermanovim telegramom, obavještajni neuspjeh koji je SAD uveo u Drugi svjetski rat (Pearl Harbor) i dramatični utjecaj kriptografije tokom Drugog svjetskog rata (razvoj „Enigme“) izuzetno su zanimljivi i važni slučajevi koji predstavljaju svojevrsne prekretnice u izučavanju ove teme.

Prvi svjetski rat se odvijao na teritoriju Europe, dok se neutralne Sjedinjene Američke Države zajedno s predsjednikom Thomasom Woodro Wilsonom nisu imale namjeru uplitati u sukob. To je odgovaralo građanima Amerike, zbog čega je 1917. Wilson dobio drugi mandat pod sloganom „On nas drži podalje od rata". Međutim, jedan izuzetno značajan događaj promijenit će stav cijele zemlje prema ratu, a osobito prema Njemačkoj. To je objavljivanje onoga, što je postalo poznato kao Zimmermannov telegram, nazvanog prema autoru, njemačkom ministru vanjskih poslova Arthuru Zimmermannu. Arthur Zimmermann u telegramu predlaže Meksiku savezništvo u slučaju da Sjedinjene Američke Države uđu u rat. Predlaže Meksiku da ukoliko do toga dođe, uspostavi rat sa SAD-om kako bi povratio ranije izgubljeni teritorij, te time ograniči broj američkih vojnika na evropskoj fronti. Zahvaljujući britanskim kriptoanalitičarima, taj plan je ubrzo razotkriven, a Amerika je proglasila rat. U neznanju, Nijemci su vjerovali kako je riječ o svojevrsnoj izdaji, te kako su kodovi kojima je telegram bio šifriran ostali povjerljivi. No, pogriješili su, dešifriranje Zimmermannovog telegrama bilo je najveće postignuće Prvog svjetskog rata. Zimmermanov telegram kodiran je pomoću šifrata „0075", dvodijelnog koda od 10 000 riječi i fraza s brojevima od 0000 do 9999. Brojevi su nasumično odabirani, kako bi se izbjegle analize frekvencija, te dodatno individualno kodirani jednostavnom supstitucijom. Šifrat je siguran sve dok knjiga kodova ostane tajna. Stariji kod „13040", već je ranije bio dešifriran od strane britanskih dešifranata, no kod „0075“ se smatrao pouzdanim. Međutim, Nijemci su podcijenili britanske dešifrante. Telegram su na putu za Washington presreli Britanci, a dešifrirali su ga u „Sobi 40", uredu za šifriranje, u kojem je radila nekolicina sposobnih kriptoanalitičara (Čavajda, 2017).

Neposredno prije Drugog svjetskog rata konstruišu se prve elektromehaničke mašine za šifriranje. Njemačka kriptografska mašina „*Enigma*“[192] predstavlja vjerovatno najpoznatiju svjetsku mašina za šifriranje poruka, uglavnom zbog vitalne uloge koju je odigrala tokom Drugog svjetskog rata. Pored Enigme, za sigurnu teleprinter komunikaciju (teleks) njemačka vojska je koristila i *Siemens T-52 Geheimschreiber* i *Lorenz SZ-40*[193]. Lorenz SZ-

[192] Sredinom 1930-ih njemačka vojska se očito pripremala za rat te je započela naručivanje strojeva Enigma-I u velikim količinama za *Wehrmacht* (vojsku) i *Luftwaffe* (zrakoplovne snage). Enigmu G koristi njemačka *Abwehr* (tajna služba). Za *Kriegsmarine* (njemačka mornarica) razvijen je model sličan kompatibilnom s Enigma-I. Postaje poznat kao Enigma M1 (1934), a kasnije slijedi Enigma M2 (1938) i konačno Enigma M3 (1940) (CryptoMuseum, 2020).

[193] Lorenz SZ-40/42 koristila je *Oberst-Kommando der Wehrmacht*, ili OKW (Visoka komanda njemačke vojske) za komunikaciju na najvišem nivou između Hitlera i njegovih generala. Stroj se zvao Schlüsselzusatz (SZ), što znači dodatak za šifriranje (CryptoMuseum, 2020).

40 bio je elektromehanički uređaj za šifriranje teleprinter signala i dešifriran je tokom Drugog svjetskog rata u Bletchley Park-u (CryptoMuseum, 2020). Za vrijeme Drugog svjetskog rata, Bletchley Park je bio glavni centar za kriptoanalizu, za razbijanje šifara. Alan Turing pridružio se GC&CS, prethodniku GCHQ[194] u septembru 1939. godine kako bi pomogao u pokušaju razbijanja koda tokom Drugog svjetskog rata, radeći zajedno s Gordonom Welchmanomi i drugim stručnjacima. 1940. Turing u saradnji sa poljskim kolegama dobio je na uvid komponente potrebne za dizajn *Bombe*[195].

Postoje i mnoge druge zanimljive mašine za šifriranje prikazane na slici ispod, o kojima se mnogo detaljnije može istražiti na stranici CyptoMuseum.com. WashingtonPost (2020) nudi uvid u operaciju „Rubikon" kojom su CIA i BND još od 1950-ih prisluškivali komunikaciju više od stotinu stranih vlada, tako što su im preko švicarske kompanije Crypto AG obezbjeđivale mašine za šifriranje poruka.[196] S druge strane, nisu rijetke pojave da pojedine države energiju usmjere na vlastito inoviranje kriptografskih uređaja.[197]

Slika 2: Izdvojeni kriptografski uređaji (CryptoMuseum, 2020)

Enigma je uređaj koji se sastoji od tipkovnice s 26 tipki poput pisaćeg stroja, zaslona s 26 žaruljica za prikaz šifriranog izlaza, tri mehanička rotora i električne prespojne ploče, a napaja se putem ugrađene baterije. Pritiskom na tipku kroz mrežu kontakata rotora i prespojne ploče zatvara se strujni krug i pali se odgovarajuća žaruljica koja označava šifrirano slovo (Posavec, 2018). Upotrebljavali su se višestruki diskovi za šifriranje posebno pozicionirani unutar Enigme, odakle su mogli simulirati različite šifrirane abecede, a sve

[194] Vladin štab za komunikacije Ujedinjenog kraljevstva Velike Britanije i Sjeverne Irske (engl. *Government Communications Headquarters*)
[195] Bomba je bila prva britanska kriptoanalitička mašina posebne namjene i dala je veliki doprinos u dešifriranju Enigme.
[196] „Bio je to najduži i najproduktivniji obavještajni projekt od Drugog svjetskog rata. Strane vlade plaćale su solidan novac SAD-u i Zapadnoj Njemačkoj kako bi dobile privilegiju da njihovu najtajniju komunikaciju čitaju barem dvije strane zemlje. Bio je to obavještajni potez stoljeća." (WashingtonPost, 2020).
[197] Kriptografski uređaj TelSec prvi je sklopovski kriptografski uređaj razvijen u Republici Hrvatskoj (Mreža.bug, 2020).

s ciljem sprječavanja uspješnog frekvencijskog analiziranja. Da bi se poruka dešifrirala, bila je potrebna knjiga kodova (koju imaju samo primatelj i pošiljatelj poruke) s pojedinostima o specifičnim postavkama za šifriranje, i to na dnevnoj bazi (Dsm, 2017).

Lienhard (2003) smatra da je glavna ideja njemačkog izumitelja Arthura Scherbiusa bila zamijeniti kriptografski sistem koji se koristio u Prvom svjetskom ratu, novim sigurnijim sistemom šifriranja. Već 1918. godine Arthur Scherbius i njegov prijatelj Richard Ritter osnivaju strojarsku tvrtku Scherbius & Ritter.

Lienhard nadalje pojašnjava kako je postupak izgledao. Naime, jedan od osnovnih dijelova Enigme je i premetačka jedinica koju čini rotor (engl. *scrambler*) koji predstavlja najvažniji dio stroja. Rotor je debeli disk isprepleten žicama koje određuju kako će se slova otvorenog teksta šifrirati. Šifrarna abeceda se poslije svake enkripcije mijenja, a zahvaljujući toj rotaciji, rotor stvara dvadeset i šest šifriranih abeceda. Dakle, stroj omogućava pisanje polialfabetskom šifrom. Enigma se sastojala od tri rotora i time je mogla zauzeti ukupno 17 576 položaja. Sigurnost se mogla povećati dodavanjem novih rotora, no time bi se istodobno povećavale i veličina i težina samog uredaja. Umjesto toga, Scherbius je odlučio povećati sigurnost povećanjem broja mogućih početnih postavki na dva načina: izmjenjivim rotorima i prespojnom pločom. Ona mijenja električne puteve između tipkovnice i prvog rotora, omogućujući inicijalnu zamjenu slova prije samog procesa šifriranja. Naprimjer, moguće je zamijeniti slova „B" i „F" tako da se pritiskanjem tipke „B" odašilje slovo „F" i obratno. Operator je imao šest kablova. Dakle, šest parova slova moglo je zamijeniti mjesta, a ostalih četrnaest slova ostalo je na istom položaju. Stoga, položaj rotora određuje 17 576 različitih ključeva, tri rotora mogu se zamijeniti na 6 različitih načina, te 6 parova slova od njih ukupno 26 mogu se prespojiti na prespojnoj ploči na ukupno 100 391 791 500 različitih načina. Množeći dobivene varijacije dobivamo ukupan broj ključeva od 10 000 000 000 000 000, što je fascinantan broj varijacija (2003).

3. OSNOVE RAZUMIJEVANJA SAVREMENIH KRIPTOGRAFSKIH POSTUPAKA

Određeni ranije prikazani postupci su poslužili kao odskočna daska za razvoj modernih sistema šifriranja. Dujella i Maretić (2007) ističu da bi se dvjema stranama omogućila komunikacija putem nesigurnog komunikacijskog kanala (unutar kojeg je prisutna i treća strana koja taj kanal nadzire) potrebno je osigurati tajnost njihove poruke. Princip je sljedeći: pošiljatelj poruke i njezin primatelj unaprijed dogovaraju ključ za šifriranje. Zatim pošiljatelj tim ključem pretvara razumljivi tekst poruke u šifrat (kriptogram, tj. nečitljive podatke) i šalje ga putem komunikacijskog kanala. 'Presretač' može doznati sadržaj šifrata, ali ne može odrediti tekst poruke. Za razliku od njega, primatelj kojem je poruka poslana zna ključ kojim je šifrirana poruka te može dešifrirati šifrat i učiniti tekst ponovno razumljivim. Takav način šifriranja/dešifriranja uključuje podijeljeni ili tajni ključ i predstavlja *simetričan* tip kriptografije. Drugi tip je *asimetrična* kriptografija. Djeluje s javnim

ključem koji je slobodno distribuiran te privatnim ključem vlasnika. Poruka se šifrira javnim ključem, a dešifrirati je može samo pridruženi privatni ključ.

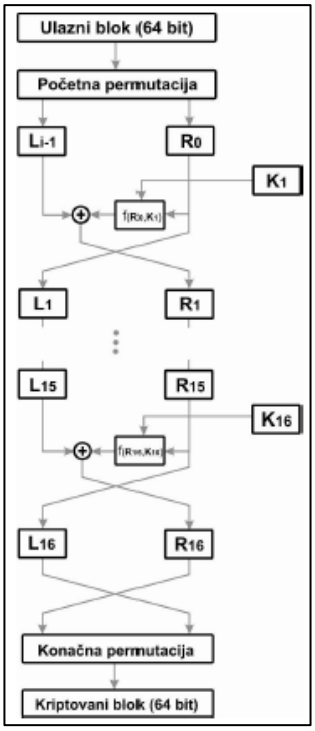
Također, Kuhn (2001) objašnjava osnovne vrste sistema šifriranja u savremenoj upotrebi: simetrični („privatni") i asimetrični („javni") sistem. U simetričnom sistemu koristi se isti ključ za obje funkcije, i za šifriranje i dešifriranje dokumenta. Čest primjer ovog oblika šifriranja je funkcija zaštite šifre obrađivača teksta, kao što je Microsoft Word, pomoću kojeg korisnik može zaključati dokument, a zatim ako isti dokument dostavi kolegi, isti će morati upotrijebiti identičnu šifru za otvaranje dokumenta. Ovaj oblik šifriranja je dovoljan za zaštitu ličnih dokumenata, gdje korisnik to želi kako bi spriječio da svi osim njega ne mogu pristupiti određenim datotekama. Međutim, simetrična enkripcija problematična je kada čovjek želi sigurno komunicirati s drugima, pri čemu stvara mogućnost da se prilikom razmjene ključeva sama komunikacija vrši preko nesigurnog kanala, čime se narušava sigurnost komunikacije prije nego što je do samog šifriranja uopće došlo. Kriptografija omogućava zaštitu osjetljivih podataka, bilo u pohrani ili u komunikaciji, i predstavlja nužnu pretpostavku bilo kojeg sigurnog e-poslovanja ili elektronskog komunikacijskog sistema (uključujući sigurnu e-poštu i glasovnu komunikaciju). Prema Posavec (2018) najpoznatiji algoritmi simetričnih kriptosistema koji se danas koriste su: DES, 3DES, DES-CBC, IDEA, RC5, RC6, AES.

Početkom šezdesetih godina prošlog veka, kompanija IBM je pokrenula istraživački projekat u cilju zaštite podataka pod nazivom *Lucifer*. Ovaj projekat okončan je 1971. godine i Lucifer je bio prvi šifrat sa blokovima veličine 64 bita koji je koristio ključ od 128 bita. Kompanija je kasnije komercijalizovala ovaj način kodiranja i nazvala ga DES (engl. *Data Encryption Standard*). 1976. godine DES je prihvaćen kao federalni standard za enkripciju podataka i korišten je u komunikacijama Američke vlade. DES je narednih dvadesetak godina bio najviše korišteni standard na svijetu. Tokom eksploatacije, DES standard je bio modifikovan i unapređivan svakih pet godina. Naslijedio ga je 2001. god. AES (engl. *Advanced Encryption Standard*), također poznat pod nazivom *Rijndael* algoritam. U poređenju sa DES, novi algoritam je bio dosta napredniji po pitanju sigurnosti podataka. Danas, DES algoritam i dalje koristi veliki broj organizacija u svijetu čime je nastavio život pružajući zaštitu u mrežnim komunikacijama, skladištenjima podataka ali i sistemima za kontrolu pristupa (Rhee, 2003).

DES suštinski predstavlja simetrični algoritam za kriptovanje blokovskog tipa, odnosno predstavlja direktnu upotrebu blok-šifre[198] (ECB mod). Kao ulaz u algoritam se koristi blok od 64-bita izvornog teksta i 56-bitni ključ. Izlaz iz algoritma je 64-bitni kriptovan tekst koji se dobija nakon 16 iteracija koje se sastoje od identičnih operacija. Ključ od 56 bita se formira od inicijalnog 64-bitnog ključa informacije ignorisanjem svakog 8 bita, tj.

[198] Šifra kojom se šifrira blok podataka fiksne dužine.

odsjecanjem ukupno 8 bitova. Na slici u nastavku prikazan je izgled DES algoritma za kriptovanje.[199]



Shema 1: DES algoritam (Buchman, 2002).

Problem s razmjenom ključeva riješen je 1970-ih pojavom asimetričnih ključnih sistema. Dok se u simetričnom sistemu ključeva isti ključ koristi za obje funkcije, u asimetričnom sistemu ključeva, jedan je ključ - *javni ključ* i koristi se za šifriranje, a za dešifriranje se koristi zasebni ključ - *privatni ključ* (Black, 2001). Vetter ističe da su i javni i privatni ključ matematički povezani (2010). Javni ključ korisnika može se učiniti općenito dostupnim (npr. objavljivanjem na web stranici) i svako ko želi korisniku poslati šifrirani dokument može preuzeti javni ključ i koristiti ga za šifriranje poruke. Međutim, poruka tada ne može

[199] Buchman (2002) objašnjava da se kriptovanje pomoću DES algoritma sprovodi u nekoliko koraka. Prvo se bitovi ulaznog bloka dužine 64 bita permutuju početnom permutacijom. Radi se o permutaciji koja vrši zamjenu bitova. Permutovan ulazni blok dijeli na dva dijela od po 32 bita, lijevi *L*i-1 i desni *R*0 deo. Nad desnim dijelom bloka se obavlja funkcija *f* (*R*0,*K*1) koja generiše 32-bitni rezultat. Nova 32-bitna vrijednost *R*1 se koristi za dalje operacije. Za lijevi dio *L*1 koristi se vrijednost *R*0 iz prethodne iteracije. Nakon ponavljanja 16 istovjetnih koraka, blokovi međusobno mijenjaju mjesta te se spajaju. Na kraju se obavlja konačna permutacija koja je inverzna početnoj. Konačna dobijena 64-bitna vrijednost čini kriptovani blok podataka.

biti dešifrovana od strane bilo koga - uključujući i originalnog pošiljaoca poruke, osim ako nema korisnikov privatni ključ, a ovaj ključ korisnik čuva (Black, 2001).

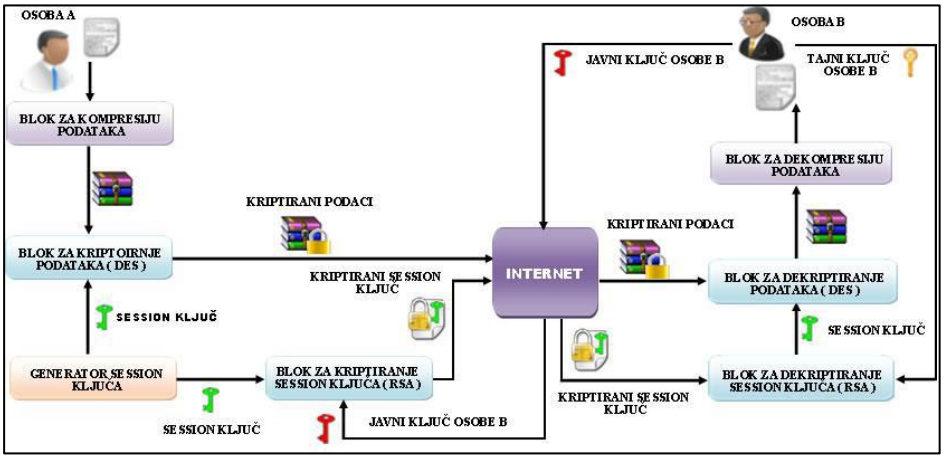
Godine 1977. dizajniran je RSA algoritam koji primjenjuje metodu šifriranja javnim ključem, te podržava šifriranje poruka i identifikaciju korisnika potrebnu za osiguravanje autentičnosti. Autori su američki kriptograf Ron Rivest, izraelski kriptograf Adi Shamir, te američki kriptograf Leonard Adleman po kojima je algoritam i dobio ime (Posavec, 2018). Prema istom autoru, najpoznatiji asimetrični algoritmi su RSA, Diffie-Hellman, ElGamal, Eliptične krivulje, Rabin.

Asimetrična kriptografija otvorila je potpuno nove vidike za šifriranje i olakšala razvoj mnogih aspekata modernog života. Sposobnost pokretanja sigurnog komunikacijskog kanala između dvije strane koje nikad dotad nisu komunicirale omogućio je, recimo, rast svih oblika e-trgovine na Internetu. Asimetrična kriptografija je u osnovi protokola *Hypertext Transfer Protocol - Secure* (u nastavku: HTTPS), koji omogućava sigurnu komunikaciju između poslužitelja i klijenata na cijelom svijetu. Bez asimetrične kriptografije sigurna komunikacija s dobavljačima e-trgovine ili dostupnost usluga internetskog bankarstva bile bi nezamislive kategorije nedostupne korisnicima.

Vetter (2010) naglašava da se sistemi šifriranja koji se danas koriste mogu učiniti izuzetno sigurnim, gdje jačinu sistema šifriranja karakteriziraju tri faktora: sigurnost šifrata, sigurnost osnovnog algoritma i dužina ključa. Sigurnost šifrata predstavlja odgovornost korisnika, i stoga je obično najmanje sigurna komponenta kriptografskog sistema.

Upotreba zajedničkog javnog ključa i privatnog ključa kojeg posjeduje samo pošiljalac danas se koristi kao oblik asimetrične enkripcije. Jedna od upotreba ove metode je da pošiljalac koristi privatni ključ za šifriranje poruke, a zatim svako ko primi poruku koristi javni ključ za dešifriranje. Na taj način primalac zna od koga je poruka morala doći. Prema Whitmanu i Mattordu (2005) ova metoda čini okosnicu digitalnog potpisa. Problemi nastaju kada komunikacija između više organizacija zahtijeva upotrebu mnogih javnih ključeva i kada se ne zna koji koristiti. Bez obzira koja metoda se koristi, kombinacija metoda koja se primjenjuju jedna za drugom će dati najbolji rezultat.

Posavec (2018) slikovito objašnjava hibridni postupak šifriranja. Osoba A izvornu poruku komprimira, radi lakšeg i bržeg slanja te dodatne zaštite. Takvu poruku šifrira nekom od metoda simetričnog šifriranja pomoću simetričnog ključa. Generiranje simetričnog ključa vrši generator pseudo-slučajnog broja u kombinaciji sa raznim korisničkim podacima unesenim tokom procesa generiranja. Tako dobiveni simetrični ključ se kriptira nekom od metoda asimetričnih algoritama pomoću javnog ključa osobe kojoj se poruka šalje te zajedno sa kriptiranom porukom šalje primaocu poruke. Dekriptiranje se vrši obrnutim postupkom. Osoba koja je primila poruku prvo dekriptira primljenu poruku koja sadrži simetrični ključ svojim tajnim ključem. Na taj način dolazi do simetričnog ključa kojim je kriptiran izvorni tekst. Kod hibridnih sistema koristi se duplo kriptiranje i tri ključa: javni i tajni ključ osobe kojoj se šalje poruka i simetrični ključ osobe koja šalje poruku.



Shema 2: Hibridni postupak šifriranja (Posavec, 2018).

Pobrojani postupci se koriste svuda u računarskim sistemima: za zaštitu pohranjenih podataka, u radu aplikacija, pri pristupu računarskim sistemima, te u mrežnim komunikacijama. U mrežnim komunikacijama koristi se već na drugom mrežnom sloju (WEP, WPA/WPA2) te na trećem i višim slojevima (IPSec, SSH, SSL, Kerberos, Radius, PGP, GPG). Za zaštitu podataka, pohranjenih na digitalnom mediju ili tokom prenosa komunikacijskim kanalom koriste se brojni algoritmi: RC4, IDEA, DES, 3DES, AES. Za zaštitu šifri, programskih aplikacija, a ponekad i podataka, koriste se hashing algoritmi koji daju jedinstveni, kratki "potpis" određenoj skupini podataka: MD5, Whirlpool, SHA-1, SHA-2 (CARNet, 2008).

4. MOGUĆNOSTI I VRSTE KRIPTOANALITIČKOG NAPADA

Kriptografija razvija algoritme koji trebaju osigurati povjerljivost i/ili tajnost, autentifikaciju i cjelovitost podataka. U načelu se zasnivaju na nekoj tajni, koju najčešće zovemo ključem i/ili posebnoj matematičkoj funkciji iskazanoj u vidu algoritma kojeg zovemo šifrom. Smisao kriptografije je sakriti otvoreni tekst (ili ključ, ili oboje) od prisluškivača[200]. Pretpostavlja se da prisluškivači imaju potpuni pristup komunikaciji između pošiljatelja i primatelja. Kriptoanaliza je upravo obrnuti napor, usmjeren na dešifrovanje tj. vraćanje kriptiranog sadržaja u otvoreni, čitljivi oblik. Prema Schneieru (1996) to je nauka o vraćanju otvorenog teksta poruke bez pristupa ključu. Uspješna kriptoanaliza može vratiti otvoreni tekst ili ključ. Također može pronaći slabosti u kriptosistemu koje na kraju vode do prethodnih rezultata. Kriptoanaliza nastoji dati rješenja u slučaju kad nemamo ključ ili šifru ili oboje. Prema tome, vodi se uvijek prisutan iscrpljujući rovovski rat između

[200] Često se nazivaju i protivnicima, napadačima, presretačima ili jednostavno neprijateljima.

napadača (kriptoanalitičara) i dizajnera (kriptografa). Pokušaj kriptoanalize naziva se napadom. Nisu rijetki slučajevi da se naruče napadi na sistem da bi se pokazala njegova slabost.

Temeljna pretpostavka u kriptoanalizi definisana od strane nizozemca A. Kerckhoffsa u devetnaestom stoljeću ističe da tajna mora biti u potpunosti u ključu. Kerckhoffs pretpostavlja da kriptoanalitičar zna sve detalje kriptografskog algoritma i postupak implementacije, što znači da je u određenoj mjeri posljedično i sigurnost takvog sistema ugrožena.

Prema Schneieru pretpostavka da kriptoanalitičar ima potpuno znanje o algoritmu šifriranja koji se koristi, predstavlja zajedničku kategoriju svim napadima (1996). Stoga, kategorizira nekoliko vrsta napada:

1. **Napad šifrata**. Kriptoanalitičar ima šifrat od nekoliko poruka, koje su sve kriptirane pomoću istog enkripcijskog algoritma. Zadatak kriptoanalitičara je da povrati otvoreni tekst što većeg broja poruka, ili još bolje da utvrdi ključ (ili ključeve) koji se koristio za kriptiranje tih poruka, kako bi se dekriptirale ostale poruke kriptirane istim ključevima.
2. **Napad poznatog otvorenog teksta.** Kriptoanalitičar ima pristup ne samo šifratu nekoliko poruka, već i otvorenom tekstu tih poruka. Njegov je zadatak izvući ključ (ključeve) koji se koristi za kriptiranje poruka ili algoritam za dekriptiranje novih poruka kriptiranih istim ključem (ili ključevima).
3. **Napad izabranog otvorenog teksta**. Kriptoanalitičar ne samo da ima pristup šifratu i otvorenom tekstu za nekoliko poruka, već također bira koji se otvoreni tekst kriptira. Ovo je snažnije od napada poznatog otvorenog teksta, jer kriptoanalitičar može izabrati određene blokove otvorenog teksta za kriptiranje, one koji mogu pružiti više informacija o ključu. Njegov je zadatak izvući ključ (ili ključeve) koji se koristi za kriptiranje poruka ili algoritam za dekriptiranje novih poruka kriptiranih istim ključem (ili ključevima).
4. **Napad prilagodljivog izabranog otvorenog teksta**. Ovo je poseban slučaj napada izabranog otvorenog teksta. Kriptoanalitičar ne samo da može izabrati otvoreni tekst koji je šifriran, već također može izmijeniti svoj izbor na osnovu rezultata prethodne enkripcije. U napadu izabranog otvorenog teksta kriptoanalitičar može samo odabrati jedan veliki blok otvorenog teksta za kriptiranje; u napadu prilagodljivog izabranog otvorenog teksta, on može odabrati manji blok otvorenog teksta, a zatim odabrati drugi na osnovu rezultata prvog, i tako dalje.
5. **Napad izabranog šifrata.** Kriptoanalitičar može izabrati različite šifrate za dešifriranje i ima pristup dekriptiranom otvorenom tekstu. Naprimjer, kriptanalitičar ima pristup neprobojnoj kutiji koja automatski dekriptira. Njegov je posao izvući ključ. Ovaj napad prvenstveno se odnosi na algoritme javnih ključeva. Napad izabranog šifrata ponekad je učinkovit i protiv simetričnog algoritma.
6. **Napad ključa.** Ovaj napad ne znači da kriptoanalitičar može odabrati ključ; znači da ima neko znanje o odnosu između različitih ključeva.

7. **Kriptoanaliza prijetnjom**. Kriptoanalitičar prijeti, ucjenjuje ili muči nekoga dok mu ne otkrije ključ. Podmićivanje se ponekad naziva napadom kupovine ključa.

Nije rijetko da kriptoanalitičar dobije šifrat u otvorenom obliku ili da podmiti nekoga da šifrira odabranu poruku. Mnoge poruke imaju standardne početke i završetke koji bi mogli biti poznati kriptoanalitičaru. Schneier naglašava da su napadi poznatog otvorenog teksta (pa čak i napadi izabranog otvorenog teksta) uspješno korišteni i protiv Nijemaca i Japanaca[201] tokom Drugog svjetskog rata.

5. OSNOVNE KARAKTERISTIKE I ULOGA KRIPTOGRAFIJE NA PRIMJERU KORIŠTENJA INTERNET PRETRAŽIVAČA I MOBILNOG TELEFONA

Prema Dooley (2018) iz kriptografske perspektive, najvažniji protokol na world wide webu je HTTPS (engl. *HyperText Transfer Protocol-Secure*). Kada web stranica koristi https: // prefiks sa URL-a (engl. *Uniform Resource Locator)*, to znači da bi preglednik trebao koristiti HTTPS protokol ali i šifrirati sav promet između pretraživača i web servera. HTTPS obično koristi jedan od dva kriptografska algoritma za kriptiranje prometa, TLS (engl. *Transport Layer Security*) ili SSL (engl. Secure Sockets Layer). Izvorna svrha HTTPS-a bila je olakšavanje komercijalnih transakcija putem svjetske mreže, ali od 2010. godine njegova upotreba raste kako bi se osigurala privatnost za sve komunikacije putem Interneta.

Kada browser želi uspostaviti vezu s web serverom, već tada započinje djelovanje TLS protokola. Prema riječima Dooleya (2018) unutar tog procesa odvijaju se sljedeće operacije:

1. Browser se povezuje na server i šalje zahtjev za vezu i spisak šifrarnih paketa (javni ključ, simetrične šifre i hash funkciju koju browser može koristiti);
2. Server bira šifrirani paket i šalje browseru poruku koja mu govori koji paket treba koristiti;
3. Server tada klijent browseru šalje svoj digitalni certifikat koji sadrži njegovo ime, vezu sa autoritetom certifikata i serverov javni ključ za šifriranje;
4. Klijent izvršava algoritam provjere valjanosti da provjeri jesu li ime i ključ servera tačni;

[201] Algoritam japanskog Purplea, podlegao je najjednostavnijim metodama kriptoanalize, kao što su *frekvencijska analiza* i *brute force* (engl. sirova sila). Koračni prekidač pokazao se vrlo predvidljivim, jer je nakon svakog 25. pritiska tipke (prilikom čega je svakim pritiskom teoretski nastajala nova abeceda) došlo do ponavljanja procesa. Cikličko ponavljanje algoritma bila je najveća mana stroja (Pađen, 2018).

5. Ako je certifikat servera potvrđen, tada će klijent započeti postupak generiranja ključa sesije za sistem simetričnog šifriranja. Da bi to učinili, klijent postupa na jedan od dva moguća načina:

a) Generira slučajni broj i kriptira ga serverovim javnim ključem za šifriranje. Onda klijent šalje šifrirani broj serveru. Server i klijent će tada koristiti nasumični broj za generiranje istog simetričnog ključa za šifriranje za odabrani simetrični šifrirani sistem.
b) Klijent i server koriste Diffie-Hellman algoritam za razmjenu ključeva da bi generirali simetrični ključ sesije.

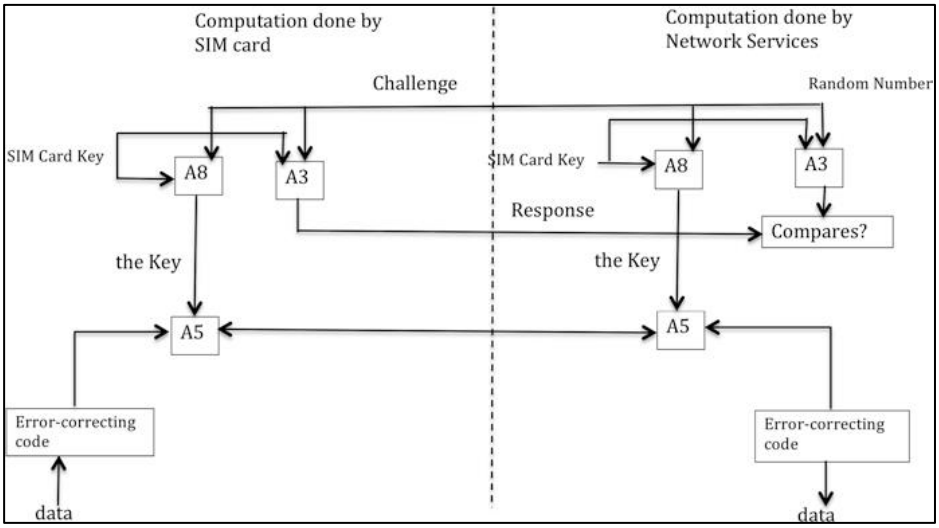
U ovom trenutku i klijent i server imaju isti simetrični šifrat ključa i započinju osigurani dio veze. Koristit će odabrani simetrični algoritam za svu komunikaciju dok veza ne bude gotova. U TLS je uključeno nekoliko sistema šifriranja javnih ključeva, uključujući RSA i Diffie-Hellman algoritam. Za simetrične algoritme, izbor uključuje AES, Camellia i ARIA, a svi koriste ili 128-bitne ili 256-bitne ključeve. Nakon uspostavljanja veze, sav se promet između browsera i web servera šifrira (Dooley, 2018).

Ova tehnika korištenja kriptografskog sistema javnog ključa i sekvence rukovanja radi uspostavljanja mrežne veze i dijeljenja simetričnog ključa, a zatim korištenja simetričnog ključa za sve preostale komunikacijske prijenose, funkcionira kao i svaka web lokacija za elektronsku trgovinu na Internetu. Svi mi koristimo šifriranje, iako toga često nismo svjesni, svaki put kada koristimo Internet za kupovinu knjige ili kada trebamo usluge internet bankarstva. Šifriranje omogućava slanje podataka o kreditnoj kartici i ostalih osjetljivih ličnih podataka putem Interneta bez otkrivanja tih podataka.

Šta se praktično dešava sa našim mobilnim telefonom? U mobilnom telefonu zapravo postoje dva „radija“. Prvi je radio koji pruža uslugu mobilne telefonije i podataka, dok je drugi radio koji će uređaj povezati s bežičnom lokalnom mrežom, a time i s Internetom (postoji mogućnost da se mobilni telefon poveže putem Bluetooth standarda kratkog dometa, no isti nije u fokusu ovog primjera).

Brookson (1994) navodi da globalni sistem za mobilne komunikacije (GSM) predstavlja najčešće korišteni digitalni protokol mobilne telefonije na svijetu. GSM postavlja pravila po kojima se mobilni telefoni povezuju s baznim stanicama mobilne telefonije, a potom i na globalnu telefonsku mrežu. GSM omogućuje šifriranu komunikaciju između mobilnog telefona i mobilne bazne stanice na koju je spojen. Iako GSM ne uključuje protokole podataka za mobilnu uslugu podataka od 1G do 4G (LTE), ti su protokoli usko povezani sa GSM-om. GSM je prvi put postao evropski standard 1987. godine i od tada se proširio po cijelom svijetu. U GSM sistemu postoje tri različita kriptografska algoritma koja omogućuju mobilnom telefonu da uspostavi vezu s mrežom, a zatim da prenosi podatke u obliku šifriranog glasa ili paketa podataka. Ova tri algoritma obavljaju tri različite funkcije: provjeru autentičnosti, stvaranje ključeva i enkripciju podataka. Prva dva algoritma, nazvana A3 i A8, pohranjena su na SIM kartici GSM telefona, dok je treći algoritam, A5

implementiran u hardveru samog telefona. Prema Dooleyu (2018) njihov odnos prikazan je na slici ispod.



Shema 3: Postupak provjere autentičnosti, stvaranja ključeva i enkripcija podataka u GSM sistemu (Dooley, 2018).

Kada se GSM mobilni telefon pokušava povezati s mrežom, u procesu autentifikacije uključene su dvije stvari, algoritam provjere autentičnosti, nazvan A3, i jedinstvena riječ spremljena na SIM kartici koja identificira telefon. Dooley (2018) prikazuje da postupak provjere autentičnosti podrazumjeva sljedeće korake:

1. Mobilni telefon pita mrežu da se pridruži. Kao dio zahtjeva, serveru šalje jedinstveni matični broj (koji se zove IMEI ili Međunarodni identifikacijski broj mobilne opreme).
2. Mrežni server generira nasumični broj i šalje ga telefonu kao "izazov."
3. Telefon koristi nasumični broj, ključnu riječ, i algoritam A3 i generira šifrirani "odgovor" koji šalje serveru.
4. Server također koristi algoritam A3, ključnu riječ telefona (koju dobiva od telefonske kompanije u kojoj korisnik ima uslugu, koristeći IMEI) i nasumični broj za generisanje šifrirane poruke.
5. Server zatim uspoređuje dvije šifrirane poruke i ako se podudaraju, uspostavlja vezu s mobilnim telefonom.

Dok mobilni telefon i mrežni poslužitelj „komuniciraju“, telefon i server također koriste nasumični broj i ključ SIM kartice zajedno s algoritmom generacije ključeva A8 za

generiranje jedinstvenog simetričnog ključa. Ovaj se ključ prosljeđuje trećem algoritmu A5[202] gdje se koristi za šifriranje prijenosa glasa i podataka nakon provjere autentičnosti veze. Niko od pružatelja usluga ili proizvođača mobilnih telefona ne otkriva koje algoritme koristi za provjeru autentičnosti i prijenos podataka.

UMJESTO ZAKLJUČKA

U ovoj specifičnoj genezi svog razvoja, kriptografija je od svojih najranijih pseudo-oblika, datiranih hiljadama godina prije nove ere, napredovala sve do kompleksne discipline u službi zaštite informacija. Osnovna kriptografska znanja su danas javno dostupna, što uključuje i postupke za mnoge moderne kriptografske metode. Neminovno je da će se ovaj trend razvitka nastaviti jer svaki primjer „neprobojne šifre" sazna svoj rok trajanja kada mu ga kriptoanaliza dodijeli.

Nemojmo zaboraviti da je kriptografija ključna za siguran rad gotovo svih organizacija i za zaštitu privatnosti pojedinaca širom svijeta. Unatoč važnosti, i uprkos činjenici da mnoge zemlje postavljaju snažna ograničenja za upotrebu kriptografija, mnogo organizacija zanemaruje razmatranje regulatornih implikacija za kriptografiju koju koriste. Sve međunarodno aktivne kompanije moraju poduzeti korake kako bi osigurali da su svi u skladu s propisima šifriranja zemlje u kojima posluju, a istovremeno moraju usvojiti najbolje prakse za maksimiziranje informacijske sigurnosti uprkos ograničenjima na korištenje kriptografije (Saper, 2013).

U prethodnom dijelu ponudili smo čitalačkoj publici osnovne informacije i kategorizacije koje mogu poslužiti kao osnova za dalja istraživanja ove izuzetno kompleksne discipline.

Razumljivo je da apsolutna zaštita bilo kojeg odabranog kriptosistema ne postoji, stoga preporučujemo da se više pažnje posveti čovjeku kao prenosiocu informacije i njegovoj povjerljivosti i lojalnosti. Također, smatramo da se treba potaknuti ulaganje u istraživanje ove oblasti i generalno u razvoj kriptografskih sistema prema svim sektorima i korisnicima za zaštitu podataka u mirovanju ali i u tranzitu.

---

[202] Zapravo postoje četiri A5 algoritma. A5/0 uopće nije algoritam, samo pokazuje da preneseni paketi podataka nisu šifrirani. A5/1 je 64-bitni algoritam šifriranja protoka koji šifrira i šalje pakete podataka (i prima i dešifrira pakete). A5/2 je slabija verzija A5/1 i izvorno se koristio za mobilne telefone koji su se prodavali izvan Europe. Od 2009. godine i A5/1 i A5/2 zastarjeli su jer se pokazalo da imaju ozbiljne kriptografske nedostatke koji ih ne čine sigurnima. Novi algoritam A5/3 uveden je 2009. godine i zasnovan je na verziji algoritma blok šifriranja nazvanoj KASUMI (koji je sam izveden iz algoritma Mitsubishi Electric Corporation pod nazivom MISTY) i namijenjen je da zamjeni A5/1 i A5/2 (Dunkelman, Keller i Shamir, 2010).

LITERATURA

1. Bagić, K. (2018). Kriptogram-vrlo kratak uvod, Croatica, XLII 62: 343–364
2. Bauer, F. (2002). Decrypted Secrets: Methods and Maxims of Cryptology. Treće izdanje, Berlin: Springer.
3. Black, T.E. (2001). Note, Taking Account of the World As It Will Be: The Shifting Course of U.S. Encryption Policy, 53 FED. COMM. L.J. 289, 292.
4. Brookson, C. (1994). GSM Security and Encryption. URL: http://brookson.com/ pristupljeno 20.11.2019. godine.
5. Buchmann, J.A. (2002). "Introduction to Cryptography", Technical University Dramstadt, New York.
6. CARnet. Kriptografija u službi napadača. URL: https://www.cert.hr/wp-content/uploads/2019/04/CCERT-PUBDOC-2008-04-226.pdf pristupljeno 30.11.2019.
7. CARNet: Steganografija, CCERT-PUBDOC-2006-04-154, URL: https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2006-04-154.pdf, pristupljeno 30.11.2019.
8. Cohen, F (1990). A short history of cryptography. URL: http://www.all.net/books/ip/Chap2-1.html pristupljeno 27.11.2019. godine.
9. Čavajda, A. (2017). Kriptografija u Prvom i Drugom svjetskom ratu. Osijek: Sveučilište J.J.Strossmayera u Osijeku.
10. Dooley, J.F. (2018). History of Cryptography and Cryptanalysis, History of Computing. Springer International Publishing AG, part of Springer Nature
11. Dujella, A. i Maretić M. (2007). Kriptografija. Zagreb: Element.
12. Dunkelman, O., Keller, N. and Shamir, A. (2010). A Practical-Time Attack on the A5/3 Cryptosystem Used in Third Generation GSM Telephony.
13. Group of authors (2006). Concise Oxford English Dictionary.Eleventh edition Hardcover
14. Katz J. and Lindell Y. (2007). Introduction to Modern Cryptography, CRC PRESS Boca Raton London New York Washington, D.C.
15. Kuhn, D. R. (2001). Nat'l inst. of standards & tech., introduction to public key technology and the federal pki infrastructure 10, URL: http://csrc.nist.gov/publications/nistpubs/800-32/sp800-32.pdf. pristupljeno 5.12.2019.
16. Lienhard, J. H. (2003). The Engines of Our Ingenuity, OUP USA.
17. Lunde, P. (2010). Tajne kodova. Razumijevanje svijeta skrivenih poruka. Prev.: D. Biličić. Zagreb: Znanje.
18. Majić, M. (2014). Šifrirne naprave. Osijek: Sveučilište J.J.Strossmayera u Osijeku.
19. Mathai, J. (2017). History of Computer Cryptography and Secrecy Systems. URL: http://www.dsm.fordham.edu/~mathai/crypto.html pristupljeno 2.12.2019.
20. Mowry, D. P. (2014). German Cipher Machines of World War 2, National Security Agency.
21. Pađen, L. (2018). Kriptologija u teoriji i praksi u prvoj polovici dvadesetog stoljeća, Zagreb: Filozofski fakultet.

22. Pawlan, M. (1998). Cryptography: the ancient art of secret messages. URL: http://www.pawlan.com/Monica/crypto/ pristupljeno 27.11.2019. godine.
23. Posavec, E. (2018). Zaštita podataka u kritičnim područjima ljudske djelatnosti-suvremene kriptografske metode. Karlovac: Veleučilište u Karlovcu.
24. Reardon, K. K. (1998). Interpersonalna komunikacija: gdje se misli susreću. Zagreb: Alinea,
25. Rhee, M. Y. (2003). "Internet Security Cryptographic principles, algorithms and protocols", School of Electrical and Computer Engineering Seoul, John Wiley & Sons, Wiltshire.
26. Rouse, M. J. i Rouse S. (2005). Poslovne komunikacije. Zagreb: Masmedia.
27. Rubin, J. (2008). Vigenere Cipher. URL://www.juliantrubin.com/encyclopedia/mathematics/vigenere_cipher.html pristupljeno 22.11.2019. godine.
28. Saper, N. (2013). International Cryptography Regulation and the Global Information Economy, Northwestern Journal of Technology and Intellectual Property, Volume 11 | Issue 7, Article 5.
29. Schneier, B. (1996). Applied Cryptography: Protocols, Algorithms, and Source Code in C. Vol. 2. Whole. New York: Wiley.
30. Singh, S. (2003). Šifre. Kratka povijest kriptografije. Zagreb: Mozaik knjiga.
31. Škrobo, M. (2017). Razumijevanje tajnih poruka. Osijek: Sveučilište J.J.Strossmayera u Osijeku.
32. Taylor, K. (2002). Number theory 1. URL: http://math.usask.ca/encryption/lessons/lesson00/page1.html pristupljeno 15.11.2019. godine.
33. Taylor, S. A. (2010). „Uloga obavještajne djelatnosti u nacionalnoj sigurnsoti", U suvremene sigurnosne studije, Alan Collins. Zagreb, Centar za međunarodne i sigurnosne studije Fakkulteta političkih znanosti Sveučilišta u Zagrebu.
34. Tilborg, Henk C.A. (2005). "Encyclopedia of Cryptography and Security", University of Technology Eindhoven.
35. Vetter, G. (2010). Patenting Cryptographic Technology, 84 CHI.-KENT L. REV. 757, 761-62.
36. Whitman, M. & Mattord, H. (2005). Principles of information security. University of Phoenix, Custom Edition e-text. Thomson Learning, Inc., rEsource, CMGT/432
37. Wrixon, F. (1998). Codes, Ciphers & Other Cryptic & Clandestine Communication: Making and Breaking Secret Messages from Hieroglyphs to the Internet. New York: Black Dog & Leventhal Publishers Inc.
38. https://www.britannica.com/topic/Vernam-Vigenere-cipher pristupljeno 15.1.2020. godine.
39. https://www.cryptomuseum.com/crypto/baudot.htm pristupljeno 15.1.2020. godine.
40. https://mreza.bug.hr/prvi-sklopovski-kriptografski-uredaj-razvijen-u-rh/ pristupljeno 15.1.2020. godine.

41. https://www.washingtonpost.com/graphics/2020/world/national-security/cia-crypto-encryption-machines-espionage/ pristupljeno 15.2.2020. godine.

Prilozi:

- Slika 1: Vigenéreov kvadrat u kombinaciji s ključem SLOBODE
- Slika 2: Izdvojeni kriptografski uređaji
- Shema 1: DES algoritam
- Shema 2: Hibridni postupak šifriranja
- Shema 3: Postupak provjere autentičnosti, stvaranja ključeva i enkripcija podataka u GSM sistemu

Kriminalističke teme
Zbornik radova
Godina XIX, Broj 5, 2019.
ISSN 1512-5505

KORIŠTENJE KOMERCIJALNE TEHNOLOGIJE U SUZBIJANJU I PRAĆENJU NEZAKONITE TRGOVINE ŽIVOTINJSKIM TROFEJIMA U CYBER-KRIMINALNIM TRGOVINSKIM MREŽAMA

USE OF COMMERCIAL TECHNOLOGY IN COUNTERING ILLEGAL WILDLIFE TRAFFICKING WITHIN CYBER-CRIMINAL TRADE NETWORKS

Pregledni naučni rad

Dr. Amer Smailbegović[203]
Dr. Nedžad Korajlić[204]

SAŽETAK

Inspiracija za rad i problem (i) koji se radom oslovljava (ju): Kao i drugi oblici ilegalne trgovine, krivolov i promet nezakonitih životinjskih trofeja je ozbiljan transnacionalni organizirani kriminal koji stvara milijarde dolara godišnje sa brzim i neometanim prihodom direktno u ruke kriminalaca.

Ciljevi rada (naučni i/ili društveni): S niskim rizikom otkrivanja i visokim potencijalom zarade, zajedno s širenjem pristupa internetu, povezujući svijet na svim razinama i svim mjestima, transnacionalni kriminalci i dalje napreduju u ovim nezakonitim radnjama.

Metodologija/Dizajn: Iako nezakonita internetska trgovina spada u širi spektar cyber-kriminala, bolji opis bi bio kao klasični kriminal s elementima cyber-a: drugim riječima, tradicionalni oblik kriminalne aktivnosti koji koristi nove tehnologije i sredstva pristupa s tradicionalnim dijelom nezakonite koristi od prometa životinjskih trofeja / životinja i povezanih fizičkih vrsti ilegalne trgovine.

Ograničenja istraživanja/rada: Uz mnoge pravne i provedbene izazove povezane s konvencionalnim kaznenim djelima za promet ili promidžbu životinjskih trofeja, internetska trgovina ilegalnim trofejima predstavlja još jedan niz problema za dužnosnike, prisiljavajući ih da djeluju u trans-pravosudnom, virtualnom prostoru u kom su i oni, i zakon, uglavnom nespremni za provodbu.

Rezultati/Nalazi: U fazi prevencije, snagama za provedbu zakona i sigurnosti nedostaje brza reakcija i korištenje obavještajnih podataka dobivenih iz otvorenih ili obavještajnih izvora. Većina pojava krivolova i naknadnog prometa / trgovine događaju se pod okriljem tame, ali u diskretnim geografskim regijama s relativno predvidljivim obrascima.

Generalni zaključak: U fazi izravnog odgovora, metode i materijalno-tehnička sredstva na raspolaganju mogu se upotrijebiti za praćenje sredstava za prijenos krijumčarene robe i usmjeravanje timova za reakciju, bilo da reagiraju na presretanje počinitelja

[203] Direktor, Rhino 911 (NVO), Reno, Nevada, SAD, a-mer@rhino911.org
[204] Dekan, Fakultet za kriminologiju, kriminalistiku i sigurnosne studije, Univerzitet u Sarajevu, Sarajevo, BiH, dean@fkn.unsa.ba

krivičnog djela ili uvrštavanje informacija u širi pojam razotkrivanja i suzbijanja transnacionalnih kriminalnih sindikata.
Opravdanost istraživanja/rada: Pomoću relativno jednostavnog praćenja internetskih domena, prometa podataka i pasivnog praćenja komunikacije u kombinaciji s civilno-komercijalnim uređajima za snimanje i otkrivanje, brzom reakcijom letjelica i komunikacijskim mogućnostima, uspjeli smo razviti dugotrajno, trajno promatranje kritičnih područja, ispitivanja područja od važnosti te usmjeravanja operativnih skupina na tlu u cilju presretanja lovokradica prije izvršenja njihovih namjera.

Ključne riječi
krivolov, krijumčarenje, trans-nacionalni kriminal, osmatranje

ABSTRACT
Reason for writing and research problem (s): Similar to the other forms of illegal trade, poaching and trafficking of endangered wildlife is a serious transnational organized crime that generates billions of dollars per year, with fast and unimpeded income, directly into the hands of criminals.
Aims of the paper (scientific and/or social): With low detection-risk and high-earning potential, along with expanding worldwide Internet access, transnational criminals continue to thrive in these particular illegal activities.
Methodology/Design: Although wildlife-traffic falls within a broader range of cybercrime, a more appropriate description would describe it as a traditional form of criminal activity that uses new cyber-technologies and means of access to further the illegal trade.
Research/Paper limitation: In addition to the many legal and law-enforcement challenges associated with the conventional offenses for the marketing or promotion of illicit wildlife trophies, the online trade poses another set of problems for officials, forcing them to operate in a trans-judicial, virtual space in which they, and the law, are mostly unprepared for.
Results/Findings: In the prevention phase, law enforcement and security forces lack the rapid response and effective use of intelligence obtained from the open-source or intelligence assets. Most poaching and subsequent traffic and smuggling activities, occur under the cover of darkness, but within discrete geographical regions with relatively predictable patterns.
General Conclusion: In the direct-response phase, the methods and material resources available can be used to monitor the means of transporting smuggled goods and directing response teams, either by responding to the interception of the offender or incorporating the obtained information into the wider picture of unmasking and combating the transnational crime syndicates.
Research/Paper Validity: Using relatively simple domain tracking, data traffic and passive communication monitoring, combined with the civil-commercial technology for the tracking and detection of communication devices, rapid aircraft response and communication capabilities, we have been able to develop a long-term, ongoing critical area monitoring. This capability uses the area-of-interest determination and ground task-force targeting for the purpose of intercepting the poachers before they carry-out their intentions.

Key words
Poaching, Smuggling, Trans-national crime, Reconnaissance

Uvod

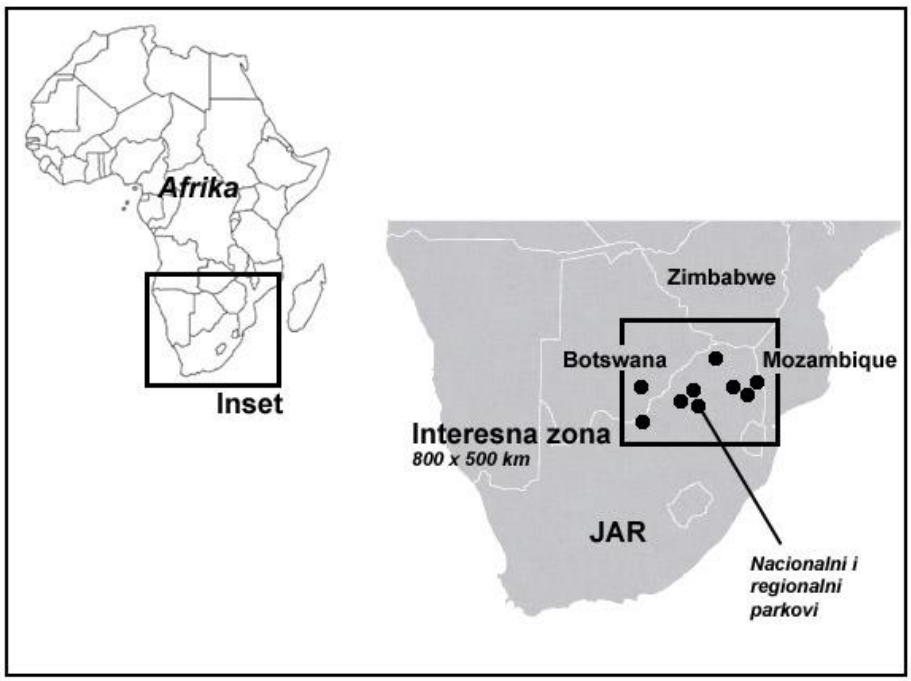
Krijumčarenje rijetkih životinjskih vrsta nije izolirana kriminalna aktivnost, ali je često povezano s drugim vrstama cyber-omogućenih transnacionalnih kriminalnih aktivnosti, a isto ima bliske poveznice sa krijumčarenjem oružja i opojnih droga, pranjem novca, pa čak i terorizmom. Ovaj rad predstavlja začetni pokušaj korištenja slobodno-dostupnih alata za praćenje i blokiranje cyber-omogućenog krivolova, transporta i transakcija; ukazuje se na njihovu primjenjivost u borbi protiv drugih vrsti kriminala koji djeluju unutar cyber-prostora. Rhino 911 je nevladina organizacija sa sjedištima u SAD i Južnoafričkoj Republici (JAR), s ciljem postizanja i primjene novih rješenja i metodologija za očuvanje rijetkih vrsta i sprečavanja kriminalnih aktivnosti.

Cilj

Neprofitne organizacije s ciljem zaštite rijetkih vrsti mogu umnogome nadopuniti i unaprijediti formalne napore u provođenju zakona, kao i pomoći u izbjegavanju blokada tzv. s-vrha-ka-dolje strategije koje mogu potkopati lokalne napore za suzbijanje krivolova i za zaštitu divljih životinja (Somersville Sustianable Conservation, 2017). Američki savezni zakon također prepoznaje kritičnu važnost očuvanja prirodnih zajednica; u članku 404, Zakona o uklanjanju, neutraliziranju i eliminaciji trgovine divljim životinjama iz 2016. godine (U.S. Congress, 2016), Kongres SAD nalaže Državnom Odjelu za Inostrane Poslove (Department of State) da podupire napore za očuvanje vrsti u pružanju podrške zajednicima putem (a) aktivnosti protiv krivolova, uključujući razvijanje policijskih mreža i mreže doušnika; (b) suradnju sa zajednicama i nacionalnim vladama na razvoju relevantnih političkih i regulatornih okvira koji bi omogućili i promicali programe očuvanja zajednice, uključujući podršku angažiranju zakona za provođenje zakona s tijelima za zaštitu divljih životinja u svrhu razmjene informacija; (c) suradnju s nacionalnim vladama kako bi se osiguralo da zajednice imaju pravovremenu i učinkovitu podršku nacionalnih vlasti za ublažavanje rizika s kojima se zajednice mogu suočiti prilikom sudjelovanja u aktivnostima borbe protiv krivolova i trgovine ljudima; (d) poboljšati zabranu i istražne kapacitete poboljšanom tehnologijom i realističnim osposobljavanjem kadra u privatnim rezervatima u kojima dolazi do pojave krivolova.

U modernom cyber-svijetu u kojem većina transakcija postaje internetska, bilo da se nudi, pregovara ili zaključuje poslovni sporazum i umrežava razmjena informacija, bitno je stvoriti sustav nadgledanja i angažmana lokalne zajednice putem programa dojave i ranog upozoravanja. Ovim sustavom namjerava se temeljno poboljšati razmjena informacija, proaktivnog djelovanja, kao i ishodu sudski-prihvatljivih dokaza protiv krivolovaca

i trgovaca. Nastojimo stvoriti okvir unutar kojeg su lokalne zajednice povezane s vladinim dužnosnicima u svojoj ali i u susjednim zemljama i zemljama tranzita, odnosno zemljama krajnjeg korisnika, tako da tužitelji mogu graditi sveobuhvatne slučajeve na temelju globalnih podataka protiv transnacionalnih zločinačkih organizacija. Iz toga mogu se stvoriti i dodatni pravni okviri kojim će se suprotstaviti trgovini narkoticima i drugim transnacionalnim zločinima kao što su pranje novca, krijumčarenje, trgovina ljudima itd. Ovaj program je prvenstveno implementiran u dijelu Južne Afrike, gdje se trenutno sprovodi kao pilot-program (Slika br.1).



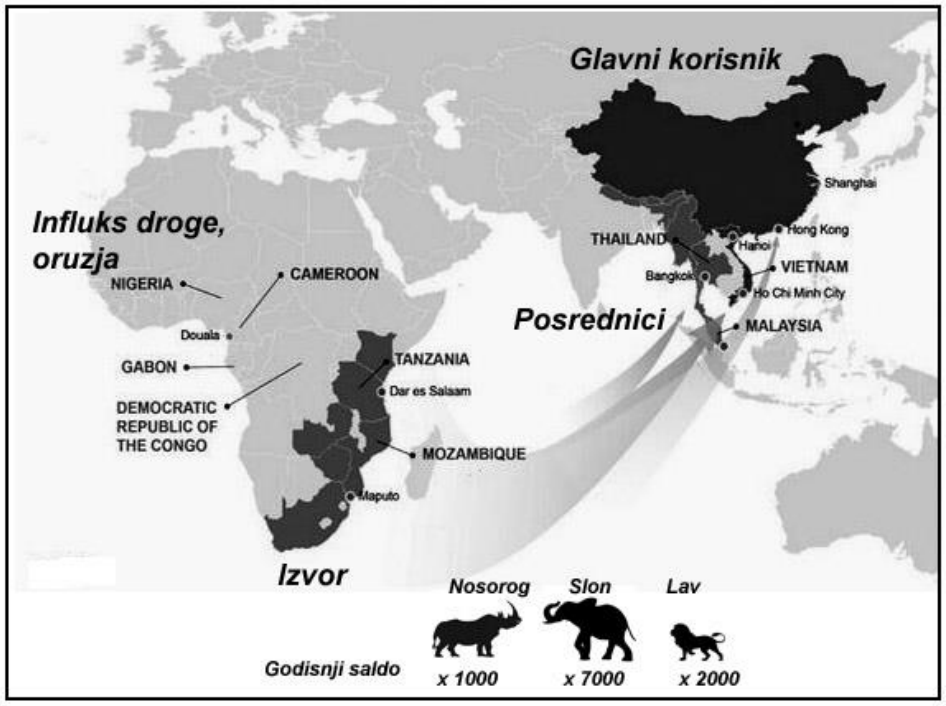
Slika 1. Zona implementiranja pilot-programa nadzora i razmjene informacija

Pozadina

Unutar posljednjeg desetljeća, krivolov i trgovina divljim životinjama evoluirali su, iz relativno snošljive pojave i okvira brige za okoliš usmjerenih na suzbijanje lokalnih incidenata i sitnog kriminala, u globalne sigurnosne prijetnje kojim upravljaju transnacionalne kriminalne organizacije (Saru, 2016) od kojih neke imaju i izravne veze s teroristima (Austin, 2019). Primjerice, ista organizacija koja nastoji da prokrijumčari velikokalibarske puške i druga pomagala (npr. nišanske naprave, termovizijske kamere) za lovokradice, prodala je teroristima eksploziv kojim su 2004. izveli napad u Madridu, u kojem je ubijeno 193 civila, a preko 2000 ih je ranjeno (Austin, 2019). Kao posljedica toga, napori na postizanju ciljeva navedenih u Nacionalnoj strategiji za borbu protiv trgovine

divljim životinjama (The White House, 2014), Zakonu o suzbijanju trgovine divljim životinjama (U.S. Congress, 2016)., i ciljevima UN-a za održivi razvoj (United Nations, 2015) tim predstavljaju mjere koje mogu utjecati na bolje sigurnosne uvjete kao i ljudska prava stanovništva koja je primorana ili da živi od krivolova, ili se nalazi unutar zahvaćenih područja gdje se takve aktivnosti odvijaju.

Čvrsti dokazi ukazuju na sve učestalije pojave gdje trgovci vrstama, ljudima ili narkoticima prelaze s fizičkih tržišta na virtualna tržišta; primjerice u samo dva mjeseca u četiri zemlje, organizacija IFAW (Međunardoni fond za dobrobit životinja) je identificirala oglase za 11 772 ugroženih i ugroženih primjeraka u vrijednosti većoj od tri miljuna funti (IFAW, 2018).



Slika 2. Zemlje iz kojih se izvoze vrste ubijene u krivolovu, zemlje krajnji korisnici te zemlje saučesnice unutar kriminalnih radnji (narkotici, pranje novca itd.). Broj jedinki koji u prosjeku svake godine strada od krivolova za tri vodeća trofejna primjerka.

Problem

Mnogi rendžeri (lovočuvari) u zaštićenim područjima subsaharskih i zemalja južne Afrike, su loše opremljeni za odbranu ogromnih područja na kojim imaju zadatak patrolirati. U prosjeku, područje veličine jednog srednje-velikog europskog grada, ophode samo dva rendžera s jednom puškom, bez radio-veze i godišnjim proračunom od svega 20 EUR. S

druge strane, ljudstvo i organizacije uključene u trgovinu ljudima koriste mobilne komunikacijske sustave, kompjuterske mreže, pomagala za navigaciju i internetsko tržište kako bi unaprijedili trgovinu i organizirali operacije, a njihov godišnji proračun iznosi milijarde (Felbab-Brown, 2018). Uz sve to, imaju i potporu složenijih i organiziranijih državnih interesa (npr. Iran, Sjeverna Koreja), krupnog kriminala (narkokarteli) i terorističke mreže (Al Shabbab, AQIM, Boko Haram) koji i sami ulaze u sukob u potrazi za profitom a tim donoseći još jednu razinu složenosti (Smart Conservation , 2018).

Metode i tehnike

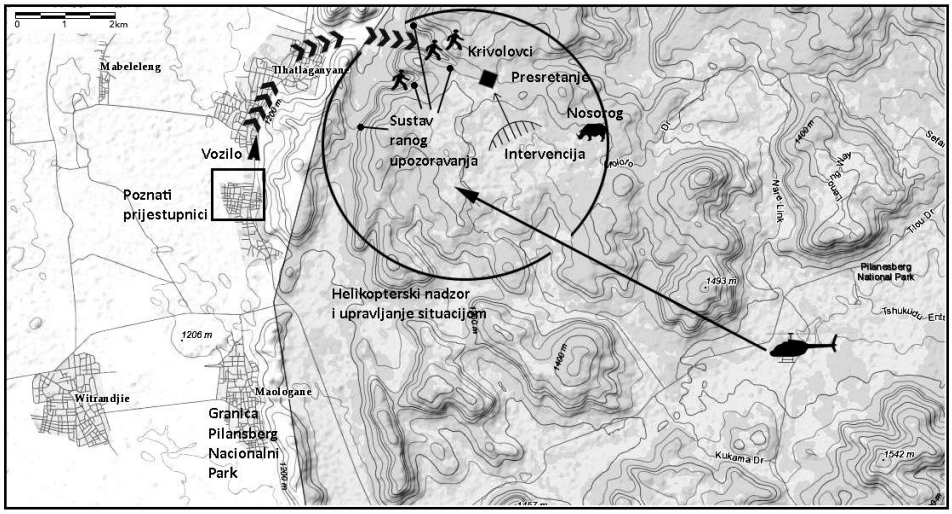
Na osnovu stanja na terenu, te informacija sakupljenih na osnovu analize incidenata u periodu od 2014-2018., naši osnovni ciljevi su definirani nastojanjima u:

1. Poboljšanju terenske komunikacije i situacijske spoznanosti na terenu (u trenutnom vremenu).
2. Korištenju indeksiranja i pretrage podataka u javnoj domeni za praćenje i povezivanje svih geografsko-specifičnih podataka u svrhu geo-lociranja subjekata.
3. Pretraga i povezivanje internetske i fizičke prisutnosti pojedinih subjekata i njihova korelacija.
4. Korištenje signala mobilnih komunikcijskih sustava za otkrivanje upada i dalje praćenje, ako je moguće.
5. Analiza i pretraga financijskih transakcija, gdje je to moguće.
6. Suradnja sa organima za provedbu zakona na gonjenju sumnjivih lica, istrazi i dokumentiranju.

U izazovnom sigurnosno-logističkom okruženju, državama s niskim godišnjim proračunima, korupcijom velikih razmjera, nedostatkom pravnog okvira i opasnim susretima, naš je primarni cilj bio iskoristiti što je moguće više javnih i privatnih resursa, kako bismo osigurali maksimalnu učinkovitost a da sami počinitelji ne budu svjesni aktivnosti koje se poduzimaju protiv njih (Schott, 2006).

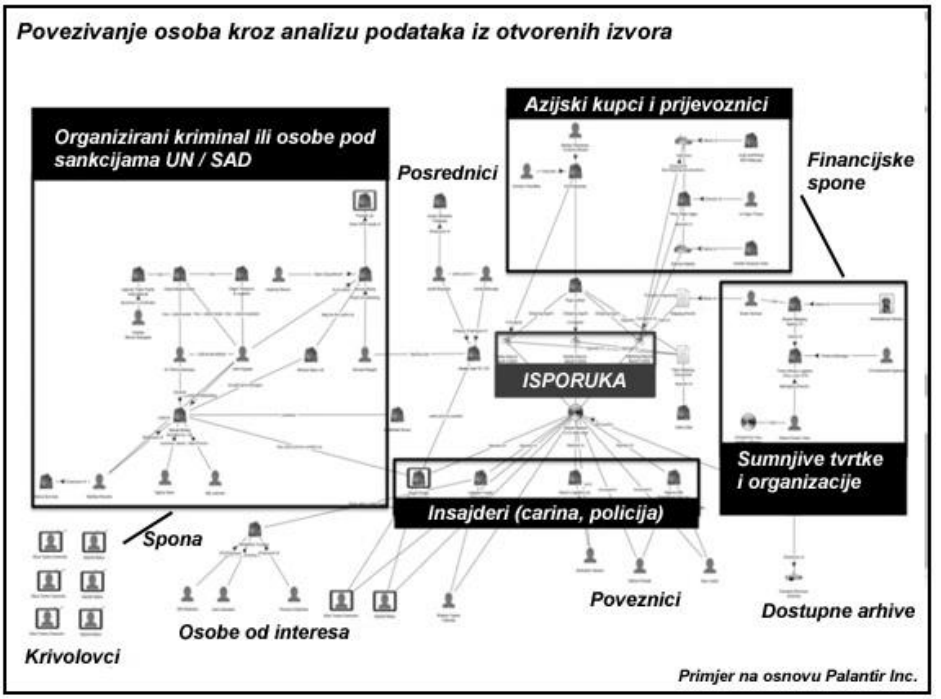
Glavna metoda za poboljšanje svijesti o vlastitom okruženju bila je upotreba otvorene tehnologije (open-source) omogućene GPS-om za planiranje patrola i distribuciju ljudstva na terenu, te implementaciji prihvatljivog (i jednostavnog) alata za praćenje njihovog položaja na terenu, kao i za snimanje bilo kakvih incidenata susretenih tijekom patrole (npr. tragovi, mjesta zločina, susreti, prerezane ograde ili druge sumnjive elemente). Korištenjem komercijalnih ili otvorenih platformi (npr. Google Maps), rudimentarnih alata za geografske informacijske sustave (GIS elementi kao npr. putanja, blizina, linearna analiza) i dostupnog softvera (Smart Conservation , 2018) koji se pokreće na mobilnim uređajima (npr. SMART softver kao i vlastiti softver razvijen za koordiniranje sa letjelicama) uspjeli smo dobiti cjelovitiju sliku mjesta gdje se događaju incidenti, gdje se

nalazi osoblje koje je raspoređeno i kako najbolje smanjiti upad u zaštićena područja putem prediktivne analize (Smailbegovic, Anklam, Aslett, & Peppin, 2006).



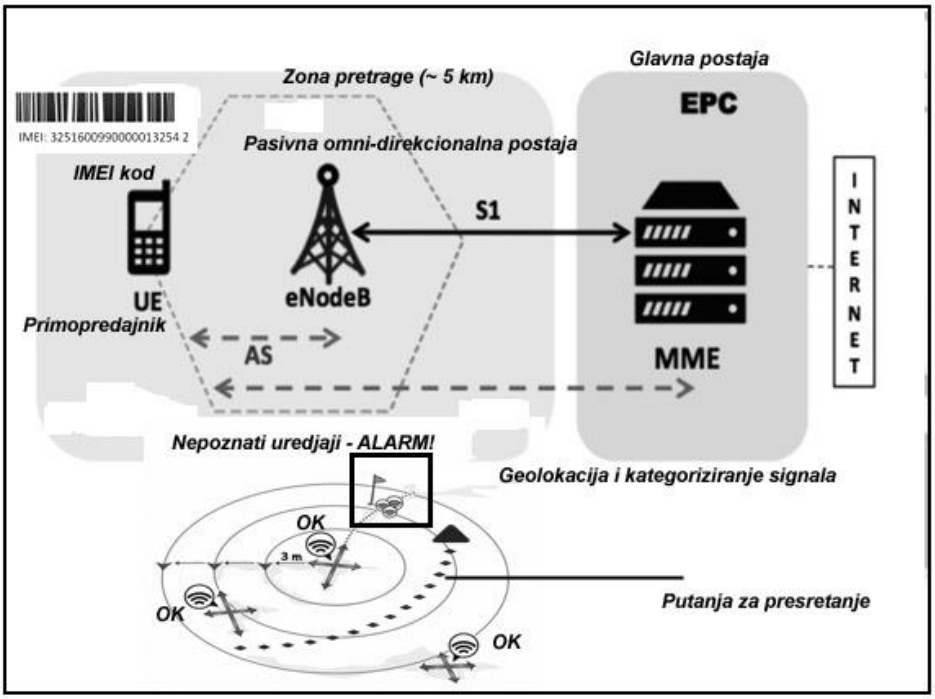
Slika 3. Prikaz praćenja upada skupine lovokradica u rezervat sa identifikacijom optimalnog mjesta za presretanje skupine kao i trenutno rasporeda ljudstva na terenu.

Pretraživanje, kategoriziranje i razvrstavanje podataka sa interneta bio je problematičniji zadatak, jer se osobe koje se bave nelegalnom trgovinom, često koriste slengom, kodnim riječima ili drugim internim referencama koje objavljaju na različitim diskusijskim forumima, trgovinskim E-platformama, pa čak i na tzv. *Dark-web*. Upotrebom lokalnog kadra koji je upoznat sa slengom, jezikom, kulturom i posebnim alatima razvijenim za obradu i pretragu medijskih postova (opsežan popis alata i njihove upotrebe opisan je u (Balakishan, 2017) za analizu teksta koristili smo geografski suženo područje (Južna Afrika, Mozambik, Zimbabve, Bocvana) kako bismo otkrili sumnjive sadržaje uz pomoć sumnjivog ponašanja korisnika te njihove komunikacije. Glavni cilj bio je prepoznati „utjecajne osobe“ (tzv. influensere) i pokušati pratiti njihovu prisutnost na internetu kao i u stvarnom svijetu, te povezati te informacije i prisustvo sa incidentima na terenu (Slika 4).



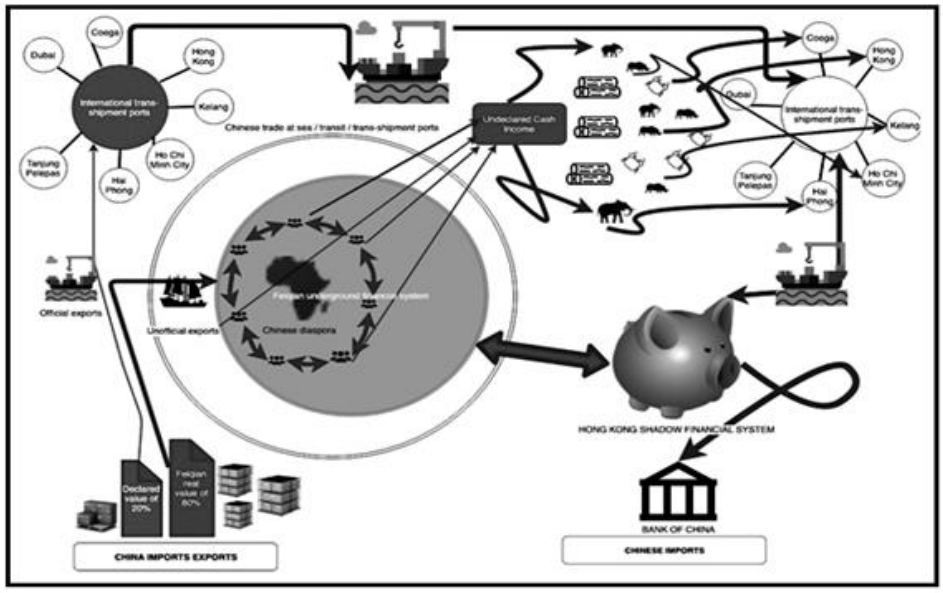
Slika 4. Prikaz povezne mreže osoba identificiranih na internetu kao i korenspondirajućih podataka iz javnih izvora i baza podataka u svrhu izgradnje korelativnih odnosa i osoba od utjecaja.

Svakom mobilnom instrumentu elektroničkog odašiljanja dodjeljuje se karakteristični identifikator poznat kao Međunarodni identifikator mobilne opreme (IMEI), a dodijeljeni broj jedinstven je za svaku jedinicu. Razvojem sustava za pasivno skeniranje (Sustek, Marcanik, Oplustil, Tomasek, & Urednicek, 2016) antena odašiljača unutar zadatog prostora, nazvanog *Impimpi* i upravljanem njime unutar područja od 5 km, u stanju smo pasivno prikupljati informacije o svakom odašiljaču, a posebice njegove kodove međunarodnog broja mobilnih pretplatnika (IMSI) te broja elektroničkih serijskih brojeva (ESN) kao i samih brojeva mobilnih telefona i vidjeti korisnika koji se nalazi u tom području. Nakon registracije prisutnosti prijemnika u sustavu, serijski ili brojevi pretplatnika se mogu usporediti s imenikom poznatih odašiljača. Ako se na tom području pojavi nepoznati odašiljač, sustav koristi karakteristični IMEI i na temelju jačine signala uređaja moguće je pronaći približno (+/- 5 m) mjesto mobilnog telefona ili drugog odašiljača kao I njegovog kretanja. Ovi se alati mogu koristiti zajedno s alatima za geografsku analizu, usmjeravanje, praćenje kretanja pripadnika sigurnosnih službi na terenu kao i za presretanje potencijalnih uljeza.



Slika 5. Konceptualni prikaz rada postaje Impimpi za pasivnu detekciju signala.

Praćenje protoka financijskih sredstava (Knobel, 2019) složenija je stvar jer zahtijeva sudjelovanje uključenih vlada i financijskog sektora (posebice banaka). Ako postoji verificirana sumnja da će se dogoditi protok sredstava namjenjenih za nezakonitu radnju, američka vlada generalno pruža podršku korištenju svoje nadležnosti unutar SWIFT sustava za blokiranje transakcije (Madinger & Zalopany, 1999), preusmjeravanje ili čak zamrzavanje sredstava prema zahtjevu (Schott, 2006). Međutim, brojne sitne transakcije koje se obavljaju putem alata za gotovinske isplate, razmjenu ili mrežno (E-uplate) plaćanje teže je pratiti i eventualno presresti. U tim slučajeva lokalna podrška dolazi do izražaja a potencijalne informacije i dojave vrlo važne, više kao faktor upozorenja da u sumnjivim kanalima ima novca i da se u skoroj budućnosti može dogoditi neki incident ili upad (npr. Priliv deviza, kupovina plaćenih kartica, povećanje količine narkotika ili kupovine oružja itd.). U ovom je konkretnom slučaju koncept lokalnog nadgledanja i upozoravanja iznimno važan (Korajlić, 2012).



Slika 6. Koncept kojim funkcionira financiranje krivolova iz zemalja krajnjeg korisnika – uglavnom putem neprijavljene vrijednosti uvoza/izvoza, gotovinskih naznama putem dijaspore i raznim transakcijama unutar luka – izvor: (Grobler, 2019).

Rad, suradnja i odnos s organima za provedbu zakona u jugoistočnoj Africi je izazovan zbog nedostatka infrastrukture, obuke, osoblja, nadležnosti te postojnosti drugih političkih faktora i rizika. Većina zločina se odvija preko linija i oblasti jurisdikcije ili u transnacionalnom prostoru, za koje su zemlje u fokusu, i njihov pravosudni aparat, loše pripremljene (Liskafu, 2018). Drugi komplicirajući faktor je da se većina preostalih jedinki ugroženih vrsta trenutno drži u privatnim rezervatima (zbog neadekvatnosti nacionalnih parkova) koji imaju vlastite snage sigurnosti, a koji nemaju dodira s policijskim snagama, osim kad je sasvim neophodno. U ovom pilot-projektu i cilju studije, glavni fokus nam je bio omogućiti obuku i razmjenu informacija između sigurnosnih snaga Nacionalnih parkova, privatnih rezervata i Nacionalne policije, usprkos nepovjerenju i drugim izazovima. Ključni elementi su bili komunikacija, dioba nadležnosti, protok informacija i obuka (Kešetović, Korajlić, & Toth, 2013) kojom bi se moglo uspješno djelovati protiv dobro financirane i dobro naoružane opozicije. Naš glavni poticaj bio je fokusiran na sustav ranog upozoravanja, izvještavanja i sudjelovanja lokalne zajednice, preko programa sigurnosti granice, a zatim naposlijetku, prekogranične suradnje, prvo između Južne Afrike i Bocvane, a zatim prema problematičnijim zonama Zimbabve-Mozambik-Južna Afrika.

Rezultati

Od početka programa 2016. godine, razdoblje između 1. 4. 2018 - 31. 7. 2019. donijelo je umjereno smanjenje ukupnog broja incidenata (476) u usporedbi s istim razdobljem prethodne godine (567) u Južnoj Africi (Creecy, 2019). Teško je utvrditi koliko su nove mjere pridonijele cjelini, međutim, na područjima na kojima su provedene, primijetili smo općeniti pad broja upada i povećan broj uhićenja. Zimbabve i Bocvana ne daju brojke o incidentima, jer u tim zemljama se sa krivolovcima postupa po kratkom postupku ukoliko su presretnuti u djelu.

Iz sigurnosnih razloga iz ovog rada se izostavljaju imena parkova i rezervata koji sudjeluju u ovom pilot-programu. U jednom od nacionalnih parkova koji sudjeluju u Južnoafričkoj Sjeverozapadnoj provinciji, 2016-2017. godina bila je izuzetno loša s 39 prijavljenih incidenata i samo 2 uspješno privedena lica. U prošloj godini smanjeno je na 28 incidenata i 7 privedenih lica, od kojih su neki bili "insajderi". Dodatna dva regionalna parka zabilježila su smanjenje upada sa samo 2 prijavljena incidenta i 4 presretnuta počinioca (koji su poznati od ranije). Privatni rezervati koji su sudjelovali u programu imali su 18 prijavljenih pokušaja, od kojih su 2 bila uspješna i 8 koji su predate organima za provedbu zakona. Privatni rezervati su imali i znatan broj incidenata razmjene vatre sa krivolovcima koja su rezultirala sa 3 ubijena prijestupnika i 4 ranjena lica, od kojih je jedan bio pripadnik sigurnosnih snaga (Austin, 2019). Između primijenjenih metoda, čini se da su situacijski obzor i praćenje imali mjerljiv učinak, osobito tamo gdje je funkcionirao sustav ranog upozoravanja, koje je omogućilo sigurnosnim snagama da pravovremeno reagiraju na upad. Sveukupno, bilo je oko 30% smanjenja broja uspješnih upada i krivolova i 40% povećanja u osujećenja sa privedenim osumnjičenicima. Ovo su umjereni ali i obećavajući, mada samo će vrijeme pokazati hoće li se učinkovitost primijenjenih metoda nastaviti u regiji. Razina uključenosti zajednice u program također varira od regije do regije i čini se najučinkovitijom tamo gdje se zajednica nađe kao sudionik i vidi vlastitu korist (Hubschle, 2017) u borbi protiv krivolova (npr. povećana zaposlenost i prihod od turizma).

U regionalnom i globalnom kontekstu teško je utvrditi utjecaj ovih napora, međutim smjernice i informacije dobivene sa terena ukazuju na promjenu strategije kriminalnih grupa kao direktan odgovor na primjenu ovih metoda na terenu. Sa druge strane, trendovi i poveznice ukazuju na još širi utjecaj zločinačkih poduhvata, od kojih neki mogu imati zloslutne sigurnosne posljedice na svjetskoj razini (npr. terorizam u Madridu, Nairobiju itd.).

Zaključak

Iako postoje jeftina i komercijalno dostupna rješenja koja se mogu lako implementirati na terenu, politička podrška i prihvaćanje istih često kasne ili u potpunosti nedostaju (razni vidovi opstrukcija, prvenstveno usljed korpupcije). Komplementarne metode predstavljene u ovom radu čine osnovicu za rano upozoravanje i praćenje visokoprofitnih zločina poput krivolova i krijumčarenja, no one se moraju primjenjivati široko sa konstantnom nadgradnjom i uz odgovarajuće sankcije kako bi bile učinkovite. Trenutno, nedostatak koordinacije, blage sankcije i nestabilna politička ali i sigurnosna klima predstavljaju izazov za šire prihvaćanje prikazanih metoda. Međutim, mjerljivo, iako umjereno smanjenje broja incidenata obećava šire opcije za prihvaćanje, upotrebu i unapređenje istražnih alata koji mogu pomoći u cjelokupnom naporu za suzbijanje ovih vrsti cyber-omogućenog kriminala, na svim njegovim razinama.

Reference

Alispahić, B. (2011). Sabotaža. In B. Alispahić, *Osnovi metodike rada obavještajno-sigurnosnih službi* (p. 117). Sarajevo: Šahinpašić.

Austin, K. L. (2019, April 22). *Follow the guns: Special Report.* Retrieved from Followtheguns.org: https://www.followtheguns.org/report.php

Babu, B., Ijyas, T., Muneer, P., & Varghese, J. (2017). Security issues in SCADA based industrial control systems. *2nd International Conference on Anti-Cyber Crimes (ICACC)*, (pp. 46-51). New York.

Balakishan, R. A. (2017, August 05). *A Systematic Review on the Suspicious Profiles Detection on Online Social Media Data.* Retrieved from Oriental Journal of Computer Science and Technology: http://www.computerscijournal.org/vol10no3/a-systematic-review-on-the-suspicious-profiles-detection-on-online-social-media-data/

Boaru, G., & Badita, G.-I. (2008). Critical Infrastructure Protection Challenges and Efforts to Secure Control Systems. In B. G.-I. Boaru Gheorghe. Romania.

Catrantzos, N. (2009). No Dark Corners: Defending Against Insider Threats to Critical Infrastructure. Monterey, California: Naval Postgraduate School.

Coady, T., & O´Keefe, M. (2004). Terorizam, pravedni rat i krajnja nužda. In T. Coady, *Terorizam i pravednost.* Zagreb.

Creecy, B. (2019). *Environment, Forestry and Fisheries Minister Barbara Creecy's report to a written parliamentary question by DA MP James Lorimer, August 2019.* Pretoria, South Africa: South African National Assembly.

Disso, J. P., Jones, K., & Bailey, S. (2013). A plausible solution to SCADA security honeypot systems. *2013 Eighth International national Conference on Broadband and Wireless Computing, Communication and Applications* (pp. (pp. 443–448)). New York: NY.

Felbab-Brown, V. (2018, 11 08). *Wildlife and drug trafficking, terrorism, and human security.* Retrieved from Prism online magazine, Brookings Instiution: https://www.brookings.edu/articles/wildlife-and-drug-trafficking-terrorism-and-human-security/

Gallagher, S. (2016, april 7). *Maryland hospital: Ransomware success wasn't IT Department's fault.* Retrieved from Ars Tehnica: https://arstechnica.com/security/2016/04/maryland-hospital-group-denies-ignored-warnings-allowed-ransomwareattack/

Garaplija, E. (2018). Proces identifikacije, analize i evaluacije rizika kritične infrastrukture u vanrednim situacijama. Sarajevo: Institut za zaštitu od požara i eksplozije.

Grobler, J. (2019, June 01). *How Chinese Flying Money 'finances' illegal wildlife trade*. Retrieved from Oxpeckers: https://oxpeckers.org/2019/06/chinese-flying-money/

Hubschle, A. (2017, September 20). *The fight against poaching must shift to empowering communities*. Retrieved from The Conversation: http://theconversation.com/the-fight-against-poaching-must-shift-to-empowering-communities-83828

IFAW. (2018, October 10). *Poaching crisis and how to tackle illegal wildlife trade under the spotlight in London.* Retrieved from International Fund for Animal Welfare: https://www.ifaw.org/news/poaching-crisis-and-how-to-tackle-illegal-wildlife-trade-under-the-spotlight-in-london

Kešetović, Ž., Korajlić, N., & Toth, I. (2013). *Krizni menadžment.* Sarajevo / Velika Gorica : Fakultet za kriminalistiku, kriminologiju i sigurnosne studije, Sarajevo i Veleučilište Velika Gorica.

Knobel, A. (2019, July 11). *SWIFT data can be a global vantage point for tackling global money laundering.* Retrieved from Tax Justice Network: https://www.taxjustice.net/2019/07/11/swift-data-can-be-a-global-vantage-point-for-tackling-global-money-laundering/

Korajlić, N. (2012). *Istraživanje krivicnih djela.* Sarajevo: Pravni Fakultet, Univerzitet u Sarajevu.

Langer, R. (2013). To Kill a Centrifuge. *A Technical Analysis of What Stuxnet's Creators Tried to Achieve*. Hamburg: The Langner Group.

Lendvay, R. L. (2016). Shadows Of Stuxnet: Recommendations For U.S. Policy On Critical Infrastructure Cyber Defense Derived From The Stuxnet Attack. Monterey, California: Naval Postgraduate School.

Lewis, T. G. (2006). Critical Infrastructure Protection in Homeland Security-Defending a Networking Nation. New Jersey: Wiley-Interscience.

Liskafu, J. (2018). Inter-regionalism and police cooperation against cross-border crime in East Africa: Challenges and prospects,. *South African Journal of International Affairs, 25:4*, 563-579.

Madinger, J., & Zalopany, S. (1999). *Money laundering: A guide for criminal investigators. 3rd Edition.* New York: CRC Press.

Metropuolos, E., & Platt, J. S. (2019). *Global Cyber Terrorism Incidents on the Rise*. Retrieved from Marsh & McLennan Insight: https://www.mmc.com/insights/publications/2018/nov/global-cyber-terrorism-incidents-on-the-rise.html

Nicholson, A., Webber, S., Dyer, S., Patel, T., & Janicke, H. (2012). SCADA security in the light of cyber-warfare. *Computers & Security*, 31, 418–436.

Pagliery, J. (2016, maj 27). *Global banking system under attack: What you need to know.* Retrieved from CNN Tech: http://money.cnn.com/2016/05/27/technology/swift-bank-hack/

Rauta, V. (2017). Proxy Wars and the Contemporary Security Environment. In P. Macmillan, *The Palgrave Handbook of Security, Risk and Intelligence* (pp. 99-115). Basingstoke, UK: Palgrave Macmillan.

Saru, E. W. (2016). *Poaching and the Funding of International Terrorism: A Case Study of Kenya.* Nairobi: Institute of Diplomacy and International Studies, University of Nairobi.

Schmidt, A. (1983). Political Terrorism. In A. P. Schmidt, *Polical Terrorism.* Amsterdam.

Schott, P. (2006). *Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism.* Retrieved from Semantics Scholar: https://www.semanticscholar.org/paper/Reference-Guide-to-Anti-Money-Laundering-and-the-of-Schott/8820c98420576fb6aa56af0ce382b7ff2c527537#citing-papers

She, J., & Jiang, J. (2011). On the speed of response of an FPGA based shutdown system in CANDU nuclear power plants. *Nuclear Engineering and Design*, 241, 2280–2287.

Smailbegovic, A., Anklam, S., Aslett, Z., & Peppin, W. a. (2006). Static, Horizontal-looking Hyperspectral Imaging of Vertical Targets. *American Association for Photogrammetry and Remote Sensing (ASPRS)* (pp. 66-69). Reno, Nevada: ASPRS.

Smart Conservation . (2018, December 1). *2018 Annual Report.* Retrieved from Smart Partnership: https://smartconservationtools.org/wp-content/uploads/2019/07/SMART%202018%20Annual%20Report.pdf

Somersville Sustianable Conservation. (2017, August 27). *The importance of community-based conservation.* Retrieved from Africa Wildlife and Conservation News, Environment: https://africasustainableconservation.com/2017/08/27/the-importance-of-community-based-conservation/

Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M., & Hahn, A. (2014). *Guide to Industrial Control Systems Security.* Gaithersburg, MD: National Institute of Standards and Technology.

Sustek, M., Marcanik, M., Oplustil, M., Tomasek, P., & Urednicek, Z. (2016). Sustek, M. et al. 2016. Interception methods and GSM. . *SECURWARE 2016 : The Tenth International Conference on Emerging Security Information, Systems and Technologies* (pp. 211-216). Nice, France: SECURWARE.

The White House. (2014, February 11). *National Strategy forCombating Wildlife Trafficking.* Retrieved from Obama White House Archives: https://obamawhitehouse.archives.gov/sites/default/files/docs/nationalstrategywildlifetrafficking.pdf

Tomaševski, K. (1983). Terorizam u suvremenom svijetu. In K. Tomaševski, *Izazov terorizma.* Beograd.

U.S. Congress. (2016, October 10). *114th Congress of the United States.* Retrieved from House of Representatives Act 2494 - Eliminate, Neutralize, and Disrupt Wildlife Trafficking Act of 2016 : https://www.congress.gov/bill/114th-congress/house-bill/2494/text

United Nations. (2015, January 15). *The 2030 Agenda for Sustainable Development.* Retrieved from UN Sustainable Development Program: https://sustainabledevelopment.un.org/sdgs

US Department of Homeland Security. (2019, 06 22). *CISA*. Retrieved from Supporting Policy and Doctrine: https://www.dhs.gov/cisa/supporting-policy-and-doctrine

Kriminalističke teme
Zbornik radova
Godina XIX, Broj 5, 2019.
ISSN 1512-5505

ZAŠTITA OD CYBER NAPADA I UPRAVLJANJE PODACIMA NA KRITIČNOJ INFRASTRUKTURI POMOĆU INOVACIONIH 3D A-LATA GIS I BIM

CYBER ATTACK PROTECTION AND CRITICAL INFRASTRUCTURE DATA MANAGEMENT WITH THE INNOVATIVE 3D GIS AND BIM INSTRUMENTS

Pregledni naučni rad

Garaplija Edin
Rizvo Samir[205]

Sažetak

Inspiracija za rad i problem (i) koji se radom oslovljava (ju): Zaštita kritične infrastrukture (KI) je jedan od ključnih bezbjednosno/sigurnosnih izazova današnjice. Sve učestalije prirodne katastrofe izazvane globalnim klimatskim promjenama, tehničko-tehnološke nesreće i udesi, te teroristička prijetnje i drugi antropogeni rizici nastali usljed ljudskog nemara ili namjere, su realna svakodnevna prijetnja po kritičnu infrastrukturu svakog razvijenog društva.

Ciljevi rada (naučni i/ili društveni): Bosna i Hercegovina, zemlja složenog društveno-političkog uređenja, na svom putu ka Euro-Atlantskim integracijama, kao i njena kritična infrastruktura, sigurno predstavljaju osnovanu bazu za realan scenario od gore pobrojanih rizika.

Metodologija/Dizajn: Ubrzanim razvojem tehnologije, prijetnje po KI, nisu samo od gore pobrojanih rizika i opasnosti, već i od sve učestalijeg "IT terorizma", "cyber napada" na pojedince i institucije razvijenih zemalja i njihovu KI.

Ograničenja istraživanja/rada: Samo NATO je mjesečno preko 500 puta meta "Cyber napada". Međunarodnim standradima i pravnim naslijeđem su definisane standardne operativne procedure za kolektovanje, analizu i razmjenu podataka od važnosti za pojedinca i organizaciju.

Rezultati/Nalazi: Radom se daje prikaz korelacije ove regulative sa novim IT tehnologijama današnjice i budućnosti, Geo-reference information system (GIS) i Building Intelligence Modeling (BIM), koje predstavljaju globalne alate za identifikaciju, analizu i vrednovanje podataka, te njihovu sigurnu pohranu i upotrebu u svakodnevnim zadacima zaštite kritične infrastrukture.

Generalni zaključak: Također, ovim radom se daje osvrt na pitanje zaštita od zloupotrebe i "presretanja" podataka od posebne važnosti za zaštitu KI.

[205] *Doktorant Edin Garaplija, predsjednik Naučnog odbora Asocijacije za upravljanje rizicima u BiH, Dr. Sc. Samir Rizvo, pomočnik ministra sigurnosti/bezbjednosti BiH za međunarodnu saradnju*

Opravdanost istraživanja/rada: Bosna i Hercegovina na svom putu priključenja EU mora ubrzanim koracima poduzeti sve neophodne mjere, kako bi sustigla zemlje regiona u pogledu zaštite kritične infratsrukture i borbe protiv terorizma, pa je s tim u vezi, od izuzetne važnosti institucionalizacija i široka primjena "pametnih" alata za zaštitu sistema kritične infratrukture i ključnih podataka za njihovo nesmetano funkcionisanje.

Ključne riječi
kritična infrastruktura, integrisana zaštita, cyber napad, GIS, BIM

Abstract
Reason for writing and research problem (s): Critical Infrastructure Protection (CI) is one of the key security / security challenges of today. Increasingly occurring natural disasters caused by global climate change, technical and technological disasters and disasters, and terrorist threats and other anthropogenic risks arising from human negligence or intent are a real daily threat to the critical infrastructure of every developed society.
Aims of the paper (scientific and/or social): Bosnia and Herzegovina, a country of complex socio-political order, on its path to Euro-Atlantic integration, as well as its critical infrastructure, is certainly a well-founded base for a realistic scenario of the risks listed above.
Methodology/Design: The accelerated development of technology, threats to CIs, are not only of the above risks and dangers, but also of the increasing frequency of "IT terrorism", "cyber attacks" on individuals and institutions of developed countries and their CIs.
Research/Paper limitation: NATO alone is the target of "Cyber attacks" over 500 times a month. International standards and legal heritage define standard operating procedures for the collection, analysis and exchange of data of importance to the individual and the organization.
Results/Findings: This paper presents the correlation of this regulation with new IT technologies of today and the future, Geo-reference information system (GIS) and Building Intelligence Modeling (BIM), which are global tools for identifying, analyzing and evaluating data, and their secure storage and use in the day-to-day tasks of critical infrastructure protection.
General Conclusion: Also, this paper addresses the issue of protection against misuse and "interception" of data of particular importance for the protection of CIs.
Research/Paper Validity: Bosnia and Herzegovina, on its path to EU accession, must take all necessary steps in order to catch up with the countries of the region in terms of critical infrastructure protection and counter-terrorism, and in this regard, institutionalization and the widespread use of "smart" tools are essential. protection of critical infrastructure systems and key data for their smooth functioning.

Keywords
critical infrastructure, integrated security, cyber attack, GIS, BIM.

1. UVOD

Iako se pojmom zaštite KI bave sve razvijene zemlje svijeta, možemo konstatovati da se po ovom pitanju najviše uradilo u SAD-u. Razvijena kritična a posebno energetska infrastruktura SAD-a potaknula je značajno njihov privredni razvoj u 20-21. vijeku. Bez stabilnog napajanja energijom, životi, zdravlje i napredak bi bili ugroženi, a privreda SAD-a ne bi mogla funkcionisati. Direktiva o predsjedničkoj politici SAD-a (PPD-21), identifkuje energetski sektor kao posebno kritičan, jer "omogućava funkcionisanje" ostalih sektora kritične infrastrukture. Ovdje moramo istaći da je više od 80% energetske infrastrukture SDA-a u vlasništvu privatnog sektora. Taj sektor opskrbljuje energijom infrastrukturu, domaćinstva i preduzeća, te druge bitne dijelove ekonomije i proizvodnje širom SAD-a.[206]

Zaštita kritične infrastrukture od internetskih i fizičkih prijetnji bit će ključni izazov za 2019. i naredni niz godina. Moramo uzeti u obzir činjenicu da je najviše prethodnih istraživanja koja tretiraju ugroze KI, obavljeno na području SAD-a. Ministarstvo domovinske sigurnosti (Department of Homeland Security) i Ministarstvo odbrane (Department of Defence) opisuje kritičnu infrastrukturu kao "fizičke i cyber sisteme i imovinu koja je toliko važna za Sjedinjene Države da bi njihovo onesposobljavanje ili uništenje imalo negativan učinak za fizičku ili ekonomsku stabilnost, javno zdravlje građana ili sigurnost zajednice." *Kritična infrastruktura je ugrožena od strane hakera, zločinačkih organizacija i unutar-državnih destruktivnih faktora, zbog njene vitalnosti za američku ekonomiju. Energetski sektor se ističe kao posebno ranjiv ako se uzme u obzir njegova prostorna zastupljenost i sveobuhvatnost: uključujući nuklearna postrojenja, hidro i termo elektrane, distribuciju, i prenosnu mrežu.* Peter Pry, član Komisije za EMP Kongresa i izvršni direktor Radne skupine za nacionalnu i domovinsku sigurnost stavio je prijetnje u zastrašujuću perspektivu: "*Prirodni EMP iz geomagnetske super oluje, kao što je Carringtonov događaj iz 1859. ili željeznička oluja iz 1921., nuklearni EMP napad od terorista ili nestabilnih država poput Sjeverna Koreja tokom nuklearne krize 2013. godine, predstavljaju egzistencijalne prijetnje koje bi mogle ubiti 9 od 10 Amerikanaca putem gladi, bolesti i društvenog kolapsa*".207

Bosna i Hercegovina je potpisnica Platforme Ujedinjenih Nacija za smanjenje rizika od katastrofa. Gledajući globalno, prekidi kritične infrastructure (KI) su uglavnom nastajali uslijed prirodnih katastrofa, koje su uzlaznim trendom prouzročile ogromne ljudske i materijalne gubitke. Ti su gubici mogli biti znatno manji, da su šira i lokalna zajednica i njena kritična infrastruktura bili pripremljeniji za ove izazove. U periodu 2008/2012. širom svijeta je preko 700 hiljada ljudi izgubilo živote, više od 1,4 miliona je povrijeđeno, a oko 23 miliona su ostala bez krova nad glavom. Više od 1,5 milijardi ljudi je pogođeno katastrofama na različite načine, uključujući žene, djecu i ranjive kategorije društva, te je ukupan

---

[206] US Department of Homeland Security Seal - https://www.dhs.gov/cisa/critical-infrastructure-sectors (31.05.19)
[207] Protecting Energy Critical Infrastructure a Key Challenge for DHS, February 16. 2019., Chuck Brooks

ekonomski gubitak bio veći od 1,3 triliona dolara. Na globalnom nivou oko 144 miliona ljudi je raseljeno uslijed posljedica od katastrofa. Ove su prirodne pojave ostavile dugotrajni trag na ekonomski napredak pogođenih zajednica, koje nisu bile, bez obzira na stepen svoje razvijenosti, pošteđene od prirodnih, tehničko-tehnoloških ili antropogenih rizika koji su imali katastrofalan uticaj na živote i zdravlje ljudi, ekonomiju, društveno političko uređenje i njenu KI.[208]

Aktuelne društvene okolnosti i sve izraženije globalne klimatske promjene, usložnjavaju problematiku zaštite kritične infrastrukture (KI), kako raznovrsnošću načina, tako i svojim intenzitetom. Neuobičajenost oblika ugrožavanja uzrokuje i posebne mjere i načine suprotstavljanja, kao odgovor na istovrsne bezbjednosno/sigurnosne probleme. Ovdje treba imati na umu da se pojam „bezbjednost" (bezbednost) odnosi na širu društveno-političku zajednicu, dok pojam „sigurnost" predstavlja uži kontekst vezan za određeni prostor ili organizaciju. Svjedoci smo sve više prirodnih, tehničko-tehnoloških i antropogenih rizika, koji izazivaju različite opasne incidente (opasnosti) sa velikim posljedicama po živote i zdravlje ljudi, njihovu imovinu i životnu sredinu. Po svom obimu, posljedicama i trajnim uticajima na održivu ekonomiju lokalnih i širih društvenih zajednica, pojedine opasnosti mogu imati karakter katastrofa ili vanrednih situacija.

Ovakvi oblici narušenih normalnih životnih situacija, predstavljaju izmjenjeno stanje društvene zajednice izazvano događajima velikih razmjera, kojima se parališe funkcionisanje društvenog sistema zemlje. Trendovi i štete izazvane ovakvim društvenim situacijama nužno nameću imperativ za organizovanim rješenjem u pogledu smanjenja i upravljanja rizicima u vanrednim situacijama sa posebnim akcentom na zaštiti KI.

Kada je riječ o odnosu nesreća i zaštite KI treba imati u vidu da je KI najčešće i sama pogođena vanrednom situacijom, te se očekuje njena hitna stabilizacija, kako bi svojom osnovnom djelatnošću uzela učešće u aktivnostima otklanjanja posljedica i stabilizacije života i rada na pogođenom području. Dakle, uspješno upravljanje rizicima od prirodnih i drugih nesreća, su u direktnoj vezi sa efikasnim sistemom zaštite KI. Mjere poput prevencije, pripremljenosti i adekvatnog odgovora povećavaju stepen sigurnosti KI.

Da bi smo bolje shvatili značaj organizovanog pristupa zaštiti KI, moraju se sagledati svi aspekti definisanja i shvatanja kritične infrastrukture, pojam kritične infrastrukture i njena klasifikacija. Bez funkcionisanja svih subjekata uključenih u integrisani sistem zaštite, nemoguće je u potpunosti ostvariti pouzdan sistem upravljanja rizicima i zaštitom KI u svim fazama njenog odvijanja. Poseban izazov za stručnu i naučnu javnost, predstavlja zaštita i upravljanje podacima na kritičnoj infrastrukturi, koja po svojoj namjeni i

[208] *Izvještaj za period 2002/2012. osiguravajuće kuće Munich RE*

strukturi, spada pod poseban značaj i šiti bezbjednosni interes za svaku razvijenu društveno-političku zajednicu.

Uporedna analiza međunarodnog upravno-pravnog okvira u oblasti zaštite KI, harmoniziranje zakonodavstva BiH sa upravno-pravnim okvirom zemalja susjedstva, te sa upravnom-pravnom regulativom i direktivama Evropske unije, trasiraju mapu puta kojim i naša zemlja treba što prije zakoračati i ispuniti svoje međunarodne obaveze i dostići najviše norme u oblasti zaštite KI. Obaveze vlasnika i operatera KI koje proizilaze procesom harmonizacije sa evropskim naslijeđem i Direktivom za zaštitu KI[209], te međunarodnim standardom za zaštitu podataka ISO 27000[210], kao i sa evropskom regulativom za zaštitu i upravljanje podacima GDPR[211], su da uspostavi efikasan preventivni sistem, ojača integrisani sistem zaštite i definiše standardne operativne procedure službama zaštite i spašavanja, a posebno sa aspekta zaštite, čuvanja i upravljanja osjetljivim podacima, bilo da se radi o onim organizaciono-procesnim ili ličnim podacima.

„Jedno od ključnih područja nacionalne i međunarodne sigurnosti na početku 21. stoljeća postalo je pitanje energetske sigurnosti i zaštite kritične infrastrukture. Kako je osiguranje transportnih pravaca i vlastite energetske infrastrukture postalo jednako važno kao i sama dostupnost energenata, tako je i zaštita energetske infrastrukture postala integralni dio koncepta zaštite sveukupne kritične infrastrukture. To se može vidjeti i na primjeru Republike Hrvatske koja je u situaciji da mora otpočeti sa sustavnim promišljanjem, planiranjem i provedbom aktivnosti vezanih uz postizanje energetske sigurnosti i zaštite kritične infrastrukture. Svjetski trendovi ukazuju na potrebu stvaranja nacionalnih strategija za zaštitu energetske i ostale kritične infrastrukture država, što se posljedično odražava i na potrebu redefiniranja njihovih temeljnih strateških dokumenata, prije svega, onih koji oblikuju sigurnosne strategije i sigurnosne politike.“[212]

Kritična infrastruktura (KI) je okosnica ekonomije, sigurnosti i zdravlja. Temeljno svojstvo KI sistema je njihova međuovisnost. Rezultat takvog svojstva je dobro poznati „domino“ efekt, što znači da poremećaj određenog IP-a može uzrokovati ogromne gubitke ne samo u razmatranom sektoru, nego i u drugim povezanim sektorima KI. Zbog toga KI mora biti sigurna i sposobna izdržati i brzo se oporaviti od svih predvidivih opasnosti. Čini se prilično jasno da je primjena metodologija procjene rizika na nižim i višim razinama i donošenje odluka na temelju tih metodologija vjerojatno najbolji postupak kojim se može pristupiti tako zahtjevnom cilju. Zapravo, metode analize rizika naširoko se koriste za donošenje odluka u područjima u kojima kvarovi opreme, ljudske pogreške, prirodni fenomeni ili

---

[209] Direktiva za zaštitu kritične infrastrukture 2008/114 EC, https://eur-lex.europa.eu/legal-content/HR/TXT/PDF/?uri=CELEX:32008L0114&from=EN
[210] ISO standardi za zaštitu podatakahttp://www.27000.org/
[211] GDPR -Evropska regulativa za upravljanje podacima 2016/679 EC, https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=celex%3A32016R0679 (18.07.19.)
[212] Energetska sigurnost i zaštita kritične infrastrukture: utjecaj na politike nacionalne sigurnosti, Talović Siniša

namjerno ljudsko ponašanje mogu izazvati značajne utjecaje na društvo. Sada je jasno da se i regija približava ovom konceptu, a što je i obveza koja proizlazi iz Direktive Vijeća 2008/114 / EZ[213].

Danas ne možemo govoriti o pojmu integrisanog modela zaštite KI, ako ga ne povežemo i sa modelom javno-privatnog partnerstva (Public Private Partnership – PPP), što je jedna od jasnih preporuka izdatih u Direktivi 2008/114 EC za zaštitu KI, kojom se ističe: "*S obzirom na vrlo značajnu uključenost privatnog sektora u nadzor i upravljanje rizicima, planiranje poslovnog kontinuiteta i oporavak nakon nepogode, pristupom Zajednice trebalo bi se poticati potpuno uključivanje privatnog sektora*". Ova preporuka je jednako važna i za zemlje članice, kao i za zemlje kandidate i potencijalne kandidate za članstvo u EU, među kojima se u ovom trenutku nalazi i Bosna i Hercegovina.

2. DEFINISANJE POJMA KRITIČNE INFRASTRUKTURE I EUROPSKO PRAVNO NASLIJEĐE ZA ZAŠTITU PODATAKA

U poslednjih dvadesetak godina, pitanje KI je postalo posebno značajno. Moderni stil života i zavisnost ljudi i privrede od struje, goriva, interneta (komunikacije uopšte) je svakim danom sve veća i veća. Bezbjednost KI je ključno pitanje savremene nacionalne bezbjednosti, jer ona predstavlja osnov za opstanak zajednice, a asimetrične prijetnje i potreba za efikasnim mjerama zaštite, postale su uobičajena potreba modernih društava.

Teroristički napad od 11. septembra 2001. godine u SAD, dao je novo značenje i novu dimenziju koncepta zaštite KI, a teroristički napadi u Madridu, Londonu, Moskvi, Mumbaiju i Islamabadu su samo potvrdili potrebu za novim pristupom u zaštiti KI. Pored toga, uragan Katrina u SAD, cunami u jugoistočnoj Aziji i cunami u Japanu su također pokazali da prirodne katastrofe mogu imati razorne posledice na infrastrukturu. Tako možemo zaključiti da je zaštita KI, u kontekstu savremenih globalnih prijetnji, predstavlja prioritetno pitanje za nacionalnu bezbjednost jedne države ili podneblja.

Potreba dinamičkog, proaktivnog i strateškog pristupa naročito je neophodna u procesu planiranja zaštite KI u uslovima različitih tipova kriznih i vanrednih situacija. Prije nego je sintagma „kritična infrastruktura" postala izuzetan predmet interesovanja u brojnim analizama koje su se odnosile na terorizam i unutrašnju bezbjednost, pojam „infrastruktura" osamdesetih godina bio je referentna tačka kreatora javne politike i bezbjednosti.

Naime, zbog sve većeg rizika povredljivosti i isključivanja iz redovnog funkcionisanja bilo je potrebno, za svaki sistem pojedinačno, predvidjeti odgovarajuće mjere. Infrastruktura se posmatrala kao logistička funkcija kojom se obezbjeđuju povoljni uslovi za kvalitetno

---

[213] *National critical infrastructure protection - regional perspective / Zoran Keković, Denis Ćaleta, Želimir Kešetović, Zoran Jeftić - Beograd : University of Belgrade - Faculty of Security Studies, 2013.*

obavljanje drugih funkcija logističke podrške. Porastom opasnosti od asimetričnih pretnji, naročito terorizma, u savremenim teorijskim analizama, ali i u praksi, sve je prisutniji izraz „kritična infrastruktura". Neposredno nakon terorističkih napada od septembra 2001. godine, KI postala je bitan i suštinski dio nacionalne bezbjednosti, a njena zaštita predstavlja jedan od prioriteta svake moderne države i društva.

U zavisnosti od kriterijuma a u cilju definisanja KI, postoji potreba za boljim sagledavanjem njenih različitih tipova. U principu, KI može biti od interesa za: državne, regione ili svijet, a to znači da možemo govoriti o nacionalnoj, regionalnoj (evropskoj, afričkoj, Evro-Azijskoj) i svetskoj (globalnoj) KI. S druge strane, u nekim državama je moguće govoriti o kritičnoj infrastrukturi na lokalnom, regionalnom (ekonomskom ili kulturnom regionu), državnom (nacionalnom) i međunarodnom nivou.

U zavisnosti od vremena potrebnog za zaštitom, KI može biti: stalna, privremena ili potencijalna. Stalna KI je ključna infrastruktura za neke države, propisana zakonom, a koja mora biti sve vrijeme u fokusu interesovanja. U kategoriju privremene KI moguće je uvrstiti neke političke, sportske ili kulturne događaje kratkog vremena trajanja, ali koji su veoma važni za državu ili na međunarodnom nivou. Za ove infrastrukture je poznato da će biti važne u neko vrijeme godine ili tokom nekih događaja. Potencijalna KI je infrastruktura koja nije u fokusu, ali u nekim situacijama može biti veoma važna. Za tu infrastrukturu je poznato da može postati KI u nekim prilikama, ali ove situacije se ne planiraju unaprijed.

Prema nekim autorima, KI u odnosu na vlasništvo unutar jedne države, može biti u posijedu: države, opštine, privatnog lica, lica za upravljanje imovinomu državnom vlasništvu, u vlasništvu pravnih lica čiji su osnivači lokalne samouprave. S druge strane, to znači da može biti KI u javnim, privatnim ili javno-privatnim rukama. Javno-privatno partnerstvo je od suštinskog značaja, jer se procjenjuje da je preko 85% od onoga što se može klasifikovati kao KI u SAD-u privatnom vlasništvu, a u Nemačkoj privatni sektor upravlja sa preko 90% KI.

Dakle, to znači da su tipovi KI veoma različiti i zavise od različitih gledišta onih koji odlučuju šta je KI, kao i od strukture i nivoa vlasti. Ali u oblasti zaštite KI postoji potreba za sveobuhvatnijim pristupom. To znači da svi nivoi vlasti u državi moraju da prepoznaju svoju KI i preduzmu mjere da ih zaštite. Ako samo jedan od nivoa nije uspeo da prepozna i zaštiti svoju KI, to bi moglo dovesti do katastrofe, jer je infrastruktura međusobno povezana i zavisna jedna od druge.[214]

Iako se rad ne bavi konkretnim mjerama integrisane zaštite kritične infrastrukture, niti zalazi u dubine preporuka datih Direktivom EU za zaštitu kritične infrastrukture 2008/114

---

[214] Čemerin, D., Trut, D., Kriteriji za određivanje hrvatske kritične infrastrukture, Zbornik radova "Hrvatska platforma za smanjenje rizika od katastrofa", Državna uprava za zaštitu i spašavanje, Zagreb, str. 33, 2010.

EC, radi šitreg sagledavanja ove problematike od strane čitalaca i akadeske zajednice, navest ćemo nekoliko njenih najznačajnijih elemenata. Naime, ovom Direktivom se uspostavlja postupak za utvrđivanje i označivanje evropske kritične infrastructure (EKI-ja) te utvrđuje pristup za poboljšanje njezine zaštite. Direktiva je primjenjiva na zemlje članice, zemlje kandidate i zemlje potencijalne kandidate za članstvo u EU. Ključne tačke Direktive su utvrđivanje i označivanje EKI-ja, na način da se definiše postupak utvrđivanja potencijalnih EKI-ja (uz pomoć Evropske Komisije ako je to potrebno). Pri utvrđivanju potencijalnih EKI-ja trebale bi primjenjivati: međusektorska mjerila kao što su moguće žrtve, gospodarske posljedice i utjecaj na javnost; i sektorska mjerila specifična za vrstu EKI-ja. Potrebno je ostvariti saradnički proces sa zemljama susjedstva, u svrhu označavanja EKI (npr. rasprave i razmjene mišljenja i iskustava s zemljama susjedstva i članicama EU) za potencijalne EKI-je koji se nalaze na njihovu državnom području. Potrebno je redovno preispitivanje utvrđivanja i označavanja EKI-ja. Direktiva je prvobitno definisala primjenu samo na ključne sektore infrastrukture: energiju i prijevoz, ali se s vremenom njezino područje primjene proširilo in a druge sektore (hrana, zdravstvo, školstvo, finanasije itd.).

Sigurnosnim planovima operatera (SPO), osigurava se da za svaki EKI postoji jasno sigurnosno planiranje. Svrha postupka SPO-a jest utvrđivanje kritične imovine EKI-ja, kao i postojećih sigurnosnih rješenja za njihovu zaštitu. Oficiri za vezu su zaduženi za sigurnost a nacionalni autoriteti osiguravaju da njihovo imenovanje u skladu sa pravilima i međunerodnim standardima. Oficir za vezu služi kao tačka za kontakt između vlasnika/operatera EKI-ja i odgovarajućeg tijela zemlje EU-a. Osigurava se pravovremeno izvještavanje, te ocjenjivanje prijetnje u odnosu na EKI-je u roku od jedne godine nakon što je označena kritična infrastruktura. Svake dvije godine Komisiji se dostavljaju izvještaji s općim podacima o vrstama rizika, prijetnjama i slabostima. Direktiva se primjenjuje od 12. januara 2009., a sve zemlje ćlanice, kandidati za članstvo i potencijalni kandidati bi je trebale uključiti u svoje nacionalno pravo.

Pet godina poslije, 2013. godine, Evropska Komisija je donijela radni dokument o novom pristupu Europskom programu za zaštitu kritične infrastrukture, European Programme for Critical Infrastructure Protection (EPCIP). Njime se definiše potreba za interoperabilnošću i međusektorskom saradnjom jer je narušavanje kritične infrastructure uzročnoposljedično povezano, npr. prekid napajanja električnom energijom, narušava telekomunikacionu, saobraćajnu i privrednu infrastrukturu. EPCIP, također definiše i uspostavu Mreže za rano upozoravanje na kritičnoj infrastrukturi, Critical Infrastructure Warning Information Network (CIWIN), čiji je zadatak da osigura sistem za razmjenu i raspravu o informacijama, studijama, dobrim praksama vezanim za KI, te razmjenu informacija i komunikacija putem digitalnog prijenosa podataka među organizacijama KI. Ova mreža ima za cilj analizirati i prikazati odabrane slučajeve paneuropskih kritičnih infrastruktura, te primati korisne i zaštićene povratne informacije od korisnika CIWIN-a. Također, mrežom se daje mogućnost pristupa savremenim IT alatima, koji uključuju i metodologije procjene rizika sa gotovim predlošcima. Mreža predstavlja digitalnu platformu domaćina za nekoliko nacionalnih CIP područja u državama članicama i može sadržavati sve relevantne informacije o saradnji sa trećim zemljama, kao što su SAD, Kanada, zemlje EFTA-e i

kandidati za članstvo. Upravo ovakav vid umrežavanja, te prikupljanja i obrade ogromnog broja informacija, predstavlja izazov za sagledavanje sigurnosne i šireg bezbjednosne problematike zaštite i upravljanja podacima. Savremene tehnike presretanja ("cyber napadi" i sl.), zahtijevaju i savremene alate za odbranu od te vrste rizika.

Međunarodni standard za informacijsku sigurnost i zaštitu podataka ISO 27000, daje smjernice za primjenu ovih normi, kojima se osigurava usklađenost aktivnosti unutar organizacije s važećom zakonskom regulativom, te se povećava pouzdanosti sistema u slučaju katastrofe, što pridonosi povećanju svijesti o nužnosti obuke i osvješćivanja svih aktera sistema vezanih uz informacijsku sigurnost[215]. Sastoji se od četiri osnovna poglavlja: sistemi za upravljanje informacijskom sigurnošću (engl. ISMS – Information Security Management System); odgovornost uprave (engl. Management Responsibility); ispitivanje sistema upravljanja (engl. Management Review); poboljšanje suistema za upravljanje informacijskom sigurnošću (engl. ISMS Improvement).

U pogledu upravljanja ova četiri poglavlja mogu se sažeti u dva bloka i to: sistem za upravljanje sigurnošću koji obuhvata: dokumentiranje, pregled, ispitivanje, odgovornost uprava, korektivne i preventivne mjere te stalno poboljšanje sistema i upravljanje informacijskom sigurnošću koji je ciklus uspostave, implementacije, rukovanja, pregledavanja, ispitivanja i poboljšanja sistema za upravljanje informacijskom sigurnošću (ISMS), a koji je opisan modelom PDCA (engl. Plan-Do-Check-Act). Faze PDCA ciklusa su: PLAN: Uspostava sistema za upravljanje informacijskom sigurnošću; DO: Upravljanje sistemom informacijske sigurnosti; CHECK: Nadzor i ispitivanje sistema informacijske sigurnosti; ACT: Poboljšanje sistema informacijske sigurnosti;

General Data Protection Regulative (GDPR) je opšta Uredba EU 2016/679 EC, o zaštiti ličnih podataka. Uredba se bavi harmonizacijom zaštite ličnih podataka na nivou EU, te definiše veći stepen kontrole za lica čiji se podaci obrađuju i unapređuje upravljanje savremenim rizicima iz ove oblasti. Kritična infrastruktura spada među najveće rukovaoce podataka o ličnosti i u postupku usklađivanja sa obavezama utvrđenih Uredbom treba da izvrši punu analizu svog postojećeg regulatornog i infrastrukturnog okvira zaštite ličnih podataka. Također, primjenom Uredbe pruža se prilika za ispravke eventualnih ranijih nedostatka u postojećim procesima, te se od organizacija očekuje podizanje opšte svijesti o standardima zaštite ličnih podataka, a posebno imajući u vidu zaprijećene stroge sankcije za slučaj neusklađenosti.

Uredbom se definišu sljedeće oblasti: područje primjene, ujednačeni propisi i jedinstveni mehanizam, odgovornost i transparentnost, pravne osnove za obradu, privola, službenik za zaštitu osobnih podataka, pseudonimizacija, povrede podataka, sankcije, pravo

---

[215] Stručni rad: Norme informacijske sigurnosti ISO/IEC 27K, Javor Bogati, Ministarstvo obrane Republike Hrvatske,

pristupa, pravo na zaborav, prenosivost podataka, integrirana zaštita podataka i evidencija o aktivnostima obrade.

Sa aspekta vanjske i unutrašnje zaštite podataka, najvažnija poglavlja su definisanje rada službenika za zaštitu ličnih podataka i integrirana zaštita podataka, kojima se daju precizne smjernice za izradu procedura i primjenu određenih mjera zaštite tajnosti podataka.

Ako se osnovne djelatnosti voditelja obrade sastoje od postupaka obrade, koji zbog svoje prirode, obima ili svrhe, iziskuju redovno i sistemsko praćenje ispitanika u velikoj mjeri, odnosno ako aktivnosti obrade uključuju opsežnu obradu posebnih kategorija podataka, potrebno je imenovati stručnu osobu sa znanjima u području zaštite podataka koja će pomoći voditelju ili izvršitelju obrade, te nadzirati usklađenost s mjerama iz GDPR-a. Od službenika za zaštitu podataka očekuje se stručnost u upravljanju IT procesima, sigurnosti podataka (uključujući odgovor na "cybernapade") i ostalim kritičnim pitanjima koja se tiču pohrane i obrade ličnih i osjetljivih podataka. Potrebni nivo znanja širi je od samog razumijevanja zakonskih propisa. Više podataka o pojedinostima i funkciji službenika za zaštitu podataka dati su u dokumentu "Smjernice o službenicima za zaštitu podataka," izdanom od strane Radne skupine za zaštitu podataka.

Mjere tehničke i integrirane zaštite podataka propisuju primjenu zaštitnih mjera u sam postupak razvoja procedura, proizvoda i usluga. Treba od početka primijeniti visoki nivo mjera za zaštitu privatnosti, a voditelj obrade mora osigurati da tehničke i prodecuralne mjere budu adekvaatne i u skladu s propisima za vrijeme cjelokupnog trajanja postupaka obrade. Voditelji obrade trebaju primijeniti mehanizme kojima bi se spriječila obrada osobnih podataka, osim ako je to potrebno za svaku od određenih svrha.

Izvještaj Agencije Evropske unije za mrežnu i informacijsku sigurnost[216] objašnjava što je potrebno da se usvoje metode integrirane i tehničke zaštite podataka. U izvještaju se navodi kako se aktivnosti enkriptiranja i dekriptiranja moraju odvijati lokalno, a ne na udaljenom poslužitelju, jer ključevi moraju biti u posjedu voditelja obrade ako je cilj zaštita privatnosti podataka. Također se navodi da je korištenje usluga za pohranu podataka, poput onih u oblaku, praktično i relativno sigurno u slučaju da samo vlasnik podataka, ali ne i pružatelj usluge u oblaku, ima pristup ključevima za dekriptiranje.

Zaštita podataka unutar sistema kritične infrastrukture je poseban izazov za stručnjake i nacionalne autoritete, ako se uzme u obzir njena osjetljivost i ranjivost na terorizam, kao jednu od najvećih prijetnji današnjice. Dosadašnji teroristički napadi na saobraćajnu infrastrukturu (metroi u Londonu, Madridu i Tokiju), su uglavnom bili usmjereni na ciljane posljedice po živote i zdravlje običnih građana, sa ciljem izazivanja panike i masovne

[216] *ENISA - https://europa.eu/european-union/about-eu/agencies/enisa_hr (pristup 18.07.19.)*

histerije i straha. Međutim, učestali "cyber" napadi na privatnost pojedinaca i organizacija, posebno onih finansijskih, te nedavni napad na elektroenergetsku infrastrukturu Venecuele u danima pokušaja "vojnog puča" otvaraju i pitanje zaštite sistema kolektovanja i upotrebe podataka, od mogućih terorističkih napada ovakve vrste. Posljedice po nezaštićenu KI, možda neće biti iskazane trenutnim brojem žrtava kao u ranijim terorističkim napadima ali će sigurno biti dugoročnije i direktno i indirektno štetnije po društveno politički poredak napadnute zemlje. Tako npr. u najgorem scenariju višednevnog prekida elektroenergetske KI, mora se uzeti u obzir i međusektorska ovisnost te posljedice koje će dugoročno a neke i trajno povećati ukupnu ranjivost zajednice. Iz tog razloga, zadatak svih vlasnika i operatere na KI, jeste da svakodnevno tragaju i čine maksimalne napore za uspostavu integriranog sistema zaštite KI, sa posebnim osvrtom na zaštitu i upravljanje osjetljivim podacima primjenom inovativnih tehnologija.

3. UPRAVLJANJE PODACIMA POMOĆU SOFTVERSKIH ALATA "GIS" I "BIM"

Pod pojmom zaštite podataka podrazumijevamo uspostavljanje sistema kolektovanja, operacionalizacije i upotrebe podataka. Kolektovanje podataka se vrši putem identifikacijskih formi, koje trebaju biti usklađene sa EUROSTAT kasifikacijom i kategorizacijom kako podataka o samim rizicima, tako i podataka o uticajiima tih rizika na ljude, imovinu i životnu sredinu, te podataka o kapacitetima integrisanih službi i mjera zaštite na KI. Pri kolektovanju podataka treba slijediti smjernice proizašle iz direktive EU za zaštitu KI. Operacionalizacija podataka dobijenih pravilnim identificiranjem i kolektovanjem, predstavlja centralni dio sistema u kome se nalaze oni najosjetljiviji podaci za nesmetan rad KI, odnosno podaci koji se svakodnevno analiziraju i odnose na, kako vanjske tako i unutrašnje, ranjivosti sistema KI. Vanjski faktori ranjivosti KI su potencijalni terorizam, te „cyber napadi" u svrhu ucjene i iznude, odnosno u cilju sticanje prednosti za konkurenciju. Unutrašnji faktori rizika predstavljaju potencijalno nezadovoljstvo samih uposlenih unutar sistema KI ili njihov nemar i neodgovorno ponašanje koji mogu dovesti do ozbiljnog narušavanja sigurnosnog sistema. Da bi se uspostavila efikasna operacionalizacija podataka i njihova adekvatna zaštita od vanjskih i unutrašnjih prijetnji, potrebno je primjeniti smjernice date međunarodnim standardom ISO 27000. Upotreba podataka predstavlja izuzetno osjetljivu fazu iz razloga što se njome mora garantovati ne samo adekvatna zaštita osjetljivih podataka o samom sistemu, već i zaštita privatnih podataka uposlenih i posjetilaca po raznim osnovama, kojima se mora garantovati potpuna privatnost i zaštita ličnih podataka od zloupotreba, u skladu sa regulativom GDPR.

Zaštita podataka dobijenih u procesu integrisane zaštite KI, predstavlja veoma važan preventivno-operativni segment koji se izvodi u tri faze: pripremnoj, operativnoj i arhivnoj. Ovaj proces počinje planiranjem sistema zaštite podataka, izradom procjene i plana IT zaštite shodno smjernicama i međunarodnim standardima. Od izuzetne je važnosti pravilno odabrati adekvatne alate za prikupljanje, obradu i arhiviranje podataka, koji svojim akreditovanim i licenciranim softverima garantuju maksimalnu zaštitu osjetljivih i ličnih podataka. Ovim radom ćemo se detaljnije osvrnuti na „GIS i BIM", kao dva najpoznatija alata za identifikaciju, analizu, vrednovanje, kontrolu i upravljanje prostornim podacima.

Odabir ovih alata za analizu je došao sa dugogodišnjim ličnim empirijskim saznanjima i istraživanjima problematike zaštite osjetljivih podataka na kritičnoj infrastrukturi.

Geografski informacionii sistem (GIS) predstavlja osnovni alat za mapiranje rizika, na globalnom svjetskom nivou. Nastao je 1960-tih, za potrebe višeslojnog upravljanja prostornim podacima i njihovim pridruženim osobinama. Kao inovacioni odgovor na izazov zaštite i funkcionalnog upravljanja velikim količinama podataka o rizicima, uticajima i kapacitetima snaga, uporedo sa fazom kvantitativnih i kvalitativnih vrednovanja podataka, potrebno je pristupiti i mapiranju georeferentnih podataka. Pomoću njih generišemo nivo transparentnosti informacije o ranom upozorenju na rizike, te omogućavamo funkcionalan pregled angažovanosti svih zainteresovanih učesnika u sistemu zaštite i spašavanja. Integracija akcija procjenjivanja i mapiranja rizika, doprinosi donošenju preciznijih, odlučnijih i efikasnijih odluka o prioritetnosti postupanja, te se pristupa najtežim rizicima sa najvišim odgovarajućim mjerama prevencije i pripravnosti.

U generalnom smislu GIS predstavlja računalni sistem sposoban za integrisanje, spremanje, uređivanje, analiziranje i prikazivanje geografskih informacija. U specifičnom smislu, GIS predstavlja "pametne karte", koje svojim korisnicima dopuštaju stvaranje interaktivnih upitnika (istraživanja koja stvara korisnik), analiziranje prostornih informacija i uređivanje podataka, preciziranih u prostoru. Najpoznatiji globalni proizvođač alata GIS-a je ArcGis, čija platforma ESRI predstavlja i zvaničnu platformu UN-a za mapiranje i upravljanje rizicima od katastrofa. Pored ArcGis-a, tu su još i proizvođači alata: ArcMap, MapInfo, CARIS i dr.[217]

Današnje GIS vektorske baze, većinom u svom kodu imaju napredni enkripcijski standard, Advanced Encryption Standard (AES), vodeni žig („water mark“), hologramsku i biometrijsku zaštitu svojim pristupima. Zaštita vektorskih mape podrazumijeva šifriranje podataka vektorskih mapa, kontrolu pristupa korisnika i identificiranje operatera, odnosno vlasnika, u cilju sprječavanja šteta, napada ili ilegalnih distribucija, koje se mogu dogoditi u proces integracije niza geografskih informacija. Istraživači su dali rješenja zaštite putem „vodenog žiga“ za zaštitu autorskih prava i metode napredne enkripcije (šifriranja), usmjerenih na različite domene, vodeći računa o međunerodnom upravno-pravnom nasljeđu, Uredbi GDPR i standardu ISO 27000.

Važan segment pripreme za digitalizaciju mapa predstavlja upotreba bespilotnih letilica (dronova), koji za kratko vrijeme mogu precizno snimiti ortofoto snimke velikih prostornih površina, što je od izuzetnog značaja za starteške kritične infrastrukture, saobraćaj i energetiku. Uz pomoć specijalističkih snimka iz vazduha, mogu se relativno za kratko vrijeme, izraditi i 3D modeli prostora i nepristupačnih terena, a posebno objekata kritične infrastrukture na njima (npr. saobrćajnice, energetski objekati, elektroprenosne mreže,

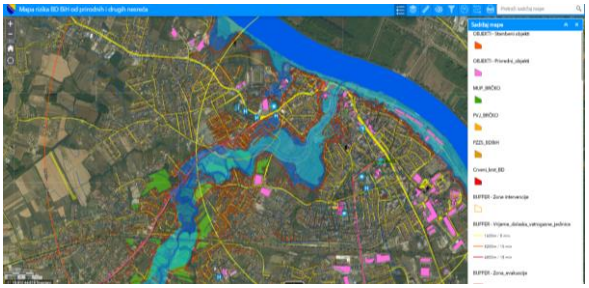
---

[217] "Inovacioni pristup za upravljanje rizicima korištenjem programskih alata GIS i BIM" Garaplija, E., Strugar, V., Međunarodna konferencija „CIBEK 2018“

javne i ustanove od značaja i sl.). Zahvaljujući snimanjima dronovim iz vazduha i GIS bazama, znatno se smanjuje upotreba resursa, te se ubrzava čitav proces digitalizacije i mapiranja. Pored upotrebe u posebnim državnim, industrijskim, sigurnosnim i vojnim svrhama, tehnologija geografskog informacijskog sistema se može koristiti i za naučna istraživanja, upravljanje resursima, planiranje razvoja, geodeziju itd. Za sve ove upotrebe, zajednička je problematika zaštita ogromnih količina osjetljivih podataka. Ovi podaci pored osjetljive operativno-tehnološke vrijednosti imaju i veliku količinu ličnih informacija, koje se putem internetskih mreža mogu zloupotrebiti. GIS, pored svoje enkripcijske zaštite podataka, također omogućava planerima da u slučaju vanjskih ili unutrašnjih ugroza i „Cyber napada", definišu prostor uticaja, vrijeme potrebno za adekvatan odgovor i potrebne kapacitete u akcijama zaštite i spašavanja. Dakle, prednosti GIS-a su u mogućnosti mapiranja putem višeslojnih „layera" (podloga), odnosno unosa više vrsta mapa ili grupa prostornih podataka, te sigurne identifikacije, operativne obrade i arhiviranja ogromnih količina georeferenciranih podataka, dokumenata, slika i drugih vidova audio i video resursa. Svi pohranjeni podaci, se lako svrstavaju i pronalaze pomoću filtera, te je sa njima moguće efikasno upravljati sa ograničenim ljudskim resursima, što također bitno utiče na unutrašnje faktore rizika u pogledu zaštite podataka.

Evropskim smjernicama za procjenjivanje rizika od katastrofa izazavanih klimatskiim promjenama ili ljudskim nemarom ili namjerom, preporučuju se sledeće mape:

1. Mape koje prikazuju očekivani prostorni raspored glavnih opasnosti. Različite opasnosti i intenziteti treba da budu predstavljeni u odvojenim „layerima".
2. Mape uticaja koje pokazuju prostornu distribuciju svih relevantnih elemenata koji treba da budu zaštićeni - kao što su populacija, infrastruktura, prirodno zaštićena područja i sl.
3. Mape kapaciteta, koje daju skupine podataka o brojnosti i materijalnim resursima snaga za suprotstavljanje izazovima i posljedicama od katastrofa.



Ilustracija 1: Interaktivna mapa Brčko distrikta BiH (www.inzagroup.eu[218])

[218] https://inzagis17.maps.arcgis.com/apps/webappviewer/index.html?id=c161bac5370542a5aba10f25bd5c2de9

Ako uzmemo u obzir da GIS predstavlja alat za mapiranje velikih prosotra, npr. lokalnih zajednica, terena i infrastrukture, dajući im njihov vanjski oblik, onda BIM (Building Information Modeling), predstavlja inteligentni softverski alat za modeliranje informacija unutar objekata, dajući im njihov još precizniji i vanjski ali i unutrašnji oblik. Ovaj alat, koji je nastao kao odgovor na sve veću urbanizaciju i globalizaciju je uspostavljen na bazi 3D modeliranja, te stručnjacima arhitekture, inženjerstva i graditeljstva (AEC) pruža uvid i alate za efikasnije planiranje, projektovanje, izgradnju i upravljanje građevinama i infrastrukturom u visoko i nisko gradnji.[219] Obzirom da je ovaj alat nastao na Autodesk projektantskoj platformi, u sebi je integrisao nekoliko značajnih funkcija, pridodatih osnovnoj funkciji projektovanja. To su prije svih 3D modeliranje, odnosno izrada trodimenzionalnog modela (sa visinama, dužinama i širinama), koji vizuelno daje mnogo bolji uvid u projektantskom smislu u odnosu na dvodimenzionalni način projektovanja putem arhitektonsko-građevinskih tlocrta. Kada se 3D modelu pridodaju i funkcije menadžmenta, odnosno upravljanja projektom u svim fazama njegove realizacije: planiranju, projektovanju, izvođenju i održavanju, onda postaje jasno zašto je ovaj alat za veoma kratak period postao pravo osvježenje u građevinarstvu[220].

Uzimajući u obzir da je BIM precizniji i složeniji alat za kolektovanje velikog broja osjetljivih informacija u odnosu na GIS, koje pored prostornih, sadrže i tehničko-ekonomske povjerljive podatke, proces zaštite njegovih podataka je samim tim složeniji izazovniji. U BIM-u se pored napredne enkripcijske zaštite podataka i "vodenog žiga" za zaštitu autorskih prava, moraju primjeniti i odredbe međunarodnog upravno-pravnog naslijeđa za zaštitu podataka.

Stari pristupi upravljanja procesima izgradnje, a posebno održavanja već izgrađenih objekata infrastrukture, nisu više u mogućnosti da budu korak s brzom urbanizacijom i rastom populacije. Evidentan je pritisak i na postojeću infrastrukturu jer njeni sistemi i dalje rastu, grade se novi a stari imaju potrebu za kvalitetnim održavanjem i prepoznavanjem rizika u njihovoj ranoj fazi, kako bi se s njima moglo upravljati prije nego izazovu neku havariju ili štetu na objektima. Urbanizacija, zagušenje, okolišni propisi i ekonomska ekspanzija, potiču potražnju za kvalitetnom gradnjom i održavanjem infrastrukture. McKinsey Global Institut[221] procjenjuje da se gotovo 49 trilijuna dolara vrijednost ulaganja u infrastrukturu treba potrošiti od 2016. do 2030. Osim toga, da bi zadržao korak s projiciranim rastom, svijet mora ulagati još 3,3 bilijuna dolara godišnje do 2030., a trenutno ulaže oko 2,5 trilijuna dolara. U ovoj pozadini, tržište planiranja, projektovanja, izgradnje i održavanja infrastrukture doživljava temeljne promjene. Primjena BIM-a obuhvata veoma širok spektar informacijskih mogućnosti, od upravljanja rizicima u fazama planiranja, projektovanja i gradnje pa sve do simuliranja otpornosti konstrukcije u

---

[219] *Autodesk Handbook, „Strategic industry foresight – The digitalization of Infrastructure"*
[220] "Inovacioni pristup za upravljanje rizicima korištenjem programskih alata GIS i BIM" Garaplija, E., Strugar, V., Međunarodna konferencija „CIBEK 2018"
[221] https://www.mckinsey.com/, (datum pregleda 11.04.2018.)

požarima, zemljotresima, orkanskim vjetrovima, i drugim fizičkim narušavanjima stabilnosti građevine. Posebna prednost BIIM-a na drugim tehnologijama je ta što se podaci kreiraju 3D okruženju, pri čemu se dodaju podaci o dinamici u 4D modelu, tehničkim i finansijski podaci u 5D, podaci neophodni za efikasno održavanje u 6D i sigurnosni podaci u 7D modelu objekta.

Identifikacijske forme, korištene za kolektovanje i klasificiranje podataka, koje sadržavatju lične i osjetljive podatke, trebaju uvrstiti pravne osnove za obradu, te pristanak i pseudonominizacija izvora podataka, tamo gdje zloupotreba podataka može izazvati štetu po organizaciju i pojedinca.

Ilustracija 2: Autodesk Revit BIM Software, u kome se kolektuju svi podaci o građevini ali mogu biti kolektovani i lični podaci izvođača i nadzora.

4. ZAKLJUČAK

Izazov zaštite prikupljanja i kolektovanja podataka putem inovativnih alata poput GIS-a i BIM-a koji predstavljaju budućnost u planiranju, gradnji i održavanju infrastrukturnih objekata u okviru lokalnih i nacionalnih prostornih planova, zahtijeva ozbiljan sistemski pristup. Zahtjevi u pogledu zaštite koje je definisala međunaordna zajednica putem svojih uredbi, direktiva i standarda, predstavljaju upravno-pravni okvir u kojem sve države članice, kandidati i potencijalni kandidati za članstvo, trebaju definisati svoje nacionalne strategije i svoju upravno-pravnu regulativu. Globalni izazovi i šarolikost lepeze prijetnji,

među kojima posebno treba istaknuti terorizam kao "modernu pošast" današnjeg vremena, predstavljaju jasne zahtjeve za vlasnike i operatore kritičnih infratsruktura, bilo da su one u javnom ili privatnom vlasništvu, u pogledu potreba za integrisanom zaštitom, koja obavezno mora uključivati planove za zaštitu osjetljivih i ličnih podataka od zloupotreba i napada. Masovnost i složenost gradnje objekata i mreža kritične infrastrukture, kreira veoma složene zadatke stručnjacima koji se bave bezbjednosno/sigurnosnim izazovima, te koji su uvažavajući specifičnosti i težinu ove problematike, usvojili dva osnovna alata GIS i BIM, kao značajnu pomoć pri identifikaciji, kolektovanju, analizi, vrednovanju i arhiviranju prostronih podataka. Ako za GIS možemo reći da predstavljajući prostorno sveobuhvatniji i primjenjiviji alat za identifikaciju, kolektovanje i analizu podataka na makro lokacijama izvan mreža kritične infrastrukture, onda za BIM možemo zaključiti da predstavlja još precizniji i obuhvatniji alat za upravljanje podacima na mikro lokacijama i unutar samih građevinskih cjelina i pojedinačnih termo-energetskih sistema privremeno ili trajno ugrađenih u objekte. Oba ova alata imaju svoju primjenu u procesu upravljanja rizicima, zbog svojih karakteristika funkcionalnog i bezbjednosno/sigurnosnog upravljanja bazama velike količine različitih podataka. Mogućnost 3D, 4D, 5D, 6D i 7D modeliranja sa ovim alatima, omogućava nam potpunu vizualizaciju i upravljanje integrisanim procesom upravljanja i zaštite prikupljenih podataka. GIS i BIM, kao globalne platforme nadopunjuju jedna drugu, te otvaraju mogućnosti funkcionalne upotrebe, dajući efikasniji model upravljanja čitavim procesom upravljanaj i zaštite osjetljivih i ličnih podataka. Dakle, zahvaljujući razvoju GIS i BIM inovativne tehnologije, pored toga što značajno ubrzavamo i čitav proces planiranja, projektovanja, gradnje i održavanja, te smanjujemo troškove i radnu snagu, upravljamo i svim fazama rizika, uključujući i izazove i prijetnje po sigurnost informacija, osjetljivih i ličnih podataka. Da bi ovakav sistem postao u potpunosti efikasan i operativan, potrebno je kreirati čvrstu zakonsku regulative i tehničke smjernice, uvažavajući upravno-pravno naslijeđe EU, te tehnički i kadrovski izgraditi i ojačati postojeće kapacitete. Kritična infrastruktura je sama po svojoj namjeni i svrsi značajna "žila kucavica" svakog modernog društveno-političkog uređenja, te je potrebno sistemski graditi i kapacitet za njenu adekvatnu zaštitu. Ovdje prije svega mislimo na edukacijsko jačanje kadrovskog potencijala službenika IT zaštite, u okviru integrisanih službi zaštite i spašavanja, koje kroz programe različitih specijalističkih edukacija, primjenu IT alata i kontinuirane treninge, možemo osposobiti i dodatno ojačati za izazove i adekvatne odgovore u procesu integrisane zaštite evropske, regionalne i nacionalne kritične infrastrukture.

5. LITERATURA

Publikacije

1. Protecting Energy Critical Infrastructure a Key Challenge for DHS**,** February 16. 2019**.,** Chuck Brooks
2. Energetska sigurnost i zaštita kritične infrastrukture: utjecaj na politike nacionalne sigurnosti, Talović Siniša
3. National critical infrastructure protection - regional perspective / Zoran Keković, Denis Ćaleta, Želimir Kešetović, Zoran Jeftić - Beograd : University of Belgrade - Faculty of Security Studies, 2013.
4. Čemerin, D., Trut, D., Kriteriji za određivanje hrvatske kritične infrastrukture, Zbornik radova "Hrvatska platforma za smanjenje rizika od katastrofa", Državna uprava za zaštitu i spašavanje, Zagreb, str. 33, 2010.
5. Stručni rad: Norme informacijske sigurnosti ISO/IEC 27K, Javor Bogati, Ministarstvo obrane Republike Hrvatske
6. "Inovacioni pristup za upravljanje rizicima korištenjem programskih alata GIS i BIM" Garaplija, E., Strugar, V., Međunarodna konferencija „CIBEK 2018“

Internet

1. Direktiva za zaštitu kritične infrastrukture 2008/114 EC, https://eur-lex.europa.eu/legal-content/HR/TXT/PDF/?uri=CELEX:32008L0114&from=EN
2. Regulativa za upravljanje podacima 2016/679 EC, https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=celex%3A32016R0679 (18.07.19.)
3. ISO standardi za zaštitu podatakahttp://www.27000.org/
4. US Department of Homeland Security Seal - https://www.dhs.gov/cisa/critical-infrastructure-sectors (31.05.19)
5. Izvještaj za period 2002/2012 osiguravajuće kuće Munich RE
6. “Cyber napadi” na medijskoj mreži Al Jazeera, http://balkans.aljazeera.net/tema/cyber-napadi (18.07.19.)
7. ENISA - https://europa.eu/european-union/about-eu/agencies/enisa_hr (pristup 18.07.19.)
8. https://inzagis17.maps.arcgis.com/apps/webappviewer/index.html?id=c161bac5370542a5aba10f25bd5c2de9 (19.07.19.)
9. Autodesk Handbook, „Strategic industry foresight – The digitalization of Infrastructure“

Kriminalističke teme
Zbornik radova
Godina XIX, Broj 5, 2019.
ISSN 1512-5505

Panel 6

DUHOVI U MREŽAMA? DIGITALNA FORENZIKA I KRIMINALISTIČKE ISTRAGE

Kriminalističke teme
Zbornik radova
Godina XIX, Broj 5, 2019.
ISSN 1512-5505

KRIMINALISTIČKO POSTUPANJE SA DIGITALNIM DOKAZIMA U PRAKSI POLICIJSKIH AGENCIJA U BIH

DIGITAL EVIDENCE HANDLING IN PRACTICE OF POLICE AGENCIES IN B&H

Izvorni naučni rad

Prof. dr. Muamer Kavazović[222]
Prof. dr. Dina Bajraktarević Pajević[223]
Prof. dr. Marija Lučić – Ćatić[224]
Predrag Puharić[225]

Sažetak

Policijske agencije u Bosni i Hercegovini, zavisno od stajališta nosilaca pravosudnih funkcija u postupanju sa digitalnim dokazima primjenjuju različite prakse. Slijedom navedenog, želja autorskog tima je da osvijetli navedeni problem i njegove eventualne posljedice. Ciljevi rada je da se utvrde načini postupanja sa digitalnim dokazima od strane policijskih agencija i ispita veza između utvrđenih obrazaca postupanja i uloge tužilaca iz perspektive stručnih lica policijskih agencija.

U radu su podaci prikupljani posredno putem analize sadržaja, ali i anketiranjem i intervjuisanjem stručnih lica policijskih agencija. U analizi prikupljenih podataka korištene su sve osnovne metode. Od opće-naučnih metoda korištene su statistička i komparativna metoda, a u analizi pravnog okvira dogmatsko-pravna metoda. Ključno ograničenje istraživanja je sadržano u činjenici da odgovori anketiranih stručnih lica odražavaju njihove lične percepcije i iskustva u pogledu postupanja sa digitalnim dokazima uslijed čega se ne mogu izvući generalni zaključci o samoj oblasti kao cjelini. Također, nije bilo moguće objektivno potvrditi sve okolnosti i detalje postupanja sa digitalnim dokazima koji su opisani od strane ispitanika. Na temelju prikupljenih podataka autori su identificirali obrasce u postupanju sa digitalnim dokazima, kao i njihove ključne nedostatke, koji mogu rezultirati sa nezakonitošću dokaza. Rad predstavlja skroman doprinos naučnoj i stručnoj raspravi o načinima otklanjanja manjkavosti u postupanju i ostvarenja harmonizacije rada u ispitivanoj oblasti. Generalni zaključak iznesen u radu je da se neujednačenost prakse domaćih policijskih agencija u postupanju sa digitalnim

[222] Fakultet za kriminalistiku, kriminologiju i sigurnosne studije Univerziteta u Sarajevu / Faculty of Criminal Justice Science, Criminology and Security Studies, University of Sarajevo; e-mail: mkavazovic@fkn.unsa.ba.
[223] Fakultet za kriminalistiku, kriminologiju i sigurnosne studije Univerziteta u Sarajevu / Faculty of Criminal Justice Science, Criminology and Security Studies, University of Sarajevo; e-mail: dbajraktarevic@fkn.unsa.ba.
[224] Fakultet za kriminalistiku, kriminologiju i sigurnosne studije Univerziteta u Sarajevu / Faculty of Criminal Justice Science, Criminology and Security Studies, University of Sarajevo; UNSA; e-mail: mlucic@fkn.unsa.ba.
[225] Fakultet za kriminalistiku, kriminologiju i sigurnosne studije Univerziteta u Sarajevu / Faculty of Criminal Justice Science, Criminology and Security Studies, University of Sarajevo; UNSA; e-mail: ppuharic@fkn.unsa.ba.

dokazima mora otkloniti kroz izmjene i dopune postojećih zakonskih odredbi, kao i kroz donošenje podzakonskih akata kojima će se jasno utvrditi pravila i procedure imajući u vidu specifičnu prirodu ovih dokaza i postojeće nedoumice i sporna pitanja u pogledu njihove zakonitosti.

Ključne riječi
digitalni dokazi, pretresanje digitalnih uređaja, vještačenje digitalnih uređaja

Abstract
Police agencies in Bosnia and Herzegovina (B&H) apply different practices in handling digital evidence depending on the position of holders of judicial functions, and especially prosecutors. Thus, the goals of this paper are to identify their methods and to examine relationship between the established patterns and role of prosecutors from the perspective of professionals (experts) from the relevant agencies. Related data were gathered indirectly through methods of content analysis, as well questionnaires and semi-structured interview with professionals of police agencies. All basic methods were used in the analysis of the collected data. The dogmatic-legal method was used in the analysis of the legal framework. A key limitation of this research is that the responses of the interviewed experts reflect their personal perceptions and experiences in regard to the handling of digital evidence and therefore no general conclusions can be made about whole area. Furthermore, it was not possible to objectively confirm all the circumstances and details of the handling of the digital evidence described by the respondents. Based on the data collected, the authors identified patterns in the treatment of digital evidence, as well as their key shortcomings, which may result in the illegality of the evidence. This paper represents modest contribution to the scientific and expert discussion on the subject of elimination of deficiencies and harmonization of the researched area. The general conclusion presented in paper is that the inconsistency of the practices of domestic police agencies in dealing with digital evidence must be eliminated through amendments to existing legal provisions, as well as by enacting by-laws that will clearly establish rules and procedures while taking into account the specific nature of this evidence and the existing concerns and issues in regard to their legality.

Key words
digital evidence, search of digital devices, forensic analysis of digital evidence

Uvod

Digitalni dokazi predstavljaju novi koncept dokaza, koji je postao sveprisutan u krivičnim postupcima, jer ne postoji oblast kriminaliteta bez digitalne dimenzije (Casey, 2011:3), međutim njegove specifičnosti nisu u fokusu rasprava u naučnim i stručnim krugovima u Bosni i Hercegovini (u daljnjem tekstu: BiH) unatoč tome što postoje nepoznanice terminološke i procesne prirode, koje su kreirale prostor za razvoj različitih pristupa u postupanju sa ovom vrstom dokaza. Provedena istraživanja ukazuju na to da su uspostavljene različite prakse koje se primjenjuju od strane policijskih tijela na različitim nivoima

državne organizacije.[226] Divergentni pristupi su uglavnom zasnovani na nejednakim stajalištima nosilaca pravosudnih funkcija o ovoj vrsti dokaza i to naročito tužilaca, imajući u vidu da im je u pravnom sistemu BiH nadležnost za sprovođenje istražnog postupka u cijelosti povjerena. Tužilac rukovodi, sprovodi i nadzire istragu (vidjeti više: Simović, 2014; Lakić, 2014). To praktično znači njegov aktivan i kontinuiran angažman u planiranju i provođenju aktivnosti ovlaštenih službenih lica, odnosno, odabiru istražnih radnji kojima se prikupljaju digitalni dokazi, ali i nadzor nad njihovom efikasnosti i zakonitosti.[227]

Pored tužioca, značajnu ulogu u postupanju sa digitalnim dokazima imaju i tzv. stručna lica. Naime, dokazna radnja pretresanje kompjuterskih sistema, uređaja za pohranjivanje kompjuterskih i elektronskih podataka, mobilnih telefona i drugih sličnih uređaja prema krivično procesnim odredbama se može poduzeti samo uz pomoć ovih lica.[228] Pojam „stručno lice“ nije definiran krivičnim procesnim zakonima, iako se koristi u nizu odredbi sadržanih u članovima: 34 (1)i (3), 51 (3), 86 (4)i (6), 94 (1), 185 (2), 187 (1), 355 (3), 356 (2), 373 (2) ZKP BiH.[229], Iz sadržaja navedenih odredbi, unatoč različitim kontekstima u kojima se koristi odredbi se može zaključiti da pojam stručno lice označava pojedinca koji raspolaže sa određenim ekspertnim znanjem koje je neophodno za uspješno obavljanje određene radnje dokazivanja. Na sličan način i Sijerčić – Čolić određuje stručno lice kao lice određene struke koju organ krivičnog postupka poziva radi razjašnjenja pojedinih tehničkih ili drugih stručnih pitanja koja se postavljaju u vezi sa pribavljenim dokazima, ili prilikom ispitivanja osumnjičenog, odnosno optuženog ili prilikom poduzimanja drugih istražnih radnji (2008:431). Upravo zbog uloge koja je dodijeljena procesnim zakonima stručnim licima u formalnom postupanju sa digitalnim dokazima, autori su se opredijelili da u okviru ovog rada pokušaju utvrditi načine postupanja sa digitalnim dokazima u praksi i ispitati vezu između utvrđenih obrazaca postupanja i stajališta tužilaca iz perspektive stručnih lica.

---

[226] Za više informacija o organizaciji policije u BiH vidjeti: Sijerčić – Čolić i Radičić, 2015.
[227] Čl. 35. (2) (a) Zakonu o krivičnom postupku BiH ("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, 93/09, 72/13, 65/18) (dalje u tekstu: ZKP BiH).
[228] Čl. 51. (3) ZKP BiH. Ista odredba je sadržana u drugim procesnim zakonima: čl. 65. (3) Zakon o krivičnom postupku Federacije BiH (”Službene novine Federacije BiH”, br. 35/03, 37/03, 56/03, 78/04, 28/05, 55/06, 27/07, 53/07, 9/09, 12/10, 8/13, 59/14 (dalje u tekstu: ZKP FBiH); 115 (3) Zakon o krivičnom postupku Republike Srpske ("Službeni glasnik RS", 53/2012, 91/2017 i 66/2018) (dalje u tekstu: ZKP RS); 51 (3) Zakon o krivičnom postupku Brčko Distrikta BiH ("Službeni glasnik Brčko distrikta BiH", br. 34/2013 - prečišćen tekst i 27/2014) (dalje u tekstu: ZKP BD BiH).
[229] Čl. 44 (1) i (3), 65 (3), 100 (4) i (6), 108 (1), 199 (2), 201 (1), 376 (3), 372 (2), 394 (2) ZKP FBiH; čl. 42 (1), 96 (2), 98 (1), 115 (3), 151 (4) i (6), 159 (1) ZKP RS; čl. 34 (1)i (3), 51 (3), 86 (4)i (6), 94 (1), 185 (2), 187 (1), 355 (3), 356 (2), 373 (2) ZKP BD BiH.

Koncept digitalnog dokaza u pravnom sistemu BiH

Pojam „digitalni dokaz" nije definiran procesno-pravnim okvirom koji je na snazi u BiH, a u domaćoj stručnoj literaturi koja se bavi pitanjem pribavljanja, odnosno postupanja sa ovom vrstom dokaza prilikom definiranja se slijedi pristup razvijen u stranoj stručnoj literaturi, prema kojem se digitalni dokaz poistovjećuje sa informacijom koja se pohranjuje ili prenosi u binarnoj, digitalnoj formi, a koja ima određenu dokaznu vrijednost u sudskom postupku. Tako Novak *et al.* digitalni dokaz definiraju kao informaciju koja je pohranjena ili prenesena u binarnom obliku, u koju se može pouzdati pred sudom (2019:17), a Casey kao bilo koju dokaznu informaciju pohranjenu ili prenesenu u digitalnoj formi koja se može upotrijebiti u sudskom postupku (2004). Isti pristup slijedi i Naučna radna grupa o digitalnim dokazima[230] i definira digitalni dokaz kao informaciju dokazne vrijednosti koja je ili pohranjena ili prenesena u binarnoj formi (2016). Međunarodna organizacija o kompjuterskim dokazima[231] na sličan način određuje digitalni dokaz kao informaciju pohranjenu ili prenesenu u binarnoj formi na koju se može osloniti pred sudom. Slijedeći prethodno navedene pristupe, Kos *et al*. u publikaciji namijenjenoj za edukaciju bh. tužioca, sudija i ovlaštenih službenih lica u agencijama za sprovođenje zakona, definiraju digitalni dokaz kao svaku informaciju u digitalnim obliku koja ima dokaznu vrijednost i koja je uskladištena ili prenesena u takvom obliku, odnosno kao bilo koja informacija koja je generisana, obrađena, uskladištena ili prenesena u digitalnom obliku na koju se sud može osloniti kao mjerodavnu, tj. svaka binarna informacija, sastavljena od digitalnih 1 i 0, uskladištena ili prenesena u digitalnoj formi, kao i druge moguće kopije originalne digitalne informacije koje imaju dokaznu vrijednost i na koje se sud može osloniti u kontekstu forenzičke akvizicije, analize i prezentacije (2013:9).

Prethodno navedene definicije daju određene indikacije šta se smatra digitalnim dokazom i nedvosmisleno ukazuju da se digitalnim dokazom smatraju informacije u digitalnom obliku, a ne predmeti, odnosno uređaji na kojima su one pohranjene (kompjuter, mobilni telefoni itd.). Krivično procesno zakonodavstvo na snazi u BiH ne sadrži definiciju informacije,[232] već samo pojam kompjuterskog podatka koji se definira kao svako iskazivanje činjenica, informacija ili koncepata u obliku prikladnom za obradu u kompjuterskom sistemu, uključujući i program koji je u stanju prouzrokovati da kompjuterski sistem

[230] Vidjeti više na: https://www.swgde.org/. Pristupljeno: 10.12.2019.
[231] Vidjeti više na: http://www.oas.org/juridico/english/cyber_links_ioce.htm. Pristupljeno: 10.12.2019.
[232] Jedina definicija informacije koja je data u pravnom sistemu BiH sadržana je u zakonodavstvu o slobodi pristupa informacijama (Zakon o slobodi pristupa informacijama u Bosni Hercegovini ["Službeni glasnik BiH", broj 28/00, 45/06, 102/09, 62/11, 100/13]) u kojem je određena kao svaki materijal kojim se prenose činjenice, mišljenja, podaci ili bilo koji drugi sadržaj, uključujući svaku kopiju ili njen dio, bez obzira na oblik ili karakteristike, kao i na to kada je sačinjena i kako je klasificirana.[232] U istom kontekstu, informacija se definira kao svaki podatak u obliku dokumenta, zapisa, dosjea registra ili u bilo kojem drugom obliku neovisno o načina na koji je prikazana (napisani, nacrtani, štampani, snimljeni, magnetni, optički, elektronički ili neki drugi zapis) – čl. 1. (a).

izvrši određenu funkciju.[233] Nažalost, ovakvo suženo definiranje podatka, preuzeto iz Konvencije o kibernetičkom kriminalu,[234] u kojem se izjednačavaju pojmovi činjenica, informacija i koncepata nema veći praktični značaj, jer uzrokuje dodatne nejasnoće kako u definiranju pojma digitalnog dokaza, tako i u kontekstu dokazivanja činjenica u krivičnom postupku putem digitalnih dokaza. Potrebno je naznačiti da ne postoji općeprihvaćeni pojam informacije,[235] odnosno, jedinstveni pristup u njenom definisanju (Madden, 2000:344), već naprotiv, tokom posljednjih sedamdeset godina su razvijeni brojni, različiti koncepti informacije. Štaviše, gotovo svaka naučna disciplina danas koristi specifičan koncept informacije unutar vlastitog konteksta (Horić, 2007).

To je vidljivo i iz definicija sadržanih u rječnicima u kojima se informacija se definira kao činjenica o situaciji, licu, događaju itd.,[236] ali kao podatak koji je tačan, pravovremen, specifičan i organiziran s određenom svrhom te prezentiran u određenom kontekstu koji mu daje značenje i važnost.[237] S druge strane Naučna radna grupa o digitalnim dokazima definira podatak kao informaciju u analognom ili digitalnom obliku koja može biti prenesena ili obrađena (6:2016). Pojam informacija označava i bilo koje objavljivanje/saopćavanje ili predstavljanje znanja kao što su činjenice, podaci ili mišljenja u bilo kojem mediju ili obliku (tekstualnom, numeričkom, grafičkom, kartografskom, narativnom ili audio-vizuelnom) (Ross *et al.* 2016).

Imajući u vidu definicije digitalnih dokaza korištene u stručnoj literaturi, najprimjerenijim se čini obrazloženje da informacija predstavlja smislenu interpretaciju ili izražavanje podataka pa u tom smislu, informacija je skup podataka s pripisanim značenjem, pri čemu se podaci sastoje od skupa kvantitativnih parametara koji opisuju određenu činjenicu ili događaj.[238] Podatak se definira i kao činjenica koja je predočena u formaliziranom obliku (npr. kao broj, riječ ili slika).[239] Dakle, podaci su osnova za uobličavanje i nastanak informacije tako što se atributira određeni značaj primljenim podacima.

Dokazna vrijednost digitalnog podatka je determinirana u svakom konkretnom slučaju sa nizom faktora koji između ostalog obuhvaćaju: fiksiranje digitalnog podatka istražnim radnjama, potvrdu vjerodostojnosti digitalnog podatka, atribuciju značenja digitalnom

---

[233] Čl. 20. (1) (v) ZKP BiH.
[234] Budimpešta, 23.11.2001; ETS – No. 185. Stupila na snagu 01.07.2004. godine, stupila na snagu u odnosu na BiH 01.09.2006. godine; objava „Službeni glasnik BiH"– Međunarodni ugovori broj: 06/2006.
[235] Pojam informacija latinskog je porijekla (infomatio/informo), međutim obuhvata i pojam forma, prijevod grčkih pojmova typos, morphe i eidos/idea (vidjeti više: Horić, 2007).
[236] Cambridge Dictionary. Dostupno na: https://dictionary.cambridge.org/dictionary/english/information. Pristupljeno 12.12.2019.
[237] BusinessDictionary. Dostupno na: http://www.businessdictionary.com/definition/information.html. Pristupljeno 12.12.2019.
[238] Leksikografski zavod Mirislav Krleža, Hrvatska Enciklopedija. Dostupno na: http://www.enciklopedija.hr/natuknica.aspx?id=27405. Pristupljeno 12.12.2019.
[239] *Ibidem*.

podatku i komparaciju sa drugim raspoloživim dokazima. Međutim, u našem krivičnom postupku vrijednost dokaza se prvenstveno zasniva na njihovoj zakonitosti (SIjerčić-Čolić, 2008:342). Nezakoniti dokazi se svrstavaju u tri osnovne vrste: a) dokazi pribavljeni povredama ljudskih prava i sloboda propisanih Ustavom i međunarodnim ugovorima koje je BiH ratifikovala, b) dokazi koji su pribavljeni bitnim povredama odredbi zakona o krivičnom postupku, i c) dokazi koji su pribavljeni na zakonit način, ali se do njih došlo na temelju dokaza koji su pribavljeni na nezakonit način (doktrina „plodova otrovne voćke") (vidjeti više: Mešanović, 2018:62). Pravno nevaljani dokazi su zabranjeni u našem pravu neovisno od toga da li su pouzdani, istiniti ili autentični (vidjeti više: Sijerčić – Čolić *et al.* [2005:63-69]), što posebno dolazi do izražaja kod digitalnih dokaza, jer se pouzdanost digitalnih podataka temelji na njihovoj autentičnosti, koja je prvenstveno uvjetovana načinima njihovog pribavljanja, a o čemu će biti više riječi u drugim dijelovima rada.

Savremene tendencije u razvoju informatičke tehnologije su neizbježno inicirale niz promjena u krivično-procesnom pravnom okviru. Tako je naprimjer postalo evidentno da je neophodno zamijeniti pravnu terminologiju koja se uobičajeno koristi u procesnom pravu sa adekvatnijim, tehnološki preciznim terminima, koji jasno opisuju procedure u odnosu na digitalne podatke, ali i dati status predmeta digitalnom podatku (vidjeti više: Bouwer; 2014) da bi se izbjegle nedoumice u kontekstu poduzimanja dokaznih radnji. Krivično procesno zakonodavstvo BiH ne prepoznaje eksplicitno podatak (ni informaciju) kao predmet, odnosno, pokretnu stvar, iako se u određenim zakonskim odredbama na to upućuje. Naime, u članu 65. (6) ZKP BiH je navedeno da se odredbe kojima se propisuje mogućnost sankcionisanja lica koje odbiju predati predmete (koji se po krivičnom zakonu trebaju oduzeti ili koji mogu poslužiti kao dokaz u krivičnom postupku), odnose na podatke pohranjene u kompjuteru ili sličnim uređajima za automatsku obradu podataka.[240] Ovakav stav je podržan i u literaturi u kojoj se prikupljanje podataka pohranjenih u kompjuteru i sličnim uređajima tretira kao jedan od pojavnih oblika privremenog oduzimanja predmeta i imovine (vidjeti: Sijerčić- Čolić, 2008:365; Halilović, 2010:161). Također i u Pravilniku o načinu i uslovima čuvanja materijalnih dokaza[241] se neposredno u čl. 19. (6) uređuje postupanje sa „podacima koji imaju vrijednost materijalnih dokaza".[242] Specifičnosti podataka su vidljive i u odnosu na moguće načine njihovog oduzimanja u procesnopravnom smislu. Obrazloženje Konvencije o kibernetičkom kriminalu[243] izdvaja sljedeće načine oduzimanja digitalnih podataka: štampanje podataka, oduzimanje materijalnog medija na kojem su podaci pohranjeni, pravljenje forenzičke kopije, odnosno duplikata podataka i njena pohrana materijalnom mediju (Nieman, 2009). Slijedom prethodno navedenog, očito je da kopija u kontekstu digitalnih dokaza mora imati drugačiji tretman u

[240] Čl. 79 (6) ZKP FBiH, 126 (6) ZKP RS, 65 (6) ZKP BD BIH.
[241] „Službeni glasnik BiH", br. 18/11.
[242] Ista odredba je sadržana u i u Pravilniku o načinu i uslovima čuvanja materijalnih dokaza koji je usvojen na nivou FBiH („Službene novine FBiH" br. 53/15).
[243] Obrazloženje Konvencije o kibernetičkom kriminalu – ETS 185, str. 32. p.187. Dostupno na: https://rm.coe.int/16800cce5b. Pristupljeno: 20.11.2019.

procesnom zakonodavstvu i poistovjetiti se sa originalom. U članu 274. (2) ZKP BiH se propisuje da se vjerodostojnost dokaznog materijala (pismena, zapisa ili fotografije) se provjerava na osnovu originala. Samo izuzetno zakon dozvoljava upotrebu kao dokaza ovjerene kopija originala, kao i kopije koja je potvrđena kao neizmijenjena u odnosu na original.[244] Krivični procesni zakoni definiraju original kao spis ili snimak ili sličan ekvivalent kojim se ostvaruje isto dejstvo od strane lica koje ga piše, snima ili izdaje,[245] pri čemu se u slučaju podataka koji su pohranjeni u kompjuteru ili sličnom uređaju ta automatsku obradu podataka, originalnom smatra i svaki odštampani primjerak ili okom vidljiv pohranjeni podatak.[246] Iz prethodno navedenog se može zaključiti da je u kontekstu prikupljanja digitalnih dokaza izuzetak o upotrebi kopije postao pravilo, ali samo ukoliko je zadovoljen uslov utvrđenosti njene neizmijenjenosti u odnosu na original. Prikupljanje, odnosno, oduzimanje digitalnih podataka u praksi u BiH se obično shvata kao oduzimanje medija na kojem su pohranjeni, a izuzetno rijetko kao kreiranje forenzičke kopije i njena pohrana na materijalnom mediju.

Kao što je već prethodno naznačeno, u pravnom okviru na snazi u BiH nije propisana zakonska definicija digitalnog dokaza niti su propisani posebni zakonski kriteriji za prihvatljivost digitalnih dokaza. Također, nije određeno u kojoj formi se oni izvode u sudskom postupku. Stoga, da bi se pokušalo definirati šta se podrazumijeva pod digitalnim dokazom u bh. pravu mora se krenuti od osnovnih koncepata iz teorije krivičnog procesnog prava: utvrđivanja činjenica u krivičnom postupku, pojma dokaza i dokazivanja te njihove zakonitosti.

U krivičnom postupku se utvrđuju činjenice (njihovo postojanje ili nepostojanje) koje su od značaja za donošenje zakonite odluke i na tako utvrđene činjenice se pravilno primjenjuje krivično materijalno i procesno pravo (Sijerčić – Čolić, 2008:325, a prema Ilić, 2001:155). Utvrditi činjenicu označava formiranje zaključka o njenom postojanju koji bi trebao odgovarati zahtijevanoj mjeri (stepenu, nivou, standardu kvaliteta i kvantiteta) uvjerenosti, odnosno utvrđenosti, primjenom dopuštenih i u konkretnom slučaju dostupnih metoda utvrđivanja činjenica (Dika, 2015:2). Premda postoje različiti stavovi u teoriji krivičnog procesnog prava o načinima utvrđivanja činjenica u krivičnim postupku kao ključni se izdvajaju: utvrđivanje činjenica vlastitim opažanjem organa krivičnog postupka i dokazivanjem (vidjeti više: Sijerčić – Čolić, 2008:336-338; Halilović, 2010:56), primarni način utvrđivanja činjenica je dokazivanjem. Zakonodavac u procesnim zakonima u BiH ne određuje pojam dokaza. U literaturi se dokaz definira kao svaki činjenični sadržaj koji je u stanju, kod tijela koje donosi odluku, formirati uvjerenje o postojanju, odnosno, ne postojanju činjenice koja je predmetom dokazivanja (Halilović, 2019:32).

---

[244] Čl. 274 (3) ZKP BIH.
[245] Čl. 20 (1) (o) ZKP BiH, 21 (1) (p), ZKP FBiH, 20 (1) (nj) ZKP RS, 20 (1) (o) ZKP BD BiH.
[246] *Ibidem*.

Kao što je već prethodno navedeno, načelo zakonitosti predstavlja jedno od temeljnih načela, jer zakonitost u prikupljanju digitalnih dokaza ima ključan značaj za njihovu vrijednost u krivičnom postupku. Međutim, u procesnim zakonima se ne definira šta se podrazumijeva pod zakonitim dokazima, već se naprotiv fokusira na koncept nezakonitih dokaza (Radovanović i Begić, 2016:14). Sistem nezakonitih dokaza je u pravnom sistemu utemeljen na stajalištu o apsolutnom isključivanju nezakonitih dokaza iz sudskog spisa, neovisno o tome da li se radi o izvorno nezakonitom dokazu ili dokazu koji je nastao kao derivat nezakonitog dokaza (Mešanović, 2018:90). Nezakonito pribavljeni dokazi su dokazi pribavljeni povredama ljudskih prava i sloboda propisanih ustavom i međunarodnim ugovorima koje je BiH ratificirala i bitnim povredama procesnog zakona. Potrebno je naglasiti da svaka povreda odredbe procesnog zakona ne znači da je dokaz pribavljen povredom te odredbe nezakonit. Prema stajalištu Vrhovnog suda FBiH,[247] zaključak o nezakonitosti nekog dokaza se ne može zasnivati na činjenici da je prilikom njegovog pribavljanja ili izvođenja povrijeđena neka odredba procesnog zakona, već se mora razmatrati: cilj odredbe (koja je prekršena, odnosno, neprimijenjena), značaj propusta da se postupi u skladu sa odredbom za osnovna prava i slobode te značaj propusta u odnosu na načela krivičnog postupka (Radovanović i Begić, 2016:15). Kada su u pitanju digitalni dokazi, izuzetno je važno dosljedno slijediti zakonom predviđenu proceduru njihovog prikupljanja kako bi se radilo o zakonitim dokazima.

Imajući u vidu navedeno, digitalni dokaz se može jednostavno definisati kao podatak koji ima specifičnu, digitalnu formu i koji je pribavljen u skladu sa relevantnim zakonom (vidjeti: Halilović, 2019:44, a prema Pavišić, 2011:415). U literaturi su iznesena i stajališta da digitalni dokazi nisu posebna vrsta dokaza, već su savremena forma dokaza ispravom (Halilović, 2019:44), kao i dijametralni stavovi o neprihvatljivosti takvog pristupa uslijed njegove ograničenosti i neučinkovitosti s obzirom na njihovu prirodu (Pisarić, 2015:237).

Na kraju je potrebno napomenuti da određenje pojma digitalnog dokaza otežava učestalo izjednačavanje pojmova „digitalni dokaz“ i „elektronski dokaz“ u teoriji i praksi, iako nisu u pitanju sinonimi (Halilović, 2019; IPROCEEDS, 2018; Stamenković *et al*. 2017; Spasić i Stevanović, 2015; Protrka, 2011; itd.).

[247] Vrhovni sud FBiH, Rješenje br. 06 0 K 005470 14 Kž od 03.09. 2014. godine.

Postupanje sa digitalnim dokazima

Kriminalističko istraživanje se fokusira na ispitivanje stvarnih promjena (internih i eksternih) prouzrokovanih krivičnim djelom, a koje se mogu spoznati, odnosno utvrditi. U okviru istraživanja poduzimaju se radnje kojima se razjašnjavaju pitanja u vezi pojave krivičnog djela, počinitelja, žrtve i ostalih važnih okolnosti. Dakle, kriminalističko postupanje označava radnje koje se poduzimaju u okviru analize vjerovatnog krivičnog djela, kojom se rekonstruiše njegova stvarna objektivna i subjektivna struktura. U sklopu navedenog postupanja radnje koje se provode mogu biti formalnog i neformalnog karaktera. Kada govorimo o radnjama formalnog karaktera iste su usko vezane za sam istražni (formalni) postupak, odnosno katalog dokaznih (istražnih) radnji koje propisuje krivično procesno zakonodavstvo. U pitanju su procesne radnje kojima se pribavljaju dokazi, a radi utvrđivanja pravno relevantnih činjenica u vezi sa predmetom krivičnog postupka (Halilović, 2019:47). Dokazne radnje propisane krivičnim procesnim zakonodavstvom uključuju: pretresanje stana, ostalih prostorija i pokretnih stvari;[248] pretresanje lica,[249] privremeno oduzimanje predmeta i imovine;[250] naredba banci i drugom pravnom licu,[251] naredba operateru telekomunikacija,[252] ispitivanje osumnjičenog,[253] saslušanje svjedoka,[254] uviđaj i rekonstrukcija[255] i vještačenje.[256]

Pored standardnih radnji dokazivanja, krivično procesno zakonodavstvo izdvojeno propisuje set posebnih istražnih radnji koje se mogu odrediti protiv lica za koje postoje osnovi sumnje da je samo ili sa drugim licima učestvovalo ili učestvuje u izvršenju određenih krivičnih djela,[257] ako se na drugi način ne mogu pribaviti dokazi ili bi njihovo pribavljanje

[248] Čl. 51. ZKP BiH, 65. ZKP FBIH, 115. ZKP RS, 51. ZKP BD BiH.
[249] Čl. 52. ZKP BiH, 66. ZKP FBIH, 116. ZKP RS, 52 .ZKP BD BiH.
[250] Čl. 65. ZKP BiH, 79. ZKP FBiH, 129. ZKP RS, 65. ZKP BD BiH.
[251] Čl. 72. ZKP BiH, 86. ZKP FBiH, 136. ZKP RS, 72. ZKP BD BIH.
[252] Čl. 72a. ZKP BIH, 86a. ZKP FBiH, 137. ZKP RS, 72a. ZKP BD BIH.
[253] Čl. 77.-80. ZKP BiH, 91.-94. ZKP FBiH, 142.-145. ZKP RS, 77.-80. ZKP BD BiH.
[254] Čl. 81.-91. ZKP BiH, 95.-105. ZKP FBiH, 146-156. ZKP RS, 81.-91. ZKP BD BiH,
[255] Čl. 92.-94. ZKP BiH, 106.-107. ZKP FBiH, 157.-158. ZKP RS, 92.-94. ZKP BD BiH,
[256] Čl. 95. – 115. ZKP BiH, 109.-119. ZKP FBiH, 160.-170. ZKP RS, 95.-115. ZKP BD BiH.
[257] Član 117. ZKP BiH propisuje sljedeća krivična djela za koja se mogu odrediti posebne istražne radnje: a) protiv integriteta Bosne i Hercegovine, b) protiv čovječnosti i vrijednosti zaštićenih međunarodnim pravom, c) terorizma, d) izazivanje nacionalne, rasne i vjerske mržnje, razdora i netrpeljivosti; protivpravno lišenje slobode; neovlašćeno prisluškivanje i zvučno ili optičko snimanje; povreda slobode opredjeljenja birača; krivotvorenje novca; krivotvorenje hartija od vrijednosti; pranje novca; utaja poreza ili prevara; krijumčarenje; organizovanje grupe ljudi ili udruženja za krijumčarenje ili rasturanje neocarinjene robe; carinska prevara; primanje dara i drugih oblika koristi; davanje dara i drugih oblika koristi; primanje nagrade ili drugog oblika koristi za trgovinu uticajem; davanje nagrade ili drugog oblika koristi za trgovinu uticajem; zloupotreba položaja ili ovlašćenja; protivzakonito oslobođenje lica lišenog slobode; pomoć počiniocu poslije učinjenog krivičnog djela; pomoć licu optuženom od međunarodnog krivičnog suda; sprečavanje dokazivanja; otkrivanje identiteta zaštićenog svjedoka; ometanje pravde; udruživanje radi činjenja krivičnih djela; organizovani kriminal; e) druga krivična djela za koja se može izreći kazna zatvora od pet godina ili teža kazna.

bilo povezano sa nesrazmjernim teškoćama.[258] U pitanju su sljedeće istražne radnje: nadzor i tehničko snimanje telekomunikacija, pristup kompjuterskim sistemima i kompjutersko sravnjanjavanje podataka; nadzor i tehničko snimanje prostorija; tajno praćenje i tehničko snimanje lica, transportnih sredstava i predmeta koji stoje u vezi sa njima, korištenje prikrivenih istražitelja i korištenje informatora; simulirani i kontrolisani otkup predmeta i simulirano davanje potkupnine; nadzirani prijevoz i isporuka predmeta krivičnih djela.[259]

Kada je riječ o neformalnim, odnosno, operativnim radnjama i one su u širem smislu propisane istim zakonodavstvom,[260] ali prilikom njihove realizacije do izražaja dolaze određene kriminalističko-taktičke radnje policijskih organa koje su uslovljene sadržajem zakonskih odredbi, ali i teorijskim postavkama kriminalistike i inventivnošću samih policijskih službenika.

Zakonske odredbe (ali ne samo odredbe krivično-procesnih zakona) predstavljaju pravni okvir za djelovanje istražnih organa. Prilikom istraživanja krivičnih djela policijske agencije su prinuđene koristiti različite istražne strategije. Te strategije bi trebale biti, na određen način, prilagođene vrsti krivičnog djela koje se u konkretnom slučaju istražuje. Istražne strategije su u najbližoj vezi sa određenim stručnim procedurama koje se primjenjuju u istraživanju i rasvjetljavanju krivičnih djela, a koje ne moraju biti sastavni dio zakonskih odredbi. Stručne procedure mogu biti formalnog (pisane i službeno usvojene, prihvaćene i zavedene od strane konkretnog policijskog organa-agencije ili ministarstva u kojem je isto organizaciono pozicionirano i stoga sadržajno obavezujuće) i neformalnog karaktera (pisane, napisane od strane određene institucije-domaće ili međunarodne, ali neusvojene od strane konkretnog policijskog organa-agencije te stoga formalno neobavezujuće). Prva kategorija procedura može biti dijelom podzakonskih akata (pravilnici, uputstva, instrukcije i sl.). Kada govorimo o ovakvoj vrsti akata najčešće mislimo na tzv. standardne operativne procedure (SOP). Iste su najčešće vezane za određenu konkretnu vrstu kriminaliteta, odnosno njegovo istraživanje. Najčešće obuhvataju tzv. najbolje prakse do kojih je konkretan policijski organ (ili neki drugi organ iste vrste) došao kroz iskustvenu spoznaju. Također, u nekim slučajevima mogu uključivati i tzv. hodograme postupanja u konkretnoj vrsti istraživanja krivičnih djela. Stručne procedure neformalnog

[258] Glava IX (čl. 116. -122.) ZKP BiH, Glava XIX (čl. 226. – 232.) ZKP RS, Glava IX (čl. 130. – 136.) ZKP FBiH i Glava IX (čl. 116 – 122) ZKP BD BiH.
[259] čl. 116. ZKP BIH, 130. ZKP FBiH, 226. ZKP RS i 116. ZKP BD BiH.
[260] Prema ZKP ovlaštena službena lica mogu prikupljati potrebne izjave od lica; izvršiti potrebni pregled prijevoznih sredstava, putnika i prtljage; ograničiti kretanje na određenom prostoru za vrijeme potrebno da se obavi određena radnja; poduzeti potrebne mjere u vezi sa utvrđivanjem identiteta lica i predmeta; raspisati potragu za licem i stvarima za kojima se traga; u prisustvu odgovornog lica pretražiti određene objekte i prostorije državnih organa, javnih preduzeća i ustanova, obaviti uvid u određenu njihovu dokumentaciju, kao i poduzeti druge potrebne mjere i radnje.

karaktera se često objavljuju u formi priručnika, na BHS jezicima i engleskom jeziku, a napisane su i za oblast postupanja s digitalnim dokazima (vidjeti: Kos *et al*. 2013).

Postupanje sa digitalnim dokazima zahtijeva posebnu predostrožnost prilikom njihovog prikupljanja, čuvanja i transporta. Uobičajeni koraci prilikom rukovanja sa digitalnim dokazima su: prepoznavanje, identificiranje, oduzimanje i osiguranje digitalnih dokaza na licu mjesta; dokumentiranje čitavog mjesta i lokaciju pronađenih dokaza; prikupljanje, obilježavanje i osiguranje digitalnog dokaza; pakovanje i transportovanje digitalnih dokaza na siguran način (vidjeti: U.S. NIJ., 2008; ENISA, 2014; INTERPOL, 2019; itd.). To zahtijeva uspostavu posebnih protokola postupanja sa digitalnim dokazima koji su razvijeni na temelju znanja i vještina iz oblasti informatičke tehnologije, a skladu sa politikama postupanja policijskog tijela/agencije, ali prvenstveno u skladu sa zakonodavnim okvirom. Prethodno navedeno također implicira da policijska tijela/agencije za provedbu zakona moraju imati službenike koji posjeduju vještine, iskustvo i kvalifikacije za postupanje sa digitalnim dokazima.

Pribavljanje digitalnih dokaza u pravnom sistemu BiH

Pribavljanje digitalnih dokaza predstavlja posebno osjetljivo pitanje u pravnom kontekstu, imajući u vidu njihovu prirodu, ali i široki spektar ličnih i povjerljivih informacija koje se čuvaju na digitalnim uređajima (Nortjé i Myburgh, 2019:5). Prema procesnom zakonodavstvu BiH, radnje dokazivanja od značaja za pribavljanje digitalnih dokaza su: pretresanje stana, prostorija, lica i pokretnih stvari, privremeno oduzimanje predmeta, uviđaj i vještačenje. Bitno je napomenuti da iako se navedenim radnjama dokazivanja pribavljaju različite vrste dokaza (prve tri se koriste za pribavljanje materijalnih dokaza, dok se vještačenjem pribavljaju personalni dokazi), vještačenje ima značajnu ulogu u tumačenju materijalnih dokaza, odnosno predmeta i tragova kao nositelja dokaznih informacija (vidjeti više: Halilović, 2019:47-48). Digitalni uređaji se najčešće pribavljaju dokaznom radnjom privremenog oduzimanja predmeta, odnosno pokretnih stvari na kojima se nalaze digitalni podaci, koja se često provodi u okviru dokazne radnje pretresanje stana, ostalih prostorija i pokretnih stvari. Pretresanje pokretnih stvari u kontekstu zakonskih odredbi obuhvaća i pretresanje kompjuterskih sistema, uređaja za pohranjivanje kompjuterskih i elektronskih podataka, kao i mobilnih telefonskih aparata.[261] Druga dokazna radnja kojom se mogu pribaviti digitalni dokazi je vještačenje pokretnih stvari – uređaja ili medija koje sadrže digitalne podatke.

[261] Čl. 51. (2) ZKP BiH, 65. (2) ZKP FBIH, 115. (2) ZKP RS, 51. (2) ZKP BD BiH.

Pretresanje kompjuterskih sistema, uređaja za pohranjivanje kompjuterskih i elektronskih podataka, kao i mobilnih telefonskih aparata

Pretres predstavlja dokaznu radnju krivičnog postupka čija je svrha pronalazak počinitelja, saučesnika, tragova krivičnog djela ili predmeta važnih za krivični postupak (Halilović, 2019:48). Objektom pretresa mogu biti stan, ostale prostorije, lica i pokretne stvari (vidjeti više: Sijerčić – Čolić, 2008:349-350).

U kontekstu pribavljanja digitalnih dokaza, kao što je prethodno naznačeno poseban značaj ima pretres pokretnih stvari. Krivično procesno zakonodavstvo propisuje da pretresanje pokretnih stvari obuhvata i pretresanje kompjuterskih sistema, uređaja za pohranjivanje kompjuterskih i elektronskih podataka, kao i mobilnih telefonskih aparata.[262] Druga odredba od neposrednog značaja za digitalne dokaze propisuje da su lica koja se koriste ovim uređajima dužna omogućiti pristup, predati medij na kojem su pohranjeni podaci te pružiti potrebna obavještenja za upotrebu tih uređaja.[263] Naravno, bitno je napomenuti da lice od kojega se traži predaja ovakvih uređaja može odbiti njihovu predaju ako su ispunjene zakonske pretpostavke u odnosu na primjenu principa da niko nije dužan pružati dokaze protiv sebe (vidjeti više: Halilović, 2019:49). Međutim, ako nisu ispunjene pretpostavke, lice koje odbije njihovu predaju može se novčano kazniti, kao i kaznom zatvora.[264]

Pretresanje kompjutera i sličnih digitalnih uređaja nije u zakonskim odredbama uslovljeno prisustvom dva svjedoka,[265] ali je propisano da se može poduzeti samo uz pomoć stručnog lica.[266]

Svi oblici pretresa se mogu izvršiti isključivo na osnovu sudske naredbe, osim u izuzetnim slučajevima propisanim odredbama procesnih zakona, ali i tada se mora odmah obavijestiti sud o izvršenom pretresu bez sudske naredbe i razlozima koji podupiru takvo postupanje. Naredba za pretresanje se izdaje na zahtjev tužioca ili ovlaštenih službenih lica koja su dobila odobrenje od tužioca.[267] Zahtjev za izdavanje naredbe za pretresanje može da se podnese u pismenoj ili usmenoj formi. Kada se zahtjev podnosi u pismenoj formi, mora biti sastavljen, potpisan i ovjeren na način kako je to propisano odgovarajućim ZKP-om.[268] U samom zahtjevu za izdavanje naredbe za pretresanje obavezno se moraju

[262] Čl. 51. (1) ZKP BiH, 65. (1) ZKP FBIH, 115. (1) ZKP RS, 51. (1) ZKP BD BiH.
[263] *Ibidem*.
[264] Čl. 65. (5) ZKP BiH. Lice koje ih odbije predati, može se kazniti do 50.000 KM, a u slučaju daljnjeg odbijanja - može se zatvoriti. Zatvor traje do predaje predmeta ili do završetka krivičnog postupka, a najduže 90 dana. Na isti način postupit će se prema službenom ili odgovornom licu u državnom organu ili pravnom licu.
[265] Vidjeti od 51. – 64. ZKP BiH.
[266] Čl. 51. (2) ZKP BiH, 65. (2) ZKP FBIH, 115. (2) ZKP RS, 51. (2) ZKP BD BiH.
[267] Čl. 53. ZKP BiH, 67. ZKP FBiH, 117. ZKP RS, i 53. ZKP BD BiH.
[268] Čl. 55. ZKP BiH, 69. ZKP FBiH, 119. ZKP RS i 55. ZKP BD BIH.

navesti činjenice koje ukazuju na vjerovatnost da će se pronaći lica koja su izvršila krivično djelo, odnosno tragovi krivičnog djela i predmeti važni za postupak.[269] Usmeni zahtjev za izdavanje naredbe (saopštava se sudu telefonski, radio-vezom ili drugim sredstvom elektronske komunikacije) za pretresanje može se podnijeti kada postoji opasnost od odlaganja.[270] Ukoliko sudija za prethodni postupak utvrdi da je zahtjev za izdavanje naredbe za pretresanje opravdan, odobrit će zahtjev i izdati naredbu za pretresanje.[271] Ukoliko sudija za prethodni postupak odluči da izda naredbu za pretresanje na osnovu usmenog zahtjeva, podnositelj takvog zahtjeva mora sam sastaviti naredbu u skladu sa zakonom i pročitat je u cjelini sudiji za prethodni postupak.[272] Sadržaj naredbe za pretres je propisan zakonom.[273] Naredba za pretresanje se mora izvršiti najkasnije 15 dana od izdavanja naredbe nakon čega se, bez odlaganja mora vratiti sudu.[274]

Naredba za pretres digitalnih uređaja, u ovisnosti od okolnosti može biti zasebna ili u okviru naredbe za pretresanje stana, prostorija i lica (Radovanović i Begić, 2016:25). Iako postoje stajališta da se odredbe o pretresanju pokretnih stvari bez sudske naredbe odnose i na pretresanje pokretnih stvari (vidjeti: Sijerčić – Čolić, 2008:359-360), zakonodavac je ovu mogućnost propisao samo u odnosu na pretresanje stana, ostalih prostorija i lica.[275] Navedeno upućuje na zaključak da se pretresanje pokretnih stvari – digitalnih uređaja može izvršiti samo na osnovu naredbe.

Odredba koja se također potencijalno odnosi na digitalne dokaze sadržana je u članu 62. (3) ZKP BiH koji propisuje da će se predmeti upotrijebljeni kod pretresanja kompjutera i sličnih uređaja za automatsku obradu podataka vratiti njihovim korisnicima nakon pretresanja, ako nisu potrebni za daljnje vođenje krivičnog postupka, lični podaci pribavljeni pretresanjem mogu se koristiti samo u svrhe krivičnog postupka i izbrisat će se bez odlaganja, kada ta svrha prestane.[276] Podaci koji se prikupljaju pretresanjem predstavljaju potencijalne dokaze koji se mogu koristiti samo za potrebe krivičnog postupka i čim prestane potreba za njihovim korištenjem takvi podaci se moraju uništiti (vidjeti više: Radovanović i Begić, 2016:25).

Iako se pretresanje digitalnih uređaja kao radnja dokazivanja može poduzeti u bilo kojoj fazi krivičnog postupka, ono se najčešće poduzima u inicijalnoj fazi istrage. U teoriji procesnog krivičnog prava su izneseni stavovi o zakonskim uslovima za provođenje ove vrsta pretresa koji su oprečni stavovima praktičara. Tako, Sijerčić – Čolić smatra da kada su u

---

[269] Čl. 55 (1) tačka b) ZKP BiH, 69 (1) (b) ZKP FBiH, 119 (1) (b) ZKP RS i 55 (1) (b) ZKP BD BiH.
[270] Čl. 56 (1) ZKP BiH, 70 (1) ZKP FBiH, 120 (1) ZKP RS i 56 (1) ZKP BD BIH.
[271] Čl. 57 (1) ZKP BiH, 71 (1) ZKP FBiH, 121 (1) ZKP RS i 57 (1) ZKP BD BiH.
[272] Čl. 57 (2) ZKP BiH, 71 (2) ZKP FBiH, 121 (2) ZKP RS i 57 (2) ZKP BD BiH.
[273] Čl. 58. ZKP BiH, 72. ZKP FBiH, 122. KZ RS, 58. ZKP BD BiH.
[274] Čl. 59 (1) ZKP BiH, 73 (1) ZKP FBiH, 123 (1) ZKP RS i 59 (1) ZKP BD BiH.
[275] Čl. 64 (1)i (2) ZKP BiH, 78 (1)i (2) ZKP FBiH, 128 (1)i (2) ZKP RS, 64 (1)i (2) ZKP BD BiH.
[276] Ista odredba je sadržana u čl. 76 (3) ZKP FBiH, 126 (3) ZKP RS i 62 (3) ZKP BD BiH.

pitanju zakonski uslovi za pretresanje stana, drugih prostorija, digitalnih uređaja i drugih pokretnih stvari, nema nikakve razlike, niti se te razlike javljaju u odnosu na pitanje o čijoj se nepokretnoj ili pokretnoj stvari radi (2008:349), dok Radovanović i Begić smatraju da postoji razlika u uslovima vršenja pretresa pokretnih i nepokretnih stvari, jer u slučaju pretresanja pokretnih stvari, a stoga i digitalnih uređaja nije propisano prisustvo dva svjedoka i pretres se obavezno vrši u prisustvu stručnog lica (2016:24; isto: Barašin i Hukeljić, 2010). Imajući u vidu odredbe procesnog zakona, može zaključiti da su opći zakonski uslovi za poduzimanje pretresanja digitalnih uređaja da „ (…) ima dovoljno osnova za sumnju da se kod njih nalaze učinitelj, saučesnik, tragovi krivičnog djela ili predmeti važni za postupak."[277] I postojanje odgovarajuće naredbe suda kao pravnog osnova za poduzimanje pretresanja,[278] dok je posebni uslov prisustvo stručnog lica.[279] Bitno napomenuti i da u procesnim zakonima nije izričito propisana obaveza sačinjavanja zapisnika pretresanju o pokretnih stvari.

Općenito, pretresanje kao radnju dokazivanja karakteriše određenost i usmjerenost što je evidentno iz sadržaja zakonske odredbe kojom se uređuje sadržaj naredbe za pretresanje u kojoj mora biti sadržana: svrha pretresanja, opis lica koje treba pronaći ili opis stvari koje su predmet pretresanja, određivanje ili opis mjesta, prostorija ili lica koje se traže sa navođenjem adrese, vlasništva, imena ili sličnog za sigurno utvrđivanje identiteta.[280] Ovaj princip ciljanog pristupa mora biti primijenjen i kod pretresa digitalnih uređaja, kada se na digitalnim uređajima moraju ciljano tražiti samo određeni podaci koji sačinjavaju informacije o određenim dokumentima, komunikaciji sa određenim licima, u određenom periodu, određene fotografije, određeni video i/ili audio zapisi itd. Ukoliko se desi da se prilikom pretresanja digitalnog uređaja otkriju podaci koji se ne odnose na krivično djelo zbog kojeg je izdata naredba već upućuju na drugo krivično djelo, treba postupiti analogno odredbi člana 61. (2) ZKP BiH: privremeno oduzeti podatke i o tome obavijestiti tužioca.

Krivični procesni zakoni propisuju da nakon oduzimanja predmeta na osnovu naredbe za pretresanje, ovlašteno službeno lice mora, bez odlaganja, vratiti sudu naredbu i predati predmete i spisak oduzetih predmeta.[281] Sud će zadržati ove predmete pod svojim nadzorom do daljnje odluke[282] ili odrediti da predmeti ostanu pod nadzorom podnositelja zahtjeva za izdavanje naredbe ili pod nadzorom ovlaštenog izvršitelja naredbe.[283] Pravilnici o načinu i uslovima čuvanja materijalnih dokaza (BiH i FBiH) u članu 19. uređuju postupanje sa zaprimljenim „kompjuterima i uređajima za automatsku obradu

[277] Čl. 51 (2) ZKP BiH, 65 (1) ZKP FBIH, 115 (1) ZKP RS, 51 (1) ZKP BD BiH.
[278] Vidjeti čl. 53.-60. ZKP BiH.
[279] Čl. 51 (3) ZKP BiH, 65 (3) ZKP FBIH, 115 (3) ZKP RS, 51 (3) ZKP BD BiH.
[280] Čl. 58 ZKP BiH, 72. ZKP FBiH, 122. KZ RS i 58. ZKP BD BiH.
[281] Čl. 63 (3) ZKP BiH, 77 (3) ZKP FBiH, 127 (3) ZKP RS i 63 (3) ZKP BD BiH.
[282] Čl. 127 (4) ZKP RS.
[283] Čl. 63 (4) ZKP BiH, 77 (4) ZKP FBiH, 63 (4) ZKP BD BiH.

podataka". Navedeni uređaji se moraju posebno označiti te ako su poznati zabilježiti ime proizvođača, model, serijski broj, operativni sistem, provajder Internet usluga i lozinku, a ako je kompjuter dio mreže, dokumente tipa softvera i lokaciju i broj servera, a sve se čuva uz naznaku "osjetljiva elektronska oprema - držati dalje od izvora magnetnog zračenja".[284] Nadalje, moraju biti zaštićeni od statičkog elektriciteta, toplote i magnetnog polja.[285] U navedenoj odredbi je posebno naznačena zabrana upotrebe kompjutera koji je dokazni materijal za vrijeme njegovog čuvanja u prostoriji suda da bi se vidjeli podaci koji su u njemu pohranjeni.[286] Poseban tretman imaju digitalni podaci kao dokazi u kontekstu ovih pravilnika nalaže se da „stručnjak za kompjutere mora što je moguće prije uraditi 'Bit Stream Image Up' da bi se kopirali i sačuvali podaci",[287] odnosno eliminirali rizici kontaminacije originalnih dokaza (vidjeti više o samom postupku u: Nelson *et al.* 2009; EC – Council, 2016; itd.).

Privremeno oduzimanje predmeta i imovine

U pitanju je procesna radnja kojom se privremeno oduzimaju predmeti koji se prema krivičnom zakonodavstvu imaju oduzeti ili koji mogu poslužiti kao dokaz u krivičnom postupku, a koja se često poduzima u okviru radnje pretresanja stana, prostorija, pokretnih stvari i lica,[288] premda se radi o samostalnoj radnji dokazivanja. U suštini, privremenim oduzimanjem predmeta i imovine se prvenstveno pribavljaju dokazi kojima se utvrđuju činjenice u krivičnom postupku. Druge svrhe ove radnje su da se sprečava vršenje/ponavljanje krivičnih djela, omogućava efikasno odvijanje krivičnog postupka, onemogućava korištenje ili otuđenje određene imovine (Sijerčić – Čolić, 2008:363, a prema Sijerčič – Čolić *et al*., 2005:208-210). Predmeti se oduzimaju na osnovu pismene naredbe koju izdaje sud na prijedlog tužioca ili na prijedlog ovlaštenog službenog lica koje je dobilo odobrenje od tužioca.[289] Oduzimanje predmeta vrši ovlašteno službeno lice na osnovu izdate naredbe. Prilikom oduzimanja predmeta naznačit će se gdje su pronađeni i opisat će se njihove karakteristike, a po potrebi i na drugi način osigurati utvrđivanje njihove istovjetnosti.[290] Realizacija navedene odredbe se najjednostavnije ostvaruje (i evidentira) kroz kreiranje zapisnika. Za oduzete predmete mora se izdati potvrda. Privremeno oduzimanje predmeta se može izvršiti i bez sudske naredbe ako postoji opasnost od

[284] Čl. 19 (1) Pravilnik o načinu i uslovima čuvanja materijalnih dokaza BiH i čl. 19 (1) Pravilnika o načinu i uslovima čuvanja materijalnih dokaza FBiH.
[285] Čl. 19 (4) Pravilnika o načinu i uslovima čuvanja materijalnih dokaza BiH i čl. 19 (4) Pravilnik o načinu i uslovima čuvanja materijalnih dokaza FBiH.
[286] Čl. 19 (5) Pravilnika o načinu i uslovima čuvanja materijalnih dokaza BiH i čl. 19 (5) Pravilnik o načinu i uslovima čuvanja materijalnih dokaza FBiH.
[287] Čl. 19 (6) Pravilnika o načinu i uslovima čuvanja materijalnih dokaza BiH i čl. 19 (6) Pravilnik o načinu i uslovima čuvanja materijalnih dokaza FBiH.
[288] U tom slučaju naredba o pretresanju stana ili prostorija, kao i lica, obuhvata i naredbu o privremenom oduzimanju predmeta (Sijerčić – Čolić, 2008:363)
[289] Čl. 65 (2) ZKP BiH, 78 (2) ZKP FBiH, 128 (2) ZKP RS i 65 (2) ZKP BD BiH.
[290] Čl. 65 (8) ZKP BiH, 79 (8) ZKP FBiH, 129 (8) ZKP RS i 65 (8) ZKP BD BiH.

odlaganja.[291] Ukoliko se lice koje se pretresa izričito usprotivi oduzimanju predmeta, tužilac će u roku od 72 sata od izvršenog pretresanja podnijeti zahtjev sudiji za prethodni postupak za naknadno odobrenje oduzimanja predmeta.[292] Ukoliko sudija za prethodni postupak odbije zahtjev tu, oduzeti predmeti se ne mogu koristiti kao dokaz u krivičnom postupku. Privremeno oduzeti predmeti će se odmah vratiti licu od kojeg su oduzeti.[293] Neovisno o toga da li je do privremenog oduzimanja predmeta došlo na temelju sudske naredbe ili ne, uvijek se provođenje ove radnje treba evidentirati putem zapisnika i potvrde u kojima mora biti obavezno sadržana deskripcija predmeta koji se oduzima, podaci o lokaciji na kojoj su pronađeni i drugi podaci ako je to potrebno radi utvrđivanja njihove istovjetnosti. Privremeno oduzeti predmeti pohranjuju se u sudu ili sud na drugi način osigurava njihovo čuvanje.[294] Način prijema, skladištenje, čuvanje, predavanje, raspolaganje i druge radnje koje se odnose na postupanje sa materijalnim dokazima - predmetima koji sadrže digitalne podatke koji su prikupljeni u toku krivičnog postupka po naredbi suda se obavlja u skladu sa odgovarajućim podzakonskim aktom (npr. prethodno razmatranim pravilnicima o načinu i uslovima čuvanja materijalnih dokaza BiH i FBiH). Tako se kompjuteri i uređaji koji su sa njima povezani moraju se posebno označiti i zabilježiti ime proizvođača, model, serijski broj, operativni sistem, pružaoca Internet usluga i lozinka.[295] Ako je kompjuter dio mreže, dokument tipa softvera i lokaciju i broj servera, a sve se čuva uz naznaku „osjetljiva elektronska oprema – držati dalje od izvora magnetnog zračenja“.[296] Ako je predmet centralna procesorska jedinica, stavlja se u originalni spremnik ako je moguće, ili u namjensku kutiju, koja se prethodno iznutra obloži blokovima stiropora, potom se kutija zalijepi dokaz-trakom, a zatim se pričvrsti etiketa na prednju stranu providnom trakom i označi sa "lomljivo, osjetljiva elektronska oprema - držati dalje od magnetnog polja".[297] Kompjuteri i uređaji koji su sa njima povezani moraju biti zaštićeni od statičkog elektriciteta, toplote i magnetnog polja.[298] Ako se kompjuter smatra dokaznim materijalom, za vrijeme njegovog čuvanja u prostoriji suda, kompjuter se ne može koristiti da bi se vidjeli podaci koji su u njemu pohranjeni.[299] Kao što je već navedeno, ako podaci imaju vrijednost materijalnih dokaza, stručnjak za kompjutere mora

[291] Čl. 66 (1) ZKP BiH, 80 (1) ZKP FBiH, 130 (1) ZKP RS i 66 (1) ZKP BD BiH.
[292] *Ibidem*.
[293] Čl. 66 (2) ZKP BiH, 80 (1) ZKP FBiH, 130 (1) ZKP RS i 66 (1) ZKP BD BiH.
[294] Čl. 70. ZKP BiH.
[295] Čl. 19 (1) Pravilnika o načinu i uslovima čuvanja materijalnih dokaza BiH i čl. 19 (1) Pravilnika o načinu i uslovima čuvanja materijalnih dokaza FBiH.
[296] *Ibidem*.
[297] Čl. 19 (3) Pravilnika o načinu i uslovima čuvanja materijalnih dokaza BiH i čl. 19 (3) Pravilnika o načinu i uslovima čuvanja materijalnih dokaza FBiH.
[298] Čl. 19 (4) Pravilnika o načinu i uslovima čuvanja materijalnih dokaza BiH i čl. 19 (4) Pravilnika o načinu i uslovima čuvanja materijalnih dokaza FBiH.
[299] Čl. 19 (5) Pravilnika o načinu i uslovima čuvanja materijalnih dokaza BiH i čl. 19 (5) Pravilnika o načinu i uslovima čuvanja materijalnih dokaza FBiH.

čim prije kreirati forenzičku kopiju memorije.[300] Oduzimanje predmeta traje privremeno i oduzeti predmeti se vraćaju vlasniku, odnosno držatelju kada u toku postupka postane očigledno da njihovo zadržavanje nije u skladu sa relevantnim zakonskim odredbama, a ne postoje razlozi za njihovo oduzimanje.[301]

U kontekstu pravnog okvira kojima se uređuje privremeno oduzimanje predmeta i imovine, sadržane su i odredbe kojima se propisuje otvaranje i pregled privremeno oduzetih predmeta i dokumentacije.[302] U pitanju je radnja koju vrši tužilac, a koji je dužan o tome obavijestiti lice ili privredno društvo (preduzeće) od kojeg su predmeti oduzeti, sudiju za prethodni postupak i branioca.[303] Otvaranje i pregled predmeta prema pojedinim autorima predstavlja uviđaj (vidjeti: Sijerčić – Čolić *et al*. 2005:222), dok drugi smatraju da u pitanju postupak usmjeren na identifikaciju predmeta (vidjeti: Radovanović i Begić, 2016:15). Ovoj radnji mogu prisustvovati vještaci ili stručna lica, ako je njihovo prisustvo potrebno zbog davanja nalaza i mišljenja, odnosno zbog pružanja odgovarajuće stručne pomoći. U zapisnik o otvaranju i pregledanju privremeno oduzetih predmeta i dokumentacije moraju se navesti: lica koja su prisustvovala ovoj radnji, kao i ona koja su odsustvovala, uz naznaku o njihovoj obaviještenosti, opis stanja omota/pakovanja i pečata (vidjeti više: Sijerčić – Čolić et al. 2005:221-222). Nakon otvaranja, zaposleniku suda se dostavlja zapisnik, koji potom po naredbi nadležnog sudije pristupa označavanju, pakovanju i skladištenju dokaza.[304] Pri otvaranju i pregledu privremeno oduzetih predmeta mora se voditi računa da njihov sadržaj ne saznaju neovlaštena lica.[305]

Kao jedan od pojavnih oblika privremenog oduzimanja predmeta i imovine u literaturi se navodi i prikupljanje podataka pohranjenih u kompjuteru ili sličnim uređajima za automatsku obradu podataka (vidjeti: Sijerčić – Čolić, 2008:365). Međutim, u samoj zakonskoj odredbi ovo nije navedeno, u članu 65. (6) ZKP BiH u kojem se referira na podatke pohranjene u kompjuteru ili sličnim uređajima za automatsku obradu podataka je propisano da se odredbe člana 65. (5) ZKP BiH kojima se uređuje obaveza držaoca da preda predmete sudu, mogućnost kažnjavanja zatvorskom i novčanom kaznom te dužina trajanja zatvora, primjenjuju i na navedene podatke. Pored toga se u navedenoj odredbi naznačava da se prilikom pribavljanja podataka pohranjenih u kompjuteru ili sličnom uređaju za automatsku obradu podataka naročito mora voditi računa o propisima koji se odnose na čuvanje tajnosti određenih podataka. Dakle, jasno je da se suštinski ne radi odredbi koja omogućava pribavljanje podataka već o odredbama koje podupiru radnju

[300] Čl. 19 (6) Pravilnika o načinu i uslovima čuvanja materijalnih dokaza BiH i čl. 19 (6) Pravilnika o načinu i uslovima čuvanja materijalnih dokaza FBiH.
[301] Čl. 74. ZKP BiH, 88. ZKP FBiH, 139. ZKP RS i 74. ZKP BD BiH. Ista odredba sadržana i u čl. 32 pravilnika o načinu i uslovima čuvanja materijalnih dokaza.
[302] Čl. 71. ZKP BiH, 85. ZKP FBiH, 135. ZKP RS i 71. ZKP BD BiH.
[303] Čl. 71 (2) ZKP BiH, 85 (2) ZKP FBiH, 135 (2) ZKP RS i 71 (2) ZKP BD BiH.
[304] Čl. 9 (3) Pravilnika o načinu i uslovima čuvanja materijalnih dokaza BiH.
[305] Čl. 71 (3) ZKP BiH, 85 (3) ZKP FBiH, 135 (3) ZKP RS i 71 (3) ZKP BD BiH.

pretresanja ovih predmeta. Štaviše, čak i ako bi zauzeli stajalište da se radnja privremenog oduzimanja predmeta odnosi na oduzimanje podataka, pri čemu se pojmu podataka daje značenje predmeta, takva naredba se može jedino realizirati u kontekstu naredbe kojom se nalaže pretresanje takvih uređaja, jer se u protivnom dovodi u pitanje njegova zakonitost. Može se samo oduzimati predmet koji sadrži digitalne podatke.

Iako se u pravilu predmeti – uređaji, mediji koji sadrže digitalne podatke privremeno oduzimaju za potrebe krivičnog postupka, u skladu sa prethodno razmatranim pravnim okvirom, kada su u pitanju digitalni podaci u bh. praksi se u određenim okolnostima javlja potreba da se ne oduzimaju predmeti koji sadrže digitalne podatke (npr. serveri privrednih društava), već samo digitalni podaci (vidjeti: Kos *et al*. 2013:29). U tom kontekstu krivično procesno zakonodavstvo ne sadrži prepreku da se oduzmu podaci i bez oduzimanja fizičkog predmeta (kompjutera), naravno putem odgovarajuće radnje dokazivanja kako bi se osigurala zakonitost. Odluka o tome u svakom konkretnom slučaju ovisi o okolnostima slučaja, stanja na terenu i vrsti krivičnog djela (IPROCEEDS, 2018:9).

Kao što je već napomenuto, zakonodavac nije propisao rokove čuvanja dokaza - čuvaju se dokle god su ti dokazi potrebni za sprovođenje krivične istrage. Zakon propisuje da će se vratit će se vlasniku, odnosno držaocu, kada u toku postupka postane očigledno da njihovo zadržavanje nije u skladu sa odredbama krivičnog procesnog zakona, a ne postoje razlozi za njihovo oduzimanje koji su nadvedeni u odredbama krivičnog procesnog zakona.[306]

Vještačenje

Vještačenje kao dokazna radnja se određuje kada za utvrđivanje ili ocjenu neke važne činjenice treba pribaviti nalaz i mišljenje lica koje raspolaže potrebnim stručnim znanjem. Ako naučno, tehničko ili druga stručna znanja mogu pomoći sudu da ocijeni dokaze ili razjasni sporne činjenice, vještak kao posebna vrsta svjedoka može svjedočiti davanjem nalaza o činjenicama i mišljenja koja sadrže ocjenu o činjenicama.[307]

U pitanju je dokazna radnja u okviru koje se lice (vještak) koja ima posebno naučno, tehničko ili drugo stručno znanje pomaže sudu da ocijeni dokaze ili razjasni sporne činjenice tako što svjedoči davanjem nalaza o činjenicama i mišljenja koja sadrže ocjenu o činjenicama.[308]

---

[306] Čl. 74. ZKP BiH. Ova odredba je preuzeta u čl. 32. Pravilnika o načinu i uslovima čuvanja materijalnih dokaza BiH.
[307] Član 95. ZKP BiH, 109. ZKP FBiH, 160. ZKP RS, 95. ZKP BD BiH.
[308] *Ibidem*.

Vještačenje uređaja koji sadrže digitalne podatke ne predstavlja obavezno vještačenje u pravnom sistemu BiH, jer nije kao takvo nije posebno propisano zakonima o krivičnom postupku (pristup da se određene činjenice u postupku utvrđuju određenom vrstom vještačenja[309]). Štaviše, ova vrsta vještačenja uopće nije posebno regulisana.[310] Na vještačenje predmeta tj. uređaja koji sadrže digitalne podatke primjenjuju se opće zakonske odredbe kojima se uređuje vještačenje.

Vještačenje se određuje pismenom naredbom izdatom od strane tužioca ili suda.[311] Treba imati na umu da, zakon propisuje i da ovlašteno službeno lice može odrediti potrebna vještačenja,[312] izuzev pregleda, obdukcije i ekshumacije leša.[313] Međutim, pismenu naredbu za vještačenje izdaje tužilac ili sud. U naredbi će se navesti činjenice o kojima se vrši vještačenje.[314] Također, na glavnom pretresu vještaka mogu angažovati optuženi i njegov branilac.[315]

Pravilo je da se vještačenja, naročito složenija, povjeravaju stručnoj ustanovi ili državnom organu specijaliziranom za određene vrste vještačenja[316] (vidjeti više: Sijerčić – Čolić, 2008:434). U tom slučaju ta ustanova ili organ određuje jednog ili više stručnjaka koji će izvršiti vještačenje.[317]

Zakon propisuje određena ograničenja u odnosu na određivanje vještaka. Naime, kao vještak se ne može odrediti lice koje ne može biti saslušano kao svjedok (vidjeti član 82. ZKP BH)[318] ili lice koje je oslobođeno od dužnosti svjedočenja (vidjeti član 83. ZKP BiH),[319] kao ni lice prema kojem je krivično djelo učinjeno.[320] Nadalje, kao vještak se ne može odrediti ni lice u odnosu na koje postoji neki drugi razlog za izuzeće kao što je radnopravni odnos u istom organu, privrednom društvu (preduzeću) ili drugom pravnom licu ili kod samostalnog privrednika, sa osumnjičenim, odnosno, optuženim ili oštećeni ili radni odnos kod oštećenog ili osumnjičenog, odnosno optuženoga.[321] Konačno, za vještaka se ne može odrediti lice koje je saslušano kao svjedok.[322] Naravno, i u odnosu na lice koje je

---

[309] Npr. vidjeti: članove 103. i 107. ZKP BiH.
[310] Kao što je npr. vještačenje poslovnih knjiga, koje je posebno regulisano uslijed značaja koji ima, ali koje nije u zakonskim odredbama tretirano kao obavezno vještačenje.
[311] Čl. 96 (1) ZKP BiH, 110 (1) ZKP FBiH, 161 (1) ZKP RS i 96 (1) ZKP BD BiH.
[312] Naravno nakon obavještavanja tužioca.
[313] Čl. 221. ZKP BiH, 236. ZKP FBiH, 229. ZKP RS i 221. ZKP BD BiH.
[314] Čl. 96 (1) ZKP BiH, 110 (1) ZKP FBiH, 161 (1) ZKP RS, 96 (1) ZKP BD BiH.
[315] Čl. 269 (1) ZKP BiH, 284 (1) ZKP FBiH, 284 (1) ZKP RS i 269 (1) BD BiH.
[316] Čl. 96 (2) ZKP BiH, 110 (2) ZKP FBiH, 161 (2) ZKP RS i 96 (2) ZKP BD BiH.
[317] *Ibidem*.
[318] Čl. 98 (1) ZKP BiH, 112 (1) ZKP FBiH, 163 (1) ZKP RS i 98 (1) ZKP BD BiH.
[319] *Ibidem*.
[320] A u slučaju da je takvo lice određeno - na njegovom nalazu i mišljenju ne može se zasnivati sudska odluka.
[321] Čl. 98 (2) ZKP BiH, 112 (2) ZKP FBiH, 163 (2) ZKP RS i 98 (2) ZKP BD BiH.
[322] Čl. 98 (3) ZKP BiH, 112 (3) ZKP FBiH, 163 (3) ZKP RS i 98 (3) ZKP BD BiH.

određeno od strane stručne ustanove ili organa kao osoba koja izvršava vještačenje primjenjuju se odredbe koje određuju ko se ne može odrediti kao vještak, odnosno odredbe o izuzeću od vještačenja.[323]

Temeljne dužnosti vještaka su dostavljanje svog izvještaja (tužiocu ili sudu koji ga je odredio), koji sadrži: dokaze koje je pregledao, obavljene testove, nalaz i mišljenje do kojeg je došao i sve druge relevantne podatke koje vještak smatra potrebnim za pravednu i objektivnu analizu.[324] Vještak ima obavezu da detaljno obrazloži kako je došao do određenog mišljenja.[325] S druge strane, vještaku je zakonodavac dodijelio i niz prava koja su definirana kao dužnosti organa koji je naredio vještačenje: upoznavanje vještaka o zakonskim odredbama o vještačenju, dužnost predočavanja predmeta vještačenja vještaku, dužnost da mu se omogući uvid u krivične spise, dužnost da mu se predoče dokazi sa kojima se raspolaže te dužnost da mu se pruže odgovarajući uslovi za provođenje vještačenja (vidjeti više: Sijerčić – Čolić *et al*., 2005:290).

Vještak može predložiti da se izvedu dokazi ili pribave predmeti i podaci koji su od važnosti za davanje njegovog nalaza i mišljenja. Ako prisustvuje uviđaju, rekonstrukciji događaja ili drugoj istražnoj radnji, vještak može predložiti da se razjasne pojedine okolnosti ili da se licu koje se saslušava postave pojedina pitanja.[326]

U odnosu na postupak vještačenja, zakonodavac je propisao da vještačenjem rukovodi organ koji je naredio vještačenje.[327] Prije početka vještačenja pozvat će se vještak da predmet vještačenja pažljivo razmotri, da tačno navede sve što zapazi i utvrdi, kao i da svoje mišljenje iznese nepristrasno i u skladu s pravilima nauke i vještine.[328] Posebno će se upozoriti da je lažno vještačenje krivično djelo. Prilikom davanja nalaza i mišljenja o predmetu koji se pregleda, vještak će se oslanjati na dokaze na koje su mu ukazale ovlaštena službena lica, tužilac ili sud.[329] Vještak može svjedočiti samo o činjenicama koje proizlaze iz njegovog neposrednog saznanja, osim ako se prilikom pripreme svog nalaza i mišljenja nije koristio informacijama na koje bi se opravdano oslanjali ostali stručnjaci iste struke.[330] U pravilu, vještak pregleda predmete vještačenja na mjestu gdje se oni nalaze, osim ako su za vještačenje potrebna dugotrajna ispitivanja ili ako se ispitivanja vrše u ustanovi, odnosno organu ili ako to zahtijevaju razlozi morala.[331] Vještak dostavlja

---

[323] Čl. 102 (1) ZKP BiH, 116 (1) ZKP FBiH, 167 (1) ZKP RS i 102 (1) ZKP BD BiH.
[324] Čl. 97. ZKP BiH, 111. ZKP FBiH, 162. ZKP RS i 97. ZKP BD BiH.
[325] *Ibidem*.
[326] Čl. 99 (3) ZKP BiH, 113 (3) ZKP FBiH, 163 (3) ZKP RS i 99 (3) ZKP BD BiH.
[327] Čl. 99 (1) ZKP BiH, 113 (1) ZKP FBiH, 163 (1) ZKP RS i 99 (1) ZKP BD BiH.
[328] *Ibidem*.
[329] Čl. 99 (2) ZKP BiH, 99 (2) ZKP BiH, 113 (2) ZKP FBiH, 163 (2) ZKP RS i 99 (2) ZKP BD BiH.
[330] *Ibidem*.
[331] Čl. 100 (1) ZKP BiH, 114 (1) ZKP FBiH, 165 (1) ZKP RS i 100 (1) ZKP BD BiH.

nalaz i mišljenje, kao i radni materijal, skice i zabilješke organu koji ga je odredio.[332] Zakon nije precizirao rokove za obavljanje vještačenja, s tim da organ koji je odredio vještačenje može u naredbi odrediti rok za dostavljanje rezultata vještačenja. U svakom slučaju, primjenjuje se opći uslov da krivični postupak mora da bude okončan u razumnom roku.[333]

Uviđaj

Još jedna dokazna radnja kojom se može doći do predmeta – uređaja koji sadrže digitalne podatke je uviđaj.[334] Prema krivično-procesnim odredbama, uviđaj se poduzima kada je za utvrđivanje neke važne činjenice u postupku potrebno opažanje.[335] Zakonodavac propisuje da se radi o opažanju neposredne prirode, što podrazumijeva upotrebu čula (vida, sluha, njuha, okusa i opipa), međutim, kroz teoriju je razvijeno stajalište da se prihvata da je dopušteno i posredno opažanje putem upotrebe instrumenata kriminalističke tehnike kao svojevrsnih „produžetaka čula“ (vidjeti: Žarković *et al*., 2012:42). Zakonodavac nije propisao formalno-pravni osnov za obavljanje uviđaja kao što je zahtjev, naredba ili rješenje o uviđaju, već je dovoljno postojanje materijalno-pravnog uslova da je za utvrđivanje neke važne činjenice u postupku potrebno neposredno opažanje[336] (vidjeti više: Sijerčić – Čolić, *et al*. 2005:273-274). Zbog njegove složenosti, uviđaj se vrši uz pomoć stručnih lica kriminalističko-tehničke ili druge struke u pronalaženju, osiguranju ili opisivanju tragova, a koja će izvršiti potrebna mjerenja i snimanja, sačiniti skicu i fotodokumentaciju ili prikupiti i druge podatke.[337] Na uviđaj se može pozvati i vještak ukoliko bi njegova prisutnost bila od koristi za davanje nalaza i mišljenja.[338] O provedenom uviđaju se mora sastaviti zapisnik koji obavezno sadržava podatke koji su važni s obzirom na prirodu takve radnje ili za utvrđivanje istovjetnosti pojedinih predmeta (opis, mjere i veličine predmeta ili tragova, stavljanje oznaka na predmetima i dr.), a ako su napravljene skice, crteži, planovi, fotografije, filmski snimci i slično, to će se navesti u zapisniku i priključiti uz zapisnik.[339] Procesna valjanost zapisnika odnosno njegova upotreba kao dokaza u krivičnom postupku ovisi o ispunjenosti prethodno navedenih zakonskih uslova.

---

[332] Čl. 101. ZKP BiH, 115. ZKP FBiH, 166. ZKP RS i 101. ZKP BD BiH.
[333] Vidjeti: član II/3.e) Ustav BiH člana 6. stav 1. Evropske konvencije. Razumnost dužine trajanja postupka se ocjenjuje u odnosu na okolnosti svakog pojedinog predmeta, pri čemu se moraju imati u vidu kriteriji uspostavljeni sudskom praksom Evropskog suda za ljudska prava, a naročito složenost predmeta, ponašanje strana u postupku i nadležnog suda ili drugih javnih vlasti te značaj koji konkretna pravna stvar ima za apelanta (vidjeti: *Mikulić protiv Hrvatske*, br. 53176/99 od 4.11.2002. godine; *Boddaert protiv Belgije*, br. 12919/87 od 22.10. 1992. godine; itd.). Vidjeti i: Ustavni sud BiH, Odluka o dopustivosti i meritumu, AP 3914/13 od 17. marta 2015. godine ("Službeni glasnik BiH", br, 29/15).
[334] Čl. 92.–94. ZKP BiH, 106.–108. ZKP FBiH, 157.–159. ZKP RS i 92.–94. ZKP BD BiH.
[335] Čl. 92. ZKP BiH, 106. ZKP FBiH, 157. ZKP RS i 92. ZKP BD BiH.
[336] *Ibidem*.
[337] Čl. 94 (1) ZKP BiH, 108 (1) ZKP FBiH, 159 (1) ZKP RS i 94 (1) ZKP BD BiH.
[338] Čl. 94 (2) ZKP BiH, 108 (2) ZKP FBiH, 159 (2) ZKP RS i 94 (2) ZKP BD BiH.
[339] Čl. 152 (3) ZKP BiH, 166 (3) ZKP FBiH, 63 (3) ZKP RS i 152 (2) ZKP BD BiH.

Iako se u bh. praksi i teoriji uviđaj ne analizira kao dokazna radnja kojom se prikupljaju digitalni dokazi, autori iz regije (Srbije i Crne Gore) razmatraju procesne mogućnosti provođenja uviđaja pokretnih stvari poput kompjutera, mobitela i drugih sličnih uređaja koji sadrže digitalne podatke, s ciljem pribavljanja digitalnih dokaza, kreirajući na taj način svojevrsno odstupanje u odnosu na konvencionalni koncept uviđaja. Polazeći od cilja uviđaja (utvrđivanje činjenica važnih za krivični postupak) i metodologije njegovog provođenja, kao i stajališta da predmet uviđaja mogu biti pokretne i nepokretne stvari (vidjeti više: Žarković *et al*. 2012:44-45), razmatra se provođenje uviđaja uređaja koje sadrže digitalne podatke. Tako prema Ivanović tzv. digitalni uviđaj kompjutera ne bi bio ništa drugo do uviđaj pokretnih stvari koji bi provodilo stručno lice čije radnje u ovom kontekstu predstavljaju radnje koje služe sprečavanju nastanka nepovratnih izmjena i oštećenja podataka na kompjuteru, odnosno, u mrežnom okruženju (2015:12). Međutim u praksi je takvo postupanje stručnog lica, imajući u vidu odredbe krivičnog procesnog zakona, izuzetno teško razgraničiti od radnje pretresanja, s obzirom na to da stručno lice, u cilju pružanja pomoći zbog koje je pozvano, može da izvrši pristup i pretraživanje memorije uređaja (Radonjić i Božović, n.o. 81-82). Ključna prednost „digitalnog" uviđaja koja se posebno ističe u odnosu na pretresanje uređaja jeste provođenje adekvatnog i potpunog zapisničkog i audio-vizuelnog evidentiranja svih mjera i radnji na mjestu i okruženju uz poseban naglasak na evidentiranje zatečenog stanja kompjutera i drugog uređaja, a što može biti od značaja za njegovo kasnije pretresanje, odnosno vještačenje (Radonjić i Božović n.o.:82; Ivanović, 2015:14). Mogućnost povrede prava pojedinaca, koja se opravdano ističe kao nedostatak postupanja na ovaj način (posebno imajući u vidu prirodu ovih podataka, kao i činjenicu da za postupanje nije potrebna naredba ili zahtjev) (Pisarić, 2015:235), pojedini autori relativiziraju isticanjem argumenta da imperativ zaštite digitalnih dokaza nadilazi prerogativ zaštite privatnosti i ličnih i porodičnih prilika, odnosno, da interes rasvjetljavanja kriminalnog događaja i provođenja istrage nadilazi stubove zaštite, analogno slučaju bioloških uzoraka (Ivanović, 2015:15).

Imajući u prethodno izneseno, evidentno je da se provođenje uviđaja u odnosu na pretresanje zagovara zbog karakteristike detaljnog evidentiranja svih poduzetih radnji, kao i bilježenja stanja uređaja i njegovog okruženja, a što se očito još uvijek smatra atipičnim pristupom u provođenju pretresanja digitalnih uređaja unatoč protokolima postupanja razvijenim kroz preuzimanje dobre prakse. Opasnost prelaska granice uviđaja i prelaska u postupak pretresanja i nužnost osiguranja zakonitosti i vjerodostojnosti digitalnih dokaza je u konačnici rezultirala da se čak i u sistemima koji prepoznaju uviđaje digitalnih uređaja u praksi oni ipak podvrgavaju pretresanju i/ili vještačenju (vidjeti: Radonjić i Božović, n.o.:82).

Istraživanje i diskusija

Ciljevi istraživanja su bili da se utvrde obrasci postupanja sa digitalnim dokazima u praksi policijskih tijela u BiH (percepcija i razumijevanje pojma digitalnih dokaza, primijenjenih radnji dokazivanja i utvrdi postojanje specifičnih intraagencijskih procedura) i ukaže na manjkavosti koje mogu rezultirati sa nezakonitošću ovih dokaza.

U okviru istraživanja, podaci su prikupljani posredno i to putem analize sadržaja dostupnih dokumenata, relevantne literature i sudske prakse te putem anketiranja i intervjuisanja stručnih lica agencija u BiH koje u okviru svog djelovanja postupaju sa digitalnim dokazima. U analizi podataka su korištene sve osnovne metode. Od opće-naučnih metoda su korištene statistička i komparativna metoda. U analizi pravnog okvira je korištena dogmatsko-pravna metoda.

Istraživanje je obuhvatilo uzorak od pet stručnih lica koja postupaju sa digitalnim dokazima prilikom obavljanja zadataka i poslova svog radnog mjesta u agencijama i institucijama na državnom nivou i nivou FBiH. Ispitivanje stručnih lica je provedeno putem *online* anketnog upitnika koji je dostavljen većem broju stručnih lica. U obradu su uzeti odgovori onih ispitanika koji su ispunili dostavljeni anketni upitnik. Nakon provođenja anketiranja, s ciljem boljeg razumijevanja načina rada i postupanja sa digitalnim dokazima, 20. 09. 2019. godine je proveden polu-struktuisan intervju sa jednim stručnim licem iz policijske agencije, koje ima neposredno, višegodišnje radno iskustvo u postupanju sa digitalnim dokazima i upoznato je sa specifičnostima bh. pravnog okvira kada je u pitanju ova vrsta dokaza. Kao što je prethodno navedeno, pod pojmom stručnog lica se podrazumijeva pojedinac koji raspolaže sa određenim ekspertnim znanjem koje je neophodno za uspješno obavljanje određene radnje dokazivanja. U kontekstu digitalnih dokaza to su prvenstveno radnje pretresanja i vještačenja kompjuterskih sistema, uređaja za pohranjivanje kompjuterskih i elektronskih podataka, kao i mobilnih telefonskih aparata. U samoj strukturi uzorka 20% ispitanika obavlja preko dvije godine zadatke i poslove koji obuhvaćaju postupanje sa digitalnim dokazima, dok jednak broj ispitanika (40%) obavlja ove poslove i zadatke preko pet godina, odnosno preko deset godina.[340] U odnosu na nivo obrazovanja stručnih lica obuhvaćenih istraživanjem, svi ispitanici imaju visoku stručnu spremu[341] iz sljedećih oblasti obrazovanja: kriminalističke nauke (40%), informatičke nauke (20%), tehničke nauke iz oblasti računarstva i informatike (20%) te

[340] Odgovor ispitanika na pitanje br. 2.2. anketnog upitnika.
[341] Odgovor ispitanika na pitanje br. 2.3. anketnog e.

elektronika i automatika (20%).[342] Pored toga, većina ispitanika je prošla specijalističke obuke (60%).[343] Većina ispitanika nema status stalnog sudskog vještaka (80%).[344]

Ograničenja ovog istraživanja se prije svega ogledaju u tome da odgovori anketiranih stručnih lica odražavaju njihove lične percepcije i iskustva u odnosu na postupanje sa digitalnim dokazima te se stoga ne mogu izvući generalni zaključci o samoj oblasti kao cjelini. Imajući u vidu da je mali uzorak stručnih lica obuhvaćenih istraživanjem, rezultati trebaju biti interpretirani sa naročitim oprezom i ne mogu se percipirati kao iskustva svih stručnih lica u BiH koja postupaju sa digitalnim dokazima. Također, nije bilo moguće objektivno potvrditi sve okolnosti i detalje postupanja sa digitalnim dokazima koje su u svojim odgovorima istakli ispitanici.

Rezultati istraživanja su prije svega ispitani stavovi ispitanika – stručnih lica u odnosu na faktore koji utiču na postupanje sa digitalnim dokazima. Dobiveni rezultati pokazuju da svi ispitanici smatraju da znanje tužioca utiče na vrijednost digitalnih dokaza (100%) u krivičnom postupku.[345] Naime, kao što je u prethodnom dijelu rada navedeno, dokazna vrijednost digitalnih podataka je determinirana sa nizom faktora koji između ostalog obuhvaćaju: fiksiranje digitalnog podatka istražnim radnjama, potvrdu vjerodostojnosti digitalnog podatka, atribuciju značenja digitalnom podatku i komparaciju sa drugim raspoloživim dokazima. S obzirom na ulogu koju tužilac ima u istrazi (rukovodi, nadzire i provodi), njegovo odlučivanje ima presudan uticaj u odnosu na svaki od navedenih faktora. Prema mišljenju većine ispitanika (80%) tužioci nemaju zadovoljavajući nivo relevantnog znanja o digitalnim dokazima i postupanju sa njima.[346] Kao obrazloženje svojih odgovora ispitanici su iznijeli mišljenje da tužioci ne znaju šta je digitalni dokaz i kako se pravilno „dokumentuje“, kao i da se u većini slučajeva prikuplja „balast“ dokaza i zahtijeva vještačenje kompjutera i telefona koji nisu već dugo u upotrebi.[347] Posebno je istaknuto da nisu upoznati sa mogućnostima digitalnih dokaza.[348] Prema mišljenju ispitanika, utjecaj (ne)znanja tužilaca na vrijednost digitalnih dokaza se neposredno manifestuje prilikom definisanja naredbi za pretresanje i vještačenje, a u slučaju kada se radi o tehnički zahtjevnim predmetima cilj tužilaca postaje nagodba.[349] Jedan od ispitanika je naveo da u slučaju kada tužilac ne posjeduje znanje o postupanju sa digitalnim dokazima dolazi do otežanog provođenja krivične istrage.[350] U kontekstu prethodno navedenog, bitno je naznačiti da je polovina ispitanika odgovorila potvrdno na pitanje da li je nedostatak

[342] Odgovor ispitanika na pitanje br. 2.4. anketnog upitnika.
[343] Odgovor ispitanika na pitanje br. 2.7. anketnog upitnika
[344] Odgovor ispitanika na pitanje br. 2.11. anketnog upitnika.
[345] Odgovor ispitanika na pitanje br. 2.14. anketnog upitnika.
[346] Odgovor ispitanika na pitanje br. 2.11. anketnog upitnika.
[347] Odgovor ispitanika na pitanje br. 2.13. anketnog upitnika.
[348] *Ibidem*.
[349] Odgovor ispitanika na pitanje br. 2.15. anketnog upitnika.
[350] *Ibidem*.

specifičnih znanja i vještina u pogledu postupanja sa digitalnim dokazima na strani tužioca i/ili istražitelja bio razlog za neprovođenje/neadekvatno provođenje krivične istrage.[351] Znanje tužioca je naročito vidljivo u kontekstu odgovora na prigovore odbrane. Prigovori koje odbrana ističe u odnosu na digitalne dokaze u praksi su: relevantnost; zakonitost oduzimanja; zakonitost pretresa; vjerodostojnost; nepropisno rukovanje oduzetim podacima; dodavanje podataka itd. (IPROCEEDS, 2018:13). Jedan ispitanik je naveo u svom anketnom upitniku da odbrana u nekim slučajevima dovodi u pitanje stručnost vještaka, nivo opreme i poduzete procesne radnje, stoga ako tužilac nije sposoban da obrazloži zašto je traženo vještačenje i da dovede u vezu digitalni dokaz sa ostalim materijalnim dokazima sud može odbaciti provedeno vještačenje.[352]

Dokazna vrijednost digitalnog dokaza prvenstveno zavisi od njihove zakonitosti. Kao što je u prethodnom dijelu rada naznačeno, pojam zakonitog dokaza nije posebno tretiran krivičnim procesnim zakonodavstvom, stoga se mora identificirati u odnosu na regulisane koncepte nezakonitih dokaza, odnosno kao dokaz koji nije:

- pribavljen povredama ljudskih prava i sloboda propisanih Ustavom i međunarodnim ugovorima koje je BiH ratifikovala;
- pribavljeni bitnim povredama odredbi zakona o krivičnom postupku;
- dokaz pribavljen na temelju dokaza koji je pribavljen na nezakonit način (doktrina „plodova otrovne voćke“).

I u drugim provedenim istraživanjima, učesnici lanca krivičnog gonjenja su identificirali ključnu ulogu tužioca u osiguranju zakonitosti dokaza kroz uspostavu i održavanje nadzora nad lancem čuvanja dokaza (vidjeti: IPROCEEDS, 2018:12). Lanac čuvanja dokaza predstavlja logičan slijed radnji u pribavljanju dokaza u okviru kojeg je svaki korak (ili radnja) u sekvenci ključan na način da njegovo pogrešno izvođenje ili neizvođenje dovodi u pitanje prihvatljivost dokaza u krivičnom postupku tj. njegovu relevantnost i zakonitost. Lanac čuvanja dokaza se temelji na pravilnom i konzistentnom slijeđenju određene procedure i stoga osigurava kako kvalitet ovih dokaza, tako i njihovu prihvatljivost, koja je često osporavana u sudskoj praksi u BiH, jer počiva na konceptu neizmijenjenosti digitalnih podataka. U svakom pojedinačnom slučaju lanac čuvanja dokaza treba biti detaljno dokumentovan da bi se prikazala svaka faza poduzetih radnji u svojoj cjelovitosti.

U odnosu na zakonitost digitalnih dokaza, kao posebno osjetljiva se izdvajaju pitanja o njihovom neposrednom pribavljanju (pretresanjem kompjuterskih sistema, uređaja za pohranjivanje kompjuterskih i elektronskih podataka, mobilnih telefonskih aparata itd.), odnosno, pribavljanja dokaza na temelju kojih su kasnije dobiveni digitalni dokazi. Prema procesnom zakonodavstvu BiH, radnje dokazivanja od značaja za pribavljanje digitalnih

[351] Odgovor ispitanika na pitanje br. 2.16. anketnog upitnika.
[352] Odgovor ispitanika na pitanje br. 2.15. anketnog upitnika.

dokaza su: pretres stana, prostorija, lica i pokretnih stvari; privremeno oduzimanje predmeta;[353] uviđaj i vještačenje.[354] Međutim, kada je u pitanju pribavljanje ovih dokaza, do predmeta, odnosno uređaja na kojima se nalaze digitalni podaci najčešće se dolazi dokaznom radnjom privremenog oduzimanja predmeta, koja se često provodi u okviru dokazne radnje pretresanje stana, ostalih prostorija i pokretnih stvari. Pri tome treba imati na umu da se u tom slučaju radi o tzv. prvoj radnji pretresanja. Druga radnja pretresanja odnosi se na pretresanje samog oduzetog uređaja (kompjuterskog sistema, uređaja za pohranjivanje kompjuterskih i elektronskih podataka, kao i mobilnih telefonskih aparata) tj. pretresanje digitalnih podataka. Jedan od problema koji je istaknut od strane ispitanika u okviru našeg istraživanja je da neznanje tužilaca utiče na definisanje naredbi o pretresanju uređaja i vještačenju uređaja,[355] a što je potvrđeno i rezultatima drugih provedenih istraživanja u BiH koji ukazuju na problem nejasnih odredbi u odnosu na ovu vrstu dokaza (vidjeti: IPROCEEDS, 2018:14). U odnosu na vještačenje, osnovni problem sa kojim se suočavaju tužioci kod pisanja naredbe je postavljanje i formuliranje pitanja vještaku, jer ne znaju u kojim granicama i na koja pitanja vještaci mogu odgovoriti (Križanić i Šmer Bajt, 2016:32). U sudskim procesima u BiH se prihvatljivost digitalnih dokaza često interpretira u odnosu na zakonitost poduzete dokazne radnje pretresanja pokretnih stvari (IPROCEEDS, 2018:9). U prethodnom dijelu teksta su razmatrani zakonski uslovi za provođenje radnje pretresanja pokretnih stvari gdje je istaknuto da zakonodavac nije propisao obaveze prisustva dva svjedoka i sastavljanja zapisnika o obavljenom pretresu pokretne stvari. Ipak, da bi se izbjegle nedoumice u pogledu zakonitosti poduzete radnje, u krivičnim postupcima u BiH se ispunjavaju uobičajeni uslovi zakonitosti radnje pretresanja pa se u praksi i pretresanje pokretnih stvari na kojima se nalaze digitalni podaci obavlja u prisustvu dva svjedoka i o tome se sastavlja zapisnik.[356] Rezultati drugih istraživanja ukazuju da se ipak ne radi o ujednačenoj praksi, jer je u prezentiranim odgovorima istaknuto da samo pojedini tužioci insistiraju na prisustvu dva svjedoka (IPROCEEDS, 2018:17). Iako zakonodavac nije postavio navedene uslove za obavljanje pretresanja pokretne stvari, neophodno je detaljnije razmotriti značaj ispunjavanja ovih uslova u odnosu na pribavljanja dokaza digitalne prirode. Prvi uslov prisustvo dva svjedoka predstavlja jedno od ključnih pravila pretresanja, koje je izričito predviđeno kada je u pitanju pretresanje stana, drugih prostorija i lica,[357] međutim ne kada je u pitanju pretresanje pokretnih stvari što je izazvalo nedoumice u stručnim krugovima u pogledu prisustva svjedoka (vidjeti: Barašin i Hukeljić, 2010; IPROCEEDS, 2018; Radovanović i Begić, 2016), naročito imajući u vidu da se ne spominje pretresanje pokretnih stvari – dakle i digitalnih uređaja u kontekstu odredbe o pretresanju bez naredbe i svjedoka.[358] Prisustvo svjedoka treba da osigura dodatni nivo kontrole pravilnosti toka i postupka pretresanja i u tom kontekstu

[353] Odgovori ispitanika na pitanje br. 3.1. anketnog upitnika.
[354] *Ibidem*.
[355] Odgovor ispitanika na pitanje 2.15. anketnog upitnika.
[356] Odgovori ispitanika na pitanja 3.5. i 3.6. anketnog upitnika.
[357] Čl. 60 (4) ZKP BiH, 74 (4) ZKP FBiH, 124 (4) ZKP RS i čl. 60 (4) ZKP BD BiH.
[358] Čl. 64. ZKP BiH, 78. ZKP FBiH, 128. ZKP RS i 64 ZKP BD BiH.

istaknu prigovore u zapisniku koji potpisuju, ali i da se saslušaju kao svjedoci o izvršenom pretresanju, stoga se mora postaviti pitanje da li se ta uloga može realizirati kada je u pitanju pretresanje uređaja koji sadrže digitalne podatke? Nepremostiva prepreka njenoj realizaciji je činjenica da svjedoci moraju posjedovati stručno znanje iz relevantne oblasti na izuzetno visokom nivou (barem na nivou stručnog lica koje obavlja pretresanje uređaja) da mogli da prate postupak pretresanja takvih uređaja koje se obavlja uz pomoć stručnog lica,[359] a što se naravno ne može očekivati od svjedoka. Stoga se mora istaći, da iako ne postoje zakonske prepreke prisustvu svjedoka, njihovo prisustvo ne doprinosi pravilnosti i zakonitosti same radnje. Naime, mora se istaći logičnost u pristupu zakonodavca (iako je do sada tumačen u stručnoj literaturi kao „nenamjerni propust zakonodavca" [vidjeti Barašin i Hukeljić, 2010]) koji je nije propisao prisustvo svjedoka pretresanju kompjuterskih sistema, uređaja za pohranjivanje kompjuterskih i elektronskih podataka, kao i mobilnih telefonskih aparata i upozoriti na apsurdnost korištenja svjedoka prilikom pretresanja ovih uređaja, razvijenog u bh. praksi, jer svjedočenje lica bez specifičnog znanja ne može imati nikakav procesni niti praktični značaj. U odnosu na drugi zakonski uslov, sastavljanje zapisnika o pretresanju, u pitanju je postupak usmjeren na sačinjavanje isprave kojom se detaljno opisuje lokacija obavljanja pretresa, karakteristike uređaja i bilježi svaka radnja u odnosu na uređaj i postupak i rezultati pretresanja te kao takav doprinosi evidentiranju zakonitog postupanja i autentičnosti pribavljenih dokaza. Stoga, za razliku od prisustva svjedoka, sačinjavanje zapisnika u kojem se detaljno evidentiraju svi podaci koji su važni s obzirom na prirodu poduzete radnje, odnosno uređaja i njegovog okruženja, kao i pravljene skica i audio-vizuelnog evidentiranja koje se prilažu uz zapisnik (i njihovo navođenje u zapisniku) otklanja, odnosno umanjuje sumnje u pogledu autentičnosti i zakonitosti rezultata pretresanja digitalnog uređaja i stoga treba postati standardni dio postupka pretresanja.

U odnosu postupak izvršenja radnje pretresanja pokretne stvari, većina ispitanika (75%) obuhvaćenih istraživanjem je potvrdila da vlasnik predmeta na kojem su sadržani digitalni podaci prisustvuje radnji pretresanja (75%).[360] Rezultati drugih istraživanja također upućuju da u praksi optuženi i njegov zastupnik mogu prisustvovati pretresanju elektronskih podataka,[361] kao i pravljenju digitalne kopije podataka (IPROCEEDS, 2018).

U stranim naučnim i stručnim krugovima se vode rasprave u pogledu odgovora na pitanje šta znači pretresti i oduzeti digitalne podatke (vidjeti: Kerr, 2005a). Tumačenje pretresanja[362] kao „pristupa temeljenog na izloženosti" zasnovano je na shvaćanju da se radi o bilo kojoj radnji kojom se pristupa podacima na bilo koji način i primaju obavijest o

[359] Čl. 51 (3) ZKP BiH, 65. ZKP FBIH, 115. ZKP RS i 51 ZKP BD BiH.
[360] Odgovori ispitanika na pitanje 3.16. anketnog upitnika.
[361] Kao što je prethodno navedeno u ovom istraživanju (IPROCEEDS, 2018) pojmovi „elektronski dokaz" i „digitalni dokaz", kao i „elektronski podatak" i „digitalni podatak" se koriste naizmjenično kao sinonimi.
[362] Potrebno je napomenuti da u domaćoj literaturi se često koristi i pojam pretraživanje umjesto pretresanje jer se radi o pogrešnom prijevodu naziva radnje sa engleskog jezika „search".

informacijama ili promatraju informacije u ljudskom razumljivom formatu (Nortje i Myburgh, 2019:9). Poznato je da je izraz pretresanje u kontekstu digitalnih dokaza izuzetno širok, jer postoje različiti konteksti pretresanja. Pojedini autori smatraju da se radi o dvije, nužne i međuzavisne faze: traženju i identificiranju uređaja koji sadrži digitalne podatke (prvo pretresanje), nakon kojega se provodi pretresanje ovih uređaja radi traženja podataka relevantnih za konkretan slučaj (drugo pretresanje) (Kerr, 2005b: 94-95). Međutim, postoje i mišljenja da ovaj oblik pretresanja pokretnih stvari obuhvaća tri faze: tradicionalni postupak pretresanja u okviru kojeg se traže i pronalaze uređaji na licu mjesta; traženje i izdvajanje relevantnih podataka na tim uređajima; analizu ili interpretaciju relevantnih podataka u kontekstu šire istrage (vidjeti: Nortje i Myburgh, 2019; INTERPOL, 2019; U.S. NIJ. 2008).

S druge strane radnje pretresanja i oduzimanja u kontekstu digitalnih podataka predstavljaju aktivnosti koje je teško razgraničiti imajući u vidu tradicionalne koncepte ovih radnji razvijene u krivičnoj procesnoj teoriji, posebno u odnosu na kreiranje forenzičke kopije. Slijedom navedenog, postavljaju se pitanja: da li stvaranje forenzičkih kopija predstavlja pretresanje ili oduzimanje originalnih dokaza, odnosno da li pretraga forenzičke kopije predstavlja pretresanje? (vidjeti: Kerr, 2005a).

Iz sadržaja domaće stručne i naučne krivično - procesne literature je evidentno da autori ne razmatraju navedena pitanja. Oduzimanje digitalnih podataka se indirektno posmatra u svjetlu radnje oduzimanja predmeta, odnosno uređaja ili medija na kojem su pohranjeni podaci. Pretresanje digitalnih uređaja, odnosno, pretresanje kompjuterskih sistema, uređaja za pohranjivanje kompjuterskih i elektronskih podataka, kao i mobilnih telefonskih aparata nije preciznije određeno od strane zakonodavca. U stručnoj literaturi radnja pretresanja podrazumijeva da se na licu mjesta izuzmu informacije u obliku koji će biti prihvatljiv kao dokaz u daljem postupku, a koje bi bilo nemoguće naknadno dobiti, kao i prikupljanje informacija koje će biti od koristi prilikom vještačenja digitalnih dokaza (Kos *et al.* 2013:8-9). Konkretno, pretresanje uređaja obuhvata radnju oduzimanja podataka u okviru koje se pravi forenzička kopija (*Ibidem*, 2013:31). Važno je napomenuti da u stručnoj literaturi iz oblasti, analiza digitalnih podataka i izvještavanje nisu predviđeni kao faze radnje pretresanja uređaja. Prema autorima iz regije pod radnjom pretresanja se podrazumijeva pristupanje uređaju i podacima koji su na njemu pohranjeni (Radonjić i Božović, n.o.:69), odnosno pregled i analiza podataka sadržanih na uređaju (Pisarić, 235:2015), a stvaranje forenzičke kopije se percipira kao postupak koji se obavlja u okviru druge dokazne radnje - uviđaja uređaja, odnosno tzv. digitalnog uviđaja (Ivanović, 2015:15; Radonjić i Božović, n.o.:82).

Dakle, s obzirom da prikupljanje digitalnih podataka počiva na stvaranju forenzičke kopije podataka obuhvaćenih istražnim postupkom kako bi mogli biti predmetom daljnjih pretraživanja i analiza, u BiH je razvijena praksa, sugerirana sadržajem stručne publikacije o pretresanju uređaja koji su prepoznati u krivičnom - procesnom zakonodavstvu (kompjuterski sistemi, uređaja za pohranjivanje kompjuterskih i elektronskih podataka i mobilnih

telefonskih aparata) da je stvaranje kopije dio postupka izuzimanja predmeta, odnosno uređaja na kojem se podaci mogu nalaziti, a koji je jedna od faza „pretresa digitalnog dokaza" (vidjeti: Kos *et al*. 2013:25-26, 31). Kreiranje forenzičke kopije se često nalazi u srži pitanja autentičnosti digitalnog dokaza. U primjeru iz sudske prakse Republike Hrvatske[363] je podnesen zahtjev za izvanredno preispitivanje pravosnažne presude zbog toga što se temelji na nezakonitim dokazu – zapisniku o pretresu prijenosnog kompjutera i kutije u kojoj su bili spremljeni CD-ovi i DVD-ovi. U zahtjevu je istaknuto da prijenosni kompjuter nije bio samo predmetom pretrage već i istovremeno sredstvo za nezakonitu pretragu SD kartice, jer je sadržaj te kartice pregledavan upravo na predmetnom prijenosnom kompjuteru, a prije otvaranja datoteka nije napravljena tzv. sigurna kopija što je imalo za rezultat da se u okviru vještačenja nije moglo utvrditi da li su kritičnog dana otvarane datoteke, uključujući datoteke koje su predmetom inkriminacije. Kao rezultat, dio zapisnika o pretrazi SD kratice je u ovom slučaju izdvojen iz spisa predmeta, kao nezakonit dokaz.

Pitanje tretmana forenzičke kopije u odnosu na koncept originala je u određenoj mjeri razriješeno odredbama procesnog zakona prema kojima se pod pojmom "originala" podrazumijeva spis ili snimak ili sličan ekvivalent kojim se ostvaruje isto dejstvo od strane lica koje ga piše, snima ili izdaje, [364] a slučaju kada su podaci pohranjeni u kompjuteru ili sličnom uređaju za automatsku obradu podataka, original je i svaki odštampani primjerak ili okom vidljivi pohranjeni podatak.[365] S obzirom da forenzička kopija predstavlja vjerodostojan duplikat (dijela ili svih) podataka pohranjenih na izvornom uređaju, odnosno mediju, može se zaključiti da je forenzička kopija podataka izjednačena sa originalnim podatkom te je stoga pregledanje vjerodostojnog duplikata jednako pregledu izvornog medija za pohranjivanje podataka.

Prema odgovorima ispitanika obuhvaćenih našim istraživanjem, u kontekstu tzv. prvog pretresanja, radnje kojima se najčešće dolazi do predmeta koji sadrže digitalne podatke u bh. praksi su: radnja pretresanja stana, prostorija i lica, gdje se uređaji oduzimaju na osnovu naredbe za pretresanje (60%) i radnja privremenog oduzimanja predmeta (na osnovu naredbe o oduzimanju predmeta) (40%).[366] Izuzetno rijetko se u praksi podnosi zahtjev sudu za izdavanje naredbe za isključivo pretresanje kompjuterskog sistema, mobitela ili drugog uređaja, jer to pretpostavlja posjedovanje znanja o činjenicama da će se ove pokretne stvari naći na označenom ili opisanom mjestu ili kod određenog lica,[367] kao i poznavanje njihovih karakteristika.[368] Stoga je uobičajeno u praksi da se predmeti koji sadrže digitalne podatke (kompjuteri, mobiteli i drugi slični uređaji i mediji) pronalaze

[363] Presuda Vrhovnog suda Republike Hrvatske broj KR-165/11 od 19. septembra 2012. godine.
[364] Čl. 21 (1) (o) ZKP BiH.
[365] *Ibidem.*
[366] Odgovori ispitanika na pitanje 3.1. anketnog upitnika.
[367] Čl. 55 (1) ZKP BiH, 69 (1) ZKP FBiH, 119 (1) ZKP RS i 55 (1) ZKP BD BIH.
[368] Čl. 58 (1) (d) ZKP BiH, 72 (1) (4)ZKP FBiH, 122 (1) (d) KZ RS, 58 (1) (d) ZKP BD BiH.

prilikom pretresanja stana i drugih prostorija i potom privremeno oduzimaju o čemu se izdaje potvrda i unosi u zapisnik o pretresanju (vidjeti: Radovanović i Begić, 2016:25, Barašin i Hukeljić, 2010:441).

U praksi se u pravilu vrši privremeno oduzimanje predmeta na kojima se nalaze digitalni podaci, jer je potrebno sačuvati njihovu originalnost, ali i zbog toga što se obično naknadno vrše potrebne forenzičke analize (IPROCEEDS, 2018:9).[369] Izuzeci od pravila razvijeni u praksi odnose na situacije kada se oduzimaju samo digitalni podaci bez oduzimanja predmeta u kojem su pohranjeni ako bi oduzimanje ovih predmeta prouzrokovalo veću štetu od one prouzrokovane krivičnim djelom i to se u pravilu odnosi na servere privrednih društava čije poslovanje je vezano za informacioni sistem, ukoliko su ispunjene tehničke i druge pretpostavke (IPROCEEDS, 2018:9,10; Kos *et al*. 2013:29).

Naredna faza u postupanju sa oduzetim predmetima, prema odredbama krivično procesnog zakonodavstva, je otvaranje i pregled oduzetih predmeta od strane tužioca.[370] Kao što je već u prethodnim dijelovima teksta naznačeno, tužilac ima obavezu da obavijesti lice ili privredno društvo od kojeg su predmeti oduzeti, sudiju za prethodni postupak i branioca kako bi mogli da prisustvuju otvaranju privremeno oduzetih predmeta, koji će u pravilu biti raspakovani, pregledani i ponovo zapakovani. O svim ovim okolnostima i poduzetim radnjama mora se sačiniti zapisnik. Cilj ove odredbe je identifikacija privremeno oduzetih predmeta. Stoga se može opravdano postaviti pitanje da li je potrebno provoditi ovu odredbu u slučaju kada su na potvrdi o privremenom oduzimanju predmeta jasno navedeni svi elementi na osnovu kojih se može predmet identificirati, odnosno kako se može opravdati njeno provođenje u odnosu na predmet koji je već identificiran? (vidjeti više: Radovanović i Begić, 2016:32). U istraživanju, praksa „otvaranja predmeta" – kada se u prisustvu tužioca, osumnjičenog i njegovog branioca predmeti oduzeti u pretresu vade iz pakovanja je poznata 40% ispitanika.[371] Iz ugla ispitanika koji su u svom dosadašnjem radu susreli sa navedenom praksom njena ulogu u kontekstu postupanja sa digitalnim uređajima se svodi na provjeru brojnog stanja i serijskih brojeva. Prema njihovom mišljenju ova radnja se vrlo često poklapa sa radnjom pretresa,[372] stoga se može zaključiti da je opravdano stajalište Radovanović i Begić da otvaranje i pregled privremeno oduzetih predmeta se treba vršiti samo u slučaju kada popis tih predmeta nije moguć, odnosno kada prilikom privremenog oduzimanja nisu taksativno popisani i identificirani zbog njihove brojnosti (2016:33).

Nakon otvaranja i pregleda predmeta koji sadrže digitalne podatke, provode se različite prakse usmjerene na pribavljanje digitalnih dokaza. Na nivou države BiH se već dugo

[369] Navedeno stajalište je potvrđeno odgovorom stručnog lica sa kojim je obavljen intervju 20.09.2019. godine u prostorijama agencije.
[370] Čl. 71. ZKP BiH, 85. ZKP FBiH, 135. ZKP RS i 71. ZKP BD BiH.
[371] Odgovori ispitanika na pitanje br. 3.10. anketnog upitnika.
[372] Odgovor ispitanika na pitanje br. 3.11. anketnog upitnika.

primjenjuje praksa da nakon "otvaranja dokaza", tužilaštvo izdaje naredbu o vještačenju (vidjeti: IPROCEEDS, 2018). Provođenje vještačenja s ciljem pribavljanja digitalnih dokaza je u stručnoj literaturi osporavano kao inkompatibilno duhu odredbi o vještačenju sadržanih u zakonu o krivičnom postupku, premda ne i nezakonito. Naime, polazeći od toga da zakonodavac propisuje da se vještačenje određuje „ (…) kada je za utvrđivanje ili ocjenu neke važne činjenice treba pribaviti nalaz i mišljenje lica koja raspolažu potrebnim stručnim znanjima. Ako naučno, tehničko ili druga stručna znanja mogu pomoći Sudu da ocijeni dokaze ili da razjasni sporne činjenice, vještak kao posebna vrsta svjedoka može svjedočiti davanjem nalaza o činjenicama i mišljenja koje sadrži ocjenu o činjenicama.“,[373] Barašin i Hukeljić ističu da se vještačenje poduzima u onim slučajevima kada je potrebno određeno znanje da se ocijeni dokaz ili razjasni sporna činjenica, stoga očitanje sadržaja, odnosno podataka sa kompjuterskih sistema uređaja za pohranjivanje kompjuterskih ili elektronskih podataka i mobilnih telefonskih aparata ne predstavlja spornu činjenicu za čije je razjašnjenje potrebno stručno znanje, jer se radi o nespornim činjenicama koje se u određenim trenutku nalaze na određenom mjestu (2010:443-444). Isto stajalište imaju i Radonjić i Božović, koji također smatraju da utvrđivanje sadržaja ili uvid u podatke sa kompjutera ili drugog uređaja predstavlja jednostavno otkrivanje i akviziciju ovih dokaza i kao takvo nije zadatak vještaka (n.o.:80). Međutim, postoje i suprotstavljena mišljenja koja podržavaju upotrebu vještačenja kao radnje dokazivanja kojom se pribavljaju digitalni dokazi, jer vještačenje omogućava cjelovitu i detaljnu analizu podataka i pruža odgovore na često sporna pitanja na koja radnja pretresanja ne može (vidjeti: Križanić i Šmer Bajt, 2016). Također, rezultati vještačenja kao dokazi u postupku uživaju reputaciju visokog nivoa pouzdanosti, gotovo neupitne dokazne vrijednosti i snage što je potvrđeno analizama sudske prakse (vidjeti: Bojanić, 2010; Kavazović, 2015; Bajraktarević Pajević *et al.* 2017; USAID, 2017). Iz odgovora ispitanika obuhvaćenih našim istraživanjem je evidentno da se u praksi češće slijede tradicionalni koncepti istražnih radnji te se oduzeti predmeti, odnosno, uređaji koji sadrže podatke se podvrgavaju dokaznoj radnji vještačenja, a ne pretresanja kako bi se došlo do dokaza. Naime, na pitanje kojom radnjom dokazivanja se u praksi dolazi do digitalnih podataka koji mogu imati ulogu dokaza u krivičnom postupku,[374] svi ispitanici obuhvaćeni istraživanjem su odgovorili da je to vještačenjem pokretne stvari - uređaja koji sadrži digitalne podatke, iako je bio ponuđen i odgovor pretresanjem uređaja. Ključni razlog zbog kojeg se u praksi daje prednost vještačenju je taj da se tako osigurava postupanje u skladu sa pravilnim forenzičkim procedurama, što predstavlja poželjnu opciju, jer je utvrđeno istraživanjima da u predmetima u kojima je tako postupano[375] se ne postavlja pitanje prihvatljivosti dokaza (vidjeti: IPROCEEDS, 2018:14). Štaviše, prezentacija dokaza digitalne prirode od strane vještaka ne samo da osigurava njihovu vjerodostojnost već čak i vjerodostojnost iskaza stručnog lica koje je provodilo pretresanje, kao i samog postupka pretresanja (ukoliko je provedeno)[376] pa se

[373] Čl. 95. ZKP BiH, 109. ZKP FBiH, 160. ZKP RS i 95. ZKP BD BiH.
[374] Pitanje 3.3. anketnog upitnika.
[375] Navedeno je da je na ovaj način obrađeno preko 350 predmeta.
[376] Odgovor stručnog lica sa kojim je obavljen intervju 20.09.2019. u prostorijama agencije.

vještačenje u praksi koristi kao ultimativno rješenje tužilaca u slučaju kada odbrana uloži prigovore (*Ibidem*). U svijetlu navedenog treba posmatrati stajalište većine ispitanika da nije svrsishodno provoditi radnju pretresanja bez provođenja radnje vještačenja (80%).[377] Stoga se u praksi u odnosu na uređaj koji sadrži digitalne podatke često provode obje radnje i pretresanja i vještačenje. Navedeno potvrđuju i odgovori većine ispitanika (80%) da je radnja dokazivanja pretresanja pokretne stvari (predmeta) praćena sa radnjom vještačenja iste pokretne stvari.[378] Zakonodavac je propisao da se obje radnje provode na osnovu naredbe.[379] Na pitanje je 60% ispitanika odgovorilo da se izdaju odvojene naredbe za svaku od navedenih radnji dokazivanja, dok je 40% ispitanika navelo da se istom naredbom obuhvaćaju obje radnje dokazivanja.[380] Provođenje obje dokazne radnje na istom uređaju znatno opterećuje stručna lica i doprinosi dugotrajnosti postupaka,[381] a imajući u vidu da vještačenje rezultira kvalitetnijim i pouzdanijim dokazima, većina ispitanika je iznijela stajalište da se ovi dokazi trebaju pribavljati samo radnjom vještačenja.[382]

Nova praksa, koja je ustanovljena u Kantonu Sarajevo, a koju postepeno uvode pojedini tužioci,[383] podrazumijeva da nakon oduzimanja, otvaranja i pregleda, tužilac ponovo podnosi zahtjev sudu da izda naredbu o pretresanju pokretnih stvari koje sadrže digitalne dokaze. U tim slučajevima meritorna odluka suda u postupku se temelji na ispravi, zapisniku o pretresanju uređaja. Radnja pretresanja se rijetko obavlja na mjestu njihovog pronalaska, već se obično obavlja u forenzičkoj laboratoriji[384] ili u prostorijama tužilaštva ili policije uz prisustvo policijskih službenika, forenzičkih stručnjaka, stručnjaka za kriminalističku tehniku, dva svjedoka, osumnjičena lica, sudske policije i advokata (IPROCEEDS, 2018).

Također na kraju je potrebno skrenuti pažnju na neadekvatnost tradicionalne procesnopravne terminologije, zbog čega se predlaže njena zamjena drugim terminima koji su informatičko-tehnološki utemeljeni poput: „pristupanje“ i „kopiranje“ (vidjeti: Nortje i Myburgh, 2019), jer se preciznije mogu opisati radnje pretresanja i oduzimanja kada se koristi terminologija iz informaciono-tehnološkog diskursa, jer je percipirana kao značenjski neutralna i može uključivati radnje kao što je kreiranje forenzičke kopije podataka (vidjeti: Casey, 2004; Nieman, 2006; Nieman, 2009). Nadalje, u stručnoj literaturi je vidljivo neujednačeno korištenje termina koji nisu adekvatno prevedeni sa engleskog jezika

[377] Odgovori ispitanika na pitanje 3.8. anketnog upitnika.
[378] Pitanje 3.7. Upitnika.
[379] Čl. 53. i 96. ZKP BiH.
[380] Odgovori ispitanika na pitanje 3.4. anketnog upitnika.
[381] Odgovor stručnog lica sa kojim je obavljen intervju 20.09.2019. u prostorijama agencije.
[382] Odgovori ispitanika na pitanje 3.19. anketnog upitnika.
[383] Provođenje ove prakse je potvrđeno od strane stručnog lica sa kojim je intervju obavljen 20.09.2019. godine u prostorijama agencije.
[384] *Ibidem*.

kao što je pretraživanje digitalnih uređaja i podataka umjesto pretresanje, forenzička analiza umjesto vještačenje, forenzički izvještaj umjesto nalaz i mišljenje vještaka, prepoznavanje lica mjesta krivičnog incidenta umjesto uviđaj mjesta kriminalnog događaja itd. što unosi dodatne nejasnoće u postupanju sa ovi dokazima i njegovom evidentiranju u kontekstu bh. krivično procesnog sistema.

Iz ugla većine ispitanika (60%) postojeći načini postupanja sa digitalnim dokazima su ocijenjeni kao adekvatni.[385] Pojedini ispitanici koji su iskazali suprotno stajalište, svoj su odgovor obrazložili navođenjem sljedećih razloga: da sa digitalnim dokazima postupa neadekvatno obučeno osoblje, prilikom oduzimanja mobilnih telefona nije obavezno da se pokuša pribaviti šifra za mobilni telefon; digitalni dokazi se ne pakuju na odgovarajući način.[386] Prema mišljenju većine ispitanika (75%), neadekvatnost postupanja sa digitalnim dokazima se prvenstveno ogleda u načinima pakovanja, skladištenja i evidentiranja pojedinačnih radnji u okviru samog postupka.[387] Posebno su zabrinjavajući sljedeći postupci koji su uobičajeni u praksi: inicijalno kreiranje samo jedne forenzičke kopije (80%)[388] i neprekidanje komunikacije u mobilnom telefonskom uređaju prilikom njegovog oduzimanja, odnosno, pakovanja (80%).[389]

U odnosu na unapređenje problematičnih aspekata postupanja sa digitalnim dokazima, percepcija ispitanika je da je potrebno unapređenje svih elemenata postupanja u odnosu na ovu vrstu dokaza, a naročito u pogledu njihovog pakovanja, skladištenja i samog rukovanja, kao i da je potrebno ukinuti praksu pretresanja mobitela i kompjutera i uspostaviti praksu direktnog upućivanja ovih uređaja na vještačenje.[390] Isto stajalište je istaknuto i od strane stručnog lica sa kojim je obavljen polu-struktuisani intervju.[391] Imajući u vidu da su svi ispitanici potvrdili da na nivou njihove institucije/agencije postoje procedure postupanja sa digitalnim dokazima,[392] koje su u skladu sa dobrim praksama postupanja sa digitalnim dokazima,[393] može se zaključiti da je problem u njihovoj implementaciji. Potrebno je napomenuti da prilikom provođenja istraživanja nije bilo moguće izvršiti uvid u sadržaj procedura koje su uspostavljene na nivou institucija/agencija i utvrditi njihovu kompatibilnost kroz postupak komparacije. Nesporno je da ujednačene procedure postupanja na području države doprinose pravnoj sigurnosti, a to svakako nije slučaj ako svaka institucija/agencija ima uspostavljene svoje procedure postupanja. Stav svih ispitanika je

[385] Odgovori na pitanje 3.16. anketnog upitnika.
[386] Odgovori ispitanika na pitanje 3.17. anketnog upitnika.
[387] Odgovori ispitanika na pitanje 3.18. anketnog upitnika.
[388] Odgovori ispitanika na pitanje 3.12. anketnog upitnika.
[389] Odgovori ispitanika na pitanje 3.13. anketnog upitnika.
[390] Odgovori ispitanika na pitanje 3.19. anketnog upitnika.
[391] Intervju je obavljen sa stručnim licem 20.09.2019. godine u prostorijama agencije.
[392] Odgovori ispitanika na pitanje 3.21. anketnog upitnika.
[393] Odgovori ispitanika na pitanje 3.22. anketnog upitnika.

da bi bilo korisno da se formalno uspostave ujednačene procedure postupanja sa digitalnim dokazima na nivou vlasti u BiH.[394]

Zaključak

U radu su prezentirana aktuelna pitanja postupanja sa digitalnim dokazima iz ugla stručnih lica u kontekstu krivično procesnog okvira koji je trenutno na snazi. Istraživanjem su identificirani različiti obrasci u postupanju sa digitalnim dokazima i manjkavosti koje u konačnici mogu rezultirati sa nezakonitošću dokaza. Uočeni pristupi se mogu interpretirati kao rezultati neimplementacije procedura postupanja sa ovom vrstom dokaza, koje su usvojene na nivou agencija, ali i tužilačkog nepoznavanja oblasti, što rezultira sa nejasnim pravnim osnovima postupanja i pribavljenim dokazima koji imaju mali dokazni značaj i često spornu zakonitosti.

Prikaz rezultata provedenog istraživanja, kao i drugih istraživanja nedvojbeno upućuje na zaključak da je potrebno otkloniti neujednačenost postupanja sa digitalnim dokazima kroz izmjene i dopune postojećih zakonskih odredbi, ali i donošenje podzakonskih akata kojima će se jasno utvrditi pravila i procedure postupanja imajući u vidu specifičnu prirodu ovih dokaza i otkloniti postojeće nedoumice u pogledu njihove zakonitosti. Prezentirane rezultate treba isključivo posmatrati kao skroman doprinos autora naučnoj i stručnoj raspravi o digitalnim dokazima i harmonizaciji rada u ispitivanoj oblasti, a ne kao definitivna stajališta o spornim pitanjima identificiranim u teoriji i praksi.

[394] Odgovori ispitanika na pitanje 3.23. anketnog upitnika.

Literatura

- Bajraktarević Pajević, D. *et al.* (2017), 'Significance of forensic expertise in proving the financial crime offences in case law of Court of B&H', str. 67-88. In: V. Pasca and Ciopec F. (eds) *Probleme atuale in dreptul penal european. Bucureşti: Universal Juridic*.
- Bojanić, N. (2010), 'Uloga vještačenja u donošenju adekvatne sudske odluke kod seksualnih delikata kao delikata nasilja', *Kriminalističke teme - časopis za kriminalistiku, kriminologiju i sigurnosne studije*, y. X, no. 3-4/2010, pp 119-134.
- Bouwer, G.P. (2014), 'Search and Seizure of Electronic Evidence: Division of the Traditional One-step Process into a New Two-step Process in a South African Context'. *South African Journal of Criminal Justice,* Volume 27, Issue 2, str. 156-171.
- Casey, E. (2004), *Digital Evidence and Computer Crime* (2nd Edition). London, San Diego: Elsevier Academic Press.
- Casey, E. (2011), *Digital Evidence and Computer Crime (3rd Edition) - Forensic Science, Computers, and the Internet*. Waltham, San Diego, London: Elsevier Academic Press.
- Dika, M. (2015), 'O standardima utvrđenosti činjenica u parničnom postupku'. *Zb. Prav. fak. Sveuč. Rij.* (1991) v. 36, r. 1, str. 1-70.
- EC-Council (2016), *Computer Forensics: Investigation Procedures and Response (CHFI).* Boston: Cengage Learning.
- ENISA (2014), *Electronic evidence - a basic guide for First Responders Good practice material for CERT first responders*. Dostupno na: https://www.enisa.europa.eu/publications/electronic-evidence-a-basic-guide-for-first-responders. Pristupljeno: 01.10.2019.
- Halilović, H. (2019), *Krivično procesno pravo – Knjiga druga: teorija dokaza i radnje dokazivanja u krivičnom postupku*. Fakultet za kriminalistiku, kriminologiju i sigurnosne studije: Sarajevo.
- Horić, A. (2007), 'Informacija – povijest jednog pojma: o Capurrovom razumijevanju pojma informacije'. *Vjesnik bibliotekara Hrvatske* Vol. 50, No. 1-2, str. 96-106.
- INTERPOL (2019), *Global guidelines for digital forensics laboratories*. Dostupno na: https://www.interpol.int/content/download/13501/file/INTERPOL_DFL_GlobalGuidelinesDigitalForensicsLaboratory.pdf. Pristupljeno 10.09.2019.
- Ilić, M. (2001) *Krivično procesno pravo*. Drugo izmijenjeno i dopunjeno izdanje. Sarajevo: Pravni fakultet Sarajevo.
- IPROCEEDS (2018), *Izveštaj o proceni u vezi sa pribavljanjem i korišćenjem elektronskih dokaza u krivičnom postupku na osnovu domaćeg zakonodavstva u zemljama jugoistočne Evrope i Turskoj*. Dostupno na: https://rm.coe.int/3156-52-IPROCEEDS-electronic-evidence-report-serbian/16807bdfe3. Pristupljeno: 05.12.2019.

- Ivanović, Z. (2015), 'Pitanje postupanja sa digitalnim dokazima u srpskom zakonodavstvu'. *Kriminalistička teorija i praksa, 2.* (1/2015.), 7-21. Preuzeto s https://hrcak.srce.hr/159734. Pristupljeno 02.01.2020.
- Kavazović, M. (2015), 'Kriminalistički sadržaji forenzičkih vještačenja rukopisa (studija slučaja Kanton Sarajevo 2002.-2007.)'. *Kriminalističke teme - časopis za kriminalistiku, kriminologiju i sigurnosne studije*, y. XV, no. 1-2/2015, str. 1-18.
- Kerr, O. S. (2005c), 'Searches and Seizures in a Digital World. *Harvard' Law Review* Vol. 119, No. 2, str. 531-585. Dostupno na: https://ssrn.com/abstract=697541. Pristupljeno 12.12.2019.
- Kos, I. *et al.* (2013), *Priručnik o pretresanju kompjuterskih sistema, uređaja za pohranjivanje kompjuterskih i elektronskih podataka i mobilnih telefonskih aparata.* Dostupno na: https://vstv.pravosudje.ba/vstv/faces/docservlet?p_id_doc=48595. Pristupljeno: 05.11.2019.
- Križanić, G. i Šmer Bajt, B. (2016), *Vještačenje u kaznenom postupku*. Dostupno na: http://pak.hr/cke/obrazovni%20materijali/Vje%C5%A1ta%C4%8Denje%20u%20kaznenom%20postupku.pdf. Pristupljeno 12.11.2019.
- Lakić, L. (2014), 'Iskustva i uočeni problemi u primjeni tužilačke istrage u BiH', str. 89-106. U: I. Jovanović i A. Petrović-Jovanović (ur.) *Tužilačka istraga regionalna krivičnoprocesno zakonodavstva i iskustva u primeni*. Beograd: Misija OEBS-a u Srbiji.
- Madden, A. (2000), 'A definition of information'. *Aslib Proceedings*, Vol. 52 No. 9, str. 343-349.
- Mešanović, M. (2018), 'Institut nezakonitih dokaza u krivičnim postupcima u BiH sa osvrtom na uporedno pravo'. *Zbornik radova Pravnog fakulteta Sveučilišta u Mostaru* br. XXVI, str. 59. - 91. Dostupno na: http://pf.sum.ba/images/preuzimanje/MESANOVIC_CL.pdf. Pristupljeno: 10.12.2019.
- Nieman, A. (2006), *Search and Seizure, Production and Preservation of Electronic Evidence* (PhD-thesis North West University 2006). Dostupno na: https://repository.nwu.ac.za/handle/10394/1367?show=full. Pristupljeno: 10.12.2019.
- Nieman, A. (2009), 'Cyberforensics: Bridging the Law/technology Divide'. *Journal of Information, Law and Technology*, Vol. 2009, No. 1. Dostupno na: https://warwick.ac.uk/fac/soc/law/elj/jilt/2009_1/nieman/. Pristupljeno: 10.12.2019.
- Nortjé J.G.J. i Myburgh D.C. (2019), 'The Search and Seizure of Digital Evidence by Forensic Investigators in South Africa'. *Potchefstroom Electronic Law Journal*, Vol. 22, 2019, str. Dostupno na: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3392338. Pristupljeno: 03.12.2019.
- Novak, M. *et al.* (2019), 'New Approaches to Digital Evidence Acquisition and Analysis'. *NIJ Journal*, Issue No. 280/2019. Dostupno na: https://nij.ojp.gov/library/publications/nij-journal-issue-no-280. Pristupljeno: 10.12.2019.

- Kerr, O. S. (2005b), 'Search Warrants in an Era of Digital Evidence'. *Mississippi Law Journal,* Vol. 75, str.85-145. Dostupno na: https://olemiss.edu/depts/ncjrl/pdf/02-KERR.pdf. Pristupljeno 12.12.2019.
- Kerr, O. S. (2005a). 'Digital Evidence and the New Criminal Procedure'. *Columbia Law Review*
- Vol. 105, No. 1, str. 279-318. Dostupno na: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=594101. Pristupljeno 12.12.2019.
- Pavišić, B. (2011). *Komentar Zakona o kaznenom postupku*. Rijeka: Dušević & Krešovnik.
- Pisarić, M. M. [2015]. Pretresanje računara radi pronalaska elektronskih dokaza. *Zbornik radova Pravnog fakulteta,* Novi Sad, 49 (1), str. 215-238. Dostupno na: https://scindeks.ceon.rs/article.aspx?query=ARTAK%26and%26elektronski%2bdokazi&page=0&sort=1&stype=0&backurl=%2fSearchResults.aspx%3fquery%3dARTAK%2526and%2526elektronski%252bdokazi%26page%3d0%26sort%3d1%26stype%3d0. Pristupljeno: 06.12.2019.
- Protrka, N. (2011), 'Računalni podaci kao elektronički (digitalni) dokazi'. *Policija i sigurnost*, 20 (1), 1-13. Dostupno na: https://hrcak.srce.hr/79204. Pristupljeno 15.12.2019.
- Radonjić, V. i Božović, D. (n.o.) *Pravni i informatički aspekt* pretresanja *računara i drugih oblika prekograničnog kriminala*, Bilten Državnog tužilaštva Crne Gore, br. 2/ str. 64-86. Dostupno na: http://sudovi.me/files/L3VkdHovZG9jL0JJTFRFTiUyMERyemF2bm9nJTIwdHV6aWxhc3R2YSUyMDIwMTcucGRm=. Pristupljeno: 09.10.2019.
- Radovanović, D. i Begić, M. (2016) *Pribavljanje zakonitih dokaza u postupku*. https://vstv.pravosudje.ba/vstv/faces/docservlet?p_id_doc=48623. Pristupljeno 05.10.2019.
- Ross, R. *et al.* (2016), *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*. Dostupno na: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r1.pdf. Pristupljeno: 20.12.2019.
- Scientific Working Group on Digital Evidence (SWGDE) (2016), *Digital & Multimedia Evidence Glossary.* Dostupno na: https://www.swgde.org/documents/Current%20Documents/SWGDE%20Digital%20and%20Multimedia%20Evidence%20Glossary. Pristupljeno 12.12.2019.
- Sijerčić – Čolić, H. (2008). *Krivično procesno pravo, Knjiga I, Krivičnoprocesni subjekti i krivičnoprocesne radnje*. Sarajevo: Pravni fakultet Univerziteta u Sarajevu.
- Sijerčić – Čolić, H. i Radičić, M. (2015), *Organizacija i nadležnost policijskih agencija u Bosni i Hercegovini*. Sarajevo: Perfecta.
- Simović, M. N. (2014), 'Koncepcija tužilačke istrage u Zakonu o krivičnom postupku Bosne i Hercegovine: stanje i problemi', str. 43-58. U: I. Jovanović i A. Petrović-Jovanović (ur.) *Tužilačka istraga regionalna krivičnoprocesno zakonodavstva i iskustva u primeni*. Beograd: Misija OEBS-a u Srbiji.

- Spasić, V. i Stevanović, B. (2015), 'Dokazivanje digitalnih povreda prava intelektualne svojine - osvrt na anglosaksonski pravni sistem'. *Zbornik radova Pravnog fakulteta u Nišu*, (69), str. 203-226. Dostupno na: https://scindeks-clanci.ceon.rs/data/pdf/0350-8501/2015/0350-85011569203S.pdf. Pristupljeno: 10.01.2020.
- Stamenković *et al.* (2017), *Vodič za sudije i tužioce na temu visokotehnološkog kriminala i zaštite maloletnih lica u Republici Srbiji*. Dostupno na: https://nwb.savethechildren.net/sites/nwb.savethechildren.net/files/library/Vodic-za-sudije-i-tuzioce.pdf. Pristupljeno: 10.01.2020.
- USAID (2017) *Analiza sistema angažovanja vještaka u predmetima korupcije i organizovanog i privrednog kriminala*. Dostupno na: www.usaidjp.ba. Pristupljeno: 10.12.2019.
- U.S. NIJ. (2008) *Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition . National Institute of Justice*. Kindle Edition.

Kriminalističke teme
Zbornik radova
Godina XIX, Broj 5, 2019.
ISSN 1512-5505

METODE OTKRIVANJA SAJBER KRIMINALA PUTEM DIGITALNE FORENZIKE

THE METHODS OF DETECTION CYBER CRIME INTO DIGITAL FORENSICS

Pregledni naučni rad

Mr. sci. Elmedin Ahmić[395]
Prof. dr. Almin Dautbegović[396]
Prof. dr. Nedžad Korajlić[397]

Sažetak

Inspiracija za rad i problem (i) koji se radom oslovljava (ju): Razvojem informaciono-komunikacionih tehnologija stvara se sve više mogućnosti sajber-kriminalcima da na lagan način "upadnu" u sistem pojedinca ili kompanija i da načine štetu. U radu će biti opisan razvoj sajber kriminala, oblici zloupotreba i prijevara, te tehnike koje se koriste za otkrivanje počinilaca. Izvlačenje ovih podataka, njihovo tumačenje i prognoziranje, te jednostavno prezentiranje pred sudom, predstavljaju moćan alat u istražnim postupcima. Dakle, nove tehnologije, novi pristup izvršenja krivičnih djela, i otkrivanja istih, inspiracija je za sve istraživače krivičnopravnih i kriminalističkih nauka.

Ciljevi rada (naučni i/ili društveni): Na osnovu uočenog problema istraživanja definisan je i *predmet istraživanja:* predmet rada ima za cilj da objasni metode primjene digitalne forenzike u otkrivanju počinilaca sajber kriminala.

Metodologija/Dizajn: Iako se digitalni dokazi, do prije nekoliko godina u našem okruženju, nisu niti priznavali u sudskim procesima, danas je situacija sasvim druga, jer ovi dokazi ukoliko se prikupe, i obrade na adekvatan način, te prezentiraju uz pomoć propisanih procedura koji se forenzičari moraju pridržavati, tada su dokazi ravnopravni sa ostalim materijalnim dokazima. U konstelaciji sa navedenim, postavljen je sljedeći *problem, a ujedno i hipoteza istraživanja:* Da li je moguće metodama digitalne forenzike obezbjediti relevantne dokaze o počiniocima i krivičnim djelima za sudske postupke validne dokaze sajber kriminala?

Ograničenja istraživanja/rada: Jedan od bitnih faktora ograničenja istraživanja sajber kriminala, predstavlja ubrzani tehnološki razvoj, te samim tim i metode izvršenja izvršilaca, koje su svakim danom sve savremenije, a tehnološka pismenost u Bosni i Hercegovini, ne prati taj korak. Razvojem informacioni tehnologija, zahtijeva prije svega obrazovni sistem prilagođem novim dostignućima, tehnološku pismenost istražitelja itd.

[395] Mr. sci. Elmedin Ahmić, Općinski sud u Travniku, elmedin_ahmic@hotmail.com
[396] Prof. dr. Almin Dautbegović, profesor Krivično-procesnog prava, advokat, aleph.ze@gmail.com
[397]Prof. dr. Nedžad Korajlić, Fakultet za kriminalistiku, kriminologiju i sigurnosne studije Sarajevo, dekan, tppaba@bih.net.ba

Rezultati/Nalazi: Istina je da koliko god uložili u sigurnost, to ne znači da će informacijski sistem biti u potpunosti siguran te da smo oslobođeni problema. U Bosni i Hercegovini do sada nije provedeno relevantno i sveobuhvatno istraživanje o pojavnosti i rasprostranjenosti ovog kriminala. Zato se mora reći da je u sigurnosnom smislu Bosna i Hercegovina nedovoljno istraženo područje. Bosna i Hercegovina nema ni strategiju ni institucije za rješavanje pitanja sajber kriminala i sajber sigurnosnih prijetnji. Ukoliko se obezbijede ulaganja u razvoj ove discipline kako u materijalne tako i u ljudske resurse, trebalo bi da se smanje ozbiljni problemi prijetnji od hakiranja internet stranica do drugih oblika ovog kriminala.
Generalni zaključak: Digitalna forenzika će nastaviti da se razvija i postat će sigurno moćna tehnika za otkrivanje digitalnih dokaza. Da bi taj razvoj bio nesmetan potrebno je da ga prati zadovoljavajuća pravna regulativa i da država ne predstavlja usporavajući faktor.
Opravdanost istraživanja/rada: Tendencije učestalosti izvršenja krivičnih djela iz oblasti sajber kriminala, uzima sve veći primat kako u svijetu, tako i u Bosni i Hercegovini. Zakonska legislativa je prva stepenica u sistematskom pristupu ovom problemu, koji treba u kontinuitetu dorađivati, mijenjati, uporedo sa razvojem tehnološki dostignuća i razvojem istih, kako bi bili na punom tragu izvršiocima ovih krivičnih djela.
Ključne riječi: Sajber kriminal, zakon, istraživanje, krivično djelo, digitalna forenzika, prevencija

Apstract

Reason (s) for writing and research problem (s): By developing information-communication techniques, more and more cyber-criminals are being created to easily "infiltrate" the system of an individual or a company and make damage. The paper will describe the development of cybercrime, forms of abuse and fraud, and technologies used to detect perpetrators. Drawing these data, their interpretation, and forecasting, and simply presenting in court, are a powerful tool in investigative proceedings. Thus, new technologies, a new approach to the perpetration of criminal offenses, and their discovery, is an inspiration for all investigators of criminal law and criminology.
Goals of this paper (scientific and/or social): Based on the identified research problem definition and subject matter of research: the subject of the paper aims to explain the methods of applying digital forensics to detecting cybercriminals.
Methodology/Design: Although digital evidence, even a few years ago in our environment, did not admit it to judicial proceedings, today's situation is quite different, as this evidence is collected and processed in an adequate manner and presented with the help of prescribed procedures that must be respected by forensicists , then the evidence is equated with other material evidence. In the constellation of the above mentioned, the next problem has been raised, and the hypothesis of the research is: Is it possible to provide relevant forensic evidence of perpetrators and criminal offenses of cybercrime to judicial proceedings?
Research/paper limitations: One of the key factors of cyber crime limitation is the accelerated technological development, and thus the execution methods of perpetrators, which are more and more contemporary and technological literacy in Bosnia and Herzegovina, are not following this step. With the development of information technology, I primarily adapt the education system to new achievements, the technological literacy of investigators and so on.
Results/Findings: It is true that as far as security is concerned, this does not mean that the information system will be completely safe and free from the problem. So far, no

relevant and comprehensive investigation into the occurrence and spread of this crime has been carried out in Bosnia and Herzegovina. That is why it has to be said that, in the security sense, Bosnia and Herzegovina is insufficiently explored. Bosnia and Herzegovina has no strategy or institution to address cybercrime issues and cyber security threats. If investment in the development of this discipline is provided both in material and human resources, serious threats from hacking websites to other forms of this crime should be reduced.

General conclusion: Digital forensics will continue to develop and will become a powerful technique for detecting digital evidence. In order for this development to be undisturbed it is necessary to follow a satisfactory legal regulation and not to represent a decelerating factor.

Research/paper validity: The tendency of the frequency of cybercriminal crime is growing in the world, as well as in Bosnia and Herzegovina. Legislative legislation is the first step in the systematic approach to this issue, which needs to be continually updated, altered, alongside the development of technological achievements and development, to be in full swing for the perpetrators of these criminal offenses.

Key words
Cyber Crime, Law, Research, Criminal Offense, Digital Forensics, Prevention

1. Uopšte o sajber kriminalu

Razvojem informatičko-komunikacijskih tehnologija donijele su sa sobom nove oblike društveno neprihvatljivog ponašanja koje se treba na adekvatan način kriminalizirati. I-pak nacionalna zakonodavstva sve više imaju problema za efikasno regulisanje sve većeg broja novih društvenih odnosa koji traže pravnu regulaciju. Posmatrajući savremeno društvo možemo uočiti brojne specifičnosti i ozbiljne probleme koji uglavnom imaju globalnu dimenziju. Do sada je potvrđeno da niti jedan normativni sistem nije uspio do kraja obuhvatiti sve relevatne društvene odnose.

Sa razvojem globalne računarske mreže stvorile su se i dodatne mogućnosti za nove oblike kriminala. Sve češće se pojavljuju pojedinci koji su posebni i tehnički potkovani te možemo reći opsjednuti i osvetoljubivi. Tim osobama se sve teže suprotstaviti i zaustaviti ih.

Naravno zbog lakoće "kretanja" po sajber prostoru pojedinac dobija osjećaj moći i neuhvatljivosti. Ovi osećaji nisu bez razloga, jer stvarno ga je izuzetno teško otkriti u momentu činjenja djela, što, uglavnom, predstavlja i “pravi” trenutak za njegovo identifikovanje i hvatanje. S druge strane, Internet koji je toliko ranjiv i nesiguran zbog ogromnog broja korisnika pretpostavlja se više od tri milijarde korisnika (Internet-Hit-3-Billion-Users, 2014), otvorenosti i neregulisanosti je i idealno skrovište kriminalaca različiti tipova. U ovim okruženjima i sa takvim pojedincima sve se češće pokušavaju izboriti ne samo mnoga nacionalna prava već i međunarodne organizacije, kao i “privatni sektori” ne bi li ublažili negativne posljedice i smanjili gubici koji nastaju zbog kriminalnih aktivnosti.

Tradicionalne kriminalne grupe i organizacije modernizuju se korištenjem ICT, a sajber prostor postaje sredina u kojoj djeluju i koja im istovremeno služi kao mjesto koje je idealno za sakrivanje. Ono postaje i okruženje u kome nastaje poseban tip kriminala – sajber kriminal (Porobić i Bajraktarević, 2012).

1.1. Pojam i definicija sajber kriminala

Možda najpotpuniju definiciju sajber kriminala možemo naći u dokumentu „Kriminal vezan za kompjutersku mrežu“ (Report of Committee II, Workshop on crimes related to the computer network) sa Desetog Kongresa Ujedinjenih nacija, posvećenog prevenciji kriminala i tretmanu počinilaca koji je održan u Beču od 10. do 17. aprila 2000. godine (Tenth United Nations Congress on the Prevention of Crime and Treatment of Offenders, Wienna, 10-17 April 2000. godine). Radna grupa eksperata u sadržaju izvještaja pod sajber kriminalom podrazumijeva „kriminal koji se odnosi na bilo koji oblik kriminala koji se može izvršavati sa kompjuterskim sistemom i mrežama, u kompjuterskim sistemima i mrežama ili protiv kompjuterskih sistema i mreža“. To je kriminal koji se odvija u elektronskom okruženju. Ako se pod kompjuterskim sistemom podrazumijeva „svaki uređaj ili skup međusobno povezanih uređaja, kojim osigurava ili čiji jedan ili više elemenata osiguravaju, prilikom izvršenja nekog programa, automatiziranu obradu podataka“ (Konvenciju o Sajber criminalu Vijeća Europe, 2011) je očigledno da bez kompjuterskih sistema i kompjuterskih mreža nema ni sajber kriminala. Pojam sajber kriminala je kompleksan i zbog čega ga mnogi smatraju tzv “kišobran terminom“ koji „pokriva“ raznovrsne kriminalne aktivnosti uključujući napade na kompjuterske podatke i sisteme, napade vezane za računare, sadržaje ili intelektualnu svojinu.

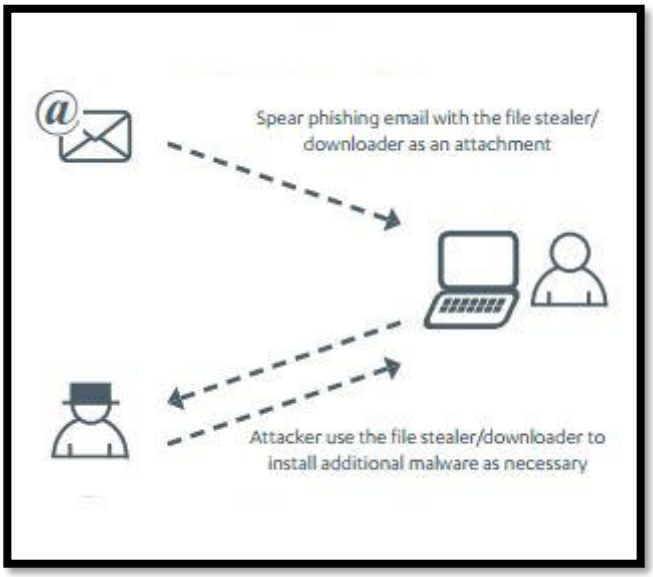
Pravni osnov za postupanje u ovoj oblasti je ustanovljen usvajenjem Konvencije o Sajber kriminalu (usvojena u Budimpešti 23. 11. 2001. g.) koji je preveden kao Konvencija o visokotehnološkom kriminalu ili kao Konvencije o kibernetičkom kriminalu. Također se treba istaći da pod pojmom sajber krivična djela treba svrstati samo krivična djela kod kojih je upotreba kompjutera odnosno kompjuterskog sistema ili kompjuterske mreže bitna za biće krivičnog djela, a ne sva krivična djela u kojima se na neki način kao sredstvo izvršenja pojavljuje kompjuter sa pripadajućom perifernom opremom (Porobić i Bajraktarević, 2012).

1.2. Sajber kriminal

Što važnija postaje mreža u širem značaju za globalno društvo i privredu, to profesionalniji postaju sajber napadači i sajber napadi. Sajber kriminal ima mnogo oblika, te je stoga sve teže se i boriti sa ovom vrstom kriminala. U uobičajene oblike sajber kriminala ubrajamo:

1.2.1. Phishing ili mrežna krađa

Phishing ili mrežna krađa je vrsta prijevare putem koje zlonamjerni pojedinac ili organizacija pokušava doći do osjetljivih, povjerljivih ili tajnih podataka, naravno lažno se predstavljajući. Podaci koji se takvim putem mogu prikupiti su razni - brojevi i PIN-ovi kreditnih kartica, E-mail lozinke, pristupni podaci za razne web servise (Facebook, Skrill, Paypal, Twitter, Ebay) itd.



Grafik 1. Phishing e-mail napad *Izvor: http://securityaffairs.co/wordpress/18206/cyber-crime.html*

Pošiljatelj šalje poruku u kojoj traži od korisnika da odgovori sa pristupnim podacima (lažno se predstavljajući kao službeni kontakt), u svrhu "poboljšanja usluge", ili sprečavanja brisanja korisničkog računa sa određene stranice (Ilustracija 1). Takve poruke gotovo redovito prati slaba pismenost, gramatičke i pravopisne greške. Lažna internetska stranica izgleda skoro identično autentičnoj stranici, ali je URL u adresnoj traci drugi. Kad korisnik upiše podatke na lažiranoj stranici, informacije dolaze do vlasnika lažirane stranice.

Phishing napadi se redovito poboljšaju te uz pomoć razni setova sada koji su dostupni naravno i pojednostavljuju proizvodnju phishing sajtova. Pošiljatelji su u prednosti i mogu lako kroz spam e-mailove da namame žrtve na stranice koje su automatski stvorili, te na kojima mogu da ukradu lične podatke i druge osjetljive podatke. Jedan od načina izbjegavanja ove vrste napada je ignoriranje poveznica danih u e-mailu. Umjesto toga preporučljivo provjeriti adresu navedene internet stranice u preglednik i provjeriti istinitosti

zahtjeva preko te stranice. Korisno je i imati na umu kako ozbiljne organizacije ne kontaktiraju korisnike na ovakve nesigurne i nepouzdane načine.

1.2.2. Hakiranje odnosno zloupotreba internet stranice ili mreže

Razlog hakiranja jesu slabo zaštićene internet stranice iz finansijskih razloga, koje pogoduju napadima i njihovoj „lakšoj" provali te na taj način usmjeravati procese sajber prostora i sigurnosnoj prijetnji kako žele napadači. Naravno takve stranice su itekako pogodne za hakere i njihovo vršenje napada. Za klasični primjer hakiranja neke internet stranice i njihovom društvenom uticaju po sigurnosni problem, predstavićemo u jednom primjeru prepoznatljivog proizvođača video igrica. Tako je Lizard Squad - Hakerska grupa koja je preuzela odgovornost za napad zbog kojeg je PlayStation Network bio offline veći dio dana. Sony je istakao da je riječ isključivo o DDoS[398] napadu i kako korisnički podaci nisu ugroženi.

Ilustracija 1*: *DDos napad na Sony Playstation *Izvor: http://www.mirror.co.uk/news/world-news/sony-hit-playstation-hack-page-4766760*

Stewart Room direktor Cyber Security Challenge je potvrdio za SCMagazine (Scmagazineuk, 2015) da je ovaj najnoviji napad došao u 'rekordnoj' godini za sajber-sigurnost. Vijest o napadu na Sony PlayStation podsjeća još jednom da su prijetnje sajber-sigurnosti raznolike kao što su i stvarne. U 2014. godini zabilježen je rekordan broj napada, a prijetnje su došle sa različitih područja, kao što su krivične prijetnje, prijetnje pod

[398] DDoS je engleska skraćenica za Distributed Denial-of-service attack, i označava sprečavanje pristupa računarskom sistemu korištenjem mnogobrojnih raspršenih resursa koji se većinom nalaze na Internetu.

pokroviteljstvom države, zlonamjerni radnika, a sada i Lizard Squad, čiji motivi i motivacija može biti više od samog hakiranja. Osim što su preuzeli odgovornost za DDoS napad na Sony-eve servere, iz Lizard Squada su na Twitteru poslali i lažnu prijetnju bombom američkoj avio kompaniji American Airlines. Cilj je bio dodatno isprovocirati Sony tako što su došli do podataka o letu na kojem je bio predsjednik Sony Online Entertainment studija, nakon čega je dotični let preusmjeren i prizemljen na najbliži aerodrom.

Ilustracija 2: Prijetnja bombom hakera Lizard Squad na Twitter-u

Glasnogovornik American Airlinesa je potvrdio kako je spomenuti let preusmjeren iz "sigurnosnih razloga".

Ovakvi i slični primjeri nam govore koliku sigurnosnu prijetnju mogu proizvesti ovakvi napadi na određene baze podataka, „hakiranjem“ te na taj način korištenjem tih podataka i svoje svrhe zloupotrebom istih, ucjenama, uticajem na promjeni nekih odluka, i sl. Iz ovog i sličnih primjera, potrebno je upoznati se sa opasnostima, ovakvih upada i računarske mreže, zaštiti ličnih podataka, njihovom zloupotrebljavanju, i kakav uticaj mogu proizvesti ovakvi hakerski napadi i koliku štetu mogu učiniti kako za određene pojedince, tako i na globalnom nivou.

1.2.3. Širenje mržnje i poticanje na terorizam

Trenutno je internet najzastupljeniji medij komunikacije, naročito među mlađim generacijama. Razvojem interneta prijenos informacija se mijenja, te informacija postaje povod za diskusiju na internetskim platformama pri čemu svi korisnici prakticiraju pravo na izražavanje (William i sar., 2011). Da ima razlike između tradicionalnih medija i interneta to možemo vidjeti kroz činjenicu da sadržaji koji pristignu budu provjereni i odobreni prije nego se puste u javnost. Internet je javno mjesto gdje je dovoljno tehnički uvjetovana

radnja (klik miša) da se sadržaj objavi i prenese u javnost, a kontrola nastupa (ako do nje i dođe) a posteriori.

Internet je zapravo prostor bez „granica" a brzina i opseg diseminacije sadržaja teško su zaustavljivi. Razlog i nemogućnost efikasnog kontroliranja interneta je što internet kao globalni medij načelno podložan različitostima pravnog uređenja u svakoj pojedinoj državi, dok je istovremeno nedovoljno regulisan na međunarodnom nivou da bi se moglo izvršiti njegovo uređenje. Zbog svega navedenog autori širenja mržnje mogu putem Interneta besplatno širiti mržnju te „dotaći" veliki broj ljudi u jako kratko vrijeme. Kroz brojne društvene mreže dijele isti interes i motivaciju mogu se povezati te tako ojačati. Također su mehanizmi kontrole nevidljivi pa tako mogu i maloljetnici imati pristup ovakvim sadržajima.

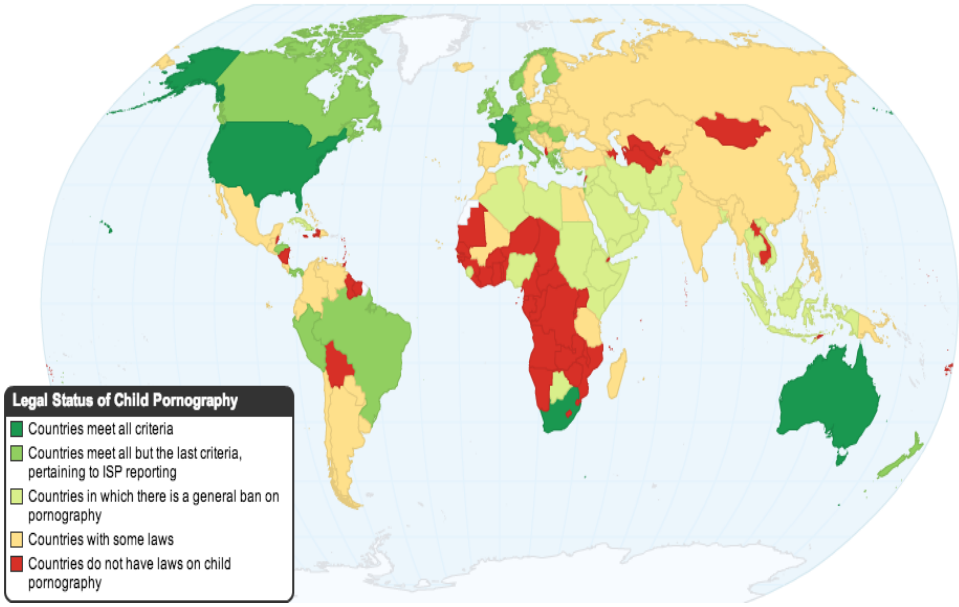
'Novi terorizam i novi mediji' zbog jednostavnosti i anonimnosti komunikacije putem društvenih mreža, sve je teže pratiti jer komunikacije terorista, odnosno protuterorističke jedinica sve je teže zaustaviti jer potencijalne napade dogovaraju na ovaj način. Teroristi se društvenim mrežama najčešće služe za propagandu, radikalizaciju i regrutiranje novih članova te im one omogućuju da 'ciljanoj publici virtualno pokucaju na vrata', odnosno ostvare direktan kontakt s njima i pokušaju ih privući sa svojim idejama. Činjenica da je širenje mržnje i terorizma zabilježeno na novom mediju, neke države smatraju da načela trebaju biti podjednako primijenjena kao npr. u slučaju djeljenja sadržaja (tzv. engl. „share" opcija na društvenim mrežama poput Facebooka) budu jednako kažnjiva kao dijeljenje letaka kojima se poziva na mržnju ili terorizam.

1.2.4. Distribucija dječije pornografije

Danas Internet svjetska informatička mreža koja je ušla u mnoge domove širom svijeta (Dragičević, 1999). Tradicionalni korisnici pornografskih sadržaja sve se više koriste Internetom, što potvrđuje i velik pad interesa za štampana izdanja nekih časopisa. Tako je npr. teksaški pornomagnat Thomas Reedy putem svoje kompanije Landslide Productions Inc. zarađivao oko 1,4 milijuna USD godišnje od pretplate koja je iznosila oko 15 USD u prosjeku po pretplatniku. Riječ je bila o mjesečnoj pretplati koja je korisnicima omogućavala pristup najodvratnijim prizorima spolnih zlopotreba djece koji se uopće mogu zamisliti (Cyber Lolita and Child Rape). Reedy je 2001. godine osuđen na 1.335 godina zatvora, što je prva kazna doživotnog zatvora izrečena za distribuciju dječije pornografije putem Interneta (Rubin, 2003). Premda se s potpunom sigurnošću ne može ustanoviti tačan broj izvora dječije pornografije na Internetu, nesporno je da ona svakodnevno raste. Tom širenju pridonose brojni faktori, od kojih treba izdvojiti anonimnost korisnika te razvoj i razmjernu dostupnost različitih multimedijalnih tehnika kojom i osobe bez posebnog znanja mogu izraditi i distribuirati nezakonite sadržaje.

Obzirom na tako opasnu pojavu, potrebno je zakonsku legislativu razvijati kontinuirano na globalnom nivou kako bi se spriječile zloupotrebe dječijih fotografija eksplicitnog

sadržaja i uopšte zabranila distribucija. Međutim, nije samo zakon koji bi garantovao sigurnost, također je potreban rad policije, pravosudnog sistema i vladajućih struktura koji moraju biti spremni za izvršenje kazni bez tolerancije za svaku povredu tih zakona.



Ilustracija 3: Pravni status dječje pornografije *Izvor: http://findingjustice.org/legal-status-child-pornography/*

Ilustracija 3. prikazuje pravni status dječje pornografije u svijetu. Nevjerovatno je da nešto tako odvratno i grešno, nije međunarodno zabranjeno.

- 5 zemalja zadovoljava sve kriterije.
- 24 zemalje zadovoljava sve, ali ne i ISP izvještaje.
- 68 zemalja imaju neki zakon koji se izričito bavi dječijom pornografijom.
- 92 zemlje nemaju zakona koji se konkretno bavi dječijom pornografijom.

Ova ilustracija, nam jasno govori kako se u svijetu pristupa problemu zaštite i zloupotrebe dječijih eksplicitnih sadržaja, njihovom korištenju, distribuiranju , a prije svega evidentno je mali broj zemalja imaju jasno opredjeljen stav u pravnom smislu kada je u pitanju prevencija i zaštita dječijih prava i sloboda.

2. Digitalna forenzika

Da bi se odgovorilo na visokotehnološki kriminal javila i se potreba za razvojem nove naučne discipline, kao i regulisanje pravnih normi vezanih za uspješno otkrivanje, a zatim i procesuiranje krivičnih djela iz ove oblasti.

Digitalna forenzička istraga predstavlja proces koji korištenjem naučnih metoda i tehnologije, razvija i testira teorije kroz hipoteze, analizirajući digitalne uređaje, koji predstavljaju relevantan dokaz u sudskom postupku. Cilj takve istrage je da se utvrdi istina o protivpravnoj aktivnosti i svih okolnosti u vezi sa počiniocem i načinom izvršenja krivičnog djela. Digitalni dokaz u tom slučaju predstavlja digitalni objekat koji sadrži pouzdane informacije koje podržavaju hipotezu. Kako bi se učinjena nezakonita djela dokazala i njihovi počinioci procesuirali i sankcionisali, potrebno je primjeniti procedure digitalne forenzike kao naučne discipline sa izuzetno značajnom praktičnom primjenom. Upravo digitalna forenzika kao relativno nova naučna disciplina (uspostavljena 1999. godine od strane IECO - International Organization on Digital Evidence) obezbjeđuje jedini pouzdani alat za istragu kompjuterskog i mrežnog kriminala, akviziciju i analizu digitalnih podataka i pripremu i prezentaciju digitalnih dokaza pred sudom. U slučaju da je došlo do zloupotrebe IKT (informaciono komunikacijska tehnologija) sistema, odnosno kompjuterskog kriminala ili potrebe za upravljanjem kompjuterskim incidentom, administrativnih zahtjeva ili civilne parnice, odgovore će nam dati digitalna forenzika koja podrazumijeva otkrivanje (pretraga, istraga) i sakupljanje (akviziciju), čuvanje (upravljanje), dokazivanje (analizu) i ekspertsko svjedočenje (prezentaciju) digitalnih dokaza pred sudom (Milosavljević i Grubor, 2009).

Digitalna forenzika je naučna disciplina koja može ponuditi relevantan dokaz odnosno digitalni dokaz. Veliki razvoj IKT-a postavlja velike izazove pred digitalne forenzičare koji moraju imati permanentnu i svakodnevnu edukaciju kako bi bili za korak ispred počinioca koji sprovode protivpravne aktivnosti u digitalnom okruženju. Brzina tehnološkog razvoja uticala je na razvijanje ove mlade naučne discipline, koja zajedno sa paralelnim razvojem drugih nauka, primjenjuje nove metode koje utiču na brzinu, i jednostavnost prikupljanja čvrstih dokaza, istražuje anti-forenzičke aktivnosti, sa ciljem da otkrije istinu u vezi sa učinjenom protivpravnom radnjom. U taksonomiji digitalne forenzike, a u odnosu na predmet forenzičke istrage, digitalnu forenziku možemo podjeliti na: forenziku računarskih sistema, forenziku mobilnih uređaja, forenziku baza podataka i forenziku računarske mreže uključujući i Internet ili kibernetičku forenziku (Marcella i Greenfield, 2002). Treba istaći da je za digitalnog forenzičara od presudne važnosti praćenje i razvoj informacionih tehnologija. Ponekad su razlike u operativnom sistemu ili verziji nekog programa od suštinskog značaja. Zato je bitno postojanje profilisanosti digitalno forenzičkih eksperata prema stručnoj oblasti (operativni sistemi, baze podataka, mrežni sistemi kao i profilisanje prema drugim IKT sistemima).

Različiti profili kompanija primjenjuju digitalnu forenziku i od policijsko-sudskih i vojno-obaveštajnih aktivnosti, civilnog i bankarskog sektora i osiguravajućih društava. Svi ovi entiteti moraju biti izuzetno oprezni sa podacima kojima raspolažu, jer u protivnom može biti prouzrokovana nemjerljiva šteta zbog industrijske špijunaže, zloupotrebe IKT sistema, ali i nekih drugih oblika protivpravnih postupaka. Procjena je, da šteta od različitih djelovanja visokotehnološkog kriminala, ne uzimajući u obzir njegove potencijalne veze sa organizovanim kriminalom, na godišnjem nivou iznosi oko 200 milijardi dolara (Prlja, 2017).

Da bi se podaci mogli koristiti kao neoborivi i čvrsti dokazi pred sudom digitalna forenzika kompjuterskog sistema obuhvata naučno ispitivanje i analizu podataka sa čvrstih diskova, fajl sistema i prostora za skladištenje podataka. Steve Haily iz Cybersecurity instituta, digitalnu forenziku posmatra kroz postupke dobijanja, očuvanja, identifikacije, tumačenja i dokumentovanja digitalnih dokaza prema propisanim pravilima, pravne procese, postupak očuvanja integriteta dokaza, kao i pružanje stručnog mišljenja pred sudom u vezi sa pronađenim dokazima. Na osnovu navedene definicije može se zaključiti da digitalna forenzika podrazumijeva upotrebu unaprijed definisanih procedura i tehnika za detaljno ispitivanje kompjuterskog sistema, a sa ciljem dobijanja relevantnih digitalnih dokaza. Često u literaturi možemo da pronađemo poistovjećivanje digitalne forenzike kompjuterskog sistema sa procesom oporavka podataka. Ovo je samo djelimično i tačno. Digitalna forenzika oporavlja podatke koje je korisnik namjerno sakrio ili izbrisao, za razliku od slučajno izgubljenih ili izbrisanih, što kao krajnji cilj ima da se obezbjedi validnost oporavljenih podataka za dokaze pred sudom. Forenzičari imaju strogo definisana pravila, pri prikupljanju medijuma (čvrste diskove i sve druge sekundarne medije za skladištenje podataka) za koje sumnjaju da se na njima nalaze digitalni dokazi, osiguravaju ih od bilo kakvih promjena, i iz velike količine digitalnih podataka moraju pronaći relevantne i održive dokaze.

Digitalna forenzika igra veliku ulogu u praćenju potencijalnih počinilaca protivpravnih aktivnosti. To se postiže identifikacijom protivpravne aktivnosti, prikupljanjem dokaza, izgradnjom "lanca nadležnosti nad digitalnim dokazima", analizom dokaza, prezentovanjem pronađenih dokaza, svedočenjem i sve to u okviru vođenja sudskog postupka protiv osumnjičenog. Digitalni dokazi mogu biti oslobađajući, optužujući ili da ukazuju na osnovanu sumnju.

2.1. Digitalni dokaz

Digitalni dokaz počiva kao elektornski podatak, bilo u formi transakcije dokumenta ili neke druge vrste medija, kao što su audio i video snimci. Skoro pa svaka današnja transakcija je digitalozovana u nekom trenutku i postaje digitalni dokaz, npr. podizanje novca sa računa, plaćanje računa na bankama, plaćanje kreditnim karticama itd... U današnjem vremenu gotovo nemoguće je u ovom povezanom svijetu da na neki način ne ostavite elektronski trag putem plaćanja bilo kakve vrste transakcije. Mnogi ljudi danas dijele

svoja svakodnevna dešavanja na socijalnim mrežama kao što su Twitter, Facebook Google+ i mnoge druge. U stanju smo da znamo pored svih slika pjesmi, politički stavova, dnevni događaja, saznamo i njihove lokacije gdje se u trenutku objave nalaze. Prilikom pisanja E-mail poruke ili dokumenta u Wordu ili Notepad-u, vozimo automobil sa uključenim GPS uređajem ili nešto plaćamo preko interneta, mi stvaramo digitalni dokaz. Prilikom surfanja internetom i telefoniranja stvara se digitlani dokaz. To su nam više poznati oblici digitalni dokaza, međutim mnogo puta radimo sve naborojane radnje, a uistinu nismo svjesni da stvaramo digitalne dokaze.

Da bi jedan digitalni dokaz bio prihvaćen od strane suda treba da posjeduje pet osobina:

a) Prihvatljivost – Potrebno je da je u skladu sa određenim pravnim pravilima, prije nego što bude dostavljen sudu. Ukoliko se koristi orginal tada kopija nema značaja, dok je u slučaju korištenja kopije potrebno koristiti najbolju kopiju. S obzirom da se danas može napraviti kopija digitalnog dokaza koja je istovjetna originalu, upotreba kopije je pravno prihvatljiva i ako postoji original. Upravo se u praksi koristi i primjenjuje prezentovanje kopije digitalnog dokaza, da bi se eliminisale sve sumnje vezane za izmjenu tj. zloupotrebu sa originalnim dokazom,
b) Autentičnost - Dokazni materijal mora nedvosmisleno upućivati na krivično djelo i počinioca. Ukoliko se ne može dokazati autentičnost digitalnog dokaza na sudu, bez obzira što je dokaz prikupljen i analiziran na propisan način, sudija može proglasiti dokaz nevažećim i neprihvatljivim za donošenje sudske odluke,
c) Kompletnost – u smislu da dokaz treba da prikaže cjeli slučaj sa svim aspektima bitnim za donošenje sudske odluke. Dokaz mora biti objektivan i prikazati sve bitne okolnosti za sudsko odlučivanje – Ukoliko postoje okolnosti koje mogu biti oslobađajuće tako i one koje se stavljaju na teret počinioca,
d) Pouzdanost –nije dozvoljeno da postojati nikakva sumnja u vezi sa načinom na koji su dokazi prikupljeni i kako je sa njima rukovano. U suprotnom, to bi bacilo sumnju na autentičnost i istinitost dokaza,
e) Vjerodostojnost i razumljivost – dokaz mora biti lako razumljiv i vjerodostojan za sud i stranke u postupku. Nema svrhe pred sud iznositi neke stručne stvari i objašnjavati npr. „memory dump— (sliku stanja memorije u računaru), s obzirom da sud nema obavezu da posjeduje takva stručna znanja pa samim tim neće razumjeti šta to znači (Schweitzer, 2003).

2.2. Forenzička istraga

Kolekcije forenzički alata se koriste za identifikaciju datoteka koje je potrebno pregledati. Prilikom procesa akvizicije alat stvara indeks pojmova koji predstavljaju osnovnu jedinice pretrage. Pojam može biti samo znak ili skupina znakova, alfanumeričkih ili numeričkih, s razmacima na obje strane. Pretraga veličine datoteka ili raspon veličina traženih (Bunting i Wei, 2006) dokumenata vrši se uz pomoć Boolove logike (I, ILI, NILI). Svaki forenzički softver posjeduje specifične ugrađene metode pretrage koje koriste boolovu logiku.

Pojmove je moguće povezati korištenjem boolovih operatora. Kako bi se stvorio traženi izraz ili moglo filtrirati rezultate. Alate za digitalnu forenzičku istragu možemo podjeliti na hardverske i softverske alate. Zatim prema platformi na kojoj rade:

- "Open Source" programi (Sleuthk Kit & Autopsy, SMART....),
- Licencirani programi: (EnCase, Helix3 Enterprise, X-Ways Forensics...).

Zatim prema platformi na kojoj rade:

- Windows platforma: (EnCase , X-Ways Forensics....),
- Linux platforma: (Sleuthk Kit & Autopsy, Helix3 Enterprise...).

Digitalni dokaz ima važnu ulogu na sudu, ali dobijanje takvih dokaza često može biti vrlo teško. Svaki od navedenih alata odgovara određenim potrebama. Njihova upotreba je od velikog značaja kada treba doći do izgubljenih, obrisanih ili oštećenih podataka koje treba povratiti. Danas, kada je broj prevara, zločina i zloupotreba računara veoma veliki, neophodno je imati odgovarajuće alate kojima je lako odgovoriti na potrebe istrage. Ono što prvo treba da svaki alat obezbijedi, jest to da eletronski ili digitalni dokaz bude takav da može da se podnese kao validan dokaz na sudu. Za to je uglavnom neophodno predznanje i obuka u vezi sa radom sa alatima. Glavni nedostatak većine alata je cijena prilikom vraćanja podataka. Eksperti za kompjuterski kriminal naplaćuju po satu, a istraga može trajati i do 10 i više sati. Iako primjena kompjuterske forenzike i alata ima svoje prednosti i nedostatke, pokazalo se da je njihova upotreba opravdana i vrlo korisna u većini slučajeva kada se može primjeniti. Predstavićemo u radu neke od najzastupljenijih alata za otkrivanje sajber prevara, kojim dokumentujemo izvršenje krivičnog djela.

2.2.1. EnCase Forensic

EnCase Forensic je vodeći software i svjetski pružatelj rješenja, usluga i obuke u području digitalne forenzike. Kako bi pratili tempo i trend, forenzički alati koji forenzičari koriste su sve kompleksniji i sa više funkcionalnosti nego ikad prije, a imaju i veću učinkovitost. Dovoljno je samo da se pogleda razlika u dodatnim funkcijama između verzija određeni verzija i može se uočiti ogromna razlika. Prošla su vremena kada se jedan alat koristio samo kako bi stvorili sliku, drugi alat se koristi samo u pretraživanju podataka, treći alat se koristi samo za stvaranje hash datoteka itd. Današnji alati ispunjavaju često zatraženo "pronalazak svih dokaza (i ispisivanje izvještaja)" klikom na dugme. Uspješni i profesionalni forenzičari u jednom trenutku moraju prenijeti svoje rezultate na treću osobu koja ima vrlo ograničeno ili malo razumijevanje računarskih operacija. Te treće strane su obično istražitelji, odvokati, suci, žiri itd. Forenzičar mora objasniti, usmeno i pisanim izvještajima, vrlo mnogo tehnički pojmova u smislu da laik može razumjeti. Potrebno je naravno vrijeme, praksa, znanje, iskustvo i kreativnost. Najviše od svega, to zahtijeva da su spremni poduzeti dodatne napore kako bi izvještaj bio uspješan. Kada se stvori

izvještaj da čitatelji mogu lako čitati i razumjeti, rezultati moraju govoriti sami za sebe (Bunting i Wei, 2006).

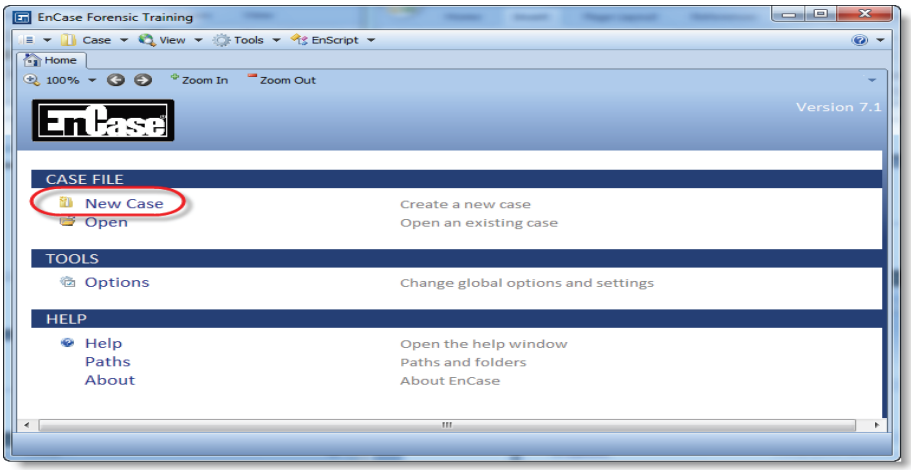
EnCase je alat za kompjutersku forenziku koji je proizveo GuidanceSoftware. Dostupan je advokatskim kancelarijama, a koristi se za prikupljanje podataka, oporavak fajlova, pretragu i parsiranje fajlova. Za korišćenje ovog softvera obično je neophodna specijalna obuka. Podaci otkriveni putem EnCase alata se uspješno koriste u raznim sudovima širom svjeta. EnCase softver omogućava korisnicima da kreiraju boot disk koji će zaštititi podatke od toga da budu upisani na neki sumnjivi disk prilikom procesa pokretanja kompjutera. Jednom kada se kompjuter pokrene i krene sa radom, forenzičar može da krene sa pravljenjem slike diska, bilo pomoću patch kabla ili serial kabla. Kada se slika kreira, EnCase softver omogućava pretraživanje hard diska na neki od sljedećih načina:

- Istraživanje slika sa hard diska pregledom pomoću galerije,
- Istraživanje fajlova korištenjem heksa pogleda (čitanje heksadecimalnih komponenti fajla),
- Pretraživanje cjelokupnog diska na ključne riječi (Advances in Digital Forensics II, 2006).

EnCase alat također posjeduje mogućnost izvještavanja što omogućava istražiteljima da sačuvaju pronađene ključne riječi, slike i da snime lične komentare u formatu koji je lak za izvještavanje. Na taj način, informacije mogu da se odštampaju ili prosljede mail-om pravnim zastupnicima koji su uključeni u slučaj. EnCase predstavlja jedan od najnaprednijih i sveobuhvatnih alata za izvođenje složenih i vremenski zahtjevnih zadataka, kroz višestruke sistemske fajlove i jezike. Nova verzija ovog programa je V7 koja uključuje nove značajke kao što su smartphone modul, eksterni pregled paketa i pristup desetinama EnScripta[399] i aplikacija u App EnCase Central-u.

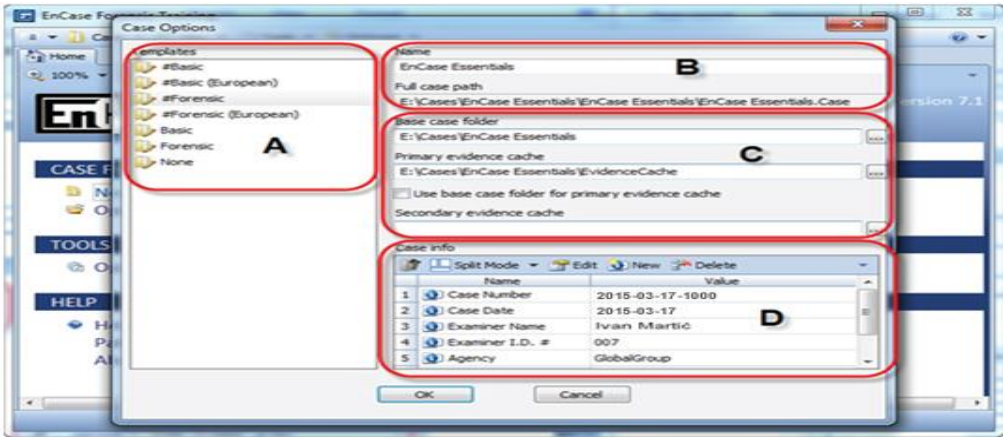
Procesor Manager za dokaze u EnCase Forensic V7 omogućava distribuciju i kontrolu obrade dokaza za jednu ili više EnCase mašine ili EnCase procesor čvorova. Sa dokazima Procesor Managera, može se pojednostaviti, automatizirati, i povećati brzina obrade dokaza i preuzimanja (EnCaseFroensicBrochure, 2014).

[399] EnScript je programski jezik korišten od strane forenzički kompjuterski programa kao što je EnCase.



Ilustracija 4: Shema novog slučaja Izvor: Vlastita izrada

Procesor Manager pruža također istražitelju potpunu kontrolu u preradi dokaza, te osim toga optimiziran je za efikasnije iskorištavanje sistemskih resursa, čime se povećava brzina obrade. Ilustracijom će biti prikazano pravljenje jednog slučaja u EnCase V7:



Ilustracija 5: Pravljenje novog slučaja Izvor: Vlastita izrada

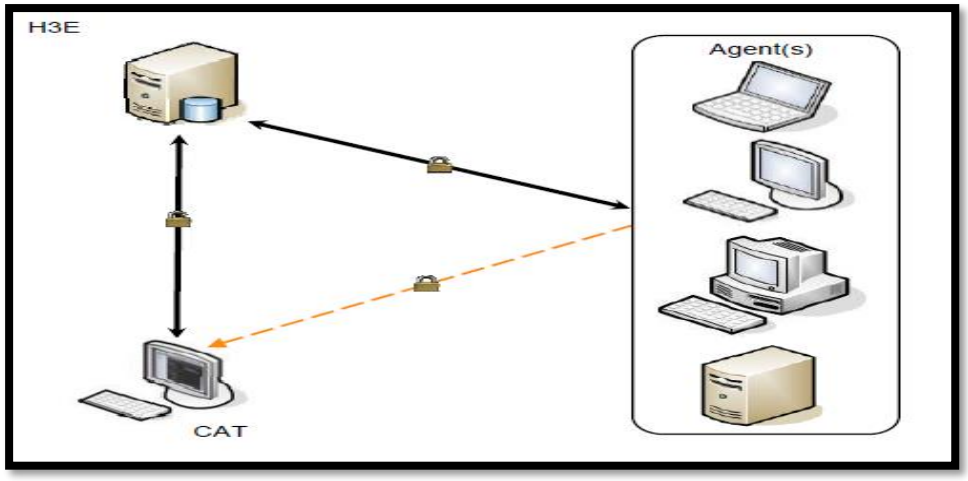
- Opcija A - Kada stvaramo novi slučaj, dobivamo popis dostupnih predložaka (templates). To su unaprijed definirani predlošci koje EnCase prikazuje uz spašene predloške. Na Ilustraciji 5, izabran je Forenzički predložak.
- Opcija B - Ime slučaja je tekst koji se unosi za identificiranje slučaja. U ovoj verziji EnCase V7, slučaj više nije sadržan u jednom fajlu, već je pohranjen unutar mape koja sadrži mnoge komponente. Naziv naveden u ovom polju koristi se za pronalazak predmeta u toj mapi.

- Opcija C - Mapa osnovnog slučaja - To je mjesto gdje se stvara nova mapa slučaja.
- Opcija D - Informacije o slučaju - Informacije o trenutnom slučaju. Ove stavke se prvenstvenstveno koriste za umetanje korisnički definirani podataka u izvještaju.

Forezičari mogu da podese vremensku zonu za svaki dio medija, omogućavajući jednostavno upoređivanje medija sa različitim zonama. Također mogu da sortiraju fajlove u odnosu na 30 različitih polja, uključujući i sva četiri vremenska pokazatelja (kada je neki od fajlova kreiran, kada mu je posljednji put pristupljeno, kada je posljednji put pisano i kada je posljednji put modifikovan), nazive fajlova, putanje, formate i slično. EnCase softver nudi više od 150 filtera, počevši od obrisanih fajlova pa sve do Word dokumenata koji su zaštićeni šifrom. Također ima ugrađenu pomoć koja brzo i jednostavno služi kao korisničko uputstvo (Mediarecovery, 2015). Završna faza forenzičkog ispitivanja je izvještaj, koji mora biti dobro organiziran i prikazan u formatu koji će ciljana publika razumjeti.

2.2.2. Enterprise

Uz pomoć Helix3 Enterprise (H3E) imamo potpunu vidljivost aktivnosti preko cijelog našeg mrežnog sistema, aktivnosti kao što su pristup neovlaštenim podacima, izvlačenje podataka ili stvaranje tajnih tunela. H3E također nam omogućuje da brzo reagujemo i bez otkrivanja korisnika odgovorimo na incidente i prijetnje. Helix3 Enterprise nam omogućuje da brzo otkrijemo, identificiramo, analiziramo, očuvamo izvještaj koji nam daje dokaze i otkriva istinu te štititi svako poslovanje. H3E rješenje je trostruka arhitektura koja se sastoji se od konzole za upravljanje (CAT), Servera i Agenata (H3E Manual, 2015).



Ilustracija: 6: Arhiktertura H3E

Svi podaci koji se razmjenjuju između CAT-a i Agenata prolaze kroz Server, osim za vrijeme prijenosa velikih slikovnih datoteka, kao što su RAM, tada CAT i agenti komuniciraju direktno. Server djeluje kao srednje spremište za sve podatke prikupljene od strane Agenata. Server autentificira i šalje naredbe iz CAT-a za Agente na mreži, a zatim istodobno prosljeđuje odgovore podataka natrag u CAT i pohranjuje ih u unutarnje SQL baze podataka. Verzija Helixa koja se najviše koristi je zasnovana na Ubuntu[400], što obećava stabilnost i laku upotrebu.

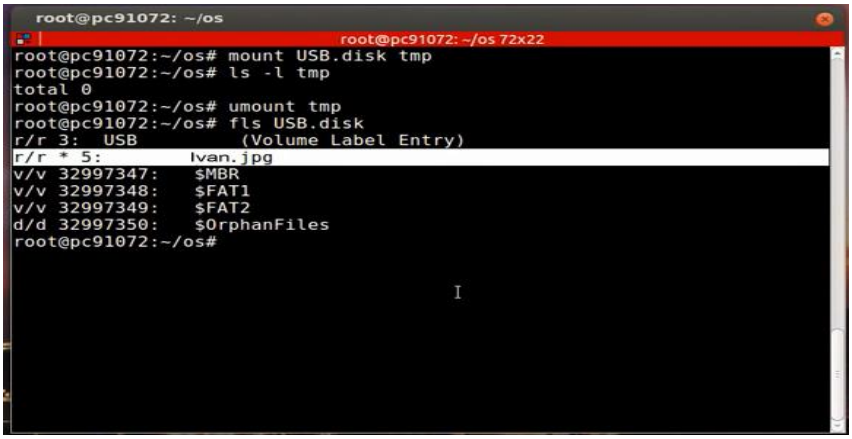
Ilustracija 7: Kontrolna ploča H3 Enterprise

Osnovni paket koji dolazi uz Helix3 sadrži moćan alat za analiziranje mreže, nekoliko anivirus alata, povratak lozinki, rezervne kopije i povratak particije, pretragu MAC particija, istraživanje binarnih fajlova itd. Može se zaključiti iz ovog da je Helix veoma koristan alat. Dual mod je posebno koristan, a to omogućava korisnicima Helix alata da pristupe problemima koji su povezani ne samo za Linux nego i sa Windows sistemom na različite načine. Helix je stabilan, kompletan paket, sa velikim opsegom mogućnosti koje mogu značajno povećati sposobnost odgovora na probleme, prijetnje i incidente iz okruženja. Pri kraju svih potrebnih analiza i pretraga obavlja se stvaranje izvještaja u PDF formatu. Helix3 Enterprise je jednostavan za korištenje i moćno rješenje kako bi se osiguralo poslovanje svakog preduzeća. Ne samo da uz H3E imamo vidljivost na cijeloj infrastrukturi, nego ovaj alat omogućuje pravovremeno reagiranje na incidente i prijetnje koji se mogu izolirati na vrijeme.

[400] Ubuntu je računarski operacijskih sistem nastao kao izvedenica sistema Debian GNU/Linux, koji pak mnoge temeljne komponente preuzima iz projekta GNU i koristi Linux kao jezgru operacijskog sistema.

2.2.3. Sleuth Kit-Autopsy

Sleuth Kit je forenzički alat za analizu i Microsoft i UNIX sistem datoteka i disk slika. Sleuth Kit je open source, što omogućuje istražiteljima da potvrde akcije alata ili ga prilagode na specifične potrebe. Sleuth Kit je razvijen nezavisno od komercijalnih i naučnih organizacija od Brian Carrier-a, koji je također razvio Autopsy Forensic Browser. Sleuth Kit je kolekcija alata za forenzičku analizu sistema pod UNIX-om baziranih na komandnoj liniji (Dowling, 2006). Alati omogućavaju ispitivanje sistemskih fajlova na sumnjivom kompjuteru na nenametljiv način. Alat nije povezan sa operativnim sistemom da bi analizirao sistemske fajlove, također prikazuje obrisane i sakrivene sadržaje.



Ilustracija 8: Prikaz obrisane slike sa USB-a *Izvor: Vlastita izrada*

Ilustracija 9: Oporavak izbrisane slike sa USB-a

Kada se izvodi kompletna analiza sistema, bolje je koristiti alat sa grafičkim okruženjem, a ne sa komandnom linijom. Autopsy Forensic Browser je alat u Sleuth Kit-u sa grafičkim interfejsom koji omogućava lakši tok istrage. Autopsy daje mogućnost menadžmenta slučaja, integritet slike, pretragu po ključnim riječima i ostale automatske operacije. Podržava NTFS, FAT, UFS1, UFS2, EXT2FS, EXT3FS, i ISO 9660 fajl sisteme. Alati mogu biti pokrenuti sa „živog" UNIX sistema tokom odgovora na incident. Ovi alati će prikazati fajlove koji su skriveni i neće modifikovati vrijeme pristupa (Dowling, 2006). Tehnike za pretraživanje dokaza sa ovim alatima su:

- Listing fajlova: Analizira fajlove and direktorije, uključujući imena izbrisanih fajlova i fajlova sa Unicode[401] baziranim imenima,
- Sadržaj datoteka: Sadržaj datoteka mogu biti pregledani u raw, hex, ili ASCII stringovi mogu biti raspakovani,
- Hash baze podataka: Pregled nepoznati fajlova u hash bazi podataka i brza identifikacija da li je dobar ili loš. Autopsy koristi NIST National Software Reference Library[402] (NSRL) bazu podataka u prepoznavanju dobri i loši fajlova,
- Sortiranje po tipu fajla: Sortitranje datoteka po poznatim tipovima. Autopsi može također izvući samo grafičke slike (uključujući minijaturni prikaz), te prikazati sve promjene ekstenzija datoteka koje su se koristile kako bi se sakrio određeni fajl,
- Pretraga po ključnoj riječi: Pretraga se može izvesti pomoću ASCII stringa i regularnih izraza. Pretraživanje je moguće izvesti na punom sistemu ili samo određeni datoteka i prostora. Stringove koji su često traženi možemo jednostavno konfigurirati u Autopsy za automatsko traženje,
- Analiza meta podataka: Meta podaci sadrže detalje o fajlovima i direktorijima. Autopsy dozvoljava pregled detalja bilo koje strukture meta podataka u sistemskom fajlu. Ovo je korisno ukoliko radimo oporavak podataka ili vraćanje izbrisanih sadržaja,
- Detalji slike: Detalji sistemski fajlova mogu biti pregledani uključujući i vremenske aktivnosti. Ovaj način nudi informacije koje su vrlo korisne tokom oporavka podataka (Sleuthkit. org, 2015).

Može se reći da svi ovi alati nude prilično dosta sličnosti, ali u nekim slučajevima EnCase ima malo više mogućnosti. U tom slučaju to sa sobom nosi i cijenu složenosti, a općenito neki korisnici se slažu da EnCase GUI nije tako intuitivan. Naravno, svaki od alata zahtijeva

[401] Unicode je standard za razmjenu podataka usmjeren na prikaz slova na način neovisan o jeziku, računarskom programu ili računarskoj platformi.
[402] Nacionalna referentna knjižnica Software-a (NSRL), je projekt Nacionalnog instituta za standarde i tehnologiju (NIST) koji održava repozitorij poznatog softvera, profila datoteka za uporabu provedbu zakona i drugih organizacija koje se bave računarsko forenzičkim istragama.

obuku ili neko predznanje. Helix, za razliku od ostala dva alata se koristi manje u sudskim procesima, a to proizilazi iz toga što je on namijenjen ne tako zahtjevnim potrebama.

2.2.4. DFRSW Model

DFRWS model je razvijen je između 2001. i 2003. godine pri digitalnoj forenzičkoj istraživačkoj radionici (engl. Digital Forensics Research Workshop). Ovim modelom su obuhvaćene digitalno istražne radnje, definisane klasama. Klase služe za kategorizaciju istražnih radnji po grupama. Modelom su predviđene liste radnji koje mogu da se izvršavaju, a neke od njih su obavezne. Specifičnost ovog okvira je ta, što za svaku pojedinačnu istragu u velikoj mjeri model mora biti redefinisan. Prema ovom modelu postoji ukupno sedam faza u procesu istrage digitalnih dokaza: *identifikacija, čuvanje, sakupljanje, pretraživanje, analiza, prezentacija i odluka.*

2.2.4.1. Identifikacija

Identifikacija u ovom modelu predstavlja osiguranje dokazno značajni elektronski zapisa koji su identifikovani, dostupni i upotrebljivi. Od izuzetne je važnosti da procedure budu jasne, a da bi se one uspješno sprovodile, neophodno je razumijevanje pravnih normi. Cilj ove faze je da se napravi dobar odabir objekata, koje treba prikupiti (fizičke i digitalne) uz što detaljnije dokumentovanje i obrazloženje svake sprovedene aktivnosti. Dokumentacija je prisutna u svim fazama istražnog postupka, ali je pri prikupljanju digitalnih dokaza najvažnija zbog uspostavljanja lanca očuvanja integriteta zapljenjenih dokaza. U tradicionalnom kontekstu prikupljanje podrazumijeva "uzimanje predmeta", a u digitalnom kontekstu se vrši prikupljanje predmeta, također ali sa tom razlikom što ti predmeti nose i "određena stanja"[403] koja mogu da se izgube nakon zapljene ili nestabilnosti elektronskih uređaja (npr. slaba baterija, prekid struje itd...).

Također, digitalni dokazi mogu postojati u velikom broju različitih formi: logovi aplikacija, biometrijski podaci, aplikacijski metadata podaci, logovi Internet servis provajdera, firevall logovi, proksi logovi, logovi mrežnog prometa, logovi sistema za detektovanje upada u sistem, sadržaji podataka iz baze podataka i logovi transakcija, logovi audit programa i mnogi drugi logovi. S obzirom na sve ovo identifikacija svih dostupnih digitalnih dokaza, nije nimalo lagan zadatak. Da bi se proces zapljene što efikasnije izveo, publikovani su i vodiči u kojima su dati praktični savjeti i principi koji su od koristi onima koji se bave digitalnim dokazima. Jedan od njih je "Electronic Crime Scene Investigation: A Guide for

[403] Ta stanja su zapisana u RAM memoriji (engl. Random Access Memory) računara koja sadrže podatke o procesima, informacije o stanju mreže, konekcije sa udaljenim računarom kao i mnoge druge. Kada dodje do isključenja sistema trenutni sadržaj RAM memorije je izgubljen i može samo dio informacija da se povrati.

First Responders"[404] publikovan od strane US Department of Justice 2001. godine u USA kao i „Forensic Examination of Digital Evidence: A Guide for Law Enforcement“ publikovan 2004. godine u USA (Ncjrs, 1999).

2.2.4.2. Prikupljanje i pohrana podataka

Forenzička pohrana naziva se i bitstream slika, zbog toga što predstavlja identičnu bit-po-bit kopiju originalnog dokumenta, datoteke, particije, slike, fotografije ili diska. Prikupljanje podrazumijeva osiguranje i pohranu osjetljivih digitalnih dokaza (dokazi koji se lako mogu izmijeniti ili nestati). Važni koraci kao što su izolovanje sistema od mreže, prikupljanje osjetljivih podataka (koji se mogu izgubiti prilikom isključivanja sistema) identifikovanje sumnjivih procesa na sistemu. U ovoj fazi pravi se kompletna forenzička kopija fizičkog sistema (mirror) na forenzičkom računaru, čime se realizuje pohrana kompletnog digitalnog krivičnog mjesta. Ove forenzičke kopije sadrže cjelokupno digitalno mjesto krivičnog djela za razliku od običnog backup-a koji čuvaju samo dodjeljene podatake (engl. allocated) u digitalnom mjestu krivičnog djela.

U zavisnosti od tipa istrage originalni hard disk može da bude čuvan kao fizički dokaz sve do završetka postupka, a može poslije postupka replikacije biti vraćen u produkciju, ako su u pitanju kritični sitemi. Ova faza je odgovorna za preduzimanje potrebnih mjera kako bi se sačuvali integriteti fizičkih i digitalnih dokaza odnosno njihova nepromjenjivost. Za uspjeh ove faze bitnu ulogu imaju alati i metodi koji se koriste, kao i sama stručnost istražitelja jer se u krivičnom postupku, uglavnom, pokušava to osporiti od suprotne strane. Veliki se broj stručnjaka digitalne forenzike slaže da od ove faze počinje prava digitalna istraga. U ovoj fazi se pravi veći broj dupliranih kopija digitalnih dokaza iz svih izvora, dok se originalni materijal katalogizira i smješta u kontrolisano okruženje u neizmjenjenom stanju. Kopija dobijena odgovarajućim forenzičkim alatima koje smo spomenuli u radu je identična kopija originalnog materijala koja služi za pregledanje ispitivanje i analize u daljim fazama digitalno forenzičke istrage.

2.2.4.3. Pretraživanje

Ukoliko se zna što se otprilike traži, moguće je naravno uvjek lakše nastaviti ovu fazu npr. pretraga po ključnoj riječi, internet pošta (web-mail) "kolačići" (cookies) datumu nastanka ili zadnje promjene datoteka itd... U fazi pretraživanja pronalaze se očigledni djelovi digitalnih dokaza koji odgovaraju tačno određenoj vrsti protivpravne aktivnosti. Ponekad se ova faza izvodi i direktno na terenu (iako je preporuka da se ova faza realizuje u forenzičkoj laboratoriji) da bi se utvrdilo da li je potrebno da se sistem donosi na punu forenzičku analizu i u tom slučaju sistem se podiže u sigurnom okruženju pomoću

[404] U ovom vodiču opisani su različiti izvori digitalnih dokaza. Na slikovit način kroz ilustracije opisuje se kako se kojim digitalnim dokazom rukuje kako bi pomogle osoblju koje prvo odgovara na incident, dostupno na adresi https://www.ncjrs.gov/pdffiles1/nij/187736.pdf

butabilnog DVD/CD/USB, da bi digitalni dokazi ostali nepromijenjeni. Naprimjer, ukoliko se radi o dječijoj pornografiji, istražni organi će prikupiti sve grafičke slike sa sistema i identifikovaće one koje bi predstavljale potencijalne dokaze. Ukoliko se radi o neovlaštenom upadu na server, istražni organi će tražiti očigledne znakove rootkit instalacija, pregledali bi se logovi aplikacija i vršila bi se pretraga za novim konfiguracionim datotekama. U zavisnosti od vještine osumnjičenog, za protivpravne aktivnosti istražitelji će izvršiti procjenu potrebnih tehnika koje će primjeniti u istrazi.

2.2.4.4. Analiza digitalnih dokaza

Cilj analize digitalnih dokaza jest pronalazak i povezivanje činjenica, njihova interpretacija te prezentacija zaključaka i pronalaska. Ova faza podrazumijeva vrlo detaljnju pretragu padataka koji su identifikovani u prethodnim fazama, te se vrše detaljani pregledi podataka kao što je tekst i njegovo značenje, te specifični formati audio i video zapisa. Ova faza ima i svoje podfaze : Fuzija i povezanost - Tokom istrage, podaci (informacije) se prikupljaju iz mnogih izvora (digitalnih i nedigitalnih). Sami za sebe podaci ne mogu da prenesu priču o istraživanom događaju, već moraju da se fuzionišu da bi se sklopila cijela priča. Primjer fuzije može predstavljati vremenski okvir nekog događaja ili radnje koji se odnosi na određeni slučaj odnosno incident. Svaka protivpravna aktivnost ili incident posjeduje hronološku komponentu gdje događaji ili radnje traju tačno određeni vremenski period. Ovim se dobijaju odgovori na gdje, kada i ponekad, kako se desio forenzički relevantan događaj (Caloyannides, 2004).

2.2.4.5. Prezentacija

Forenzički stručnjak mora na jednostavan način obrazložiti rezultate istrage vodeći računa o tome da se isti mogu ponoviti ili da neko drugi može doći do istih zaključaka. Izvještaj povezuje zaključke analize, dokaze i dokumentaciju, te sadrži vrijeme i datum analize i detaljan opis rezultata. Stvaranje izvještaja je najvažnija faza digitalne forenzike i treba sadržavati detaljnu dokumentaciju alata, procesa i metodologije. Složenost izvještaja ovisi o njegovoj namjeni. Kada je istraga zaključena i slučaj predat sudu, rezultati istrage se prezentiraju odvokatima, tužilaštvu, sudiji ili poroti. Nekada od načina prezentacije umnogome zavisi i tok cijelog slučaja, gdje forenzičar mora biti u stanju na jednostavan način obrazložiti rezultate, a nerijetko odvokati, suci, tužilac ili porota prolaze osnovne kurseve računarske forenzike kako bi što kvalitetnije mogli sudjelovati u sudskom procesu.

2.2.4.6. Odluka

Digitalna forenzika ima isti cilj kao i klasična forenzika, a to je sastaviti istinitu verziju događaja potkrijepljenu dokazima. Ključ provođenja digitalne forenzičke istrage je ne samo postaviti prava pitanja, već i znati interpretirati način na koji računar odgovori na pitanja (Volonino i Anzaldua, 2008). Kao krajnji korak provedenog prikupljanja informacija i

obavljene analize je dokument i odluka vještaka čiji je važni dio jasno napisan u kojemu se povezuju do sada prikupljeni i analizirani podaci u cjelovitu priču. Ako se npr. radi o kriminalu u kojem su ukradene kreditne kartice neke banke, onda se svaki broj računa koji je pronađen mora navesti u izvještaju, a sud će na temelju svih rezultata vještačenja i cjelovite priče donijeti odluku.

3.**Perspektive digitalne forenzike u BiH**

U borbi protiv sajber kriminala prije svega se treba usredočiti na stvaranje pravnih ali i tehničkih preduslova, kao što je primjena i razvoj digitalne forenzike. Kao mudar odgovor za ovaj trend potrebno je pristupiti izgradnji preventivnih mehanizama i ulaganja u naučnu disciplinu kao što je digitalna forenzika. Velika važnost digitalne forenzike ogleda se u situacijama kada se već i dogodio sajber napad, koji nismo uspjeli spriječiti ni mjerama informacijske sigurnosti. Tada nam je digitalana forenzika od velike koristi, jer nam pomaže da pronađemo počinitelje i ono što se dogodilo, te identificira osobe odgovorne za napad pomoću dokaza.

Grafikon 2 : Rangirani oblici organizovanog kriminala kojima vlast treba da daje prioritet *Izvor: Centar za sigurnosne studije, Sarajevo - Studija o organizovanom kriminalu u Bosni i Hercegovin.i*

Kako se na grafikonu 3. može primijetiti, građani smatraju da se manje pažnje u definisanju prioriteta djelovanja u predstojećem periodu treba posvetiti aktivnostima

usmjerenim protiv zloupotrebe autorskih prava i kompjuterskog kriminala. Prema stavovima ispitanika, borba protiv kompjuterskog kriminala za Bosnu i Hercegovinu je trinaesti prioritet u budućem djelovanju vlasti. Ovo su pokazatelji koliko građani, a samim tim i odgovorni, a nestručni ljudi iz ove oblasti, smatraju koliko je važna ili bitna borba protiv sajber kriminala u širem kontekstu i koliki negativan efekat može proizvesti po društvo i privredu.

Istina je da koliko god uložili u sajber sigurnost, to ne znači da će informacijski sistem biti u potpunosti siguran te da smo oslobođeni problema. Međutim, tu opasnost možemo svesti na najnižu moguću mjeru uvodeći sisteme digitalne forenzike. Ipak moramo imati na umu da ni tada nismo sigurni. U Bosni i Hercegovini do sada nije provedeno relevantno i sveobuhvatno istraživanje o pojavnosti i rasprostranjenosti ovog kriminala. Zato se mora reći da je u sigurnosnom smislu Bosna i Hercegovina nedovoljno istraženo područje. Bosna i Hercegovina nema ni strategiju, dok se određene institucije bave otkrivanjem sajber kriminala i sajber sigurnosnih prijetnji. Vijeće ministara još nije usvojilo Akcioni plan za formiranje BIH CERT-a (Computer Emergency Response/Readiness Team – Tim za odgovore na računarske incidente). Izvještaji o krivičnim djelima koje pripremaju organi za provođenje zakona u Bosni i Hercegovini se ne odnose na sajber kriminal. Oni ne daju tačne podatke o broju slučajeva, istragama ili osumnjičenima. Digitalna forenzika i druga tehnička sredstva za borbu protiv sajber kriminala na državnom i međunarodnom nivou su ograničena i nedovoljna. Direkcija za koordinaciju policijskih tijela je određena kao stalno dostupna kontakt tačka 24 sata svih sedam dana u skladu s Konvencijom o sajber kriminalu (Budimpeštanska konvencija), ali za to nedostaju potrebni kapaciteti. Na više mjesta u radu je naglašeno kako se u slučaju primjena digitalne forenzike radi o veoma mladoj naučnoj disciplini, koja svoje opravdanje u investiciona ulaganja imaju u jednoj činjenici, a to je otkrivanju počinioca sajber kriminala. Osnivanje i djelovanje tima za digialnu forenziku zahtijeva znatna sredstva. Potrebno je osigurati osim radnog prostora, opreme, i aktuelne programske alate s nužnim nadogradnjama, te stalno školovanje osoblja. Korišteni programski alati obično trebaju biti licencirani, bilo na ime agencije ili članova tima koji ju koriste.

U razvoju digitalne forenzike najvažniju ulogu imaju ljudski resursi. To podrazumijeva da bi zaposleni morali prvenstveno biti obrazovani sa iskustvom i da stalno rade na sopstvenom usavršavanju koje svakako nije samo iz oblasti informatike. To bi morali biti ljudi čije je znanje na vrlo visokoj ljestvici pravne regulative i informatike. Sadašnje stanje sajber kriminala u Bosni i Hercegovini zahtijeva da se ova naučna disciplina što brže, a i bolje uključi u sve zakonske propise i naravno da se što hitnije primjenjuje kako na tekuće probleme tako i na rješavanje i otkrivanje problema iz prethodni godina.

Kada je u pitanju valjanost digitalnih dokaza nije sporna ukoliko se slučaj rješava po propisima i metodama digitalne forenzike. Dokazi su mnogo ranjiviji od konvencionalnih fizičkih dokaza i zbog toga se prilikom rukovanja potrebno pridržavati određenih smjernica kako ih se ne bi uništilo ili oštetilo. Da se dokazi mogu lako izgubiti može se uočiti pri gašenju kompjutera i transporta u laboratorij radi provođenja temeljite analize. Svi

podaci nastali tokom rada računara, koji nisu pohranjeni na tvrdi disk, time su nepovratno izgubljeni. Naravno i nestručnim rukovanjem dokazi mogu biti oštećeni i tako obezvrijeđeni u potencijalnom sudskom postupku.

4. Zaključak

Digitalna forenzika će nastaviti da se razvija i postat će sigurno moćna tehnika za otkrivanje digitalnih dokaza. Da bi taj razvoj bio nesmetan potrebno je da ga prati zadovoljavajuća pravna regulativa u Bosni i Hercegovini i da ne predstavlja usporavajući faktor. Zemlje zapadne Evrope i SAD su odavno uočile ovu konstataciju i čine sve da pruže pravnu podršku digitalnoj forenzici.

U regulisanju ovog pitanja Bosna i Hercegovina daje određene napore, međutim nedovoljno, iz više razloga. Nadu budi prijedlog zakona o organizaciji i nadležnosti državnih organa za borbu protiv sajber kriminala kojim je predviđeno obrazovanje posebnih organizacionih jedinica koje bi se bavile krivičnim djelima predviđenim tim zakonom. Vjerovatno kao posljedica ovog prijedloga zakona, postoje informacije da će biti formirano posebno odjeljenje policije koje bi se bavilo sajber kriminalom i digitalnom forenzikom (trenutno radi SIPA i njihova Agenciji za forenzična ispitivanja i vještačenja - AFIV), kao i određene aktivnosti FUP. Dok se to sve ne ozvaniči ostaje konstatacija da kasnimo za razvijenim informatičkim državama i da bi se trebalo unaprijediti postojeće stanje. Dok se ne donesu pravni mehanizmi nama ostaje da radimo na unapređenju postojeće metodologije i tehnika. Problem sajber kriminala je kompleksan fenomen. Da bi se zaustavilo moguće širenje sajber kriminala, u zvaničnoj istrazi neophodno je uspostaviti multidisciplinarne timove za istragu, koji se sastoje od digitalnog forenzičara, pripadnika organa unutrašnjih poslova i tužilaštva. Za dokazivanje ovih elemenata neophodno je sprovesti adekvatne istražne radnje, analizirati način, vrijeme izvršenja djela i obim štete pomoću tehnika i alata digitalne forenzike i uspješno procesuirati ta djela u pravnom sistemu. U svemu tome najznačajniji doprinos ima upravo digitalna forenzika kao naučna disciplina koja daje precizne odgovore na pitanja koja se postavljaju kako u rješavanju problema izazvanih kompjuterskim kriminalom tako i u postupku preventivne zaštite mreže i kompjuterski sistema. Digitalna Forenzika nije samo svojstvena agencijama za sprovođenje zakona, nego je njena primjena danas velika i u organizacijama i poduzećima, gdje je potrebno uz metode digitalne forenzike, utvrditi neke činjenice, te dokazati na sudu dokaze koji trebaju biti prihvaćeni. Iako se digitalni dokazi , do prije nepunih nekoliko godina u našem okruženju , nisu niti priznavali u sudskim procesima, danas je situacija sasvim drugačija, jer ovi dokazi ukoliko se prikupe, i obrade spomenutim metodama, te prezentiraju uz pomoć propisanih procedura koji se forenzičari moraju da drže, tada su dokazi ravnopravni sa ostalim materijalnim dokazima.

Ovaj rad je nadamo se obezbjedio dovoljno detaljan opis najznačajnijih aktuelnih kretanja iz digitalne forenzike te može biti primjenljiv i koristan kako studentima za dalja istraživanja iz ovih oblasti, tako i stručnjacima iz sigurnosnih agencija i pravosuđa.

5. Literatura

- Albert J. Marcella i Robert S. (2002). *Greenfield Cyber Forensics,* CRC Press LLC
- Babić, V. (2009). *Kompjuterski kriminal,* Metodologije kriminalističkih istraživanja, razjašnjavanja i suzbijanja kompjuterskog kriminaliteta, Sarajevo.
- Beebe N. L. i Clark J. G. (2005). *A hierarchical*, objective-based framework for the digital investigations process, In Proceedings of the 2005 Digital Forensics Research Workshop. Bajraktarević M.iI Porobić M. (2012). *Cyber crime, pranje novca i finansijske istrage* – Sarajevo.
- Bunting S. i Wei W. (2006). *EnCase Computer Forensics*: The Official EnCE: EnCase Certified Examiner Study Guide, Indianapolis, IN: Wiley Publishing
- Caloyannides M. A. (2004). *Privacy Protection and Computer Forensics Second Edition*, Artech ouse Inc.
- Carrier B. (2002). *Open Source Digital Forensics Tools* - The Legal Argument, @tstake.
- Dragičević, D. (2004). *Kompjuterski kriminalitet i računarski sistemi*, Zagreb.
- Dowling., A. (2006). *Digital Forensics*: A Demonstration of the Effectiveness of The Sleuth Kit and Autopsy Forensic Browser.
- Kruse II G. W. i Heiser G. J. (2010). *Computer Forensics Incidend response essentials*, 14th printing, New York: Addison Wesley.
- Kipper G. (2007). *Wireless crime and forensic investigation*, Auerbach Publications Taylor & Francis Group.
- Leschke T. R. (2010). Shadow Volume Trash: *Recycle Bin Forensics for Windows 7 and Windows Vista Shadow Volumes,* U.S. Department of Defense Cyber Crime Institute.
- Milosavljević M. i Grubor G. (2009). *Istraga kompjuterskog kriminala metodološka* – tehnološke osnove, Univerzitet Singidunum, Beograd.
- McClure S., Scambray J. i Kurtz G. (2006). *Hakerske tajne*: zaštita mrežnih sistema, prevod petog izdanja, Mikro knjiga, Beograd.
- Prlja D. (2017): *Cyber kriminal*, predavanje održano na Pravnom fakultetu Univerziteta u Beogradu, 16.11.2017, dostupno na http//www.prlja.info/sk2008.pdf
- Rubin, J. (2003). *Teacher, doctor nabbed in porn probe Police make plea for resources to stop spread of 'evil'*, Staff reporter thestar.com, with files from Canadian press.
- Schweitzer D. (2003). *Incident Response* - Computer Forensics Toolkit, Wiley Publishing, Inc, Indianapolis
- Volonino L. i Anzaldua, R. (2008). „*Computer Forensics*",Wiley publishing.
- William D., Dopatka, A., Hills, M., Ginette L. i Nash, V. (2011). *Freedom of connection* – Freedom of expression The Changing Legal and Regulatory Ecology Shaping the Internet,
- Konvenciju o Sajber criminalu Vijeća Europe od 23.novembra 2011.godine („Službeni glasnik BiH",broj 06/06 Međunarodni ugovori), Član 1. stav 1.pod a).

- Krivični zakon Federaciji Bosne i Hercegovine,Službene novine Federacije BiH, broj 34/03, Sarajevo , 2003. godine.
- Krivični zakon Republike Srpske, Službeni glasnik Republike Srpske, broj 49, Banja Luka, 2003 godine.
- Krivični zakon Brčko Distrikta , *(Službene glasnik Brčko DC, broj 10/03),* 2003 godine.

Dokumenti i izvještaji:

- Advances in Digital Forensics II: IFIP International Conference on Digital Forensics, National Center for Forensic Science, Orlando, Florida, January 29-February 1, 2006.

Izvori gdje nedostaju autori:

- https://www.guidancesoftware.com/products/Pages/encase-forensic/overview.aspx
- http://www.dedoimedo.com/computers/helix.html 29.01.2015.
- http://www.e-fense.com/h3-enterprise.php 29.01.2015.
- http://www.sleuthkit.org/autopsy/v2/ 20.03.2015.
- http://www.emarketer.com/Article/Internet-Hit-3-Billion-Users-2015/1011602 15.9.2014
- http://www.scmagazineuk.com 20.02.2015.
- http://www.mediarecovery.pl/doc/encase-forensic/Detailed_Product_Description.pdf 17.03.2015.
- https://www.ncjrs.gov/pdffiles1/nij/199408.pdf

Kriminalističke teme
Zbornik radova
Godina XIX, Broj 5, 2019.
ISSN 1512-5505

PRETRESANJE UREĐAJA ZA AUTOMATSKU OBRADU PODATAKA I AUTOMATSKO RAČUNARSKO PRETRAŽIVANJE PODATAKA

SEARCH AND SEIZURE OF THE AUTOMATIC DATA PROCESSING DEVICE AND AUTOMATIC COMPUTER DATA SEARCH

Pregledni naučni rad

Ivanović Zvonko[405]
Žarković Milan[406]

Abstrakt

Inspiracija za rad i problem (i) koji se radom oslovljava (ju): U primeni novih metoda za otkrivanje izvršilaca krivičnih dela, sve više se, kao osnovni metodi, javljaju računarski metodi otkrivanja, pronalaženja i obezbeđenja digitalnih relikata krivičnih dela i njihovih izvršilaca ili veza sa njima.

Ciljevi rada (naučni i/ili društveni): U Republici Srbiji je nekoliko metoda prepoznato kao veoma ekstenzivnih i značajno zadirućih u slobode i prava građana, te su, iz tih razloga, oni i njihova primena definisani u okvirima dokaznih, odnosno, posebnih dokaznih radnji.

Metodologija/Dizajn: Konkretno u pitanju su pretresanje uređaja za automatsku obradu podataka, kao i automatsko pretraživanje podataka. Osnovni *ratio* ovakvog restriktivnog odnosa prema svemu što je tehnički naprednije nije nov u istoriji krivičnog zakonodavstva. Svaka nova metoda i mera je prema stavu zakonodavaca uvek prihvatana uz zadršku i sa značajnom rezervom. Ovakvo shvatanje i stav su razumljivi ali treba ukazati na neke aspekte takvog tretmana, koji nisu neophodni za pojedine aktivnosti u vezi sa digitalnim podacima. Ograničenja istraživanja/rada:

Opravdanost istraživanja/rada: Naime, ovakvim radnjama se teško mogu izmeniti sadržaji digitalnih podataka, a da se isto ne primeti od strane stručnog lica. Šta više, moguće je putem postojećih načina i metoda evidentiranje aktivnosti utvrditi svaku radnju koja je preduzeta na uređaju sa velikom preciznošću. Drugi razlozi tiču se obima podataka.

Rezultati/Nalazi: Kada se malo više udubi u značenje, domašaje, svrhu i logiku shvatanje restriktivnog odnosa prema ovim radnjama gubi smisao.

Generalni zaključak: U ovom radu pokušavamo da prikažemo značaj i domašaj ovih radnji i njihove limite – ograničenja i krajnje obuhvate, kako bi prikazali nepotrebnost limita kojima ih daruje zakonodavac.

[405] Vanredni profesor na KPU, e-mail:zvonko31@gmail.com
[406] Redovni professor na KPU, e-mail:milan.zarkovic@kpu.edu.rs

Ključne riječi:
automatsko računarsko pretraživanje podataka, pretresanje računara, digitalni dokazi, elektronsko okruženje, dokazne radnje

Abstract
In the implementation of new methods for the detection of perpetrators of criminal acts, the methods of detection, finding and providing digital relics of criminal offenses and their perpetrators or connections with them are becoming more and more the basic methods. In the Republic of Serbia, several methods have been recognized as very extensive and significantly embittered in the freedoms and rights of citizens, and for these reasons, they and their application have been defined within the frames of evidence or special evidentiary actions. Specifically, they include automatic data processing utensils (devices) search (or Scanning the automatic data processing device) as well as automatically searching already processed data. The basic ratio of such a restrictive relationship to everything that is technically more advanced is not new in the history of criminal legislation. Every new method and measure, according to the attitude of the legislators, is always accepted with delay and significant reserve. This understanding and attitude are understandable, but one should point out some aspects of such treatment, which are not necessary for certain activities related to digital data. When it comes to a little more meaning, scope, purpose, and logic, understanding the restrictive attitude toward these actions loses its meaning. Namely, such actions can hardly change the contents of digital data, without being noticed by an expert. What's more, it is possible through the existing ways and methods to record activities to determine any action taken on a device with high precision. Other reasons concern data volume. In this paper, we try to show the importance and scope of these actions and their limitations and ultimate coverage, in order to show the unnecessary limits imposed by the legislator.

Keywords
automatic computer search of data, computer search, digital evidence, electronic environment, evidence actions

Uvod

Potreba za inkriminisanjem radnji izvršenih protiv, odnosno, upotrebom računara – nastala je još u vreme kada su računari postali dostupni široj javnosti. U svetu, već 1973. godine, otpočinje se sa pravnim regulisanjem kompjuterskog kriminaliteta, kada je u Švedskoj donet propis koji poznaje krivično pravnu zaštitu od kompjuterskog kriminaliteta, gde je u čl. 21. predviđeno krivično delo „neovlašćeni programski pristup". Tako su, ostale države, implementirale i razvile sopstvene propise koji bliže uređuju ovu materiju. Tek kasnije dolaze u fokus i radnje kojima se pribavljaju dokazi u elektronskom vidu sa ovakvih uređaja.

Narodna skupština Republike Srbije je početkom 2009. godine, posebnim zakonima ratifikovala Konvenciju Saveta Evrope o visokotehnološkom kriminalu i Dodatni protokol uz

tu Konvenciju, koji se odnosi na inkriminaciju dela rasističke i ksenofobične prirode izvršenih preko kompjuterskih sistema, nakon čega su doneti i drugi važni propisi iz ove oblasti.

Poznato je da je Konvencija Saveta Evrope o visokotehnološkom kriminalu potpisana u Budimpešti 23. novembra 2001. godine[407], dok je Dodatni protkol koji se odnosi na inkriminaciju dela rasističke i ksenofobične prirode izvršenih preko kompjuterskih sistema[408] sačinjen u Strazburu 28. januara 2005. godine. Takođe, Republika Srbija je 16. aprila 2005. godine u Helsinkiju potpisala ovu Konvenciju o visokotehnološkom kriminalu i Dodatni protokol uz tu Konvenciju, ali ih sve do 2009. godine nije ratifikovala. Važan deo Konvencije o visokotehnološkom kriminalu posvećen je obavezama država da stvore normativne pretpostavke za uvođenje dodatnih procedura i ovlašćenja, kako bi se omogućilo efikasno otkrivanje i procesuiranje slučajeva kompjuterskog kriminala.

Konvencija o visokotehnološkom kriminalu, usvojena u Budimpešti, 23. novembra 2001, jer su države svesne rizika da se kompjuterske mreže i elektronske informacije mogu, takođe, koristiti za izvršenje krivičnih dela i da dokazni materijali koji se odnose na takve prestupe mogu biti uskladišteni u tim mrežana ili prenošeni preko njih. Konvencijom se, po prvi put, uvode pravne norme koje se tiču kršenja prava intelektualne svojine, prevara izvršenih korišćenjem računara, zloupotrebe maloletnika u pornografske svrhe, protivpravnog pristupa zaštićenom računaru i računarskoj mreži, presretanju podataka, takođe se propisuju i radnje i mere, kako materijalno, tako i procesnopravne prirode, koje su usmerene ka negativnom sankcionisanju društveno štetnog ponašanja u ovoj oblasti. Ovom Konvencijom omogućava se primena savremenih istražnih metoda prilikom otkrivanja i gonjenja izvršilaca krivičnih dela, kao što su pretraga računarskih mreža i presretanje računarskih podataka i ona, trenutno, predstavlja jedini međunarodno pravno priznati pravni instrument u oblasti visokotehnološkog kriminala. Konvencija Saveta Evrope o visokotehnološkom kriminalu pre svega se zalaže za usklađivanje domaćih materijalnih krivičnopravnih odredbi u oblasti računarskog kriminala i omogućavanje domaćem pravnom okviru da nadležnim državnim organima pruži ovlašćenja koja su neophodna za otkrivanje i gonjenje izvršilaca ovih krivičnih dela, kao i uspostavljanje brzog i efektivnog okvira međunarodne saradnje u ovoj oblasti. Sastoji se iz tri dela, pri čemu prvi sadrži materijalno pravne odredbe, drugi procesno – pravne, treći odredbe kojima se reguliše međunarodna saradnja. Cilj propisivanja materijalnopravnog okvira Konvencijom jeste poboljšanje zakonskih odredbi radi sprečavanja i gonjenja specifične vrste kriminaliteta koji se izvršava pomoću računara i u računarskom okruženju uz korišćenje računarskih mreža. Krivična dela koja su određena konvencijom su: neovlašćeni (protivpravni) pristup, neovlašćeno (protivpravno) presretanje, ometanje toka podataka, ometanje rada

[407] https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185 poslednji put pristupljeno 15.08.209. god.
[408] https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189 poslednji put pristupljeno 15.08.209. god.

računarskog sistema, zloupotreba uređaja, falsifikovanje izvršeno pomoću računara, prevara izvršena pomoću računara, krivična dela dečje pornografije (iskorišćavanja dece i maloletnika u pornografske svrhe), i krivična dela autorskih i srodnih prava.

Zemlje koje su ratifikovale Konvenciju obavezne su da donesu procesnopravne norme radi uspostavljanja i primene ovlašćenja, a čije će propisivanje biti u skladu sa domaćim pravnim okvirom. Ove odredbe mogu uključivati i takvu vrstu zaštitnih odredbi koje su na domaćem - nacionalnom nivou predviđene u okviru Ustava, pravnog poretka, sudskog i javnotužilačkog sistema, i slično.

Kada govorimo o procesnim odredbama, predviđeno je: 1. hitno čuvanje pohranjenih podataka, 2. hitno čuvanje i delimično otkrivanje podataka o saobraćaju, 3. naredbu za dostavljanje, 4. pretragu i zaplenu računarskih podataka, 5. prikupljanje podataka o saobraćaju u realnom vremenu, 6. presretanje podataka o saobraćaju.

U trećem odeljku, Konvencija sadrži odredbe koje se odnose na tradicionalne i računarski povezanepravne instrumente međusobne saradnje, tj. međunarodne saradnje u krivičnom pravu, kao i pravila zauspostavljanje takozvane „7/24“ mreže za hitno reagovanje radi omogućavanja brze i efektivne saradnje izmeđunadležnih organa strana potpisnica (Stamenković i dr. 2017:17).

Zakonodavni okvir

Narodna skupšina Republike Srbije usvojila je Zakon o potvrđivanju Dodatnog protokola uz Konvenciju o visokotehnološkom kriminalu ("Sl. glasnik RS", br. 19/2009) koji se odnosi na inkriminaciju dela rasističke i ksenofobične prirode izvršenih preko računarskih sitema, koji je objavljen 18. marta 2009. godine u Službenom glasniku Republike Srbije. U skladu sa Dodatnim protokolom pod pojmom "rasistički i ksenofobični materijal" označavaće se svaki pisani materijal, slika ili drugo predstavljanje ideja ili teorija koje zagovaraju, promovišu ili podstiču mržnju, diskriminaciju ili nasilje, protiv bilo kojeg pojedinca ili grupe pojedinaca, zasnovano na rasi, boji kože, naslednom, nacionalnom ili etničkom poreklu, kao i veri, ako se koriste kao izgovor za bilo koji od tih faktora. U poglavlju II pod nazivom „Mere koje treba da se preduzmu na nacionalnom nivou“ u članu 3. pod nazivom „Širenje rasističkog i ksenofobičnog materijala preko računarskih sistema“ u stavu 1. stoji da države potpisnice treba da usvoje zakonodavne i druge mere, neophodne da bi se kao krivično delo u domaćem pravu propisalo kao kažnjivo ako je izvršenosa namerom i protivpravno: širenjem ili na drugi način činjenjem dostupnim javnosti, preko računarskog sistema, rasističkog i ksenofobičnog materijala. U stavu 2. stoji da strana ugovornica može da zadrži pravo da krivična odgovornost ne postoji za ponašanje propisano u stavu 1. ovog člana, kada materijal, kako je propisano u članu 2. stav 1. zagovara, promoviše ili podstiče diskriminaciju, koja nije povezana sa mržnjom ili nasiljem, pod uslovom da su dostupni drugi delotvorni pravni lekovi. Takođe, stoji i da potpisnice mogu da zadrže pravo da ne primenjuju stav 1. ovog člana na one slučajeve diskriminacije za koje,

usled uspostavljenih načela u domaćem pravnom sistemu u vezi sa slobodom izražavanja, ne mogu da obezbede efikasne pravne lekove kako je pomenuto u stavu 2.

Napred navedenim se, između ostalog, propisuju i one radnje koje su osobene za govor mržnje na internetu, kao što je javno izlađanje poruzi lica ili grupe zbog pripadnosti određeno rasi, boji kože, veroispovesti, etičkog porekla ili drugog ličnog svojstva. Inkriminišu se radnje kojima se izaziva ili pospešuje nacionalna, veska ili rasna netrpeljivost među narodima ili etičkim zajednicama koje žive u Republici Srbiji.

Zakonodavac Republike Srbije je u periodu od aprila 2005. do marta 2009. godine usvojio više propisa u kojima je implementirao Konvenciju Saveta Evrope o suprotstavljanju sajberkriminalu, (kod nas odomaćenu kao visokotehnološki kriminal) CETS 185 i Dodatni protokol CETS 189 u naš pravni sistem. Najvažniji među njima su: Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala ("Sl. glasnik RS", br. 61/2005 i 104/2009), Krivični zakonik ("Sl. glasnik RS", br. 85/2005, 88/2005 - ispr., 107/2005 - ispr., 72/2009, 111/2009, 121/2012, 104/2013, 108/2014 i 94/2016), Zakon o odgovornosti pravnih lica za krivična dela ("Sl. glasnik RS", br. 97/2008), Zakonik o krivičnom postupku – ZKP ("Sl. glasnik RS", br. 72/2011, 101/2011, 121/2012, 32/2013, 45/2013, 55/2014 i 35/2019), Zakon o policiji ("Sl. glasnik RS", br. 6/2016, 24/2018 i 87/2018), Zakon o autorskim i srodnim pravima ("Sl. glasnik RS", br. 104/2009, 99/2011, 119/2012 i 29/2016 - odluka US), Zakon o elektronskim telekomunikacijama ("Sl. glasnik RS", br. 44/2010, 60/2013 - odluka US, 62/2014 i 95/2018 - dr. zakon), Zakon o elektronskom potpisu ("Sl. glasnik RS", br. 94/2017), Zakon o posebnim ovlašćenjima radi efikasne zaštite prava intelektualne svojine ("Sl. glasnik RS", br. 46/2006 i 104/2009 - dr. zakoni).

Krivični zakonik Republike Srbije sadrži određen broj krivičnih dela koji bi mogla biti obuhvaćena pojmom visokotehnološkog kriminala. Ova krivična dela možemo podeliti u dve grupe. Prvu grupu čine krivična dela kojima se povređuje sam sistem kompjuterske tehnologije oštećenjem ili uništenjem računarskog podatka ili programa, ili ometa njihovo korišćenje, ili se vrši neovlašćen pristup računarskoj mreži i obradi elektronskih podataka. U drugu grupu se ubrajaju dela kod kojih se koristi računarska tehnologija, kako bi se pomoću nje vršila krivična dela. Sva krivična dela iz ovih grupa čine se sa umišljajem.

Radi suzbijanja nedozvoljenih ponašanja u vezi sa upotrebom informacionih tehnologija kao *ultima ratio* u Krivičnom zakoniku u glavi 27. je propisano osam krivičnih dela protiv bezbednosti računarskih podataka

Zakonom o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala, po prvi put, se uspostavljaju zakonski okviri za uspostavljanje institucija za borbu protiv visokotehnološkog kriminala. Takođe, ovim zakonom uređuje se obrazovanje, organizacija, nadležnost i ovlašćenja posebnih organizacionih jedinica državnih organa radi otkrivanja, krivičnog gonjenja i suđenja za krivična dela određena ovim zakonom.

Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala primenjuje se radi otkrivanja, krivičnog gonjenja i suđenja za: 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 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;

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, u skladu sa članom 2. stav 1. ovog zakona.

U navedenim pravnim i instituciopnalnim okvirima u toku 2007. godine, u Ministarstvu unutrašnjih poslova Republike Srbije u Službi za borbu protiv organizovanog kriminala obrazovano je Odeljenje za borbu protiv visokotehnološkog kriminala. Ovo odeljenje sastoji se od dva odseka: Odsek za suzbijanje kriminaliteta u oblasti intelektualne svojine i Odsek za suzbijanje elektronskog kriminala.

Za postupanje u predmetima krivičnih dela na osnovu Zakona o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala nadležno je Više javno tužilaštvo u Beogradu za teritoriju Republike Srbije. U Višem javnom tužilaštvu u Beogradu obrazovano je posebno odeljenje za borbu protiv visokotehnološkog kriminala tj. Posebno tužilaštvo. Radom Posebnog tužilaštva rukovodi Posebni tužilac za visokotehnološki kriminal. Posebnog tužioca postavlja Republički javni tužilac iz reda zamenika javnih tužilaca koji ispunjavaju uslove za izbor za zamenika višeg javnog tužioca, uz pismenu saglasnost lica koje se postavlja. Prednost imaju zamenici javnih tužilaca koji poseduju posebna znanja iz oblasti informatičkih tehnologija. U Posebnom tužilaštvu pored rukovodioca angažovana su još dva zamenika Višeg javnog tužioca specijalizovana za ovu oblast kao i dva tužilačka savetnika uz prateće administrativno osoblje. Od osnivanja početkom 2006. godine zaključno sa 1. oktobrom 2011. godine, Posebno tužilaštvo za visokotehnološki kriminal je postupalo ili postupa u preko 1700 predmeta u okviru svoje nadležnosti[409].

U našem zakonodavstvu, primena specijalnih istražnih tehnika u dužem periodu bila ograničena samo na dostavljanje podataka o stanju poslovnih i ličnih računa osumnjičenih, ali samo za krivična dela za koja je propisana kazna zatvora od najmanje četiri godine. Zbog toga se pribavljanje elektronske pošte osumnjičenog, odnosno, okrivljenog od

[409] http://www.beograd.vtk.jt.rs/ poslednji put pristupljeno 20.08.2019.god.

internet provajdera, uz naredbu suda (po pravilu sudije za prethodni postupak), sprovodi na taj način što se vrši predaja pisama, telegrama i drugih pošiljki od strane subjekata registrovanih za prenos informacija, upućenih okrivljenom ili koje on odašilje, ako postoje okolnosti zbog kojih se može osnovano očekivati da će date pošiljke poslužiti kao dokaz u krivičnom postupku. Poštanska, telegrafska i druga preduzeća, društva i lica registrovana za prenošenje informacija su dužna da ovlašćenim službenicima policije omoguće izvršenje navedenih mera. Iako su se na ovaj način prikupljali dokazi postojali su problemi u praksi zbog specifičnosti načina pribavljanja dokaza za tako specifična krivična dela, budući da se do njih često često dolazi monitoringom na mreži u realnom vremenu (''*on line*'').

Za suzbijanje visokotehnološkog kriminala značajno je i to što u ZKP –u (član 147. stav 3.) u predmete koji se mogu privremeno oduzeti spadaju i uređaji za automatsku obradu podataka i oprema na kojoj se čuvaju ili se mogu čuvati elektronski zapisi. Lice koje se koristi ovim uređajima i opremom dužno je da organu koji vodi postupak, na zahtev suda, omogući pristup i da pruži obaveštenja potrebna za njihovu upotrebu. Ono što možemo odrediti kao nedostatak ovde je to da za propuštanje ove obaveze nije predviđena sankcija. Pre oduzimanja ovih predmeta organ koji vodi postupak će u prisustvu stručnog lica izvršiti pregled uređaja i opreme i popisati njihovu sadržinu. Najzad, ako korisnik prisustvuje ovoj radnji može staviti primedbe.

U teoriji je izražen i stav da je od posebnog značaja za borbu protiv visokotehnološkog kriminala mogućnost da sudija za prethodni postupak, na pisani i obrazloženi predlog javnog tužioca, naredi nadzor i snimanje telefonskih i drugih razgovora ili komunikacija drugim tehničkim sredstvima (npr. telefaksom, teleprinterom, pejdžerom, elekronskom poštom - Internetom i dr.) onih lica za koja postoji osnovana sumnja da su sama ili sa drugim licima izvršila određena krivična dela. S tim u vezi treba naglasiti da se za otkrivanje nekih od tipičnih dela visokotehnološkog kriminala može koristiti i mera računarskog pretraživanja podataka, koja je značajna zbog sve izraženije kompjuterizacije ličnih i drugih podataka, te velikih mogućnosti koji ti podaci pružaju u vezi pribavljanja dokaza. Ovu radnju, po naređenju sudije za prethodni postupak, sprovode: kriminalistiška policija, Bezbednosno-informativna agencija, Vojno-bezbednosna agencija, organi carinske službe ili drugi državni organi, odnosno druga pravna lica koja na osnovu zakona vrše određena javna ovlašćenja. Mera može trajati najviše tri meseca, a zbog neophodnosti daljeg prikupljanja dokaza može se izuzetno produžiti još najviše dva puta u trajanju od po tri meseca. Računarsko pretraživanje podataka sastoji se u automatskom pretraživanju već pohranjenih, ličnih i sa njima neposredno povezanih, podataka i njihovom automatskom poređenju sa podacima. Po svojoj suštini ovo je „ negativna raster“ potraga koja doprinosi eliminaciji određenih lica iz kruga osumnjičenih automatizovanim pretragama kroz policijske, administrativne i druge evidencije. Drugim rečima, ovaj metod eliminiše određena lica iz kruga onih koja se služe lažnim identitetom, tuđim kreditnim karticama i tome slično.

Računarsko pretraživanje podataka

Računarsko pretraživanje podataka i njihova elektronska obrada može se preduzeti ako postoje osnovi sumnje da je učinjeno krivično delo za koja je posebnim zakonom određeno da postupa javno tužilaštvo posebne nadležnost, ako se na drugi način ne mogu prikupiti dokazi za krivično gonjenje ili bi njihovo prikupljanje bilo znatno otežano. Izuzetno se može odrediti i ako postoje osnovi sumnje da se priprema neko od krivičnih dela za koja je posebnim zakonom određeno da postupa javno tužilaštvo posebne nadležnost, a okolnosti slučaja ukazuju da se na drugi način delo ne bi moglo otkriti, sprečiti ili dokazati, ili bi to izazvalo nesrazmerne teškoće ili veliku opasnost. Suština ovog metoda je slobodan pristup policije svim evidencijama koje se vode automatizovano, što odudara od načela zaštite prava na privatnost građana i informatičko samoodređenje.

Opšti uslovi za određivanje posebnih dokaznih radnji propisani su u čl. 161. ZKP-a. U literaturi se susreću shvatanja po kojima uslovi za primenu posebnih dokaznih radnji predstavljaju činjenični i pravni osnov za određivanje ovih radnji. Činjenični osnov predstavlja stepen verovatnoće (osnovi sumnje) da je određeno lice učinilo krivično delo za koje se ove dokazne radnje mogu odrediti. Standard na kome insistira Evropski sud za ljudska prava u svojim odlukama jeste usmerenost posebnih dokaznih radnji prema određenom licu za koje postoji sumnja da priprema ili je izvršilo krivično delo. Taj sud, prema objavljenim presudama, smatra da nacionalno zakonodavstvo koje se bavi specijalnim istražnim metodama mora da osigura adekvatne i efikasne garancije da neće doći do zloupotreba prilikom primene tih metoda. U tom smislu, nije dozvoljen opšti nadzor primenom ovih mera, već nadzoru mogu da budu izložene isključivo osumnjičene i „pretpostavljenje" kontakt osobe (European Court of Human Right, 2019). Pravni osnov za određivanje ovih dokaznih radnji, kao što je već navedeno, sadrži element restriktivnosti, dakle, ove radnje se mogu odrediti samo ako se na drugi način ne mogu prikupiti dokazi za krivično gonjenje ili bi njihovo prikupljanje bilo znatno otežano (Subotić, D, 2013). Neki autori, ipak, uslove za primenu posebnih dokaznih radnji identifikuju kao materijalne i formalne. Materijalni uslov odnosi se na vrste krivičnih dela za koje je dozvoljeno da se primeni radnja, kao i postojanje dokaznih poteškoća koje uskovljavaju primenu posebnih dokaznih radnji. Formalni uslov za primenu radnji sastoji se, takođe, od dva kumulativna elementa. Prvi element čini procesna inicijativa nadležnog javnog tužioca u vidu obrazloženog predloga, a prihvatanje predloga sudije za prethodni postupak, i to u formi naredbe za sprovođenje konkretne posebne dokazne radnje, drugi element formalnog uslova (Ignjatović, Škulić, 2010).

Mera se sastoji u računarskom pretraživanju već pohranjenih ličnih i drugih, sa njima neposredno povezanih podataka i u njihovom automatskom poređenju sa podacima koji se odnose na krivično delo iz čl. 162. st.1 tač. 1. i 2. ZKP i na osumnjičenog, da bi se kao mogući osumnjičeni isključila lica u pogledu kojih ne postoji verovatnoća da su povezana sa krivičnim delom. Naredba sadrži podatke o osumnjičenom, zakonski naziv krivičnog dela, opis podataka koje je potrebno računarski pretražiti i obraditi, označenje državnog organa koji je dužan da sprovede pretragu traženih podataka, obim i vreme trajanja posebne dokazne radnje.

Računarsko pretraživanje podataka može trajati najviše tri meseca, a zbog neophodnosti daljeg prikupljanja dokaza može se izuzetno produžiti još najviše dva puta u trajanju od po tri meseca. Sprovođenje računarskog pretraživanja podataka se prekida čim prestanu razlozi za njegovu primenu. Po završetku računarskog pretraživanja podataka državni organ, odnosno pravno lice dostavlja sudiji za prethodni postupak izveštaj koji sadrži: podatke o vremenu početka i završetka računarskog pretraživanja podataka, podatke koji su pretraženi i obrađeni, podatke o službenom licu koje je sprovelo posebnu dokaznu radnju, opis primenjenih tehničkih sredstava, podatke o obuhvaćenim licima i rezultatima primenjenog računarskog pretraživanja podataka. Sudija za prethodni postupak će izveštaj dostaviti javnom tužiocu. Ako javni tužilac ne pokrene krivični postupak u roku od šest meseci od dana kada se upoznao sa materijalom prikupljenim korišćenjem posebnih dokaznih radnji ili ako izjavi da ga neće koristiti u postupku, odnosno da protiv osumnjičenog neće zahtevati vođenje postupka, sudija za prethodni postupak će doneti rešenje o uništenju prikupljenog materijala. (Čl. 163).

O donošenju rešenja sudija za prethodni postupak može obavestiti lice prema kome je sprovedena posebna dokazna radnja iz člana 166. ZKP ako je u toku sprovođenja radnje utvrđena njegova istovetnost i ako to ne bi ugrozilo mogućnost vođenja krivičnog postupka. Materijal se uništava pod nadzorom sudije za prethodni postupak koji o tome sastavlja zapisnik.

Ako je pri preduzimanju posebnih dokaznih radnji postupljeno suprotno odredbama ovog zakonika ili naredbi organa postupka, na prikupljenim podacima se ne može zasnivati sudska odluka, a sa prikupljenim materijalom se postupa u skladu sa članom 84. stav 3. ZKP.

Digitalni dokazi

Sa razvojem tehnike i tehnologije pojavile su se novi načini njihove zloupotrebe, kao što je kompjuterski kriminalitet. Razvoj informacione tehnologije obeležava ogroman protok digitalnih podatakau vidu elektronskih (računarskih) zapisa, a koji se nalaze u računaru ili se prenose putem njega, a kao takvi mogu biti ključni dokaz u otkrivanju i dokazivanju zloupotrebe računara i računarskih mreža. Glavni cilj istrage u oblasti kompjuterskog kriminaliteta je, kao i slučaju klasičnog kriminala, izgraditi za pravosudne organe neoboriv ili čvrst dokaz krivice ili dokaz za oslobađanje osumnjičenog, i/ili pravedno sankcionisanje učinjenog dela. Direktan (neposredan) dokaz u slučaju kompjuterskog kriminala gotovo je nemoguće obezbediti, ali moguće je izgraditi čvrst digitalni dokaz, bez tzv. pukotina,od niza posrednih dokaza. Savremeni pojavni oblici kriminaliteta traže i inovacije u vezi sa metodikom otkrivanja krivičnih dela, odnosno pribavljanje dokaza u elektronskoj formi, odnosno elektronskih, softverskih ili kompjuterskih dokaza. Osnovna funkcija kompjuterskog sistema je obrada i distribucija podataka u elektronsku sredinu. Elektronski podaci 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 i tako sačuvati u neizmenjenom obliku, a da bi se čulno opazili, možemo ih preformulisati u čoveku čitljive oblike u tekst, fotografiju, video zapis, zvuk ili drugi oblik koji je pogodan za ljudsko opažanje i razumevanje (Komlen Nikolić i dr. 2010:217).

Može se uočiti da zapravo postoje dve kategorije elektronskih zapisa: one koje je računar generisao i one koji su u računaru samo arhivirani. U prvoj kategoriji elektronskih zapisa su oni zapisi koje je sam računar stvorio nezavisno od korisnika (npr. zapisi provajdera internet usluga koji se tiču identifikacije korisnika prilikom uključuvanja na mrežu). Drugu kategoriju čine zapisi koje je kreirao korisnik a koji se u računaru samo čuvaju (npr. e-mail poruke) (Banović, 2006).

U postupku prikupljanja i analize digitalnih dokaza potrebno je da svi generalni forenzički i proceduralni principi budu primenjivani; da pre, u toku i posle uzimanja digitalnih dokaza ni jedna preduzeta akcija ne dovede do izmene digitalnog dokaza; samo stručno lice može pristupi originalnom digitalnom dokazu, kada se za to ukaže potreba; sve aktivnosti koje se odnose na sakupljanje, skladištenje, pristup ili transfer digitalnih dokaza moraju biti potpuno dokumentovane, sačuvane i raspoložive zastavljanje na uvid, bilo kojoj zainteresovanoj strani u sporu; lice koje rukuje digitalnim dokaznim materijalom je odgovorno za sve aktivnosti u odnosu na digitalni dokaz, kada je isti u njegovom posedu; izuzeti dokazi se moraju dobro skladištiti.

Policijski službenik koji prikuplja dokaze sa računara ili računarske mreže, mora pravilno postupiti i prikupiti te podatake, u suprotnom ti podaci ne mogu biti iskorišćeni u sudskom postupku. Digitalni dokaz je kompjuterski podatak koji može potvrditi da je izvršeno krivično delo, ili ukazuje na uzročno – posledičnu vezu između krivičnog dela i žrtve, krivičnog dela i njegovog izvršioca. U većini slučajeva, kod ovakvih krivičnih dela, informacija koja je pohranjena na kompjuteru može biti jedini trag, koji će istragu odvesti na pravi put. Veoma mali broj ovakvih dokaza moguće je otkriti ''klasičnim alatima'', većina se otkriva samo posebnim alatima. 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. Na taj način se izbegavaju oštećenja koja bi mogla nastati na originalu prilikom istraživanja;
- pomoću pravilnih alata moguće je vrlo lako odrediti da li je digitalni dokaz menjan 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;
- digitalnim dokazima se može lako manipulisati.

Obezbeđivanje digitalnih dokaza

Da bi se došlo do čvrstih dokaza potrebno je na mestu događaja utvrditi šta se stvarno desilo, da li je nastala šteta i koliki je njen iznos, kao i da li je akt koji se desio, u stvari, krivično delo iz oblasti visokotehnološkog kriminala. Dokaze treba prikupljati na mestu događaja uz objektivan pristup. Policijski službenik koji prvi stigne na mesto događaja potrebno je da zna da se podaci ili informacije mogu izgubiti u toku procesa isključivanja računara i da mora obezbediti mesto događaja do dolaska stručnog lica koje će pre isključivanja računara pronaći i presnimiti potrebne podatke, jer se može desiti da se posle isključivanja ne može doći do njih (npr. vlasnik šifre za pristup odbija saradnju ili ga je nemoguće locirati). Takođe, podaci uskladišteni na hard disku se lako mogu izmeniti, a pojedinim podacima se može pristupiti samo u određeno vreme (npr. šifrovani podaci). Podaci se mogu koristiti kao dokazi u postupku samo ako su adekvatno izuzeti i ako zadovoljavaju kriterijume u sudskom veštačenju. U ovom slučaju posredni dokaz je onaj dokaz, koji se sakupi analizom samog softvera, računara i/ili računarske mreže, a da bi bio prihvatljiv za sud, mora biti takav da potvrđuje hipotezu o čvrstom dokazu, ili da je pobija.

Digitalni dokazi moraju zadovoljiti i sve ostale zahteve pravosudnih organa, koji se odnose na sudske dokaze i to:

- ako je potrebno koristiti kopiju, ona mora biti najbolja,
- ako je original na raspolaganju onda kopija ne važi,
- kopija može zadovoljiti sve zahteve za izvođenje dokaza ako postoji orginalna datoteka u računaru za upoređenje,
- sudski veštak za IT mora posvedočiti kako je kopija napravljena, kao i druge detalje rukovanja sa datotekom i kopijom.

Što se tiče procesnog aspekta, uviđaj je najznačajnija dokazna radnja koju preduzima organ krivičnog postupka po službenoj dužnosti, kada je za utvrđivanje ili razjašnjenje kakve važne činjenice potrebno neposredno opažanje organa postupka. Neposredno opažanje se vrši čulnim opažanjem, ali se mogu koristiti određena sredstva (kao što su hemijska sredstva, fotoaparat i sl.), koja omogućavaju da se tragovi učine vidljivim i da se fiksiraju. U tom cilju moguće je izvršiti određena merenja, opisivanjem, upoređivanjem i fiksiranjem, kako bi se mogao pribaviti relevantan dokaz. Ove aktivnosti organ postupka može raditi sam ili uz pomoć stručnih lica, čijom pomoći će on potpunije razumeti stanje i situacije na licu mesta.

Pored dokaznih radnji za otkrivanje i dokazivanje krivičnih dela koriste se i operativno taktičke ili potražne radnje a koje omogućavaju sprovođenje radnji koje imaju dokazni značaj.

Za prikupljanje dokaza najčešće se koristi uviđaj računara, a kako je zakonodavac uveo posebnu radnju pretresanja uređaja za automatsku obradu podataka, kao i opreme na kojoj se čuvaju ili se mogu čuvati elektronski zapisi (preduzima se na osnovu naredbe suda i, po potrebi, uz pomoć stručnog lica) postavlja se pitanje razlike između ove dve radnje. Pretresanje računara i uređaja nosilaca digitalnih tragova može se odrediti kao najširi oblik zahvatanja (zadiranja) u prava i slobode. Prema Zakoniku o krivičnom postupku ovo nije ni potražna radnja, ni posebna dokazna radnja, već dokazna radnja, i sprovodi se na osnovu naredbe suda (sudije za prethodni postupak) a na obrazloženi predlog javnog tužioca. Kao blaži oblik radnje koja zadire u slobode i prava čoveka sprovodio bi se uviđaj i to kao dokazna radnja. Prva radnja koja bi predstavljala vid najblažeg zadiranja u privatnost a sprovodila bi se nakon saznanja za delo i učinioca je radnja obezbeđenja mesta kriminalnog (krivičnog) događaja, kao preduslov vršenja uviđaja, kao potražna ili operativno – taktička mera i radnja. Najviši stepen uslova zadiranja u slobode i prava vezuje se za posebne dokazne radnje[410].

U cilju obezbeđenja dokaza moguće je pribaviti evidencije i podatke provajdera komunikacionih usluga. Sve korporacije koje obavljaju delatnost pružanjem internet usluga u cilju omogućavanja bilo kakvog oblika komunikacije trebalo bi smatrati „telekomunikacionim operaterima“. Zahtev za dobijanje podataka mora biti u skladu sa Zakonikom o krivičnom postupku i Zakonom o elektronskim komunikacijama.

Podaci o komunikaciji su:

- podaci kojim se utvrđuje identitet lica, sprave ili lokacije sa koje se komunikacija obavlja, obavljena je ili će biti;
- informacije u vezi lica koja koriste neku telekomunikacionu ili poštansku uslugu;
- informacije o licu kojem se pruža ili je već pružena telekomunikaciona ili poštanska usluga.

Zahtevi za dobijenje podataka o komunikacije upućuju se poštanskom ili telekomunikacionom operateru, preko Službe za specijalne istražne metode. Sadržaj komunikacije na osnovu Zakonika o krivičnom postupku se dobija upućivanjem zahteva nadležnom tužilaštvu, radi iniciranja posebne dokazne radnje i dobijanja Naredbe nadležnog suda. Policijski službenici mogu po osnovu Zakonika o krivičnom postupku (čl.161, 162) i Zakona o elektronskim komunikacijama (čl. 128) zahtevati podatke od veb satova koji obavljaju

[410] Reč je o radnjama koje su za nas u ovom radu značajne: automatskom računarskom pretraživanju ličnih i sa njima vezanih podataka i tajnom nadzoru komunikacija

delatnost „onlajn usluga". Veliki broj ovakvih usluga pružaju organizacije, koje se nalaze van naše države i u tom slučaju za dobijanje podataka potrebna je pomoć inostranih policijskih organa[411]. Da bi se sprečio gubitak podataka dok traje postupak međunaronih upita, preporučuje se da se vlasniku podataka (internet provajderu) izda Zahtev za očuvanje podataka kojim će se obavestiti koji su podaci potrebni. Na taj način se podaci čuvaju dok se ne dobije odgovarajući pravni dokument (međunarodna zamolnica za pružanje pravne pomoći). Zahtev za očuvanje podataka se upućuje preko kontakt tačke 24/7 pri Odeljenju za borbu protiv visokotehnološkog kriminala, ili preko Uprave za međunarodnu operativnu policijsku saradnju a u cilju ubrzanja postupka i obezbeđivanja podataka neophodnih za zamolnicu.

Sa razvojem tehnologije ljudi su počeli da svoje elektronske podatke skladište onlajn, jer im je taj način najjednostavniji za pristup sa bilo kog računara koji ima pristup internetu, mobilnog telefona, laptopa. Ovaj sistem skladištenja podataka naziva se „računarstvo u oblacima" (eng. *computer cloud*). U većini slučajeva kopije fajlova se ne čuvaju na personalnom računaru, već su čuvani u šifrovanom obliku na serverima (dok su na korisničkim računarima isti skladišteni samo restriktivno). Na ovaj način se najčešće skladište elektronske poruke i multimedijalni fajlovi. Prilikom obavljanja razgovora sa osumnjičenim licem, policijski službenik će ga pitati da i ima pristup bilo kom onlajn nalogu gde se mogu pohraniti elektronski podaci. Ukoliko da potvrdan odgovor, trebalo bi od njega tražiti saglasnost za pristup i kopiranje podataka. Ukoliko taj nalog sadrži pohranjene privatne poruke, policijski službenik, pored pristanka vlasnika tog naloga mora da postupi po odredbama iz čl. 152 st.3 i čl. 157 st.4 i st.5 Zakonika o krivičnom postupku, a koje se odnose na pretresanje uređaja za automatsku obradu podataka i sam postupak pretresanja.

Prilikom obavljanja razgovora sa oštećenim licem ili svedokom, potrebno je utvrditi da li poseduju ili kontrolišu neki uređaj, koji može sadržati elektronske dokaze. Kako su isti podložni oštećenju ili uništenju, potrebno je preduzeti mere kako bi se dokazala njihova dokazna verodostojnost. Policijski službenik bi trebao da od oštećenog lica ili svedoka zatraži da sarađuju i pristanu da se uređaj obezbedi kako bi se njegovim veštačenjem moglo doći do dokaza. U slučaju da polcijski službenik od navedenih lica ne dobije saglasnost, onda može da uređaj privremeno oduzme na osnovu čl. 147 st. 3 Zakonika o krivičnom postupku. Kada se policijski službenik zakonito nađe u prostorijama, može da oduzme svaki predmet za koji postoji osnovana sumnja da je dokaz krivičnog dela i da je njegovo oduzimanje neophodno kako bi se sprečilo da uređaj bude oštećen, sakriven, izmenjen ili uništen. Policijski službenik može zahtevati da materijal koji privremeno

[411] U ovakvim slučajeivma koriste se takozvani MLAT-i (*Mutal legal assistance act* – ili zamolnica za međunarodnu pravnu pomoć) koji se koriste u skladu sa zakonom o međunarodnoj pravnoj pomoći u krivičnim stvarima ("Sl. glasnik RS", br. 20/2009).

oduzima bude sačinjen u obliku koji omogućava lak prenos, jasnoću i čitljivost, odnosno da se napravi adekvatna kopija.

Pretresanje uređaja za automatsku obradu podataka i opreme na kojoj se čuvaju ili se mogu čuvati elektronski zapisi preduzima se na osnovu naredbe suda i, po potrebi, uz pomoć stručnog lica.

Kako bi bolje razumeli suštinu obezbeđivanja digitalnih dokaza potrebno je napraviti razliku između uviđaja kao dokazne radnje na računaru od pretresanja računara. Uviđaj računara jeste uviđaj pokretnih stvari koji sprovodi stručno lice u cilju sprečavanja nastanka nepovratnih izmena i oštećenja podataka u računaru, odnosno u mrežnom okruženju. Zakonikom o krivičnom postupku je prvi put regulisano pretresanje uređaja za automatsku obradu podataka i nosilaca digitalnih dokaza i vršenje uviđaja na stvarima. Pre nego što se pristupi uviđaju nad računarima, neophodno je prikupiti što više podataka o vrsti računarskog sistema, hardveru, softveru i operativnom sistemu, konfiguraciji računara uopšte, u cilju da se utvrdi gde su tražene informacije pohranjene i na koji način su obezbeđene.

Pretresanje predstavlja detaljniju radnju u odnosu na uviđaj, iako neminovno radnju uviđaja u većinislučajeva prati i pretresanje. Pretresanjem se direktno zadiranje u srž predmeta pretresanja. Tako se kod pretresanja računara, tableta, telefona ili drugih uređaja za obradu podataka, zadire u privatnost lica na taj način što se primeljuju mnoge alatke kojima se vrše detaljne pretrage uređaja tako što se pretražuju uređaji i sadržina svih memorijskih jedinica se kopira i čuva na nakom od uređaja za skladištenje podataka. To je moguće jer svaki uređaj ostavlja određeni digitalni trag na uređaju sa kojeg nešto izuzima, iako se mogu koristiti *write-blocker* uređaji, koji omogućavaju prikupljanje informacija na hard disku bez stvaranja mogućnosti slučajnog oštećenja sadržaja hard diska. Oni to rade tako što dozvoljavaju da pročitaju naredbe, ali blokiraju naredbe za pisanje, otuda i njihovo ime.

Pre nego što se otpočne sa pretresanjem policijski službenici će prikupiti što više informacija o vrsti, mestu i konekciji svakog računara. Od izuzetnog je značaja da svi policijski službenici koji prisustvuju pretresanju budu dobro informisani, kako ne bi neobučeni policijski službenici uništili ili oštetili dokaze. Pre početka pretresanja potrebno je proveriti da li torba za pretresanje mesta događaja tzv. „torba za upad“ sadrži odgovarajući materijal koji će se koristiti prilikom oduzimanja računara i drugih uređaja za pohranjivanje elektronskih podataka.

Prilikom uviđaja treba ispitati hardverske komponente, pretražiti kompjuterske datoteke i direktorijume, izraditi kopije podataka, zaštititi elektronske zapise koji mogu poslužiti kao dokaz. Uviđaj se sprovodi da se ne bi uticalo na uništenje, oštećenje izmenu tragova i predmeta nastalih izvršenjem krivičnog dela, pa ga je potrebno sprovesti što hitnije i objektivnije. Najveći problem koji se javlja u praksi jeste taj da se prilikom pretresanja

stana i ostalih prostorija zatiču uređaji za automatsku obradu podataka, a policijski službenici ne poseduju adekvatna znanja u vezi toga, pa može doći do uništenja dokaza. Kako bi se u praksi izbegao ovaj problem i definisala odgovornost lica za postupanje sa ovakvim dokaznim materijalom, kao i obezbeđenje lanca dokazivanja, doneta je obavezna instrukcija o prikupljanju elektronskih dokaza. Čuvanje podataka koji se nalaze u radnoj memoriji ovih uređaja RAM ili ROM memoriji je specifična jer oni sadrže informacije o poslednjim pregledanim materijalima sa interneta, odnosno skorijim izmenama pojedinih dokumenata, a njihova postojanost je kratka, pa namernim ili slučajnim gašenjem uređaja ili „čupanjem" iz naponskih instalacija radi prekidanja nekih procesa dolazi do nepovratnog gubitka ovih podataka. U ovakvoj situaciji samo stručno lice može preduzeti mere i, na taj način, bezbedno izuzeti dokaze i ono samo pomaže organu postupka da kvalitetno obavi uviđaj, dok je organ postupka taj koji neposredno opaža činjenice i konstatuje ih. Tragovi i predmeti do kojih se dođe prilikom uviđaja postaju predmet veštačenja, ali ukoliko organ postupka pre sprovođenja uviđaja proceni da bi prisustvo veštaka bilo od koristi za davanje nalaza i mišljenja, može na uviđaj pozvati i veštaka.

Prilikom uviđaja računara, za razliku od pretresanja, adekvatno i potpuno se evidentiraju sve mere i radnje na mestu i virtuelnom okruženju vršenja ove radnje. Na taj način se smanjuje verovatnoća prigovora na postupanje i omogućava se sprovođenje neophodnih analiza nakon vršenja uviđaja. Tako se na mestu događaja može izvršiti audio vizuelno snimanje aktivnosti stručnog lica dok vrši pregled, uviđaj računara ili pretresanje. Ovu radnju prati zapisnik i službena beleška radi potpunijeg objašnjenja postupanja. Organ postupka će angažovati lica koja imaju stručnost i specijalizovana znanja u postupanju sa uređajima za automatsku obradu podataka tj. digitalnim tragovima. Ovako obezbeđeni predmeti i tragovi, zabeleženo stanje računara, kasnije mogu poslužiti u veštačenju ali i pretresanju računara. Prilikom vršenja uviđaja stručno lice može da napravi idealnu kopiju računara, bez menjanja sadržaja ili drugog oblika uticaja na računar, koja može služiti za upoređivanje sa stanjem računara koji se pretresa u nekom kasnijem momentu. Prilikom vršenja uviđaja postoji verovatnoća da je propušten neki važan dokaz, pa se računar može privremeno oduzeti dok traje istraga. Sve prikupljene posredne dokaze treba obraditi kao da su deo celine uz jednaku važnost za dalji postupak, jer se samo na takav način može doći do neoborivog dokaza[412].

Pretresanje uređaja za automatsku obradu podataka i privremeno oduzimanje predmeta

[412] Postoje četiri opšta principa kojih se policijski službenici moraju pridržavati kako bi se sačuvali dokazi:
1. ne treba menjati datum na računaru ili uređaju za skladištenje podataka;
2. ukoliko stručno lice smatra a treba pristupiti prvobitnom datumu na računaru ili uređaju za skladištenje podataka, mora da pruži dokaz uz objašnjenje zašto je to relevantno i na šta ukazuje taj postupak;
3. trebalo bi napraviti i sačuvati trag svih postupaka primenjenih na elektronske dokaze sa računara. Bilo bi poželjno da nezavisna treća strana pregleda ove postupke i dobije isti rezultat;
4. policijski službenik koji zaduži predmet odgovoran je za postupanje ostalih po zakonu i ovim principima.

Privremeno oduzimanje predmeta predstavlja dokaznu radnju čijim se preduzimanjem obezbeđuju predmeti kao izvor materijalnih dokaza. Ova radnja je, često, usko povezana sa pretresanjem stana i lica, ali se može preduzeti i kao samostalna radnja. Cilj ove radnje jeste privremeno oduzimanje predmeta koji se po krivičnom zakoniku mogu oduzeti, kao i predmeti koji mogu poslužiti kao dokaz u krivičnom postupku.

Predmeti koji se po krivičnom zakonu imaju oduzeti jesu predmeti koji su upotrebljeni ili namenjeni za izvršenje krivičnog dela ili predmeti koji su nastali izvršenjem krivičnog dela. S druge strane, predmeti koji mogu poslužiti kao dokaz u krivičnom postupku jesu svi oni koji su nosioci tragova u vezi krivičnog dela ili učinioca. U ove predmete Zakonik izričito ubraja i uređaje za automatsku obradu podataka, kao i uređaje i opremu na kojoj se čuvaju ili se mogu čuvati elektronski zapisi. Da bi se moglo izvršiti pretresanje računara (Odnosno uređaja za automatsku obradu podataka - UAOP) potrebno je da postoji posebna naredba suda.

Lice koje drži predmete mora da omogući organu postupka pristup predmetima, kao i da pruži obaveštenja neohnodna za njihovu upotrebu i da ih preda na zahtev organa. Organ postupka može pregledati predmete, pre nego što se predmeti oduzmu, po potrebi, uz prisustvo stručnog lica. Lice može da odbije da omogući pristup predmetima, pruži obaveštenja koja su neohodna za njihovu upotrebu ili da ih preda, i u tom slučaju, javni tužilac ili sud, takvo lice, može kazniti novčano do 150.000 dinara, u slučaju da nakon toga odbije da ispuni svoju dužnost, može biti kažnjeno istom kaznom još jednom, na šta može uložiti žalbu, koja neće zadržati izvršenje rešenja, i o njoj odlučuje sudija za prethodni postupak ili veće. Ova odredba (čl. 148. ZKP) je od neverovatnog značaja za kasnije situacije. Naime, za pretresanje UAOP neophodno je da postoji naredba za pretresanje, lice treba da obezbedi uputstvo za upotrebu i pristup predmetima, a ako to ne uradi i odbije može biti kažnjeno.

Određene kategorije lica su oslobođene dužnosti da predaju predmete, pruže obaveštenja o njima i omoguće pristup. Tu se pre svega misli na okrivljenog, ali i na lice koje bi svojim iskazom povredilo dužnost čuvanja tajnog podatka ili profesionalne tajne.

Potvrda o oduzetim predmetima izdaće se licu od koga su predmeti oduzeti, koji će se vratiti držaocu kada se otklone razlozi zbog kojih su oduzeti, a nepostoje razlozi za njihovo trajno oduzimanje, ako je predmet neophodno potreban držaocu, uz obavezu da ga na zahtev organa postupka donese. Ako je predmet neophodno potreban držaocu, on mu se može vratiti i pre prestanka razloga zbog kojeg je oduzet, uz obavezu da ga na zahtev organa postupka donese (čl. 151 st. 1 i 2 ZKP). Pojedini predmeti će se vratiti i licu koje je učinilo krivično delo (npr. poklon, odnosno druga korist, koji budu oduzeti od lica koje je primilo mito mogu se vratiti davaocu mita, u slučaju da je učinilac krivičnog dela davanja mita dao mito na zahtev službenog lica i prijavio delo pre njegovog otkrivanja ili saznanja da je delo otkriveno – čl. 368 st. 6 KZ).

Detaljnim opisom predmeta koji se privremeno oduzimaju se predupređuju slučajne ili zlonamerne zamene predmeta veće vrednosti predmetom manje vrednosti, u cilju sticanja koristi, a stvaraju se i pretpostavke za eventualnu procenu i naknadu štete licu od koga je predmet oduzet, a za koji je doneta odluka da se mora vratiti vlasniku (u slučaju oštećenja ili gubitka predmeta).

U slučaju privremenog oduzimanja nosioca digitalnih podataka, odnosno uređaja za automatsku obradu podataka, fizički će se oduzeti nosilac podataka. Ukoliko je reč o digitalnim podacima koji se nalaze u računaru, pametnom telefonu, mrežnoj opremi korisnika, serverima koji nisu u posedu lica od kojeg se oduzimaju, javljaju se drugi načini postupanja. U ovom slučaju način pribavljanja digitalnih podataka, koji se privremeno oduzimaju je drugačiji, pa se tako pribavljanje digitalnih podataka realizuje kroz dokaznu radnju pretresanja uređaja za automatsku obradu podataka (odnosno računara), a može se primeniti dokazna radnja vršenja uviđaja na stvarima, ali do one granice u kojoj bi zatečen računar (telefon, mrežna oprema) mogao oduzeti i naknadno bi se pribavila naredba za pretresanje uređaja za automatsku obradu podataka, jer je samo radnja pretresanja uređaja za automatsku obradu podataka predviđena ZKP –om a ne i uviđaj, i to samo na osnovu naredbe suda. Pregledanje uređaja bi u tom slučaju predstavljalo potražnu aktivnost a koja mora prethoditi svakom oduzimanju predmeta. Zakonikom o krivičnom postupku predviđena je radnja privremenog oduzimanja uređaja za automatsku obradu podataka, pa se na taj način omogućava privremeno oduzimanje kojim se onemogućava menjanje i uticaj na podatke u uređaju a potom može uslediti pretresanje u prostorijama organa postupka, na osnovu naredbe.

Iako nije izričito propisano prisustvo dva punoletna svedoka (opštim pravilima pretresanja jeste ali ne kod pretresanja UAOP), prilikom pretresanja, a radi onemogućavanja zloupotrebe i izmene dokaza, poželjno bi bilo upotrebljavati adekvatne uređaje (komercijalizovana kombinovana softversko – hardverka rešenja, npr. EnCase[413]) koji bi predstavljali i sredstvo pretresanja i fiksiranja radnje – pošto ovakvi metodi sadrže digitalne zapisnike a, ujedno, predstavljaju i oblik nadzora nad vršenjem radnje pretresanja i na taj način bi se uvrstilo obavezno evidentiranje aktivnosti stručnih lica u postupku.

Pretresanje ovih uređaja, u širem smislu, predstavlja fizičko pregledanje spoljašnosti i (digitalne) sadržine uređaja za automatsku obradu podataka (i nosilaca digitalnih podataka) u cilju pribavljanja njihovih karakteristika i vršenja uvida, od strane stručnih lica, u oblike veza koje ti uređaji imaju sa drugim uređajima, i tada je, moguće vršiti privremeno oduzimanje uređaja za automatsku obradu podataka. Rok za započinjanje sprovođenja ove naredbe je isti kao i u slučaju svakog pretresanja 8 dana od izdavanja (čl.155 ZKP), ukoliko se ne počne sprovoditi organ postupka je dužan da je vrati sudu i pretresanje se ne može preduzeti. U svim opisanim slučajevima privremeno oduzimanje uređaja za automatsku

[413] https://www.guidancesoftware.com/ poslednji put pristupljeno 27. 08. 2019. god.

obradu podataka, kao i nosilaca digitalnih podataka, javlja se kao radnja fizičkog oduzimanja ovakvog uređaja.

Takođe, uređaje za automatsku obradu podataka nije neophodno po svaku cenu oduzimati, već je moguće, primenom forenzičkih mera, napraviti verne kopije, jer se ista svrha postiže i pravljenjem verne kopije ovakvog uređaja u datom trenutku u vremenu. Na ovaj način se celokupan sadržaj uređaja klonira i nakon toga moguće je pretraživanje uređaja različitim softverskim alatkama a za šta je potrebna naredba suda (tada se pravi više kopija, na kojima će se kasnije vršiti realno pretresanje). Ovakvo kopiranje stanja uređaja sa sobom nosi i konotaciju pretresanja računara - uređaja za automatsku obradu podataka. Tako da se u tom slučaju neće oduzimanjem računara ili mobilnog telefona lice lišiti mogućnosti njegovog korišćenja, pristupa Internetu, komunikacije sa bliskim licima.

U svakom slučaju pretresanje uređaja za automatsku obradu podataka se može sprovesti samo na osnovu naredbe suda a koja se izdaje na obrazložen predlog Javnog tužioca. Sadržaj takvog predloga ili zahteva za izdavanje naredbe mora odražavati smisao i potrebe izdavanja iste, te je u njemu značajno odrediti uređaje koji se imaju pretresati sa svim individualnim i grupnim karakteristrikama, iz kojih razloga se očekuje da se ovakvom radnjom mogu pribaviti dokazi i činjenice vezane za izvršenje krivičnog dela (osnovni uslov za pretresanje u čl.152. ZKP jeste verovatnoća da se pretresanjem mogu pronaći predmeti i tragovi odnosno određena lica), organe koji će u pretresanju učestvovati i u kom svojstvu. Iako se u većini slučajeva ne mogu precizno definisati predmeti i tragovi koji se mogu pronaći prilikom ovakvog pretresanja (na primer promena tipa datoteke), ovakvo precizno definisanje radnje omogućava da se pretresanjem ne zadire previše u privatnost lica.

Kod primene ove radnje uočava se da se Zakonikom nisu definisali uslovi pod kojima je moguće izvršiti radnju pretresanja uređaja za automatsku obradu podataka bez naredbe nadležnog sudskog organa. U cilju operativnijeg postupanja ovaj nedostatak bi se mogao otkloniti na taj način što bi se ova radnja predvidela Zakonikom o krivičnom postupku, čak i bez prisustva svedoka uz obavezno evidentiranje svih aktivnosti i njihovo fiksiranje kroz neki oblik zapisnika, audio vizuelnog snimanja i sl. Dakle, moguće je predvideti da se u sklopu uviđaja na uređajima za automatsku obradu podataka obavezno mora napraviti verna kopija svih raspoloživih memorija, a da se kasnije ista može, uz dodatne oblike sigurnosnog pristupa takvoj kopiji i analizirati. Naredbom za pretresanje uređaja za automatsku obradu podataka definišu se zadaci i subjekti koji u istom učestvuju uz predmete ka kojima je radnja pretresanja usmerena. U ovim slučajevima će odbrana angažovati stručnog savetnika, radi kontrole zakonitosti i poštovanja pravila postupanja organa gonjenja u slučajevima ovakvog pretresanja.

Pretresanje uređaja za automatsku obradu podataka, u užem smislu, podrazumeva pretraživanje računara uz pomoć različitih softverskih paketa, koji koriste pretrage datoteka u virtuelnom okruženju operativnog sistema računara, kao i drugim raspoloživim memorijama uređaja, na način kojim se konstatuju i pronalaze određene datoteke svi digitalni

elementi virtuelnog okruženja kao i pristupi uređaju, konekcije, oblici šifrovanih delova računara i njihova veličina i sl. Pregled računara predstavlja spoljašnji pregled uređaja i fiksiranje stanja na radnoj površini uređaja, konstatovanje postojećih veza na uređaju i aktivnih bežičnih veza u okruženju i samog uređaja kao i okruženje radnog prostora oko uređaja.

Da bi se obezbedio i očuvao dokazni kredibilitet oduzetih predmeta potrebno je poštovati sistem njihovog čuvanja i kontrolu manipulisanja. Sistem čuvanja podrazumeva označavanje, kategorizaciju, fotografsko i video snimanje, prikupljanje i pakovanje materijalnih dokaza, ali i postojanje pisanih podatka o službenim licima koja su postupala sa njima. Čuvanje takvih predmeta obezbeđuje organ postupka. Na ovaj način pruža se garancija da su dokazi koji se predstavljaju na sudu upravo oni koji su, kao takvi, prikupljeni na mestu događaja, odnosno pronađeni pretresanjem ili oduzeti od lica. Zbog toga se smatra da je u slučaju adekvatnog obezbeđivanja dokaznog materijala, gde se zahteva neraskidivi lanac dokazivanja (en. *chain of custody*) najbolje da se isti nalaze kod malog broja ljudi. Posebnu pažnju treba usmeriti ka oduzimanju i pakovanju onih predmeta koji su po svojoj prirodi izvor opasnosti. Za pojedine predmete, uz obavezu oduzimanja, zakonodavac predviđa i obavezu njihovog uništavanja: predmeti kojima je neovlašćeno iskorišćavano autorsko delo ili srodno pravo (čl. 199 st. 5 KZ), predmeti kojima je izvršeno neovlašćeno uklanjanje ili menjanje elektronske informacije o autorskom i srodnim pravima (čl. 200 st. 2 KZ), predmeti kojima je izvršena povreda pronalazačkog prava (čl. 201 st. 5 KZ).

Pretresanje uređaja za automatsku obradu podataka i opreme na kojoj se čuvaju ili se mogu čuvati elektronski zapisi

Pod automatskom obradom podataka podrazumeva se postupak obrade podataka automatskim sredstvima, pre svega računarima. Podaci koji se na ovaj način unose, kao i oni koji su dobijeni obradom, čuvaju se na memorijskim jedinicama. Uređajima za automatsku obradu podataka i opremi na kojoj se čuvaju ili se mogu čuvati elektronski zapisi, podrazumevamo svaki proizvod koji se koristi za obradu i/ili skladištenje elektronskih (digitalnih) podataka: računari (desktop, laptop, ili serveri), mobilni uređaji (pametni telefoni, Personal Digital Assistant - PDA, tableti, uređaji za satelitsku navigaciju...), memorijski medijumi (HD, CD/DVD, USB diskovi, SD kartice, ...), određena mrežna oprema (npr. modemi, ruteri, svičevi...), digitalne kamere, *Cloud Data* serveri i dr. Ovi uređaji se pretresaju kako bi se pronašle informacije u elektronskom (digitalnom) obliku koje imaju dokaznu vrednost, a koje su ili uskladištene ili prenesene u takvom obliku.

Postoje dve osnovne kategorije elektronskih podataka mogu činiti elektronski dokaz:

1. Nestalni (nepostojani, *Volatile*) podaci: - oni koji se nalaze u radnoj memoriji (RAM), ili se nalaze u prenosu, a gube se nakon isključivanja računara (npr. mrežni status i veze, aktivni procesi...);

2. Stalni (ali osetljivi) podaci uskladišteni na memorijskom medijumu (npr. na čvrstom disku - HD) i koji su sačuvani i nakon isključivanja računara. Neki od tih podataka se mogu lako izmeniti (npr. poslednje vreme pristupa), a nekima je moguće samo uslovno pristupiti (npr. podaci na šifrovanom disku koji su privremeno dostupni samo dok je računar uključen, a gde nakon isključenja i ponovnog startovanja računara njihova dostupnost zavisi od posedovanja odgovarajuće šifre).

Elektronski dokazi su podložni promeni, oštećenju, čak i uništenju usled nepravilnog rukovanja ili ispitivanja. Zato je neophodno preduzeti posebene mere postupanja kako bi ovakav, dokazni materijal, bio prihvatljiv za izvođenje u sudskom postupku u okviru dokaznih radnji.

Pretresanje uređaja za automatsku obradu podataka i opreme na kojoj se čuvaju ili se mogu čuvati elektronski zapisi, preduzeće se od strane stručnog lica i to:

1. u forenzičkoj laboratoriji ukoliko je izvršeno privremeno oduzimanje navedenih predmeta;
2. na licu mesta na uređaju koji je uključen (tzv. *live* forenzika), ukoliko u svom posedu ima za to specijalizovane alate.

Važno je napomenuti da, kada je god to moguće, stručno lice će napraviti forenzičku kopiju uređaja, tako da će se radi očuvanja originalnog dokaza, sve metode i alati za analizu elektronskih dokaza primenjivati na forenzičkoj kopiji, a ne na originalnom uređaju. Kako bi bila obezbeđena proverljivost dobijenih rezultata, po pravilu se prave dve forenzičke kopije - jedna radna i jedna rezervna. Istovetnost forenzičke kopije i originala potvrđuje se određivanjem njihovih heš (hash[414]) vrednosti koje moraju biti identične. Upravo ovakav forenzički postupak ukazuje na pravce o kojima je već obrazlagano ranije u radu.

Isključivanjem i oduzimanja uređaja radi njegove forenzičke analize, dolazi do gubitka velike količine nestalnih podataka. Zato se danas, pre isključenja računara, neophodnim smatra postupak čuvanja trenutnog sadržaja radne memorije (RAM-u), kao vrednog izvora kratkotrajnih i nestalnih informacija koje između ostalih mogu uključivati i: lozinke za šifrovane particije (TrueCrypt, BitLocker, PGP Disk), identifikacione podatke za prijavljivanje na različite naloge i servise (Gmail, Yahoo Mail, Hotmail; Facebook, Twitter, Google Plus; Dropbox, Flickr, SkyDrive, i dr.), spisak aktivnih procesa i sl. Za tu svrhu se mogu iskoristiti alati (koji se kao forenzički testirani i potvrđeni mogu pokrenuti sa DVD/CD-ROM ili USB uređaja) koji omogućavaju dampovanje sadržaja memorije bez unošenja bilo

[414] Više na https://en.wikipedia.org/wiki/Hash_function poslednji put pristupljeno 21.08.2019. god.

kakvih promena u elektronske podatke posmatranog uređaja (npr. Helix, Belkasoft Live RAM Caputer, AccessData FTK Imager, PMDump i dr.).

Ukoliko je iz bilo kojeg razloga nemoguće izvršiti privremeno oduzimanje uređaja za automatsku obradu podataka, pretresanje će se od strane stručnog lica obaviti na mestu događaja, primenom odgovarajućih forenzičkih alata, u postupku koji se naziva live forensics. U ovom slučaju, potraga za elektronskim dokazima sprovodi se u realnom vremenu, na uređaju koji radi. Ovakav postupak bi trebao biti pravilo, a ne izuzetak.

Zaključak

Prikazane radnje predstavljaju osnovne metode i sredstva u aktualnom suprotstavljanju organizovanom kriminalitetu, šta više, oni predstavljaju nezaobilazne dokazne odnosno posebne dokazne radnje u cilju pribavljanja dokaza. Njihov obim zadiranja u slobode i prava čoveka i građanina nije isti u svakom slučaju, ali ih zakonodavac u Srbiji veoma plastično etiketira. Kao što je prikazano, uslovi koji se vezuju za posebne dokazne radnje su značajnije oštro postavljeni u odnosu na "obične" dokazne radnje. U našem slučaju pretresanje UAOP ima i još značajnije garancije u odnosu na "obično" pretresanje stana i ostalih prostorija iako oba imaju karakter dokazne radnje, a još blaži su uslovi za sprovođenje radnje uviđaja koji je takođe dokazna radnja. Obrazloženja u vezi sa pooštravanjem uslova za pretresanje UAOP u odnosu na pretresanje stana i ostalih prostorija nikako nisu na mestu – naročito ako se ima u vidu ustavna garancija nepovredivosti stana, dok sama radnja pretresanja predviđa izuzetke od neophodnosti postojanja odluke suda za pretresanje stana i ostalih prostorija. Dakle, postoji protivrečnost u odnosima teorije i realnog stanja u Ustavu i zakoniku u pogledu odnosa prema ove dve procesne radnje. Isto bi trebalo promeniti kako i sugerišemo u ovom radu u pravcu propisivanja uslova za sprovođenje ove radnje i bez naredbe. Takođe, u pogledu radnje računarskog pretraživanja podataka opravdano su sniženi kriterijumi za primenu i pružena je mogućnost da širi set organa primenjuje ovu radnju, što je opravdano, sa stanovišta kako materije koju dotiče radnja, tako i sa aspekta delokruga organa kojima je povereno moguće vršenje.

Literatura:

1. Banović, B.: Elektronski dokazi, Revija za kriminologiju i krivično pravo, 2006. god, 3/ 06, str. 226
2. European Court of Human Right, CASE OF KLASS AND OTHERS v. GERMANY, Application no. 5029/71), JUDGMENT, STRASBOURG, 6, September 1978, <http://hudoc.echr.coe.int/eng?i=001-57510> 27. 8. 2019.
3. Ignjatović, Đ.; Škulić, M.; Organizovani kriminalitet, Beograd, 2010, str. 275
4. Komlen Nikolić, L. Gvozdenović, R. Radulović, S. Milosavljević, A. Jerković R. Živković, V. Živanović, S. Reljanović M. Aleksić, I.: Suzbijanje visokotehnološkog kriminala, Udruženje javnih tužilaca i zamenika javnih tužilaca Srbije, 2010, str. 217.
5. Stamenković, B. Živanović, S. Paunović, B. Stevanović, I: Vodič za sudije i tužioce na temu visokotehnološkogkriminala i zaštite maloletnih lica u Republici Srbiji, Pravosudna akademija, 2017, str. 17
6. Subotić, D.; Posebne dokazne radnje, Beograd, 2013, str. 126–127

Internet izvori:

1. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185 poslednji put pristupljeno 15.08.209.god.
2. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189 poslednji put pristupljeno 15.08.209.god.
3. http://www.beograd.vtk.jt.rs/ poslednji put pristupljeno 20.08.2019.god.
4. https://www.guidancesoftware.com/ poslednji put pristupljeno 27.08.2019.god.
5. Više na https://en.wikipedia.org/wiki/Hash_function poslednji put pristupljeno 21.08.2019.god.

Kriminalističke teme
Zbornik radova
Godina XIX, Broj 5, 2019.
ISSN 1512-5505

Panel 7

VIŠEKOMPONENTNI POGLED NA CYBER SIGURNOST

Kriminalističke teme
Zbornik radova
Godina XIX, Broj 5, 2019.
ISSN 1512-5505

NACIONALNA PLATFORMA REPUBLIKE SEVERNE MAKEDONIJE ZA IZGRADNJU SAJBER BEZBEDNOSTI

Pregledni naučni rad

Sašo MITEVSKI, Phd[415]
Blagojčo SPASOV, MA.[416]

SAŽETAK

Inspiracija za rad i problem (i) koji se radom oslovljava (ju): U okviru savremenog sveta, kao i u mnogim državama u svetu, Republika Severna Makedonija nije imuna na savremene rizike i pretnje. Posebna meta ugrožavanja predstavlja sajber infrastruktura objekata od bitnog značaja za bezbednost države koji su svakodnevno predmet napada različitih kriminalnih struktura.
Ciljevi rada (naučni i/ili društveni Fokus istraživanja koje će biti sprovedeno obuhvatiće sajber bezbednost i sajber kriminal u Republici Severnoj Makedoniji kao savremeni oblik savremenog ugrožavanja.
Metodologija/Dizajn: Istraživanje, utvrdiće indikatore koji ukazuju na pojavu i širenje sajber napada u Republici Severnoj Makedoniji poslednjih nekoliko godina kao i utvrđivanje sposobnosti bezbednosnog sistema da se suoči sa ovom vrstom savremenih pretnji, preko analize nacionalne strategije i zakonske regulative koja određuje ovu vrstu ugrožavanja.
Ograničenja istraživanja/rada: Počevši od činjenice da je Republika Severna Makedonija cilj savremenih oblika ugrožavanja preko različitih formi sajber napada, postoji potreba od ozbiljnog pristupa i ozbiljnog istraživanja faktora koji omogućuju pojavu i širenje sajber kriminala u Republici Severnoj Makedoniji.
Rezultati/Generalni zaključak: U analizi koja je napravljena prema dostupnoj literaturi koja određuje bezbednost, javna bezbednost je predstavljena kao funkcija države koja garantuje zaštitu građana, institucija i organizacija od rizika pretnje institucija i organizacija od rizika i pretnji njihovom funkcionisanju, blagostanju i postojanju.
Opravdanost istraživanja/rada: Opravdanost istraživanja se ogleda u potrebi da se prizna važnost uspostavljanja nacionalne platforme Republike Severne Makedonije za izgradnju sajber bezbednosti.

Ključne reči
sajber kriminal, sajber zaštita, bezbednost, nacionalna strategija, kritična infrastruktura

[415] Ministarstvo Unutrašnjih poslova Republike Severne Makedonije Saso_Mitevski@moi.gov.mk
[416] Ministarstvo Unutrašnjih poslova Republike Severne Makedonije blagojcospasov@yahoo.com

ABSTRACT

Within the modern world, like many other countries in the world, the Republic of North Macedonia is not immune to contemporary risks and threats. A special target of threat is the cyber infrastructure of facilities vital to the security of the state that are subject to attacks from various criminal structures on a daily basis.

Starting from the fact that the Republic of North Macedonia is a target of modern forms of endangerment through various forms of cyber attacks, there is a need for serious approach and serious research into the factors that enable the emergence and spread of cybercrime in the Republic of North Macedonia.

The focus of the research that will be conducted will include cyber security and cybercrime in the Republic of North Macedonia as a modern form of modern endangerment.

The survey will determine the indicators that indicate the emergence and spread of cyber attacks in the Republic of North Macedonia in the last few years, as well as determining the ability of the security system to deal with this type of contemporary threats by analyzing the national strategy and legislation that Determines this type of endangerment.

Key words

cyber crime, cyber security, security, national strategy, critical infrastructure.

UVOD

Ugrožavanje sajber bezbednosti danas ide u korelaciji sa brzim razvojom visoke tehnologije koja pravi komjuterske sisteme vrlo ranljive. Sajber zakane se svakim danom više i više nameću kao savremeni problem, zahvaljujući faktu da vladine i javne službe, industrije, delovni subjekti i finsnsijske institucije, se sve više temelje na informatičku mrežnu povezanost to jest korišćenje digitalnih podataka i prenos informacija.

Društva se grade na osnovu složenih kompjuterskih mreža i sistema koji praktično upravljaju ukupnom kritičnom infrastrukturom u državi. Upravo to podiže stepen rizika neovlšćenog pristupa, zloupotrebe i uništavanje informacija od strane širokog sprektra zainteresovanih strana.

Uobičajeno, ove kompjuterske napade vrše bivši radnici u postojećim kompanijama, vladini i nevladini subjekti kao i terorističke formacije ali i anonimni i nezavisni hakeri. Globalne kriminalne mreže stiču sve veću sposobnost da prodru u računarske sisteme podataka, gde su skaldirani ogroman broj suštinskih informacija, da bi ih preuzeli i neovlšćeno koristili. Prodiranje u kompjuterske sisteme daje kriminalcima priliku da pristupe i iskoriste sve dostupne lične, finansijske, komercijalne i vladine podatke. Sve to ostavlja prostor za manipulaciju sa najosjetljivijim segmentima u svakom društvu. Pojava komjuterskih virusa već omogućava potpuno narušavanje integriteta informatičkog sistema.

Korišćenje termina sajber bezbednost ne znači samo hakovanje računarskih sistema, krađu ili zloupotrebu ličnih podataka. U današnjem razvijenom svetu, ugrožavanje sajber bezbednosti, dovodi do direktne pretnje po nacionalnoj sigurnosti svake države. Ranjivost država u smislu sajber bezbednosti je činjenica da je ukupna kritična infrastruktura u jednom modernom društvu povezana sa nacionalnom ili međunarodnom kompjuterskom mrežom. To je dovoljan pokazatelj osjetljivosti i ranjivosti nacionalnih kapaciteta u smislu sajber pretnji. Nema potrebe da se komentariše šteta koja bi rezultirala javnom ili nacionalnom bezbednošću kao rezultat zanemarivanja ili nedovoljne izgradnje sajber bezbednosti u društvu.

Dosad navedene informacije predstavljaju jednu ozbiljniju potrebu za istraživanjem koje će se tumačiti kroz sadržaj ovog rada, a radi se o analizi i određivanju načina na koji se sajber bezbednost gradi i održava u Republici Severnoj Makedoniji i u Evropskoj uniji. Polazeći od osetljivosti i aktuelnosti ove predmetne problematike ovog naučnog istraživanja, rezultati koji će biti dobiveni biće plasirani u okviru Republike Severne Makedonije i šire kako bi doprineli razmeni iskustava i građenje kapaciteta za suočavanje sa sajber pretnjama i regionu pa i šire.

1. TERMINOLOŠKA DIVERGENCIJA POJMOVA BEZBEDNOSTI, SAJBER BEZBEDNOSTI, KOMPJUTERSKI KRIMINAL

Bezbednosna situacija je složeni fenomen koji daje pregled obema i intenziteta više elemenata koji zagrožavaju nacionalnu bezbednost (opasnosti, rizici i izazovi), koji u određeno vreme pojedinačno ili kombinovano utiču na bezbednost građana, zajednica ili specifične pretnje čak i državi. Bezbednosna situacija se sadrži od više faktora ili indikatora. Oni pokazuju kakva je bezbednosna situacija u vezi sa pitanjima javnog reda i mira, dinamika kriminala (koji utiče na ličnu bezbednost, bezbednost stečenih materijalnih dobara građana i društvene svojine), uticaj stranih elemenata na unutrašnju bezbednost, pretnje od ekstremističkih organizacija, razvoja bezbednosnih dešavanja u regionu i svetu, međunarodnih odnosa zemlje i drugih (Rajkovcevski, 2014).

Jedna od osnovnih funkcija države za postizanje svojih ciljeva je bezbednosna funkcija. Funkcija bezbednosti je prisutna od samog nastanka države, koja se konstantno razvija i usavršava (Dončev, 2007).

U analizi koja je napravljena prema dostupnoj literaturi koja određuje bezbednost, javna bezbednost je predstavljena kao funkcija države koja garantuje zaštitu građana, institucija i organizacija od rizika pretnje institucija i organizacija od rizika i pretnji njihovom funkcionisanju, blagostanju i postojanju (Mijalković, 2011).

Bezbednost kao fenomen, odnosno njeno tumačenje je veoma složeno i kompleksno, što omogućava postojanje različitih mišljenja i interpretacija ovog pojma (Kotovčevski, 2011).

Termin sajber bezbednost odnosi se na bezbednost u sajber prostoru a to je prostor (informatička mreža) koji je potreban da bi ta sajber bezbednost funkcionisala. Sajber spejs podrazumeva sve ono što se odnosi na komjutere, internet, mobilne uređaje i ostale pametne uređaje koji su vezani u nekoj mreži. Sajber prostor je pun kritičnih informacija neovisno o tome da li su to nečija privatna svojina ili svojina neke vladine institucije. Današnji načini komunikacije podrazumeva nezamislivo veliku razmenu podataka i informacija preko sajber prostora. Zbog toga bezbednost ovih informacija je od suštinskog značaja za njihovo prenošenje od početne tačke do krajnog korisnika.

Grupa renomiranih autora definiše ovaj komjuterski kriminal u užem i širem smislu, gde u užem smislu navode kompjuterske prevare, sabotaže, špijuniranja, a u šire značenje odnosi se na zloupotrebu kompjutera i njegovih komponenti od krađe, pronevere i slično (Šarkić, i ostali, 2011).

Autor Spasić., u svojoj definiciji o sajber kriminalu navodi da se radi o zločinu koji se odvija u digitalnom okruženju i predstavlja specifičan oblik nezakonitog ponašanja u kojem se računarska mreža pojavljuje kao sredstvo, meta ili dokaz za izvršenje krivičnog dela (Spasić, 2006).

Ulazak u kompjuterske sisteme daje kriminalcima mogućnost da pristupe i manipulišu ličnim, finansijskim, komercijalnim i vladinim podacima. Uvođenje kompjuterskih virusa može sasvim narušiti integritet sistemu sa podacima (Lajman.D.M., Poter.V.G, 2009).

U dostupnoj literaturi u kojoj ovi termini gravitiraju, može se odrediti razlika od nesuštinskog značaja u definiranju pojmova bez promene njenog pravog istinitog značaja.

2. MEHANIZMI EVROPSKE UNIJE ZA GRAĐENJE SAJBER BEZBEDNOSTI

Sajber bezbednost je od ključnog značaja za evropski prosperitet i evropsku bezbednost, sa razlogom da svakodnevni život i evropska ekonomija sve više zavise od digitalnih tehnologija. Incidenti u sajber bezbednosti su raznoliki iz aspekta ko je odgovoran i šta sa tim incidentima želi da postigne. Naglašene sajber aktivnosti ne samo da ugrožavaju evropsku ekonomiju, već su i usmerene prema digitalnom jedistvenom tržištu, a prodiru i u funkcionisanje evropske demokratije, slobode i vrednosti. Evropska bezbednost zavisi od stepena sposobnosti relevantnih nadležnih službi sa obzirom na činjenicu da se, civilna infrastruktura i vojni kapaciteti, oslanjaju na sigurne digitalne sisteme (EU Global strategy, II, 2018).

U mnogim izveštajima Evropske komisije zabeleženo je da sajber bezbednost u Evropskoj uniji može biti ugrožena od strane nedržavnih i državnih subjekata. Ugrožavanja sajber bezbednosti najčešće imaju krivičan, politički i strateški cilj, ali najradije je reč je o ugrožavanju zbog sticanja brze zarade i lakog profita. Kriminalni aspekat se pojačava približavanjem granice između kompjuterskog kriminala i "tradicionalnog" kriminala, budući da

kriminalci koriste internet kao način na koji povećavaju svoje aktivnosti, a isto tako i kao izvor za pronalaženje novih metoda i sredstava za izvršenje krivičnih djela. Evropsko iskustvo kaže da su u mnogim slučajevima šanse za praćenje kriminala minimalne, a šanse za krivično gonjenje još manje (European commission, 2017).

Mrežne infiltracije u tuđim kompjuterskim sistemima dovode do nezakonitog pristupa, objavljivanje privatnih podataka (povrede podataka) ili intelektualne svojine. Kao takvi su u stalnom porastu a, spominje se brojka od stotinu milijona zapisa globalno ugroženih svake godine. Kompromitovani podatci mogu se koristiti za razne kriminalne svrhe, uključujući prevaru i iznudu. Neke zemlje - članice potenciraju da su česta meta napada sektori ili mreže koje imaju podatke koji mogu biti "dobra zaradnja" (SOCTA, 2017).

Ovi državni i nedržavni subjekti koji postoje, deluju na području Evrope, sve više ispunjavaju svoje geopolitičke ciljeve ne samo korištenjem klasičnih alata kao vojne sile, već i putem sofisticiranih sajber alata, čime omogućavaju i mešanje u unutrašnje demokratske procese pojedinih zemalja. Korišćenje sajber - prostora kao domen ratovanja, bilo sam, ili kao deo hibridnog pristupa, sada je široko prihvaćen. Kampanje o dezinformacijama, lažnim vestima i sajber operacijama usmerene prema kritičnoj infrastrukturi su sve češće i zahtevaju odgovore. Iz tog razloga, u dokumentu u kome je tema razmišljanje o budućnosti evropske odbrane, neophodna je potreba za saradnju između nadležnih subjekta u državama u oblasti sajber odbrane (SOCTA: 2017).

U izveštaju Evropske komisije od 13.09.2017. godine, stoji da će se sajber rizik povećavati u suglasnosti sa digitalnim transformacijama. Očekuje se da će desetine milijardi uređaja sa "Internet stvarima" biti povezane na internet do 2020. godine, ali sajber bezbednost još uvek nije prioritet u njihovom dizajnu. Neuspeh proizvođača da zaštite uređaje koji će kontrolisati naše električne mreže, automobile i transportne mreže, fabrike, finansije, bolnice i domove mogu imati katastrofalne posledice i naneti veliku štetu poverenju potrošača u novim tehnologijama. Rizik od politički motivisanih napada na civilne ciljeve, kao i nedostatci u vojenoj sajber odbrani, još više produbljuju rizik (European commission: 2017).

Agencija Evropske unije za bezbednost mreža i informacija (ENISA) igra ključnu ulogu u jačanju sajber otpora u odgovorima na na temi sajber bezbednost Evropskoj uniji. Ona aktivno doprinosi u uspostavljanju visokog nivoa mrežne sigurnosti i informacija unutar Unije, od kada je osnovana od 2004. godine. Ona takođe doprinosi razvoju kulture bezbednosti mreže i informiranja u društvu i kako bi se podigla svest o bezbednosti o informacijama i mrežama, što zauzvrat dovodi do pravilnog funkcionisanja unutrašnjeg tržišta. Agencija u biti sarađuje sa zemljama – članicama i privatnim sektorom, gde daje savete i rešenja. Ona organizuje pan-evropske sajber-bezbednosne vežbe, razvoj nacionalne sajber-bezbednosne strategije i građenje kapaciteta, ali isto tako radi i studije za bezbedno prihvatanje i rešavanje pitanja vezana za zašitu podataka, tehnologije za poboljšanje privatnosti i privatnost novih tehnologija, identifikovanje sajber pretnje, pejzaže i drugo.

ENISA ujedno podržava razvoj i sprovođenje politike i zakona Evropske unije po pitanjima vezana sa bezbednosti mreža i informacija (ENISA: 2019).

Da bi poboljšao učinak agencije, Evropska komisija je predstavila ambiciozan predlog reforme, uključujući i stalni mandat za agenciju. Reforma će omogućiti agenciji da pruži podršku državama članicama, institucijama i preduzećima Evropske unije u ključnim oblastima, uključujući implementaciju Direktive o mrežnoj sigurnosti i informacionim sistemima i predloženog okvira za sertifikaciju sajber-bezbednosti (Directive 1148: 2016).

Reforma će omogućiti agenciji da ima snažnu savetodavnu ulogu u razvoju i implementaciji politika, uključujući promoviranje koherentnosti između sektorskih inicijativa i Direktive o sigurnosti i mreži, kao i pomoć u uspostavljanju centra za razmenu informacija i analiza u kritičnim sektorima. Očekuje se da će Agencija ojačati evropsku spremnost organiziranjem godišnjih pan-evropskih sajber bezbednosnih vežbi kombinirajući odgovor na različnom nivou. Takođe će podržati razvoj sertifikacije Evropske unije o sajber bezbednosti za politiku informacionih i komunikacionih tehnologija (IKT) i igraće važnu ulogu u jačanju operativne saradnje i upravljanje krizama širom Evropske unije. Agencija će također služiti kao žarišna točka za informacije i znanje u zajednici za kibernetičku sigurnost (European commission: 2017).

Na osnovu navedenih incidenata koji proizlaze iz sajber-bezbednosti mogli bi značajno uticati na funkcionisanje kritične infrastrukture Evropske unije kao i na svakodnevni život ljudi, tako da postoji potreba da se utvrdi mogućnost uspostavljanja tela za reagovanje u vanrednim situacijama koje izaziva sajber napad. Ovo telo može biti formirano koristeći model drugih alata Unije koji se pojavljuju iz upravljanja krizom, ali i drugih područja Evropske unije. Ovo će omogućiti državama članicama da traže pomoć na nivou Evropske unije tokom ili nakon velikog incidenta, pod uslovom da država članica uspostavi sistem sajber bezbednosti pre incidenta, uključujući punu implementaciju neophodnih direktiva, profesionalno upravljanje rizicima i nadzorne okvire na nacionalnom nivou. Takav fond, dopunjavajući postojeće mehanizme za upravljanje krizama na nivou Evropske unije, mogao bi primijeniti sposobnosti brzog reagovanja u interesu solidarnosti i finansirati specifične akcije reagiranja na katastrofe, kao što je zamjena ugrožene opreme ili primjena alata za ublažavanje ili odgovor, oslanjajući se na nacionalnu ekspertizu u skladu sa mehanizmom civilne zaštite Evropske unije (HIGH REPRESENTATIVE OF THE UNION FOR FOREIGN AFFAIRS AND SECURITY POLICY: 2017).

Europol je agencija za sprovođenje zakona u Evropskoj uniji i pomaže državama članicama u borbi protiv teškog međunarodnog kriminala i terorizma. Osnovana kao agencija Unije u 2009 –toj godini, Europol ili Evropska policijska kancelarija je srce evropske bezbednosne arhitekture i nudi jedinstveni spektar usluga. Europol je centar za poddršku policijskim operacijama, informativni centar o zločinima i centar za ekspertizu za sprovođenje zakona. Analiza je srž aktivnosti Europola. Kako bi svojim partnerima pružio dublje znanje o zločinima s kojima se suočavaju, Europol vrši redovne procjene koje nude sveobuhvatne, progresivne analize kriminala i terorizma u Evropskoj uniji (SOCTA: 2017).

U cilju održavanja visoke sajber-bezbednosti, Europol kao nadležni organ Evropske unije za suočavanje sa teškim i organizovanim kriminalom u 2013. godine uspostavio je Evropski centar za kibernetički kriminal kako bi ojačao implementaciju zakona o sajber kriminalu u Evropskoj uniji i na taj način pomoći u zaštiti evropskih građana, preduzeća i vlada od kriminala na internetu. Od svog osnivanja, Evropski centar za kibernetički kriminal je dao značajan doprinos borbi protiv sajber kriminala, bio je uključen u desetine operacija visokog profila i stotine operativnih priključaka, što je rezultiralo stotinama hapšenja i analizom stotina hiljada datoteka, od kojih je većina pokazala se zaraženom. Prema Evropskom centru za kibernetički kriminal, iako je teško dati pouzdane procene, neki izvještaji u industriji pokazuju da su globalni troškovi kibernetičkog kriminala stotine milijardi eura godišnje. Evropski centar za kibernetički kriminal svake godine objavljuje procenu pretnje s Interneta za organizirani kriminal putem strateškog izvještaja o ključnim nalazima i novim pretnjama i zbivanjima u oblasti kibernetičkog kriminala. Strateški izvještaj pokazuje koliko je širok i raznolik kompjuterski kriminal i kako je Evropski centar za kibernetički kriminal ključni deo Europola i odgovor EU. Evropski centar za kibernetički kriminal ima trostruki pristup u borbi protiv sajber kriminala: forenzike, strategije i operacije (EUROPOL: 2019).

U Evropskoj uniji postoji osećaj da će digitalizacija i povezivanje doneti veće rizike od kibernetičkog kriminala, što čini celim društvom osjetljivijim na kibernetičke pretnje, a osim društva i građana, oni se suočavaju sa sve većim opasnostima, uključujući ugrožene kategorije kao što su deca. Da bi se ovaj rizik ublažio društvu, evropske zemlje moraju preduzeti sve neophodne mere za poboljšanje sigurnosti u Uniji, kako bi bolje zaštitile mrežne i informacijske sisteme, telekomunikacijske mreže, digitalne proizvode, usluge i uređaje koje koriste građani, vlade i nevladine organizacije.

3. NACIONALNA STRATEGIJA REPUBLIKE SEVERNE MAKEDONIJE ZA SAJBER BEZBEDNOST

Republika Severna Makedonija je u proteklom periodu uložila ogromne napore da ojača sajber bezbjednost svojih građana, svojih nacionalnih kapaciteta i kritične infrastrukture. U tom pravcu, analiziran je veliki broj međunarodnih iskustava i sproveden je veći broj studijskih poseta u mnogim zemljama Evropske unije i šire u oblasti sajber bezbednosti. Koristeći dobijene informacije, na osnovu bogatog međunarodnog iskustva, stručnjaci iz oblasti Severne Makedonije doneli su Nacionalnu strategiju kibernetičke sigurnosti za period 2018-2022. godine i Akcioni plan za implementaciju Nacionalne strategije, koji su bili ključni dokumenti za poboljšanje sajber bezbednosti u državi za duži vremenski period. Nacionalna strategija pokriva sajber izazove i trendove, određuje principe sajber bezbednosti, definiše viziju, misiju i ciljeve nacionalne strategije, odnosno uspostavlja metodologiju za njihovu implementaciju u pravcu izgradnje sajber bezbednosti u Republici Severnoj Makedoniji. Postojanje strateških dokumenata vezanih za ovaj izazov je ključno u naporima za jačanje kapaciteta u oblasti sajber bezbednosti. Razvoj Nacionalne strategije za sajber bezbednost ima primarnu funkciju za poboljšanje okvirnih uslova u ovoj oblasti.

Potreba za razvojom i usvajanjem Nacionalne strategije za kibernetičku sigurnost uglavnom se odnosi na sljedeće: (NSSB 2018-2022: 2019).

1. Aktivnosti, društvene interakcije, ekonomija, kao i osnovna ljudska prava i slobode usko su povezani sa primenom informacionih i komunikacionih tehnologija, zbog čega je neophodno obezbediti otvoren, siguran i bezbedan sajber prostor;
2. Upotreba sistema informacionih i komunikacionih tehnologija i razvoj elektronskih usluga povećava rizik od sajber nezgoda i zloupotreba, čineći ove pretnje ozbiljnijim u pogledu na nacionalnu bezbednost;
3. Definiranje i razvoj politike sajber odbrane;
4. Uspostaviti integrirani, multidisciplinarni pristup kako bi se osigurala bliža saradnja i koordinacija između sektora odbrane i sigurnosti, institucija uključenih u borbu protiv sajber kriminala, privatnog sektora, građana i građanskih organizacija civilnog društva, kao i drugih relevantnih strana;
5. Jačanje operativnih kapaciteta, koordinacije i saradnje između relevantnih institucija i organizacija uključenih u borbu protiv sajber kriminala;
6. Uspostaviti zajedničke standarde, obuku i obrazovanje svih institucija i organizacija uključenih u razvoj sajber bezbednosti;
7. Jačanje institucionalnog i pravnog okvira u oblasti sajber bezbednosti;
8. Jačanje nacionalnih kapaciteta za prevenciju i zaštitu od sajber napada, kao i sprovođenje aktivnosti usmjerenih na podizanje nacionalne svesti o sajber bezbednosti.

Nacionalna strategija za poboljšanje sajber bezbednosti može se posmatrati kroz prizmu tekućih reformi u Republici Severnoj Makedoniji koje su u poslednjih nekoliko godina provedene u sferi sigurnosno-obavještajne zajednice. U ovoj oblasti već postoji u nacionalnom zakonodavstvu Operativna tehnička agencija OTA koja praktično proizilazi iz procesa reforme koji se provodi u Upravi za bezbednost i kontraobavještajne poslove pri Ministarstvu unutrašnjih poslova. Izgradnja nacionalne strategije za sajber bezbednost i implementaciju svih reformskih procesa u ovoj sferi predstavlja veliki korak napred za Republiku Severnu Makedoniju u njenim severnoatlantskim aspiracijama prema Evropskoj uniji.

Razvoj bezbednog društva i primena svih bezbednosnih praksi i procesa kroz saradnju svih zainteresovanih strana će obezbediti da preduzeća ostanu poverljiva i pristupačna korisnicima, i stoga profitabilna. Povećanje povjerenja građana u digitalne usluge i elektronsku trgovinu direktno će doprinijeti razvoju digitalne ekonomije. To će doprineti u prepoznavanju Republike Severne Makedonije kao sigurnog mesta za investicije i poslovanje (NSSB 2018-2022: 2019).

4. ZAKONSKA REGULATIVA U REPUBLICI SEVERNOJ MAKEDONIJI

U globalnom i regionalnom kontekstu, sajber pretnje predstavljaju opasan i moderan fenomen koji narušava opštu sigurnost u informativnoj sferi, čime se reflektirajuće ugrožava i javnost i nacionalna sigurnost. Kao takav, ovaj fenomen je pokriven krivičnim zakonom svake zemlje koja je usvojila mnoge zakone koji određuju mehanizme i načine zaštite od ovog globalnog fenomena. U Republici Severnoj Makedoniji, pretnje sajber bezbednošću najčešće se vrše kroz različite oblike kibernetičkog kriminala. Ove sajber pretnje se u zemlji smatraju novijim kriminalnim fenomenom koje se prema svojim karakteristikama razlikuju od drugih kriminalnih ponašanja, najčešće načinom kriminalne aktivnosti ili samog objekta krivičnog napada, gde su u većini slučajeva glavni cilj računarski sistemi i elektronski podaci.

Kompjuterizacija makedonskog društva stvara sve veću opasnost od njihove moguće zloupotrebe, što podrazumeva povećanje broja krivičnih dela u oblasti sajber sfere.

U nacionalnom zakonodavstvu u borbi protiv kompjuterskog kriminala u Republici Severnoj Makedoniji postoji Krivični zakonik, Zakon o praćenju komunikacija, Zakon o elektronskim komunikacijama i drugi relevantni zakoni.

Krivični zakonik u svom sadržaju određuje predmet u kojem je propisano sljedeće:[417]

1. Stavom 26. člana 122. propisano je da je kompjuterski sistem je bilo kakav uređaj ili grupa međusobno povezanih uređaja, od kojih jedan ili više obavlja automatsku obradu podataka u skladu sa određenim programom.
2. Stav 27. člana 122. propisuje da se pod terminom kompjuterski podaci podrazumevaju propisani fakti, informacije ili koncepti u obliku koji je pogodan za obradu putem kompjuterskog sistema, uključujući program sličan kompjuterskom sistemu za njegovo stavljanje u funkciju.

Član 149. odnosi se na zloupotrebu ličnih podataka kao što je predviđeno:[418]

1. Lice koje, suprotno uslovima utvrđenim zakonom bez saglasnosti građanina, prikuplja, obrađuje ili koristi tuđe lične podatke, biće kaznjen novčanom kaznom ili kaznom zatvora do jedne godine.
2. Kazna iz člana 149. stav 1. izriče se licu koje ulazi u informacioni sistem računara sa ličnim podacima koje ih namerno koristi za sebe ili za drugog da bi ostvarilo određenu korist ili prouzrokovalo štetu drugom.

---

[417] Krivični Zakon Republike Severne Makedonije, Službeni list, 80/99, 4/02, 43/03, 19/04, 81/05, 60/06, 73/06, 7/08, 139/08, 114/09, 51/11, 135/11 , 185/11, 142/12, 166/12, 55/13, 82/13, 14/14, 27/14, 28/14, 115/14, 132/14 (2019).
[418] Isto.

3. Ako je krivično delo iz stavova 1. i 2. ovog člana izvršeno od strane službenog lica u vršenju svoje dužnosti, kazniće se zatvorom od tri meseca do tri godine.
4. Pokušaj u vezi sa stavovima 1 i 2 takođe će biti kažnjiv.
5. Ako je delo iz ovog člana izvršeno od strane pravnog lica, kazniće se novčanom kaznom.
6. Šteta i neovlašćeni ulazak u kompjuterski sistem je takođe kažnjivo delo.

Član 251. ovog Zakona predviđuje:[419]

1. Lice koje neovlašćeno briše, menja, oštećuje, prikriva ili na drugi način čini neupotrebljive kompjuterske podatke ili program ili uređaj za održavanje informatičkog sistema ili otežava korišćenje komjuterskog sistema, podataka ili programa ili kompjuterske komunikacije, kazniće se novčanom kaznom ili kaznom zatvora do tri godine.
2. Stavom 4. člana 251. navodi se da će on / ona počiniti djela iz stavova (1), (2) i (3) ovog člana prema kompjuterskom sistemu, podacima ili programima zaštićenim posebnim zaštitnim merama ili korištenim u rad državnih organa, javnih preduzeća ili javnih institucija ili u međunarodnim komunikacijama ili kao član grupe koja je stvorena za vršenje takvih krivičnih dela, kazniće se zatvorom od jedne do pet godina.
3. Stav 1. člana 251-b propisuje: Osoba koja, sa namerom da pribavi nezakonitu imovinsku korist za sebe ili drugog, unoseći u računar ili informacioni sistem neistinite podatke, ne predstavljajući istinite podatke promenom, brisanjem ili suzbijanjem računarskih podataka, falsifikovanjem elektronskog potpisa ili na drugi način izazvati neistinit rezultat u elektronskoj obradi i prenosu podataka, kazniće se novčanom kaznom ili kaznom zatvora do tri godine.

Zakon o praćenju komunikacija proizilazi iz nacionalnog zakonodavstva koje ima veliki uticaj u smislu sprečavanja ugrožavanja sajber pretnji i definiše: proceduru za sprovođenje posebne istražne mere: praćenje i evidentiranje telefonskih i drugih elektronskih komunikacija, uslove i postupak za sprovođenje mera za praćenje komunikacija u cilju zaštite interesa sigurnosti i odbrane države, uključujući metapodatke, nadzor i kontrolu nad sprovođenjem mera monitoringa komunikacija, obaveza Operativno-tehnička agencija i telekom operateri.[420]

Prema članu 4. stav 7. ovog zakona, nadležni organi za sprovođenje mera za praćenje komunikacije radi zaštite interesa bezbednosti i odbrane države su: Ministarstvo unutrašnjih poslova - Uprava za bezbednost i kontraobaveštaj i Ministarstvo odbrane - Služba

[419] Isto.
[420] Zakon za praćenje komunikajcija, Službeni list RSM 71/18 (2019).

vojne bezbednosti i Inteligencija, a u delu frekvencijskog spektra radio-talasa na visokim, vrlo visokim i ultra visokim frekvencijama (HF, VHF i UHF), ovlašćeni organ za provođenje mjere za praćenje komunikacije je Centar za elektronski uvid Armije Republike Makedonije koji funkcioniše u službi odbrane države. Navedene vlasti su ovlašćene da sprovode mere za presretanje komunikacija u svrhu obavljanja delatnosti za koje su nadležne u skladu sa zakonom.[421]

Članom 18. ovog zakona definisane su mere praćenja komunikacija radi zaštite interesa sigurnosti i odbrane države: praćenje i evidentiranje telefonskih i drugih elektronskih komunikacija, praćenje i snimanje u unutrašnjosti zgrada, zatvorenih prostorija i objekata i ulazak u onim objektima, zatvorenim prostorijama i objektima, u cilju stvaranja uslova za sprovođenje mere, praćenja i svjetlosnog snimanja osoba na otvorenom prostoru i na javnim mestima i praćenja i audio snimanja sadržaja komunikacija osoba na otvorenom prostoru i na javnim mestima.[422]

Nalog za utvrđivanje mera za praćenje saopštenja iz člana 18. donosi nadležni sud u Republici Sjevernoj Makedoniji po prethodnom zahtevu nadležnih institucija koje imaju ovlaštenje za praćenje elektronskih komunikacija, odnosno Javnog Tužioca.

Imajući u vidu činjenicu da su informacije od vitalnog značaja za javnu i nacionalnu bezbednost u Republici Severnoj Makedoniji klasifikovanog karaktera, pomenut ćemo Zakon o klasificiranim informacijama koji je od suštinskog značaja za rešavanje sajber pretnji u smislu zaštite informacija sa stepenom klasifikacije zaštite informacija.

Svrha Zakona o klasifikovanim informacijama u Republici Severnoj Makedoniji je da se osigura zakonito korištenje tajnih podataka i da se spreči bilo kakav oblik nezakonitog pristupa informacijama, kao i da se utvrdi stepen zaštite informacija koje bi trebale odgovarati stepenu štete koja bi nastala za Republiku Severnu Makedoniju sa neovlašćenim pristupom ili neovlašćenim korišćenjem informacija. Informacije koje su predmet klasifikacije odnose se naročito na: javnu bezbednost; odbrane; inostrane poslove; bezbednosne, obaveštajne i kontraobaveštajne aktivnosti organa državne uprave Republike Makedonije; sistemi, uređaji, projekti i planovi od značaja za javnu bezbednost, odbranu, spoljne poslove; naučna i tehnološka, ekonomska i finansijska pitanja od značaja za Republiku Severnu Makedoniju.[423]

Zakon o elektronskim komunikacijama takođe ima veliki uticaj na izgradnju sajber bezbednosti u Republici Severnoj Makedoniji. Ovaj zakon predviđa: Podsticanje razvoja javnih elektronskih komunikacionih mreža i usluga u Republici Severnoj Makedoniji u cilju

---

[421] Isto.
[422] Isto.
[423] Zakon o klasifikovanim informacijama, Službeni list RSM, 09/04, 113/07, 145/10, 80/12, 41/14, 21/18 (2019).

osiguranja ekonomskog i društvenog razvoja; podsticanje korišćenja i razvoja širokopojasnog pristupa uslugama (broadband); zaštitu prava korisnika, uključujući krajnje korisnike sa invaliditetom i krajnje korisnike sa posebnim socijalnim potrebama; obezbeđivanje efikasne i održive konkurencije na tržištu elektronskih komunikacija; pružanje univerzalne usluge; efikasno korišćenje radiofrekvencijskog spektra i numeracije; promovisanje razvoja i podsticanje investicija u javne elektronske komunikacione mreže uvođenjem novih tehnologija i usluga, a posebno uvođenjem sledećih generacija javnih elektronskih komunikacionih mreža i obezbeđivanjem poverljivosti komunikacija.[424]

5. ULOGA MINISTARSTVA UNUTRAŠNJIH POSLOVA U SPREČAVANJU SAJBER PRETNJI

Ministarstvo Unutrašnjih Poslova u Republici Severnoj Makedoniji ima ključnu ulogu u ranom otkrivanju i suzbijanju sajber pretnji koje svakodnevno napadaju sajber strukture u Republici Sjevernoj Makedoniji. Nadležnosti Ministarstva unutrašnjih poslova proizilaze iz Zakona o unutrašnjim poslovima, Zakona o policiji i Zakona o presretanju komunikacija.

Prema Zakonu o unutrašnjim poslovima, Ministarstvo unutrašnjih poslova je odgovorno za: realizaciju sistema javne i državne bezbednosti; sprečavanje nasilnog rušenja demokratskih institucija utvrđenih Ustavom Republike Severne Makedonije; zaštitu života, lične sigurnosti i imovine građana; sprečavanje nanošenja nacionalne, rasne ili verske mržnje i netolerancije; sprečavanje izvršenja krivičnih dela i prekršaja, otkrivanje i hapšenje njihovih počinilaca i preduzimanje drugih mera propisanih zakonom za krivično gonjenje počinilaca tih dela; građanskim stvarima i drugim pitanjima utvrđenim ovim i drugim zakonima.[425]

Ministarstvo unutrašnjih poslova svoje nadležnosti obavlja preko Zavoda za javnu bezbednost i Direkcije za bezbednost i kontraobaveštajne poslove.

Preko Biroa za javnu bezbednost obavljaju se policijski poslovi, gde se u članu 5. Zakona o policiji predviđa: zaštita života, lične bezbednosti i imovine građana; zaštita sloboda i prava pojedinca i građana garantovanih Ustavom Republike Severne Makedonije, zakonima i ratifikovanim međunarodnim sporazumima; sprečavanje izvršenja krivičnih dela i prekršaja, otkrivanje i hapšenje njihovih počinilaca i preduzimanje drugih mera propisanih zakonom za krivično gonjenje počinilaca tih dela; utvrđivanje i traženje direktne i indirektne imovinske koristi stečene izvršenim krivičnim djelom; održavanje javnog reda i mira; regulisanje i kontrolu drumskog saobraćaja; kontrolu kretanja i boravka stranaca;

[424] Zakon o elektronskim komunikacijama, Službeni list RSM, 39/14, 188/14, 44/15, 193/15, 11/18, 21/18, (2019).
[425] Zakon o unutrašnjih poslova, Službeni list RSM, 42/14, 116/14,33/15 (2019).

granične kontrole i nadzor granica; pružanje pomoći i zaštita građana u slučaju potrebe; obezbjeđivanje određenih osoba i objekata i drugih aktivnosti utvrđenih zakonom. [426]

U okviru Biroa za javnu bezbednost postoji Odeljenje za prevenciju organizovanog i teškog kriminala, koje ima širok spektar nadležnosti i mehanizama za rano otkrivanje i sprečavanje sajber pretnji u zemlji, a ima i nadležnost da otkrije počinioce takvih nezakonitih radnji i njihovo lišavanje sloboda.

U prevenciji i suzbijanje sajber pretnji uključena su ministarstva unutrašnjih poslova, koja su sastavni dio Zavoda za unutrašnje poslove, gdje se redovnim policijskim stanicama pružaju redovne informacije građanima i njihovo upoznavanje s opasnostima koje proizlaze iz sajber zločina.

U Birou za javnu bezbednost kao zasebnu organizacisku strukturu postoji Sektor za kompjuterski kriminal i digitalnu forenziku, koji ima širok spektar nadležnosti u delu: (MUP RSM:2019).

- Efikasnu prevenciju;
- Otkrivanje počinilaca sajber kriminala;
- Pružanje odgovarajućih dokaza;
- Digitalnu forenziku;
- Krivično gonjenje počinilaca krivičnih dela;
- Pokretanje krivičnog postupka protiv počinilaca krivičnih dela u oblasti kompjuterskog kriminala;

Sektor za kibernetički kriminal i digitalnu forenziku je specijalizovana organizaciona struktura za borbu protiv ove vrste kriminala i trajno sarađuje sa regionalnim sektorima unutrašnjih poslova radi razmjene podataka i informacija za lica koja vrše ovu vrstu kriminala, pružanje stručne pomoći i direktno učešće u realizaciji potencijalnih slučajeva u koordinaciji sa Sektorom za unutrašnje poslove (MUP RSM: 2019).

Sektor za kibernetički kriminal i digitalnu forenziku takođe ima aktivnu međunarodnu saradnju u vezi sa Interpolovim i Europolovim odnosima, kao i sa drugim relevantnim međunarodnim bezbednosnim strukturama u cilju razmene informacija i ranog otkrivanja takvih zločina.

Uprava za bezbednost i kontraobaveštajnu službu iz člana 23. Zakona o unutrašnjim poslovima odgovorna je za vođenje unutrašnjih poslova vezanih za bezbednost i kontraobavještajnu delatnost koja se odnosi na: kontraobavještajnu delatnost; suzbijanje i zaštita od terorizma; zaštitu od drugih aktivnosti u cilju ugrožavanja ili prisilnog rušenja

[426] Zakon o policiji, Službeni list RSM, 114/06, 06/09, 145/12, 41/14, 33/15 (2019).

demokratskih institucija utvrđenih Ustavom Republike Severne Makedonije i težih oblika organizovanog kriminala koji potiču ili su usmjereni prema demokratskim institucijama sistema utvrđenih Ustavom Republike Sjeverne Makedonije i mogu dovesti do njihovog ugrožavanja ili uticaj na bezbednost države.[427]

Imajući u vidu gore navedeno, možemo zaključiti da Ministarstvo unutrašnjih poslova igra ključnu ulogu u prevenciji, otkrivanju i zadržavanju počinilaca kibernetičkog kriminala na teritoriji Republike Sjeverne Makedonije i šire putem razmene informacija i podataka sa nadležnim institucijama i agencijama na regionalnom i globalnom nivou.

ZAKLJUČNA SAGLEĐIVANJA:

1. Republika Severna Makedonija je potencijalna meta sajber napada, od raznih domaćih kriminalnih formacija, ali i od međunarodnih kriminalnih grupa;
2. Imajući u vidu da slučajevi sajber bezbednosti mogu značajno da utiču na funkcionisanje ekonomije, stabilnost i svakodnevni život ljudi, čini Republiku Severnu Makedoniju ranjivom u aspektu sajber bezbednosti;
3. Vlada Republike Severne Makedonije je razvila nacionalnu strategiju za sajber bezbednost za period 2018-2022;
4. Implementacija nacionalne strategije direktno zavisi od implementacije Akcionog plana za implementaciju strategije od strane Vlade RSM;
5. Evropske direktive o jačanju kapaciteta za bavljenje kibernetičkim pretnjama su veoma primenjive na implementaciju nacionalne strategije i takođe su obavezujući element za evroatlantske integracije Republike Severne Makedonije;
6. Nacionalna strategija za kibernetičku sigurnost mora se stalno nadograđivati u skladu sa nacionalnim prioritetima, direktivama i mehanizmima za sigurnost mreže i informacionih sistema u Evropskoj uniji;
7. Postoji potreba za povećanjem svijesti o sajber bezbednosti, preventivnim aktivnostima i razvoju programa veština, e-uprave i kampanja za podizanje znanja i veština u cilju sajber prijetnji;
8. Zaključivanje bilateralnih sporazuma sa proizvođačima informacionih tehnologija u cilju jačanja obuke o sajber bezbednosti za krajnje korisnike i olakšavanja pristupa njihovim proizvodima, uslugama i procesima biće od suštinskog značaja za poboljšanje sajber bezbednosti u Republici Severnoj Makedoniji i šire;
9. Republika Severna Makedonija ima zakonsku regulativu koja određuje ovu pojavu, ali joj je potrebna stalna dopuna kako bi ostala jednaka razvoju novih sajber prijetnji;

[427] Zakon unutrašnjih poslova, Službeni list RSM, 42/14, 116/14,33/15 (2019).

10. Kažnjena politika Republike Severne Makedonije predviđa visoke kazne i zatvorske kazne za počinioce ove vrste zločina, što je pokazatelj da se država zaista bori protiv ove negativne pojave;
11. Republika Severna Makedonija ima odgovarajuće institucionalne kapacitete za rano otkrivanje, poduzimanje zakonskih mera i ublažavanje štete na kritičnoj infrastrukturi uzrokovane kibernetičkim napadima;
12. Reforme u bezbednosno-obaveštajnoj zajednici u Republici Severnoj Makedoniji će pozitivno uticati na nadležne institucije za brz i efikasan odgovor na eliminisanje potencijalne sajber pretnje;
13. Ministarstvo unutrašnjih poslova je ključni faktor u bavljenju kibernetičkim pretnjama i garantuje neophodnu sajber bezbednost za sve građane na celoj teritoriji Republike Severne Makedonije.

KORIŠĆENA LITERATURA:

1. Dončev, A. (2007), Sovremeni bezbednosni sistemi, Aleksandar Dončev, Skopje.
2. Directive 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.
3. European Union, Serious and organized crime threat assessment, (2017), Crime in the age of technology, Europol.
4. Gillespie, A. A., (2015), Cybercrime: Key Issues and Debates Florence, Kentucky (USA)
5. Joint communication with the European Parliament and the Council, (2017) European commission, High representative of the union for foreign affairs and security policy, Brussels.
6. Kotovcevski, M., (2011), Nacionalna bezbednost, Filozofski fakultet, Skopje.
7. Lajman.D.M., Poter.V.G., (2009), Organiziran kriminal, Magor, Skopje.
8. Mijalković. V, S., (2011), Nacionalna bezbednost, Kriminalističko policijska akademija, Beograd.
9. Nacionalna strategija za sajber bezbednost na Republika Severna Makedonija (2018) 2018-2022, Vlada na RSM, Skopje.
10. Rajkovčevski, R., (2014), Gradenje bezbednosna politika: slučajot na Republika Makedonija, Fondacija Konrad Adenauer, Kancelarija Skopje.
11. Resilience, Deterrence and Defense (2017): Building strong cyber security in Europe, Tallinn Digital Summit.
12. Spasić, V., Aktuelna pitanja u oblasti sajber kriminala (članak), Bilten sudske prakse Vrhovnog suda Republike Srbije broj. 1/2006, Beograd.
13. Šarkić, N., Prlja, D., Damnjanović, K., Marić, V., Ţivković, V., Vodinelić, V., Mrvić-Petrović, N.: (2011), Pravo informacionih tehnologija, Beograd.

ZAKONSKA AKTA:

1. Krivični zakon Republike Severne Makedonije, Službeni list, 80/99, 4/02, 43/03, 19/04, 81/05, 60/06, 73/06, 7/08, 139/08, 114/09, 51/11, 135/11 , 185/11, 142/12, 166/12, 55/13, 82/13, 14/14, 27/14, 28/14, 115/14, 132/14 (2019).
2. Zakon o klasifikovanim informacijama. Službeni list RSM, 09/04, 113/07, 145/10, 80/12, 41/14, 21/18 (2019).
3. Zakon o praćenju komunikacija, Službeni list Republike Severne Makedonije 71/18 (2019).
4. Zakon o unutrašnjim poslovima, Službeni list Republike Severne Makedonije, 42/14, 116/14, 33/15 (2019).
5. Zakon o policiji, Službeni list Republike Severne Makedonije, 114/06, 06/09, 145/12, 41/14, 33/15 (2019).

6. Zakon o elektronskim komunikacijama, Službeni list Republike Severne Makedonije, 39/14, 188/14, 44/15, 193/15, 11/18, 21/18, (2019).

INTERNET STRANICE:

1. https://www.enisa.europa.eu/about-enisa,
2. https://www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme,
3. http://www.europarl.europa.eu/doceo/document/A-8-2018-0264_HR.pdf,
4. https://www.europol.europa.eu/socta/2017/introduction.html,
5. https://mvr.gov.mk,

Kriminalističke teme
Zbornik radova
Godina XIX, Broj 5, 2019.
ISSN 1512-5505

ZLOUPOTREBA SAJBER PROSTORA U IZBORNOM PROCESU KAO GLOBALNA POLITIČKA I SIGURNOSNA PRIJETNJA

ABUSE OF CYBER SPACE IN THE ELECTION PROCESS AS A GLOBAL POLITICAL AND SECURITY THREAT

Pregledni naučni rad

Bakreski Oliver, PhD[428]
Bardjieva Miovska Leta, MS[429]

Sažetak

Inspiracija za rad i problem (i) koji se radom oslovljava (ju): Sajber-prostor kao termin dobija potrebnu pažnju zbog svog ogromnog prostora, a istovremeno prazninu, kako za konstruktivne mogućnosti tako i za negativne implikacije.

Ciljevi rada (naučni i/ili društveni): Svrha ovog rada je da analizira i opiše zloupotrebu sajber prostora i sajber aktivnosti i njihovu povezanost sa izbornim procesima. Teorijska implikacija ima za cilj sagledavanje terminoloških odstupanja u smislu upotrebe i zloupotrebe sajber prostora i druge veze sajber bezbjednosti sa izbornim procesom kao globalne političke i bezbjednosne prijetnje.

Metodologija/Dizajn: Primenjena metodologija će omogućiti neophodnu analizu i sintezu otvorenih pitanja vezanih za sajber prostor i njenu zloupotrebu iz suštinskog, pragmatičnog i sadržajnog aspekta.

Ograničenja istraživanja/rada: Ograničenja istraživanja su u domenu institucionalnih kapaciteta za sprečavanje i iskorjenjivanje ovih aktivnosti.

Rezultati/Nalazi: Rezultati ili nalazi sastoje se od opšte situacije i dimenzije sajber prijetnji koje se mogu usmjeriti u samu srž demokratskih procesa.

Generalni zaključak: Kada je u pitanju rješavanje pitanja vezanih za sigurnost, Direktiva Član 19. definiše da zaštita fizičkih lica u pogledu obrade ličnih podataka od strane nadležnih organa u svrhu sprečavanja, istrage, otkrivanja ili krivičnog gonjenja krivičnih djela ili izvršenja krivičnih sankcija, uključujući zaštitu od i sprečavanje prijetnji javnoj sigurnosti i slobodno kretanje takvih podataka, predmet je posebnog pravnog akta Unije. Stoga se ova Uredba ne bi trebala primjenjivati na aktivnosti obrade u te svrhe. Međutim, lični podaci koje obrađuju javni organi prema ovoj Uredbi trebali bi se, kada se koriste u te svrhe, regulirati specifičnijim pravnim aktom Unije, naime Direktivom (EU) 2016/680 Europskog parlamenta i Vijeća.

Opravdanost istraživanja/rada: Planiranje oporavka od katastrofe pretpotstavlja proces koji uključuje procjenu rizika, određivanje prioriteta, razvoj strategija oporavka u situacije katastrofe. Svaka institucija i privatnih preduzeća treba da

[428] oliverbakreski@yahoo.com
[429] Institut za bezbjednost, odbranu i očuvanje mira. lbardjieva@gmail.com

ima pripremljen plan oporavka od katastrofe kako bi se što pre nastavio sa normalnim funkcionisanjem nakon katastrofalnih situacija.

Ključne reči
bezbjednost, sajber bezbjednost, izbori, strano miješanje, lažne vesti

Abstract
Reason for writing and research problem (s): Sajber-prostor kao termin dobija potrebnu pažnju zbog svog ogromnog prostora, a istovremeno prazninu, kako za konstruktivne mogućnosti tako i za negativne implikacije.
Aims of the paper (scientific and/or social): Svrha ovog rada je da analizira i opiše zloupotrebu sajber prostora i sajber aktivnosti i njihovu povezanost sa izbornim procesima. Teorijska implikacija ima za cilj sagledavanje terminoloških odstupanja u smislu upotrebe i zloupotrebe sajber prostora i druge veze sajber bezbjednosti sa izbornim procesom kao globalne političke i bezbjednosne prijetnje.
Methodology/Design: Primenjena metodologija će omogućiti neophodnu analizu i sintezu otvorenih pitanja vezanih za sajber prostor i njenu zloupotrebu iz suštinskog, pragmatičnog i sadržajnog aspekta.
Research/Paper limitation: Ograničenja istraživanja su u domenu institucionalnih kapaciteta za sprečavanje i iskorjenjivanje ovih aktivnosti.
Results/Findings: Rezultati ili nalazi sastoje se od opšte situacije i dimenzije sajber prijetnji koje se mogu usmjeriti u samu srž demokratskih procesa.
General Conclusion: Kada je u pitanju rješavanje pitanja vezanih za sigurnost, Direktiva Član 19. definiše da zaštita fizičkih lica u pogledu obrade ličnih podataka od strane nadležnih organa u svrhu sprečavanja, istrage, otkrivanja ili krivičnog gonjenja krivičnih djela ili izvršenja krivičnih sankcija, uključujući zaštitu od i sprečavanje prijetnji javnoj sigurnosti i slobodno kretanje takvih podataka, predmet je posebnog pravnog akta Unije. Stoga se ova Uredba ne bi trebala primjenjivati na aktivnosti obrade u te svrhe. Međutim, lični podaci koje obrađuju javni organi prema ovoj Uredbi trebali bi se, kada se koriste u te svrhe, regulirati specifičnijim pravnim aktom Unije, naime Direktivom (EU) 2016/680 Europskog parlamenta i Vijeća.
Research/Paper Validity: Planiranje oporavka od katastrofe pretpotstavlja proces koji uključuje procjenu rizika, određivanje prioriteta, razvoj strategija oporavka u situacije katastrofe. Svaka institucija i privatnih preduzeća treba da ima pripremljen plan oporavka od katastrofe kako bi se što pre nastavio sa normalnim funkcionisanjem nakon katastrofalnih situacija.

Keywords
security, cyber security, elections, foreign interference, fake news

1. Uvod u sajber bezbjednost i sajber kriminal kao globalnu prijetnju - opće odredbe

Pojam sajber sigurnost, također nazvan informacijska sigurnost, aludira na primjenu integriteta, pouzdanost, poverljivost i dostupnost informacija. Sajber bezbjednost sadrži evoluirajući skup mehanizama, pristupa upravljanju rizikom, tehnologijama, obukom i najboljim praksama dizajniranim da zaštite mreže, uređaje, programe i podatke od napada ili neovlaštenog pristupa.[430]

Merriam Webster rečnik definiše pojam sajber bezbjednosti kao mjere koje se preduzimaju za zaštitu računara ili računalnih sistema od neovlašćenog pristupa ili napada.[431]

Sajber bezbjednost ili bezbjednost informacija su tehnike i tehnologije koje se primjenjuju za zaštitu podataka, računara, mreža i programe od napada i aktivnosti sa svrhom eksploatacije.[432] Sajber bezbjednost se može dalje kategorizovati u sljedećim oblastima: bezbjednost informacija, bezbjednost aplikacija, bezbjednost mreže i oporavak od katastrofe.

Informacijska sigurnost štiti informacije od neovlaštenog pristupa kako bi se spriječila krađa identiteta i kako bi se osigurala zaštita privatnosti. Najčešće tehnike koje se primjenjuju u ovom smjeru su:

- Identifikacija korisnika, autentifikacija i autorizacija
- Kriptografija

Bezbjednost aplikacije obuhvata mjere i kontra mjere koje se primjenjuju tokom razvoja aplikacija i njihovog životnog ciklusa kako bi se zaštitile od prijetnji koje se javljaju zbog nedostataka u dizajnu, razvoju, nadogradnji ili održavanju aplikacije. Osnovne mjere za sigurnost aplikacije su:

- Provjera ulaznih parametara
- Autentikacija i autorizacija korisnika / uloga
- Upravljanje sesijama i manipulacija parametrima i upravljanje iznimkama
- Auditing i logging

---

[430] What is Cyber Security? Cyber Security Defined, Explained and Explored. https://www.forcepoint.com/cyber-edu/cybersecurity (11.05.2019)
[431] Cyber Security. Definition of Cyber Security. Merriam Webster. https://www.merriam-webster.com/dictionary/cybersecurity (07.06.2019)
[432] Definition of "Cyber Security". The Economic Times. https://economictimes.indiatimes.com/definition/cyber-security (05.05.2019)

Sigurnost mreže odnosi se na aktivnosti koje se poduzimaju radi zaštite i osiguranja korištenja, pouzdanosti, integriteta i sigurnosti mreže. Efikasna mrežna bezbjednost pokriva zaštitu od različitih prijetnji i spriječava ih da prodire mrežu ili se šire u njoj. Komponente mrežne sigurnosti su sledeće:

- Anti-virus i anti-spyware
- Zaštitni zid kao blokada za neovlašteni pristup u mreži
- IPS - Sistemi za sprečavanje upada za brzo prepoznavanje prijetnji
- VPN - Virtualne privatne mreže koje pružaju siguran daljinski pristup.

Planiranje oporavka od katastrofe pretpotstavlja proces koji uključuje procjenu rizika, određivanje prioriteta, razvoj strategija oporavka u situacije katastrofe. Svaka institucija i privatnih preduzeća treba da ima pripremljen plan oporavka od katastrofe kako bi se što prije nastavio sa normalnim funkcionisanjem nakon katastrofalnih situacija.

U savremenim uslovima, cyber sigurnost predstavlja značajan aspekt sigurnosti državnih organa, vojske, korporativne institucije, finansijski sektor, kao i zdravstvene ustanove. Organizacije prikupljaju, obrađuju i skladiraju velike količine podataka na računarima i drugim uređajima. Veliki dio ili količina tih podataka može biti osjetljiva informacija, bilo da je riječ o intelektualnom vlasništvu, financijskim podacima, osobnim informacijama ili drugim vrstama podataka za koje neovlašteni pristup ili izloženost mogu imati negativne posljedice.

Organizacije prenose osetljive podatke preko mreža i drugih uređaja u toku poslovanja, a sajber bezbjednost opisuje disciplinu posvećenu zaštiti tih informacija i sistema koji se koriste za obradu ili skladištenje informacija. Šifrovanje je proces kodiranja podataka koji ga čini nerazumljivim i često se koristi tokom prijenosa podataka kako bi se spriječila krađa u tranzitu.

Kao obim i sofisticiranost cyber napada raste, kompanija i organizacija, posebno onih koji su zaduženi za čuvanje informacije koje se odnose na nacionalnu sigurnost, zdravstvenih ili finansijski podaci, potrebno je poduzeti korake kako bi zaštitili svoje osjetljive poslovne i osobne informacije.

U posljednjih nekoliko godina, istaknuto je i naglašeno da cyber napadi i digitalno špijuniranje su vrhu prijetnju nacionalnoj sigurnosti, prevazići čak i prijetnje od napada terorizma.[433]

[433] What is Cyber Security? Definition, Best Practices & More. https://digitalguardian.com/blog/what-cyber-security (04.05.2019).

Izazovi vezani za cyber sigurnost sastoje se od nekoliko elemenata koji definiraju stanje efektivne cyber sigurnosti. Elementi sajber bezbjednosti mogu se opisati na sljedeći način:

- Sigurnost mreže
- Sigurnost aplikacije
- Endpoint security
- Sigurnost podataka
- Upravljanje identitetom
- Sigurnost baze podataka i infrastrukture
- Cloud security
- Mobilna sigurnost
- Planiranje oporavka od katastrofe / kontinuiteta poslovanja
- Obrazovanje krajnjih korisnika

2.1. Elementi sajber bezbjednosti

Snažan položaj sajber bezbjednosti oslanja se na sistematski pristup koji obuhvata sljedeće domene:

- **Sigurnost aplikacije**
  Ranjivosti web aplikacija predstavljaju zajedničku tačku upada za sajber kriminalce. Kako aplikacije igraju sve važniju ulogu u poslovanju, organizacije hitno moraju da se fokusiraju na sigurnost web aplikacija kako bi zaštitile svoje klijente, njihove interese i svoju imovinu.[434]
- **Bezbjednost informacija**
  Informacije su u srcu svake organizacije, bilo da se radi o poslovnim knjigama, ličnim podacima ili intelektualnoj svojini. ISO / IEC 27001: 2013 (ISO 27001) je međunarodni standard koji obezbeđuje specifikaciju za najbolji sistem upravljanja informacijskom sigurnošću (ISMS).
- **Sigurnost mreže**
  Sigurnost mreže je proces zaštite upotrebljivosti i integriteta mreže i podataka. To se obično postiže provođenjem test mrežne penetracije , koji ima za cilj da proceni mrežu za ranjivosti i bezbjednosna pitanja u serverima, hostovima, uređajima i mrežnim uslugama.
- **Planiranje kontinuiteta poslovanja**
  Planiranje kontinuiteta poslovanja (BCP) podrazumijeva pripremu za poremećaj

[434] What are the Biggest Cyber Security Threats in 2019? Forbes. April 2 2019. https://www.forbes.com/sites/quora/2019/04/02/what-are-the-biggest-cybersecurity-threats-in-2019/#21d14d2c4b30 (09.06.2019)

tako što se rano identificiraju potencijalne prijetnje za organizaciju i analizira se kako bi to moglo utjecati na svakodnevne operacije.[435]

- **Operativna sigurnost**
  Sigurnost operacija (OPSEC) štiti osnovne funkcije organizacije praćenjem kritičnih informacija i sredstava koja su u interakciji s njom radi identifikacije ranjivosti.
- **Obrazovanje krajnjih korisnika**
  Ljudska greška ostaje vodeći uzrok kršenja podataka, a strategija sajber bezbjednosti je jaka samo kao najslabija karika. Organizacije moraju biti sigurne da je svaki zaposleni svjestan potencijalnih prijetnji s kojima se suočavaju, bilo da se radi o phishing e-pošti, dijeljenju lozinki ili korištenju nesigurne mreže.
- **Posvećenost liderstvu**
  Posvećenost liderstvu je ključ za uspješnu implementaciju bilo kojeg projekta sajber bezbjednosti. Bez toga je veoma teško uspostaviti, implementirati i održavati efikasne procese. Najviše rukovodstvo mora biti spremno da investira u mjere kibernetičke sigurnosti. viši menadžment treba da da adekvatan prioritet sajber bezbjednosti kako bi podržao dalje ulaganje u tehnologiju, resurse i vještine.[436]

Kada je u pitanju definisanje sajber bezbjednosti i njenih uobičajenih tipova, ove kategorije su označene da suže teorijski pojam i praktičnu primjenu:

- Sigurnost mreže - štiti mrežni saobraćaj kontrolom dolaznih i odlaznih veza kako bi se spriječilo da prijetnje ulaze ili se šire na mreži.
- Prevencija gubitka podataka (DLP) - štiti podatke fokusirajući se na lokaciju, klasifikaciju i praćenje informacija u mirovanju, u upotrebi i u pokretu.
- Cloud Security - pruža zaštitu podataka koji se koriste u uslugama i aplikacijama zasnovanim na oblaku.
- Sistemi za otkrivanje upada (IDS) ili sistemi za sprečavanje upada (IPS) - radi na identifikaciji potencijalno neprijateljske sajber aktivnosti.
- Upravljanje identitetom i pristupom (IAM) - upotreba usluge autentifikacije za ograničavanje i praćenje pristupa zaposlenika radi zaštite internih sistema od zlonamjernih entiteta.
- Antivirus / anti-malware rešenja skeniraju računarske sisteme za poznate prijetnje. Savremena rješenja mogu čak i da otkriju nepoznate prijetnje na osnovu njihovog ponašanja.

---

[435] Three Key Elements of Cyber Security Strategy. *CIO Applications Europe*. December 3 2018. https://www.cioapplicationseurope.com/news/three-key-elements-of-cybersecurity-strategy-nid-484.html (26.04.2019)
[436] Roohparvar, R.: Elements of Cyber Security. *Infoguard Cybersecurity*. March 2 2019. http://www.infoguardsecurity.com/elements-of-cybersecurity/ (28.04.2019)

Zanimljiva činjenica koju treba spomenuti je inicijativa koja omogućava radnicima na daljinu i dovođenje vlastitog uređaja (BYOD)[437] Ovakve politike su proširile perimetar, smanjile vidljivost u sajber aktivnostima i proširile površinu napada.[438]

2. Zloupotreba sajber prostora u koruptivne svrhe - lažne vijesti, namještanje, strano uplitanje, izborno spajanje

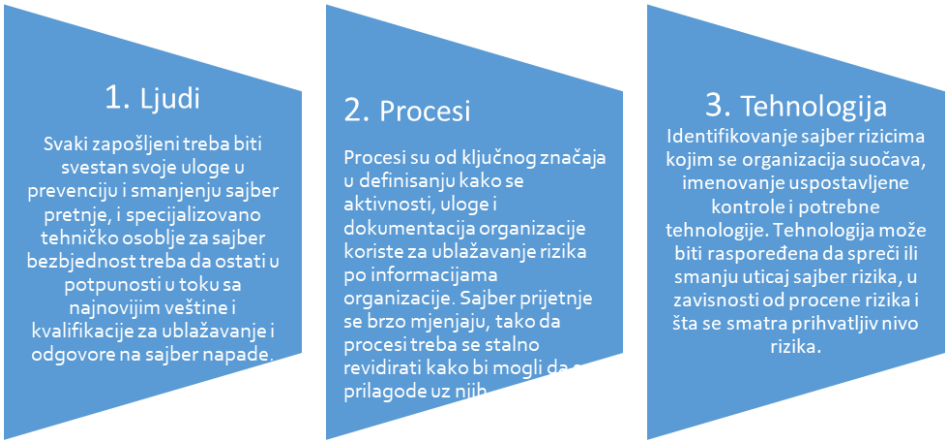
Tradicionalna sajber bezbjednost je centrirana u domenu implementacije odbrambene mjere oko definiranog perimetra. U današnjim događajima, upada u kibernetičkom prostoru rastu brzim tempom, uprkos rekordnim iznosima potrošnje sigurnosti. Jaka sajber sigurnost je ključni odbranbeni sistem vezan protiv sajber kvarova i grešaka i zlonamerne sajber napada, tako da je od vitalnog značaja imati sajber sigurnosne mjere koje štite određene organizacije.[439] Novi propisi i zahtjevi za izvještavanje čine nadzor nad rizikom po sajber bezbjednosti izazov.[440] Da bi se odgovorilo na suvremene prijetnje, organizacije širom svijeta okreću se ljudskoj centricnoj sajber bezbjednosti, novom pristupu koji stavlja fokus na promjene u ponašanju korisnika umjesto eksponencijalnog broja rastućih prijetnji. Ovaj pristup se zasniva na analitike ponašanje.

Humanocentrična sajber bezbjednost pruža uvid u to kako krajnji korisnik stupa u interakciju s podacima i proširuje sigurnosne kontrole u sve sisteme u kojima se nalaze podaci, čak i ako nisu isključivo pod kontrolom organizacije. Na kraju, ovaj pristup je dizajniran da identifikuje anomalije u ponašanju kako bi se izašlo na površinu i odredili prioriteti za najozbiljnije prijetnje, smanjujući vrijeme otkrivanja istraga i prijetnji.

Sajber bezbjednost se može podeliti na tri stuba:

---

[437] Bring your own device (BYOD) refers to employees who bring their own computing devices - such as smartphones, laptops and tablet PCs - to work with them and use them in addition to or instead of company-supplied devices. https://www.techopedia.com/definition/29070/bring-your-own-device-byod (05.06.2019)
[438] Top 15 Cyber Threats for 2019. Cyber Security Insiders. https://www.cybersecurity-insiders.com/top-15-cyber-threats-for-2019/ (10.05.2019)
[439] 8 Cyber Security Risks That May Impact Organizations in 2019. February 13 2019. *Security Magazine*. https://www.securitymagazine.com/articles/89864-cybersecurity-risks-that-may-impact-organizations-in-2019 (18.05.2019)
[440] Discussion Drafts. Cybersecurity Requirements. https://interact.gsa.gov/sites/default/files/Cyber_Risk_Management_Plan_Interact_Release.pdf (01.05.2019)



Cyber napadi postaju sve sofisticiraniji, a taktike i metode koje koriste napadači također se razvijaju i šire u raznolikosti kako bi iskoristile prednosti ranjivosti, među kojima su socijalni inženjering, malware i ransomware. U tom kontekstu, organizacije i institucije će nastaviti da traže garancije od menadžmenta da će njihove strategije za cyber rizik smanjiti rizik od napada i ograničiti finansijske i operativne uticaje.[441]

Ovaj kontekst postavlja pitanje: Koje su posljedice sajber napada? Sajber napadi mogu poremetiti i prouzrokovati znatnu finansijsku i reputacijsku štetu čak i najotpornijoj organizaciji. Ako određena organizacija, institucija ili preduzeće pretrpi cyber napada, oni vjerovatno će se suočiti sa gubitkom imovine, ugleda i poslovanja, i potencijalno će se suočiti sa regulatornim kaznama i parnicama - kao i troškovi sanacije.[442]

Generalno, sajber napadi su počinjeni zbog motive koristi napadača. Oni ulažu u različite tehnike, tehnologije i alate kako bi ostvarili svoje motive. Jedan od najčešćih motiva je finansijska korist, ali sajber napadi može se dogoditi zbog političkim, intelektualnim ili društvenim poticajima.[443]

Tabela 1 : Uobičajeni tipovi kibernetičkih pretnji. Izvor: https://digitalguardian.com/blog/what-cyber-security

[441] UNDP Guidelines on prevention of election violence. The electoral knowledge network. http://aceproject.org/electoral-advice/archive/questions/replies/438369727 (23.04.2019)
[442] The Definition of Cyber Security. IT Governance UK. https://www.itgovernance.co.uk/what-is-cybersecurity (28.05.2019)
[443] 2019 Cyber Security Risk Report. What's Now and What's Next. February 2019. AON's Cyber Solutions. https://www.aon.com/getmedia/4c27b255-c1d0-412f-b861-34c5cc14e604/Aon_2019-Cyber-Security-Risk-Report.aspx (20.05.2019)

Malware	Zlonamerni softver kao što su kompjuterski virusi, špijunski programi, trojanski konji i keyloggeri
Ransomware	Malver koji blokira ili šifrira podatke dok se ne plati otkupnina
Phishing Attacks	Praksa dobijanja osetljivih informacija (npr. Lozinke, informacije o kreditnoj kartici) putem prikrivene e-pošte, telefonskog poziva ili tekstualne poruke
Advanced Persistent Threat	Napad u kojem neovlašćeni korisnik dobija pristup sistemu ili mreži i tamo ostaje duževrijeme bez otkrivanja.
Social Engineering	Psihološka manipulacija pojedinaca za dobijanje povjerljivih informacija; često se preklapa sa phishing-om.

3. Sajber bezbjednost u izbornom procesu

Pravični izbori predstavljaju okosnicu demokratije. Kredibilitet organizovanja izbora, kampanja, ishoda i implementacije u velikoj mjeri zavisi od primijenjenih metoda i tehnika glasanja. Tokom ljudske egzistencije u istoriji, izbori su sprovođeni na gravirane ploče, kuglice u boji ili grahu, papirnim glasačkim listićima, mehaničkim polugama, optičkim skenerima, perforiranim karticama, računarima i kompjuterskom softveru, internet glasanju itd.[444] Svrha ovog rada je da naglasi potrebu za organizovanjem sigurnih izbora koji će garantovati vladavinu prava i poštovanje demokratskih principa državne uprave. Izbori predstavljaju osnovu za uspostavljanje vlade, a oni imaju značajnu ulogu u određivanju strateškog stanovišta na kojem će zemlja poduzeti korake u pogledu unutrašnjih i vanjskih poslova, ekonomije, socijalnih politika, vladavine prava i sigurnosti i stabilnost. Ograničenja u istraživanju su u domenu institucionalnih kapaciteta za obezbjeđivanje optimalnog nivoa održavanja izbora na demokratski način, uz transparentnu kampanju, sprečavanje širenja propagande i lažnih izvora vijesti i web stranica.[445]

Strano uplitanje, sumnjivo finansiranje kampanja, namještanje izbora, izborne prevare, širenje lažnih vijesti i spinova samo su neki od faktora koji mogu potkopati izborne procese i čak stvoriti plamište za izborno nasilje. U tom pravcu, diskusija o strategija prevencije koje bi se mogle provesti kako bi se ublažilo izborno nasilje prvo zahtijeva

[444] Helios: Web-Based Open-Audit Voting. 17th USENIX Security Symposium. http://static.usenix.org/event/sec08/tech/full_papers/adida/adida.pdf (30.05.2019)
[445] A Handbook for Elections Infrastructure Security. Center for Internet Security. CIS. Version 1.0 february 2018. https://www.cisecurity.org/wp-content/uploads/2018/02/CIS-Elections-eBook-15-Feb.pdf (19.04.2019)

identifikaciju različitih vrsta izbornog nasilja koje može doći ako je identifikovano sajber sigurnosnu prijetnju ili ako sajber napad prekine izbornog procesa.[446]

Ovaj nalaz ukazuje na potrebu razlikovanja nasilja koje ima za cilj ometanje izbora od strane aktera koji uopće ne žele da se izbori održe, i nasilje izazvano rivalstvom između kandidata / stranaka koje se natječu. Ako dođe do prvi vid nasilja, nacionalnih snaga sigurnosti može se mobilizirati i ciljaju opstrukcionisti, što dovodi do pažnju na navedenih vrste sukoba, gdje neke stranke se ne slažu o tome da li ili kada će održati izbore, što izaziva njihovi motivi za razmatranje i izvršenje sajber napada i drugih oblika izbornog ometanja. Kada se analizira i procjeni razlog i motivi za aktivno prekidanje procesa glasanja spojler grupa zbog straha od gubitka moći ili u svrhu mijenjanja rezultata i ishoda, te je s odbijanjem da učestvuju na izborima, treba uzeti u obzir prethodni razvoj ili oblik ranije pregovore .[447] Da li se radi o širem političkom, geopolitičkom, sekuritizovanom procesu, sklonom stranom uplitanju i elementima proxy hibridnog uticaja, i rezultatima izbora koji će imati širi uticaj na političku, ekonomsku i bezbjednosnu klimu na regionalnom i međunarodni nivo.[448]

Pored toga, vrijedno je naglasiti povezanost između sajber bezbjednosti i bezbjednosti izbora sa činjeničnom nasilnom eskalacijom. Posebno u smislu nedovoljnog institucionalnog kapaciteta, postoji mogućnost transformacije prijetnje, počevši od kibernetičke prijetnje i odvijajući se kao nasilni nemiri koji dovode do žrtava, materijalne štete i gubitka poverenja. Kada je riječ o analizi izbornog nasilja tokom izbornog procesa, može se podijeliti na određene komponente, uključujući:

- motivi,
- žrtve,
- počinioci,
- odgovora, kao i
- uticaja nasilja.

Posljednjih godina, paralelno sa razvojem IT sistema i mrežnih tehnologija, mnoge zemlje su uvele elektronske glasačke listiće i softverske programe u cilju sprovođenja izbornog procesa. Računarski uređaji za glasanje mogu se definirati kao digitalni model tradicionalnog glasačkog modela glasačkih listića. One predstavljaju dostupnost, pouzdanost, upotrebljivost i provjerljivost sistema e- glasanja. Ali, ima još toga, jer su te tehnologije po

[446] Elections Cyber Security. Center for Democracy and Technology. https://cdt.org/issue/internet-architecture/election-cybersecurity/ (08.05.2019)
[447] Ellena, K., & Petrov, G. (2018). Cyber Security in Elections. Developing a Holistic Exposure and Adaptation Testing (HEAT) Process for Election Management Bodies. http://aceproject.org/ero-en/ifes-cybersecurity-in-elections (21.05.2019)
[448] Election Cyber Security. Politico LLC. 2019 https://www.politico.com/tag/election-cybersecurity (01.06.2019)

prirodi ranljive i predstavljaju sigurnosni izazov. To znači da su računari i programi za glasanje pod prijetnjom hakiranja i manipulacije kako bi se kompromitovao integritet izbora od strane treće strane.[449]

U tom pravcu, razvijena je praktično primjenljiva enkripcija koja obezbjeđuje siguran sistem za glasanje zasnovan na kriptografiji bez curenja . Ovo pretpostavlja tajne potvrde o glasanju koje sprečavaju uplitanje treće strane, kao i efektivno eliminišu mogućnost za prodaju, kupovinu i prinudu glasa. Ovaj dizajn enkripcije razvijen na anonimnom kanalu ili kaskadnoj mreži se zove *semantički siguran*. Time se osigurava privatnost birača, sprečavanje kupovine, prodaje ili prisile glasača, kao i osiguravanje integriteta glasačkih listića i provjerljivost glasova.[450]

Što se tiče izbornog procesa, kompjuterski glasački sistemi mogu biti hakirani, oteti ili narušeni ovim sredstvima:

- Malver korišćen za promjenu glasova unutar digitalnih glasačkih mašina
- Zlonamjerni softver umetnut na osobnim računalima radi promjene glasova na online izborima
- Poremećeni DDoS napadi na izborne servere
- Lažne izborne internet stranice i zavaravanje birača[451]

Ograničenje i nemogućnost za efikasnu zaštitu od izbornih sajber napada, iskorenjivanje stranih izbornih miješanja, i tako dalje, proizlazi iz brojnih faktora koji su u pitanju. One obuhvataju različite dimenzije, kao što su instalacija i rad bot centara koji šire zlonamjernih programa, lažne vijesti, propagandu ili klasificirane informacije, koje su komplicirane za lociranje od strane odgovarajućih sektora ministarstva unutrašnjih poslova; korupcije na visokom nivou u samoj zemlji sa višeslojnim vezama sa predstavnicima stranih zemalja, itd.

Izborni proces predstavlja značajan demokratski čin za postizanje političke moći mirnim putem i ovaj proces u savremenom okruženju je ranjiv u nekoliko aspekata u pogledu bezbednosti. Prijetnja sajber napadom izbornih podataka, hakerski upadi na zvanične web stranice, kao i širenje lažnih novosti i propagande na internetu ugrožava izborni proces u svakoj fazi. Čak i prije početka zvanične kampanje, kao i tokom perioda nadzora i

[449] Nemati, R., H., Yang, L. (2011): Applied Cryptography for Cyber Security and Defense: Information Encryption and Cyphering. New York, Information Science Reference.
[450] Handbook for the Observation of New Voting Technologies. OSCE/ODIHR 2013, Warsaw Poland. https://www.osce.org/odihr/elections/104939?download=true (09.06.2019)
[451] Zetter, K.: The Crisis of Election Security. *The New York Times Magazine*. September 26 2018. https://www.nytimes.com/2018/09/26/magazine/election-security-crisis-midterms.html (11.05.2019)

ispravki biračkih spiskova, i sve do prebrojavanja glasova i rezimiranja rezultata nakon završetka ankete, rizik ostaje prisutan.

Izbori su borba za legitimnu vlast koja se može opisati kao nenasilna konkurencija, koja se vodi u okviru političkog foruma. U ovom kontekstu, važno je prepoznati da izbori ne izbjegavaju konfrontaciju, već se fokusiraju na upravljanje i ograničavanje unutar prihvaćenih granica. U praksi, osiguranje pravične sigurnosti tokom izbornog procesa je od suštinskog značaja za zadržavanje poverenja i predanosti učesnika izborima. Shodno tome, bezbjednost je i sastavni deo cilja izbora i neodvojivi dio izbornog procesa. Ne postoji jedinstveni model izbora ili demokratije koji je univerzalno primjenjiv na sve zemlje. Izbor je jedinstven; definisan ne samo izbornim pravilima, već i društvenim vrijednostima, politikom, religijama, istorijom i kulturom naroda. Na isti način, bezbjednost izbora je jedinstvena za okolnosti u kojima se sprovodi. Ulozi pojedinih izbora su različiti, čak i ako se periodično održavaju u istoj zemlji, zbog promjenljivih sila koje oblikuju nacionalni interes i odgovarajuću političku agendu.[452]

Kada se govori o sigurnosti i sigurnosti izbora i pouzdanosti izbora, pravni aspekt mora biti označen na odgovarajući način. Znači, postoje brojni standardi koji su uvedeni na međunarodnom nivou, ali još mnogo toga treba uraditi kako bi se one u potpunosti implementirale i prilagodile sve većim prijetnjama i izazovima u pogledu sigurnosne dimenzije izbora. Usvojeni standardi su sljedeći:

- The Universal Declaration on Human Rights. Article 21, Paragraph (3). UN General Assembly Resolution 217A
- ICCPR - International Covenant on Civil and Political Rights Resolution 2200A (XXI) (Article 25) adopted by the General Assembly of the United Nations
- UN General Assembly Guidelines for the Regulation of Computerized Data Files (1990). Resolution 45/95
- UN Resolution 34/7. The right to privacy in the digital age. UN Privacy and Data Protection Principles (2017)[453]
- Recommendation CM/REC (2017)5 of the Committee of Ministers to member states o standards for e-voting Council of Europe e-voting standards (2017): Appendix I, Section VIII. Reliability and Security of the System
- Open Government Declaration (2011) Global Report 2019. Democracy Beyond the Ballot Box

Izbor kao demokratski instrument ima snažan potencijal koji se širi i izvan političkih implikacija. Razvoj društva i rastuća interakcija i složenost ljudskih aktivnosti nameću potrebu za odgovarajućim rješenjem u pogledu održavanja modernih izbora. Uključujući značajnu

[452] Council of Europe: E-Voting. https://www.coe.int/en/web/electoral-assistance/e-voting (12.05.2019)
[453] Election Technology and Cyber Security: Standards, Good Practice and Guidelines. The Electoral Knowledge Network. http://aceproject.org/election-technology-and-cyber-security-standards (23.04.2019)

predizbornu kampanju, siguran proces glasanja, precizan i provjerljiv broj glasova i adekvatnu implementaciju izbornih rezultata. Osiguranje sigurnosnog aspekta ovog značajnog akta je imperativ za savremena društva. U tom pravcu su nastojanja da se uspostave univerzalni standardi i sigurnosne procedure i mjere za garantiranje pouzdanog ishoda.[454]

Ipak, uprkos trendovima inicijativa za e-glasanje, proces implementacije se odvija sporije nego što se očekivalo, a to je zbog nekoliko faktora koji uključuju tehničku, socijalnu i kulturnu dimenziju. Paralelno s tim, harmonizacija sistema elektronskog glasanja, u okviru različitih zakonskih i statutarnih oznaka, također predstavlja izazov koji ostaje da se prevlada.

Izborna 'namještanja' ili percipirano namještanje izbora mogu uzrokovati nasilje, ali nasilje je često samo oblik namještanja. Prilikom ispitivanja veza između namještanja i nasilja, važno je uočiti evoluciju namještanja, manipulacije ili iskrivljavanja rezultata tokom posljednjih godina i razmotriti šta se može učiniti kako bi se to riješilo. Treba identifikovati odnose između državnih resursa i namještanja, nasilja i namještanja.[455]

Ne postoji univerzalna definicija "izborne prijevare", jer se ona razlikuje u vremenu i na različitim lokacijama. Drugi izrazi koji se koriste kao zamjena za prijevaru su zloupotreba, nedolično ponašanje, nepravilnosti i manipulacija. Izborna prijevara podrazumijeva samo obmanu, ali ne i svi izborni zločini uključuju samo varanje. Postoje i prakse koje nisu same po sebi nezakonite, ali nisu u skladu sa međunarodnim standardima. Ove nezakonite prakse uključuju sljedeće:

- sprečavanje birača da popune glasačke listiće,
- netačna kampanjska literatura,
- prisilno povlačenje protivnika (a),
- plačanja olakšice, i
- propuste u dužnoj pažnji izbornih zvaničnika.[456]

[454] Election Security. Homeland Security. https://www.dhs.gov/topic/election-security (23.05.2019)
[455] Elections – Critical Infrastructure. US Election Assistance Commission. https://www.eac.gov/election-officials/elections-critical-infrastructure/ (25.05.2019)
[456] Fiddler, D., P.: Policy Dimensions of Strenghtening Elections Cybersecurity. Council on Foreign Relations. October 18 2017.
https://sites.nationalacademies.org/cs/groups/pgasite/documents/webpage/pga_182365.pdf (01.06.2019)

Kako bi se utvrdio nivo i tip ranjivosti koje postoje, procjena rizika za izborni kriminal bi trebala biti provedena od strane relevantnih tijela . Procjena historije izbornih namještanja može ukazati na potencijalnu veličinu i utjecaj na ishode.[457] Može se identifikovati:

- mjesta na kojima se očekuje da će se dogoditi zločini,
- u kojoj fazi izbornog ciklusa mogu se desiti, i
- da li su zločini vjerovatno epizodni ili sustavni.[458]

Unutar izbornog ciklusa, rizik se može identificirati kao da se odvija u sljedećim fazama:

- identifikaciju i registraciju birača,
- politička kampanja,
- glasanje na dan izbora,
- transport osjetljivih izbornih materijala,
- tabeliranje glasovanja, i
- adjudikacija i sertifikacija.[459]

Ovi obrasci su na raspolaganju vladinim institucijama, izbornim komisijama, sigurnosnim snagama, kao i drugim uključenim akterima, kako bi se implementirala alternativa koja će u konačnici spriječiti ili ublažiti daljnje izborno nasilje.[460]

4. Zaključak

Što se tiče nalaza i elaboriranih podataka u ovom radu, četiri hipoteze se mogu izvući kao zaključci.

Prva tvrdnja je sve veća dimenzija bezbjednosti kao stanje i cilja - koja obuhvata domenu sajber bezbjednosti. To pretpostavlja da sajber bezbjednost i alati za osiguranje njenog uključivanja u integralni aspekt upravljanja sigurnošću idu ruku pod ruku sa ekonomskom sigurnošću, kritičnom bezbjednošću infrastrukture, političkom stabilnošću itd.

---

[457] Lin, H.: Election Hacking, As We Understand it Today, is not a Cyber Security Issue. January 5 2018. *Lawfare*. https://www.lawfareblog.com/election-hacking-we-understand-it-today-not-cybersecurity-issue (11.06.2019)

[458] EU Member states Test Their Cyber Security Preparedness for Fair and Free 2019 EU Elections. European Commission. http://europa.eu/rapid/press-release_IP-19-2011_en.htm (19.05.2019)

[459] H2020 – EU 3.7.4. – Improve Cyber Security. https://cordis.europa.eu/programme/rcn/664471/en (12.06.2019)

[460] Elections, Violence and Conflict Prevention. European Commission United Nations Developing Programme. Joint Task Force on Electoral Assistance. June 2011. https://www.undp.org/content/dam/brussels/docs/Other/JTF%202011.06_Summary_report-Barcelona_workshop_Elections&conflict.pdf (24.04.2019)

Druga tvrdnja koja proizilazi iz analiziranih podataka u ovom radu sumira aspekt upravljanja sajber bezbjednošću i procenu rizika sajber sigurnosti. Upravljanje od top menadžmenta do nižeg nivoa je nosilac inicijativa za sajber bezbjednost i davanje prioriteta ovom pitanju u okviru organizacije ili korporacije. Kada je u pitanju upravljanje sajber bezbjednošću i zaštitom podataka u datom preduzeću, procene sajber rizika fokusiraju se na tri ključna aspekta:

1. Identifikacija najvrednijih podataka organizacije koji zahtijevaju zaštitu,
2. Identificiranje rizika i prijetnji u pogledu njegove zaštite i
3. Označavanje štete nanesene u slučaju gubitka podataka ili nezakonite izloženosti.

Treći zaključak iz ove hipoteze odnosi se na potrebu stvaranja i pridržavanja propisa kada je u pitanju prikupljanje, čuvanje i sigurnost podataka. Ova razmatranja treba da se urade i u pravcu procene rizika. Kao pravni odgovor na rastuće pitanje vezano za sajber bezbjednost i temeljno pravo na prirodnu privatnost i zaštitu podataka, Evropski parlament i Vijeće izdali su uredbu EU 2016/679 (Direktiva 95/46 / EZ o općoj uredbi o zaštiti podataka).[461]

Kada je u pitanju rješavanje pitanja vezanih za sigurnost, Direktiva Član 19. definiše da zaštita fizičkih lica u pogledu obrade ličnih podataka od strane nadležnih organa u svrhu sprečavanja, istrage, otkrivanja ili krivičnog gonjenja krivičnih djela ili izvršenja krivičnih sankcija, uključujući zaštitu od i sprečavanje prijetnji javnoj sigurnosti i slobodno kretanje takvih podataka, predmet je posebnog pravnog akta Unije. Stoga se ova Uredba ne bi trebala primjenjivati na aktivnosti obrade u te svrhe. Međutim, lični podaci koje obrađuju javni organi prema ovoj Uredbi trebali bi se, kada se koriste u te svrhe, regulirati specifičnijim pravnim aktom Unije, naime Direktivom (EU) 2016/680 Europskog parlamenta i Vijeća.

Četvrti zaključak povezan je sa sajber bezbjednošću i izborima. Od predsjedničkih izbora u SAD 2016. godine i Mueller-ovog izvještaja o istrazi o ruskom uplitanju doveli su do kontroverzi i izazvali debatu i sumnju u ranjivost prema izbornim procesima i rezultatima, sajber bezbjednost na izborima dobila je središte pažnje u organizaciji i održavanju izbora u mnogim zemljama u svijetu.

[461] The EU General Data Protection Regulation (GDPR). 2018 Reform of Data Protection Rules. European Commission. https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en (30.05.2019)

5. Literatura:

1. Ayala, L. (2016): Cyber Security Lexicon. New York, Springer Science and Apress.
2. Delta, G., B., Matsuura, J., H. (2019): Law of the Internet, Fourth Edition. Volume 1, Supplement. New York, Wolters Kluwer.
3. Goldstein, M., J., Gitlin, M.. (2015): Cyber Attack. Minneapolis, Twenty First Century Books.
4. Hackett, R. (2018): Cyber Security: Hacking, the Dark Web and You. Tampa, FL, Time Books Edition.
5. Heitkamp, K., L. (2019): Interference in Elections. New York, Greenheaven Publishing.
6. Kamar, H. (2018): What is Cyber Security? New York, Britannica Educational Publishing.
7. Li, K, Chen, X., Susilo, W. (2019): Advances in Cyber Security: Principles, Techniques and Applications. Singapore, Springer Nature.
8. Lucas, G. (2017): Ethics and Cyber Warfare: The Quest for Responsible Security in the Age of Digital Warfare. Madison Avenue, New York, Oxford University Press.
9. Nemati, H., R., Yang, L. (2011): Applied Cryptography for Cyber Security and Defense: Information Encryption and Cyphering. Hershey New York, Informational Science Reference.
10. Norris, P. (2017): Strengthening Electoral Integrity. Cambridge, Cambridge University Press.
11. Norris, P., Cameron, S., Wynter, T. (2019): Electoral Integrity in America: Securing Democracy. New York, Oxford University Press.

Kriminalističke teme
Zbornik radova
Godina XIX, Broj 5, 2019.
ISSN 1512-5505

BEZBEDNOST I ZAŠTITA PODATAKA O LIČNOSTI U ZDRAVSTVENIM USTANOVAMA

SECURITY AND PERSONAL DATA PROTECTION IN HEALTHCARE INSTITUTIONS

Pregledni naučni rad

Prof. dr Zoran Keković[462]
Prof. dr Gordana Pejović[463]

Sažetak

Inspiracija za rad i problem (i) koji se radom oslovljava (ju): Stupanjem na snagu Opšte uredbe o zaštiti podataka (GDPR), kao i odgovarajućih nacionalnih propisa koji su transponovali odredbe ove uredbe u zakonodavstvo zemalja koje nisu članice EU, pred zdravstvene ustanove u regionu stavlja se nimalo lak zadatak da usklade svoje procedure sa ovim odredbama.

Ciljevi rada (naučni i/ili društveni): Cilj rada je da se omogući objedinjeni prikaz važećih bezbednosnih standarda, kao i odgovarajućih smernica za bezbednost u zdravstvu, čija primena omogućava veću bezbednost zaposlenih, pacijenata i drugih ljudi koji posećuju zdravstvene ustanove. Takođe, u radu će biti prikazani i regulatorni zahtevi koji se odnose na posebne kategorije podataka o ličnosti – podatke o zdravstvenom stanju.

Metodologija/Dizajn: U radu se daje pregled normativnih aspekata bezbednosti u zdravstvu, kao i zaštite podataka o ličnosti, faktičkom stanju u ovoj oblasti, te izazovima koje donose novi propisi u ovoj oblasti.

Ograničenja istraživanja/rada: Podaci o zdravstvenom stanju građana, kao posebno osetljivi podaci o ličnosti, podrazumevaju posebne mere zaštite i specifične tehničke, fizičke i organizacione kontrole, tako da je u radu prikazan samo jedan od mogućih pristupa u sprovođenju ovih mera.

Rezultati/Nalazi: Ističe se značaj adekvatnog razumevanja i primene odredaba zakonske regulative, kao i srazmernih kontrola za osiguranje bezbednosti lica i podataka o ličnosti.

Generalni zaključak: Naročite napore treba uložiti da se u zdravstvene ustanove implementiraju mere koje će garantovati bezbednost podataka o ličnosti, imajući u vidu istoriju čestih i ozbiljnih incidenata narušavanja ovih podataka.

Opravdanost istraživanja/rada: Opravdanost rada nalazi se u činjenici da je potrebno garantovati pacijentima, građanima i zaposlenima u zdravstvenim ustanovama adekvatan nivo zaštite podataka o ličnosti, ali i ličnu bezbednosti tokom procesa koje obavljaju.

[462] Univerzitet u Beogradu, Fakultet bezbednosti, zorankekovic@yahoo.com
[463] Univerzitet u Beogradu, Fakultet organizacionih nauka, SGS Beograd doo, gordana.pejovic@sgs.com

Ključne riječi
bezbednost, zaštita podataka o ličnosti, zdravstvena zaštita

Abstract
Reason for writing and research problem (s): By entering the General Data Protection Regulation (GDPR) into force, as well as the relevant national regulations transposing provisions of this Regulation into the legislation of non-EU countries, the healthcare institutions in the region got the complex task to harmonize their procedures with these provisions.
Aims of the paper: The aim of the paper is to provide a review of the applicable safety standards, as well as the relevant safety guidelines in healthcare, the application of which allows for greater safety of employees, patients and other people visiting health facilities. Also, the paper will show the regulatory requirements related to special categories of personal data – data concerning health.
Methodology: The paper presents a review of the normative aspects of safety in health care, as well as the protection of personal data, the factual situation in this field, and the challenges brought by the new regulations in this field.
Research/Paper Limitation: Data concerning health, as special category of personal data, imply special protection measures and special technical, physical and organizational controls, so that only one of the possible approaches in the implementation of these measures is presented in the paper.
Results / General Conclusion: The importance of adequate legal provisions understanding and implementation is emphasized, as well as the application of proportional controls for ensuring the safety of the person and personal data.
Conclusion: Efforts should be made to implement measures that will guarantee the protection of personal data in healthcare institutions, bearing in mind the history of frequent and serious breaches of healthcare data.
Research / Paper Validity: The justification of work is in the fact that it is necessary to guarantee patients, citizens and employees in healthcare institutions an adequate level of protection of personal data, as well as personal safety during the processes they perform.

Key words
safety, personal data protection, healthcare

Uvod

Zdravstvene ustanove, medicinski personal, kao i korisnici zdravstvenih usluga, uključujući i imovinu i osetljive informacije od značaja za te usluge, sve više su izloženi bezbednosnim rizicima ljudskog porekla.

Primena bezbednosnih standarda i odgovarajućih zakonskih propisa u zdravstvu može varirati u zavisnosti od tipa zdravstvene ustanove, zbog čega je važno da oni budu prilagođeni specifičnostima sredine i potrebama zaštite. *Direktivom EU o kritičnim infrastrukturama* (*2008/114/ES),* kao i *Zakonom o kritičnim infrastrukturama* (Službeni glasnik RS", broj 87 od 13. novembra 2018.) sektor zdravstva prepoznat je kao kritična infrastruktura

što pretpostavlja poseban nivo bezbednosti u cilju obezbeđivanja kontinuiteta zdravstvene zaštite u raznim uslovima. Takođe, stupanjem na snagu Opšte uredbe o zaštiti podataka (GDPR), kao i odgovarajućih nacionalnih propisa koji su transponovali odredbe ove uredbe u zakonodavstvo zemalja koje nisu članice EU, pred zdravstvene ustanove u regionu stavlja se nimalo lak zadatak da usklade svoje procedure sa ovim odredbama.

Cilj rada je da se omogući objedinjeni prikaz važećih bezbednosnih standarda, kao i odgovarajućih smernica za bezbednost u zdravstvu, čija primena omogućava veću bezbednost zaposlenih, pacijenata i drugih ljudi koji posećuju zdravstvene ustanove. Takođe, u radu će biti prikazani i regulatorni zahtevi koji se odnose na posebne kategorije podataka o ličnosti – podatke o zdravstvenom stanju.

Međunarodni i evropski standardi od značaja za bezbednost u zdravstvu

Jedan od krovnih nadnacionalnih standarda koji definiše oblast bezbednosti u zdravstvu jeste Uputstvo za menadžment bezbednosti u zdravstvenim ustanovama - CEN/TS 16850:2015. Ovaj evropski standard definiše zaštitu lica, kritičnih procesa, imovine i informacija od bezbednosnih pretnji i primenjuje se u bolnicama i drugim ustanovama koje pružaju zdravstvene usluge.

Pored toga što ističe značaj pravnih, regulatornih i drugih zahteva u vezi sa menadžmentom bezbednosti u zdravstvenim ustanovama, ovaj standard ukazuje na značaj identifikovanja zakonskih ograničenja za određene bezbednosne procedure i njihove posledice u vezi sa bezbednošću, što se posebno može reći za zakonske zahteve u oblasti zaštite podataka o ličnosti zaposlenih, kao i svih korisnika zdravstvenih usluga.[464] U navedenom smislu, posebno je važna odredba da bezbednosni menadžment u zdravstvenim ustanovama treba da bude usklađen sa drugim politikama i da poštuje prava pacijenata i posetilaca.

U vezi sa menadžmentom rizikom, ističe se da zdravstvena organizacija treba da uspostavi, implementira i održava formalne i dokumentovane procese procene rizika sa ciljem identifikovanja bezbednosnih rizika prouzrokovanih namernim i nenamernim pretnjama koje mogu izazvati direktne ili indirektne posledice po bezbednost, imovinu i zainteresovane strane.

Nadalje, politika bezbednosnog menadžmenta treba da sadrži ciljeve organizacije, što bi sa aspekta zaštite informacije značilo da se artikuliše jasna veza između zaštite informacija i ciljeva i politike organizacije, uključujući i politiku menadžmenta bezbednosti. Ne

[464] Ове процедуре су у већини случајева саставни део стандарда система менаџмента, нпр система менаџмента квалитетом

manje važno je da ciljevi organizacije u vezi sa zaštitom informacija budu dostupni i jasno predstavljeni svim zaposlenim u organizaciji, što će imati uticaj na sistem odgovornosti i posvećenost konkretnom cilju. Navedena politika treba dalje da se konkretizuje putem *plana menadžmenta bezbednosti*, a na osnovu procenjenih rizika. Takav plan bi trebalo posebno da obuhvati identifikaciju bezbednosno osetljivih tačaka i zona, pregled dužnosti i aktivnosti u vezi sa pretpostavljenim ciljevima bezbednosti, sistem dokumentacije (tj. evidencije i izveštaji), kao i programe obuke koji obuhvataju različite kategorije zaposlenog osoblja.

Od posebnog značaja za bezbednost informacija je povezivanje menadžmenta bezbednosti informacija sa drugim sistemima menadžmenta čime se menadžment bezbednosti informacija usklađuje sa sistemima menadžmenta kvalitetom, sistemom menadžmenta životnom sredinom itd.

Standard definiše operativno uputstvo i opšte procedure zdravstvene organizacije za kontrolisane zone kao prostore zaštićene od neovlašćenog pristupa, uključujući i konkretne sisteme za kontrolu pristupa, bezbedno skladištenje i čuvanje osetljivih i klasifikovanih informacija. U vezi sa tim, definisana su i operativna uputstva za bezbednosnu proveru lica, tj. personala, kojima se obezbeđuje usklađenost sa propisima u oblasti zaštite lica, imovine i informacija.

Kao posebne kategorije koje zahtevaju primenu bezbednosnih standarda i procedura, ovaj standard prepoznaje posetioce, pacijente, i, što je posebno važno, decu i njihovu bezbednost. U smislu zaštite informacija, podaci o deci mogu se ticati pitanja vezanih za moguće zlostavljanje dece, sporove oko starateljstva, deci kao žrtvama kriminalnih aktivnosti, uključujući i krijumčarenje.

Kada je reč o odgovoru na bezbednosni incident, definisani su kriterijumi šta se može smatrati bezbednosnim incidentom, između ostalog: gubitak, kompromitovanje ili zloupotreba osetljivih ili vitalnih informacija.

Evropska regulativa u oblasti zaštite informacija dobila je nov kvalitet donošenjem evorpskog standarda *SRPS EN 15224:2017 Zdravstvene usluge – Sistemi menadžmenta kvalitetom – Zahtevi zasnovani na SRPS EN ISO 9001:2015.* Ovaj standard, poznat i kao „ISO 9001 za zdravstvenu zaštitu“, između ostalog, stavlja akcenat na zdravstvenu zaštitu orijentisanu prema pacijentu, uključujući njegov fizički, psihološki i socijalni integritet.

U okviru bezbednosti zdravstvenih ustanova, u centru pažnje ovog standarda su, pored pacijenata i drugih korisnika zdravstvenih usluga, zaposleno osoblje, imovina i informacije. Kao poverljive (naročito osetljive) informacije smatraju se: lični podaci pacijenta/korisnika; podaci koji se odnose na zdravstveno stanje pacijenta; i podaci o dijagnostičkim procedurama i lečenju pacijenta. Sa aspekta zakonske regulative, ova materija je pokrivena propisima o zaštiti podataka ličnosti, o pravima pacijenta (pravo na privatnost i

poverljivost), itd. Zdravstvena ustanova mora imati uspostavljen sistem za zaštitu informacija o pacijentu od neovlašćenog pristupa i zloupotrebe.

Zaštita podataka o ličnosti u sistemu zdravstvene zaštite

Kada je Opšta uredba o zaštiti podataka Evropske unije (General Data Protection Regulation – GDPR, u daljem tekstu: Uredba) stupila na snagu 25. maja 2018. godine, izazvala je ozbiljne reakcije u različitim sektorima i industrijama širom sveta. Uredba postavlja novi standard u pogledu privatnosti podataka: utiče na bilo koju organizaciju koja obrađuje podatke građana EU, bez obzira gde se ti podaci prikupljaju, obrađuju ili čuvaju. Ovim regulativa dobija mnogo širi obim, proširujući domet na teritorije izvan EU i utičući na organizacije širom sveta, u bilo kojoj industriji. Za oblast zdravstvene zaštite, koja zahteva različite vrste ličnih podataka, to je prilika da se poboljšaju sistemi, politike i procesi kako bi se izbegle potencijalne pretnje za informacije o institucijama i pacijentima.

Prema odredbama evropske i važeće nacionalne regulative u Srbiji (Zakon o zaštiti podataka o ličnosti, "Sl. glasnik RS" br. 87/2018 od 13.11.2018.) podaci o zdravstvenom stanju spadaju u posebne vrste podataka o ličnosti, kojima su obuhvaćeni i genetski podaci i biometrijski podaci. Uredba generalno zabranjuje bilo kakvu obradu ovih podataka, osim ako nije dat izričiti pristanak ili nisu ispunjeni vrlo specifični uslovi. Postoje izuzeci - obrada je uglavnom dozvoljena za procenu radne sposobnosti za zapošljavanje, za upravljanje zdravstvenim sistemima ili sistemima socijalne zaštite i uslugama ili za javni interes.

Potrebno je istaći da su zdravstvene organizacije u specifičnoj poziciji, jer se bave čitavim spektrom podataka - od finansijskih podataka i informacija o zdravstvenom osiguranju do rezultata ispitivanja pacijenta i biometrijskih informacija. Neki od ovih vidova podataka su osetljiviji od tipičnih informacija koje prikupljaju nezdravstvene organizacije: one su jedinstveno povezane sa pojedincem i uglavnom su nepromenjive.

Upravljanje medicinskom dokumentacijom, koja sadrži posebno osetljive lične podatake, zahteva da su procesi monitoringa dizajnirani s posebnom pažnjom. Po pravilu, u zdravstvenim ustanovama primenjuje se dugi rok arhiviranja dokumenata. Što je duži rok čuvanja dokumentacije – proces je skuplji, složeniji, riskantniji i generalno zahtevniji. Dodatno, ovo nosi sa sobom potencijalni rizik: samo jedan izgubljeni (ili oštećeni, nedostupan ili prekasno dostupan) dokument može značiti razliku između uspeha i neuspeha u lečenju.

Zdravstvene ustanove, koje prema odredbama važeće regulative predstavljaju rukovaoce podacima o ličnosti, dužan da preduzme odgovarajuće tehničke, organizacione i kadrovske mere kako bi obezbedio da se obrada vrši u skladu sa propisanim odredbama. Potrebno je istaći da zakonodavac daje mogućnost da u primeni navedenih mera rukovalac podacima o ličnosti može uzeti u obzir nivo tehnoloških dostignuća i troškove njihove

primene, prirodu, obim, okolnosti i svrhu obrade, kao i verovatnoću nastupanja rizika i nivo rizika za prava i slobode fizičkih lica koji proizilaze iz obrade podataka o ličnosti.

Uredba jasno određuje individualnu odgovornost svake organizacije koja obrađuje podatke o ličnosti, što u praktičnom smislu znači da je dužnost svake organizacije da se samostalno pripremi za primenu Uredbe i uskladi svoje interne procese obrade podataka zahtevima Uredbe. Uredba određuje obavezu izvršenja takozvane „Procene uticaja obrade podataka" („Data Processing Impact Assessment") u situacijama kada se podaci vezani za zdravstveno stanje obrađuju u „velikom obimu". Dodatno, propisuje se obaveza ugovornog regulisanja odnosa i odgovornosti u vezi sa zaštitom ličnih podataka između organizacija koje su rukovaoci obrade i organizacija koje im pružaju uslugu spoljnje obrade podataka (eksterni isporučioci usluge), koji su u tom slučaju obrađivači podataka (npr. između klinike i dijagnostičke laboratorije koja za kliniku vrši uslugu).

Svaka organizacija je dužna samostalno da proceni koliki je obim posla potreban za usklađivanje sa odredbama regulative, imajući u vidu puno različitih faktora kao što su, na primer, kompleksnost obrade podataka kojom se organizacija bavi, broj individualnih korisnika usluga, veličina organizacije i slično.

Osnovne mere zaštite podataka o ličnosti u informacionim sistemima

Potrebno je istaći da je sama regulativa definisala neke od mere zaštite podataka o ličnosti u informacionim sistemima, kao što su enkripcija i pseudonimizacija. Takođe, druge, veoma korisne mere zaštite mogu imati svoju primenu: razdvanje zaduženja, kontrola pristupa dokumentima i podacima (na „*need to know*" osnovi), razmena podataka o ličnosti u skladu sa procenom rizika, obezbeđenje redundantosti da bi se izbegao „*single point of failure*", monitoring aktivnosti, uključujući privilegovane korisnike, kontrola spoljnjeg pristupa mrežama i razdvajanje mreža, učenje iz incidenata itd.

Pseudonimizovani podaci su podaci od kojih su uklonjene informacije pomoću kojih se osoba može identifikovati. Drugim rečima, podaci iz kojih se ne može nedvosmisleno utvrditi identitet osobe smatraju se pseudonimizovanim. Na primer, imena u tablici koja su zamenjena nasumičnim rečima/brojevima (identifikatorima) po ključu jedan za jedan. Podaci su i dalje tu i može se utvrditi da se radi o nekome, ali ne tačno i o kome.

To su i dalje podaci o ličnosti i ne smatraju se potpuno nerizičnima, ali rizik je znatno smanjen.

Druga mera koja je regulativom preporučena je enkripcija. Visokorizični podaci idealan su kandidat za enkripciju, i to tokom čitavog njihovog životnog ciklusa. To uključuje trenutak primanja podataka od korisnika, za šta se koriste mrežni kriptografski protokoli, obrade (enkripcija memorije) i naknadnog arhiviranja. Dobro zaštićeni podaci sami su po sebi sigurni, čak i u slučajevima povrede podataka, takvi su podaci korisnicima

neupotrebljivi. Iz tog razloga se kriptovanje u Zakonu o zaštiti podataka o ličnosti izričito navodi kao primer dobre prakse za zaštitu podataka.

Sigurnosnim kopijama štite se podaci koje organizacija može izgubiti usled malicioznih napada, slučajnog brisanja ili kvara na opremi. Sigurnosne kopije treba pripremati u skladu sa intervalima koje je zdravstvena organizacija propisala kao najpogodnije i redovno ih ažurirati, uz napomenu da sigurnosne kopije posebnih kategorija podataka o ličnosti treba raditi češće (i pažljivije). Po pravilu, sve kopije se čuvaju na sigurnom mestu s ograničenim pristupom, dok se medije treba čuvati na mestu koje odgovara njihovim radnim parametrima (vlažnost, temperatura, itd.).

Zaključak

U radu se daje objedinjeni prikaz važećih međunarodnih i evropskih bezbednosnih standarda, kao i odgovarajućih smernica za bezbednost u zdravstvu, čijom se primenom omogućava veća bezbednost zaposlenih, pacijenata i drugih ljudi koji posećuju zdravstvene ustanove.

Od posebnog značaja su i regulatorni zahtevi koji se odnose na posebne kategorije podataka o ličnosti – podatke o zdravstvenom stanju. Primenom odgovarajućih tehničkih, organizacionih i kadrovskih mera zdravstvene organizacije će osigurati da su adekvatne politike i procedure za zaštitu podataka o ličnosti uspostavljene. Procesom implementacije i usaglašavanja sa odredbama Uredbe i nacionalne regulative u ovoj oblasti osiguraće se da su svi poslovni procesi detaljno preispitani, kao i da se unapredi upravljanje organizacijom.

Regulativa zahteva preduzimanje proporcionalnih mera u slučaju da dođe do povrede podataka o ličnosti, obaveštavanje odgovarajućih nadležnih organa, što će temeljna analiza sistema i procesa omogućiti da se izvrši u najboljoj mogućoj meri. Kada su kadrovske mere u pitanju, one podrazumevaju prethodnu detaljnu obuku svih zaposlenih, ali i uspostavljanje adekvatnih politika obrade podataka, koje treba da budu napisane razumljivim jezikom, i koje mogu biti dostupne u elektronskom obliku.

Literatura

1. Direktiva EU o kritičnim infrastrukturama (2008/114/ES)
2. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016.
3. SRPS EN 15224:2017 Zdravstvene usluge – Sistemi menadžmenta kvalitetom
4. Uputstvo za menadžment bezbednosti u zdravstvenim ustanovama - CEN/TS 16850:2015.
5. Zakon o kritičnim infrastrukturama (Službeni glasnik RS", broj 87 od 13. novembra 2018.)
6. Zakon o zaštiti podataka o ličnosti, „Sl.glasnik Republike Srbije“, br. 87/2018 od 13.11.2018. godine

Kriminalističke teme
Zbornik radova
Godina XIX, Broj 5, 2019.
ISSN 1512-5505

KORIŠTENJE ELEKTRONSKOG I KORESPONDENTNOG BANKARSTVA ZA AKTIVNOSTI PRANJA NOVCA

USE OF ELECTRONIC AND CORRESPONDENT BANKING FOR MONEY LAUNDERING ACTIVITIES

Stručni rad

Ajla Šurković, MA[465]

Sažetak

Inspiracija za rad i problem (i) koji se radom oslovljavaju: Napredak u razvoju informacione tehnologije uticao je na pojavu novih oblika pranja novca koje karakteriše sofisticiranost, prikrivenost, veći nivo organizacije, međunarodni karakter kao i kreativnost kriminalaca. Elektronski transferi novca sa jednog računa na drugi, te brzina kojom se isti realizuje omogućava prikrivanje stvarnog izvora tog novca.

Ciljevi rada (naučni i/ili društveni): Naučni cilj rada ogleda u opisivanju faktora koji utiču na pojavu pranja novca u elektronskom i korespondentnom bankarstvu. Društveni cilj odnosi se na informisanje akademske i stručne javnosti o specifičnostima pranja novca korištenjem elektronskog i korespondentnog bankarstva.

Metodologija/Dizajn: Pri izradi rada koristit će se literatura domaćih i stranih autora te ostali naučni i stručni članci dostupni na internetskim stranicama. U radu će biti korištene sljedeće metode: metoda analize te deduktivna i induktivna metoda. Kada je u pitanju metoda prikupljanja podataka bit će korištena analiza sadržaja.

Ograničenja istraživanja/rada: Ograničenje ovog rada je teorijsko razmatranje pranja novca korištenjem elektronskog i korespondentnog bankarstva. Naime, u istom će biti prikazana postojeća naučna saznanja kada je u pitanju predmet istraživanja. Stoga, ovim radom nije moguće ukazati na praktična rješenja koja bi mogla uticati na sprečavanje pranja novca u oblastima koje će biti obrađene u radu.

Rezultati/Nalazi: Pranje novca korištenjem elektronskog bankarstva iako obuhvata tri tradicionalne faze pranja novca ima određene specifičnosti u pogledu mjesta i načina na koji se preduzimaju određene aktivnosti. Internet bankarstvo i Mobilno bankarstvo kao distrubucijski kanali elektronskog bankarstva mogu omogučiti prikrivanje kako porijekla novčanih sredstava tako i identiteta klijenata koji koriste te usluge što povećava rizik od pranja novca. S druge strane, korespondentno bankarstvo se koristi za aktivnosti pranja novca jer predstavlja vrstu poslovnog odnosa koji omogućava poslovanje sa rezidentnom bankom bez tačnih i pouzdanih informacija o porijeklu novčanih sredstava. Posebno su rizični korespondentni odnosi sa *shell* bankama koje fizički ne postoje niti u jednoj zemlji te osnivanje ofšor finansijskih centara pomoću kojih određene pravne i fizičke osobe ostvaruju „finansijske pogodnosti“.

[465] ajlasurkovic@fkn.unsa.ba

Generalni zaključak: Uzimajući u obzir zajedničku karakteristiku elektronskog i korespondentnog bankarstva koja se odnosi na fizičko odsustvo stranaka sa kojima se vrši poslovanje, može se zaključiti da navedene djelatnosti pospješuju aktivnosti pranja novca.
Opravdanost istraživanja /rada: Opravdanost ovog rada ogleda se u spoznaji pojavnih oblika pranja novca koje su omogućili elektronski transferi.

Ključne riječi
pranje novca, elektronsko bankarstvo, korespondentno bankarstvo, *shell* banke

Abstract
Inspiration for the research and problem (s) referred to in this work: Progress in development of informational technologies has affected the emergence of new forms of money laundering that is characterized by sophistication, concealment, higher level of organisation, international character as well as the creativity of criminals. Electronic transfers of money from one back account to another and the speed of its realization, allows a cover-up of the true money source.
Research goals (scientific and/or social): Scientific goal reflects itself in the description of factors that affect the emergence of money laundering within electronic and correspondent banking. Social goal refers to the informing of academic and expert public regarding specifics of money laundering using electronic and correspondent banking.
Methodology/Design: During the execution of this work, literature of regional and foreign authors will be used as well as other scientific articles and articles of expertise available on internet sites. In said work following methods will be used: method of analysis, and deductive and inductive method. Regarding the data collecting method, content analysis will be used.
Limitations in the research/work: The limitation of this particular work lies in the theoretical deliberation of money laundering through electronic and corresponding banking. More specifically, through said deliberation, existing scientific findings in reference to the subject of research will be presented. Therefore in this work, it is not possible to address practical solutions that would affect prevention of money laundering within areas included in this research.
Results/Findings: Although it includes three traditional phases, money laundering through the use of electronic and correspondent banking has certain specifics in regards to the place and the way certain activities are done. Internet Banking and Mobile Banking as channels for electronic banking distribution can allow for concealment of origin of funds as well as the identity of clients, increasing the risk of money laundering. On the other hand, correspondent banking is being used for money laundering activities because it presents a form of business relationship that allows for commerce with the residential bank without precise and reliable information about the origin of the funds. Especially risky are correspondent relations with "shell" banks that physically do not exist in any country, as well as establishment of "off-shore" centers that provides certain legal and physical persons with certain "financial benefits".
General Conclusion: Considering a common characteristic of electronic and correspondent banking related to the physical absence of parties with which business relationship is established, it can be concluded that said activities enhance money laundering activities.
Validity of the research/work: This work's validity reflects itself within the acknowledgement of manifestations of money laundering enabled by electronic transfers.

Keywords
money laundering, electronic banking, correspondent banking, *shell* banks

Uvod

Pranje novca predstavlja aktivnost usmjerenu na prikrivanje stvarnog porijekla novčanih sredstava te ulaganja isti u finansijski i nefinansijski sistem s ciljem njegove legalizacije. S obzirom na njegovu učestalost, pranje novca je opisano kao kriminal 90-tih, pa čak i kao kriminal 21. stoljeća (Madinger, 2012, str. 300). Napredak u razvoju informacione tehnologije uticao je na pojavu novih oblika pranja novca koje karakteriše sofisticiranost, prikrivenost, veći nivo organizacije, međunarodni karakter kao i kreativnost kriminalaca. Pojava novih finansijskih usluga (mobilno bankarstvo, internet bankarstvo) i sistema plaćanja (elektronsko plaćanje) stvara uslove koji povećavaju rizik od pranja novca. Elektronski transfer novca sa jednog računa na drugi, te brzina kojom se isti realizuje omogućava prikrivanje stvarnog izvora novca.

U ovom radu bit će predstavljeno korištenje elektronskog i korespondentnog bankarstvo za aktivnosti pranja novca. „Prema Odluci o upravljanju informacionim sistemom u banci, Agencije za bankarstvo Federacije Bosne i Hercegovine, član 2. pod n) elektronsko bankarstvo je sistem koji omogućava klijentima banke obavljanje bankarskih poslova sa udaljene lokacije putem javnih komunikacionih mreža ili slično.“ Korespondentsko bankarstvo je pružanje bankarskih usluga jedne banke drugoj banci, što podrazumijeva postojanje korespondentskog računa jedne finansijske institucije koji ona drži kod druge finansijske institucije za svoj račun i u svoje ime (Zirojević, 2017. str. 19).

Naučni cilj rada ogleda u opisivanju faktora koji utiču na pojavu pranja novca u elektronskom i korespondentnom bankarstvu. Društveni cilj odnosi se na informisanje akademske i stručne javnosti o specifičnostima pranja novca korištenjem elektronskog i korespondentnog bankarstva. Kada je u pitanju struktura rada, prvi dio se odnosi se na definisanje pranje novca, faze od kojih se sastoji, krivično pravno određenje kao i karakteristike istog. U drugom dijelu rada, prije svega, je definisano elektronsko bankarstvo, zatim, prikazani domaći i međunarodni napori usmjereni na sprečavanje zloupotrebe istog i na kraju, predstavljeni mobilno i internet bankarstvo kao distributivni kanali elektronskog bankarstva. Korespondentno bankarstvo, kao specifičan oblik poslovnog odnosa i mogućnosti njegovog korištenja za aktivnosti pranja novca prikazani su u trećem dijelu rada.

Pri izradi rada koristit će se literatura domaćih i stranih autora te ostali naučni i stručni članci dostupni na internetskim stranicama. U radu će biti korištene sljedeće metode: metoda analize te deduktivna i induktivna metoda. Kada je u pitanju metoda prikupljanja podataka bit će korištena analiza sadržaja. Ograničenje ovog rada je teorijsko razmatranje pranja novca korištenjem elektronskog i korespondentnog bankarstva.

Naime, u istom će biti prikazana postojeća naučna saznanja kada je u pitanju predmet istraživanja. Stoga, ovim radom nije moguće ukazati na praktična rješenja koja bi mogla uticati na sprečavanje pranja novca u oblastima koje će biti obrađene u radu.

Pranje novca

Pranje novca predstavlja fenomen kojim osobe koje su stekle novac na nezakonit način nastoje prikriti stvarno porijeklo istog. Pojam "pranje novca" odnosi se na sve vrste postkriminalnih aktivnosti usmjerenih na prikrivanje imovinske koristi ili vrijednosti stečene na nezakoniti način (Meštrović, 2002). U ekonomskom smislu sam pojam pranja novca znači legalizacija kapitala stečenog kriminalnom djelatnošću, odnosno finansijske transakcije radi prikrivanja stvarnog porijekla novca i drugih oblika kapitala na tržištu (Bjelopoljak, 2012). Kako bi postigli navedeno osobe koje se bave pranjem novca poduzimaju različite radnje te stalno usavršavaju svoje aktivnosti korištenjem različitih tehnika pranja novca. Zajedničke karakteristike tih tehnika su (Gilmor, 2006, str. 33):

- oni koji „peru" novac moraju da sakriju pravi identitet vlasnika i porijeklo novca,
- moraju da zadrže kontrolu nad sredstvima, i
- moraju da promjene oblik sredstava.

Sofisticiranost, inventivnost i maštovitost raznih oblika pranja novca obuhvaćaju i usluge raznih financijskih stručnjaka, poreznih savjetnika, brokera, investicijskih kuća, konzultanata i advokata (Cindori, 2010, str. 20).

Pranje novca kao krivično djelo propisano je članom 209. Krivičnog zakona Bosne i Hercegovine te je stavom 1. istog definisan je osnovi oblik krivičnog djela pranja novca određeno je sljedeće:

1. „Ko novac ili drugu imovinu za koje zna da su pribavljeni počinjenjem krivičnog djela primi, zamijeni, drži, raspolaže njima, koristi u privrednom ili drugom poslovanju, vrši konverziju ili njihov prijenos ili na drugi način prikrije ili pokuša prikriti njihovu prirodu, izvor, lokaciju, raspolaganje, kretanje, vlasništvo ili drugo pravo, a takav novac ili imovinska korist su pribavljeni počinjenjem krivičnog djela:

a. u inostranstvu ili na teritoriji cijele Bosne i Hercegovine ili na teritoriji dvaju entiteta ili na teritoriji jednog entiteta i Brčko Distrikta Bosne i Hercegovine; ili
b. koje je propisano Krivičnim zakonom Bosne i Hercegovine ili drugim zakonom na državnom nivou, kaznit će se kaznom zatvora u trajanju od jedne do osam godina.

Članom 2. u stavovima a) i b) Zakona o sprečavanju pranja novca i finansiranja terorističkih aktivnosti određeno je sljedeće:

a) „Pranje novca podrazumijeva:

1. zamjenu ili prijenos imovine, ako je ta imovina stečena kriminalnim radnjama, a s ciljem prikrivanja ili zataškavanja nezakonitog porijekla imovine ili pružanja pomoći nekom licu koje je umiješano u takve aktivnosti radi izbjegavanja zakonskih posljedica počinjenih radnji;
2. prikrivanje ili zataškavanje prave prirode, mjesta porijekla, raspolaganja, kretanja, prava na ili vlasništva nad imovinom ako je ta imovina stečena kriminalnim radnjama ili činom učešća u takvim radnjama;
3. sticanje, posjedovanje ili korištenje imovine stečene kriminalnim radnjama ili činom učešća u takvim radnjama;
4. učešće ili udruživanje radi izvršenja, pokušaja izvršenja, odnosno pomaganja, podsticanja, olakšavanja ili davanja savjeta pri izvršenju bilo koje od navedenih radnji;
5. svrha, znanje, namjera potrebni kao elementi radnje pranja novca mogu se zaključiti na osnovu objektivnih i činjeničnih okolnosti.
6. pranjem novca smatrat će se i to kada su radnje, kojima je stečena imovina koja se pere, izvršene na teritoriji druge države."

Suština pranja novca je transformacija potencijalne kupovne moći[466] u djelotvornu (Madsen, 2009). Navedeno se postiže pretvaranjem „prljavog" novca u bankovni saldo, te uklanjanje njegove očigledne veze sa kriminalnim aktivnostima (Siwi, (2018). Dakle, cilj je promjena nezakonito stečenih novčanih sredstava u neki drugi oblik imovine nastojeći prikriti njegov nezakonit izvor. Iako proces pranja novca izgleda veoma komplikovano, isti uglavnom obuhvata tri faze i to: plasiranje, uslojavanje i integraciju[467] (Bjelopoljak, 2012). Različite finansijske usluge i platni sistemi omogućava bezbroj mogućnosti za stvaranje komplikovanih shema za prijenos novca. Pojava Interneta uticala je na nastajanje novih pojavnih oblika pranja novca kojim osobe koje se bave tim aktivnostima nastoje prikriti nezakonito stečen prihod. Novi pojavni oblici pranja novca povezani su s elektronskim poslovanjem i transakcijama realiziraju se putem korespondentnih računa, kreditnih kartica, Internet bankarstva, smart kartica i sl. U svrhu dugotrajnog pranja novca, može se koristiti novac uložen u firme, turističke objekte ili kockarnice. U slučajevima kada se pranje novca vrši uz pomoć gotovine, novac će se najčešće vraćati putem korespondentnog bankarstva u zemlju porijekla, u skladu s međunarodnim platnim prometom (Savić, 2016, str. 12).

[466] „Polman, Effron i Thomas (2018) kupovna moć ima osnovno svojstvo novca. Novac ima vrijednosti jer se može zamijeniti za robu ili uslugu, a stepen njegove vrijednosti zavisi od količine i kvaliteta robe ili usluge koja se može kupiti."

[467] Vidjeti više u: Savona, U. E. (1997). *Responding to money laundering: international perspectives.* Harwood Academic Publishers; 1 edition, str.23-27.

Elektronsko bankarstvo

Stalne tehnološke inovacije utiču na razvoj bankarskih proizvoda i usluga koje su stanovništvu dostupne putem elektronskih distributivnih kanala. Novi bankarski proizvodi i usluge uključuju elektronsko bankarstvo koje predstavlja upotrebu bankarskih usluga i izvođenje bankarskih transakcija koje obavlja sama stranka, vlasnik računa i komitent banke, posredstvom osobnih računara ili terminala s lokacija s kojih je moguć pristup telekomunikacijskoj mreži za prijenos podataka (Leko, 1998). Dostupnost različitih, prilagodljivih i cjenovno konkurentnih bankovnih usluga uz upotrebu modernih tehnologija, postaje temelj današnjeg bankarstva i društva (Bejatović i Kovačević, 2009).

Elektronsko bankarstvo predstavlja poslovanje kreditnih institucija pomoću telekomunikacijske mreže, a uključuje sve proizvode i usluge dostupne strankama tim putem te poslove koje kreditna institucija obavlja u svoje ime i za svoj račun koristeći se navedenim distribucijskim kanalom (Porobić, Bajraktarević, 2012, str. 85). Elektronskim se transferima teško ulazi u trag upravo zbog minimuma identifikacijskih informacija o stranci, čime se omogućava međunarodno kretanje ogromnih iznosa novca u samo jednoj sekundi. „Samo se jedan takav transfer kreće u rasponu i do milion dolara, dok procjene govore da se na dnevnoj razini razmjenjuju čak i trilioni dolara (u novčanicama i obveznicama (Savona, 2004, str. 153-154).

Kao i tradicionalni oblici pranja novca, pranje novca korištenjem elektronskog bankarstva obuhvata fazu plasmana, uslojavanja i integraciju. „Prema Daniali (2014) u fazi plasmana osobe koje koristeći usluge elektronskog bankarstva kupuju proizvode čiju vrijednost je teže utvrditi te je navedena aktivnost manje rizična. U fazi uslojavanja anonimnost i brzina koje karakterišu elektronsko bankarstvo onemogućava „ulazak u trag“ sumnjivim aktivnostima. Pranje novca u fazi integracije odvija se putem različitih metoda poput ulaganja, krivotvorenja isprava, transakcija prodaje i kupnje čije otkrivanje je teže jer se iste obavljaju u virtualnom prostoru.“

S ciljem sprečavanja pranja novca donesen je Zakon o sprečavanju pranja novca i finansiranju terorističkih aktivnosti. Istim je u članu 32. određeno da „pružalac usluge plaćanja i naplate dužan je prikupiti tačne i potpune podatke o nalogodavcu i uključiti ih u obrazac ili poruku koja prati elektronski transfer sredstava poslatih ili primljenih, bez obzira na valutu. Ti podaci moraju pratiti elektronski transfer tokom cijelog puta u lancu plaćanja, bez obzira na to da li posrednici u lancu plaćanja postoje i bez obzira na njihov broj.“

Međunarodni napori sprečavanja pranja novca i finansiranja terorizma putem elektroniskih transfera novca, a samim time i elektronskog bankarstva, istaknuti su u tački 14.

uvoda Treće direktive[468], članu 26. Zakona o sprečavanju pranja novca i finansiranja terorizma[469], kao i u VII Specijalnoj preporuci FATF koja ističe značaj i opasnosti napredne tehnologije.

Nivoi elektronskog bankarstva su različiti. U nastavku će biti taksativno prikazani (Yubin, 2003):

1. Osnovne e-bankarske informacije – web sajtovi koji informišu o bankarskim proizvodima i uslugama;
2. Jednostavne e-bankarske transakcije – web sajtovi koji nude upotrebu aplikacija za postavljanje upita o računima klijenta, ali bez mogućnosti transfera novca;
3. Napredne e-bankarske transakcije – web sajtovi koji klijentima omogućuju elektronski transfer na/sa računa, kao i onlajn upravljanje drugim bankarskim transakcijama.

Prednosti banaka koje koriste elektronsko bankarstvo su brojne. Neke od njih su (Vuksanović, 2006, str. 218):

- Stvaranje imidža inovativne firme koja je u stanju da svojim korisnicima ponudi najsavremenija tehnološka rješenja;
- Veće i bolje interaktivne mogućnosti – za banku koja se u tržišnim uslovima bori za svakog svog komitenta, najvažnija je komunikacija sa njim;
- Mogućnost racionalizacije potencijala banke – banka prenošenjem određenih servisa na internet smanjuje troškove poslovanja jer ne mora zbog povećanja broja komitenata da otvara novi poslovni prostor, da ga oprema i zapošljava nove službenike. Ovo je posebno interesantno za one geografske regione gdje banka nema mrežu ekspozitura ili ima mali broj komitenata;
- Samouslužno bankarstvo je korisno podjednako i za banku i za komitenta, jer komitent ima servise 24 časa dnevno, 7 dana u nedelji, a banka bez povećanja broja zaposlenih tako radi 365 dana u godini;
- Banka svojom pojavom na internetu dokazuje svoje konkurentne mogućnosti i svoj razvoj kao solidna, stabilna i tehnološki napredna firma

Primjena informacione tehnologije u bankarstvu praćena ekspanzijom elektronskog novca i elektronskog bankarstva nosi sa sobom pojavu novih oblika rizika. Pritom je

[468] Tačka 14. uvoda Treće direktive njezin obuhvat proširuje na sve radnje radnje koje institucije i osobe obuhvaćene direktivom obavljaju na Internetu.
[469] Članom 26. Zakona o sprečavanju pranja novca je propisana obaveza kreditnim i finansijskim institucijama, uključujući društva koja obavljaju određene usluge platnog prometa ili prijenosa novca prikupljanja tačnih i potpunih podataka o uplatiocu i uključiti ih u obrazac ili poruku koja prati elektronski prijenos novčanih srestava, poslanih ili primljenih u bilo kojoj valuti.

potrebno posebnu pažnju obratiti na upravljanje rizikom[470] koji proizlazi iz korištenja informacijskog sistema kako bi poslovanje banke bilo sigurno. Iako je osiguranje sigurnosti suštinski problem, set specifičnih rizika čine: operativni rizik[471], reputacioni rizik, pravni rizik, rizik internacionalnog poslovanja i ostali rizici.

Korištenje distributivnih mreža elektronskog bankarstva za aktivnosti pranja novca

Dio distributivne mreže elektronskog bankarstva čine Internet bankarstvo i Mobilno bankarstvo. Kako navodi Antonić (2012) Internet bankarstvo predstavlja obavljanje bankarskog poslovanja direktno od kuće, putem Interneta. Banka pruža usluge i omogućava plaćanje roba i usluga preko Interneta, izdaje platne kartice, otvara tekuće račune, obavlja mjenjačke poslove, omogućava provjeru stanja na računu vrši transfer elektronske gotovine i drugo. Internet bankarstvo je jedan od najpoznatijih načina za pranje novca u takozvanom sajber okruženju. Naime, zloupotrebom Internet bankarstva u svrhe pranja novca, banka može posredstvom svog servera da potvrdi da je klijent pristupio serveru sa određenog računa, u određeno vrijeme i veličinu transakcije koja je obavljena, ali nema mogućnost da izvrši tačnu identifikaciju klijenta, niti sa kojeg mjesta je pristupljeno serveru što omogućava da jedno lice kontroliše veliki broj računa i izvršava veliki broj transakcija bez znanja banke (Antonić, 2012, str. 68-69). Pored toga, osobe koje se bave aktivnostima pranja novca nastoje prenijeti nezakonito stečen novac putem regularnih finansijskih posrednika takozvanih „novac mazgi[472]“. „Novac mazge“ su veoma korisne kriminalnih organizacijama, jer se na taj način onemogućava otkrivanje glavnih aktera. Bankovni računi su otvoreni na ime „novac mazge“ koje se iskorištavaju od strane organiziranih kriminalnih grupa. Nekoliko studija potvrđuje važnu ulogu „novac mazgi“ u preusmjeravanju novca ukradenog od strane sajber (cyber) kriminala koji se bave

[470] „Kako navode (Poborić, Bajraktarević, 2012, str. 89) „na osnovu obavljene procjene rizika banka će, izmjenu ostalog, odrediti adekvatne kriptografske metode čija će primjena smanjiti rizik od narušavanja temeljnih načela informacijskog sistema. Kriptografske metode predstavljaju jednu vrstu logičkih kontrola kojima se dodatno osigurava zaštita informacija i smanjuje rizik od narušavanja temeljnih načela informacijskog stava. Kriptografija se najčešće upotrebljava za enkripciju (šifriranje podataka), elektronsko potpisivanje, očuvanje integriteta podataka i utvrđivanje autentičnosti korisnika (verifikacija stranke)“.

[471] Baselski odbor za nadzor banaka (2011) definirao je operativni rizik kao „rizik od gubitaka koji nastaje zbog neprimjerenih ili neuspješnih unutarnjih procesa, ljudi ili sistema ili zbog vanjskih događaja“.

[472] „Novac mazge“ je termin koji podrazumijeva osobe koje kriminalci iskorištavaju s ciljem prijenosa novca sa bankovnih računa. Te osobe se obično regrutuju putem oglasa uvjeravajući ih da će na taj način mogu zaraditi dosta novca (Bank safe online, 2008).

finansijskim krivičnim djelima u sajber okruženju, kao što su karding (carding)[473] i fišing (pfishing)[474] napadi.

Osim korištenja „novac mazgi" s ciljem izbjegavanja krivičnog progona novac se djeli na manje iznose koji ne zahtijevaju izvještavanje nadležnih organa od strane finansijskih institucija, te se na taj način može brzo i lahko izvršiti prijenos sa jednog na više bankovnih računa u više finansijskih institucija (Weaver, 2005). Kao što je istaknuto u izvještaju Vijeća Evrope, na osnovu studija slučaja otkriveno je da su osobe koje se bave aktivnostima pranja novca ponekad provodili stotine besmislenih transakcija preko različitih bankovnih računa, nakon čega slijedi ograničen broj podizanja gotovine (Council of Europe, 2012).

Mobilno bankarstvo kao dio distributivne mreže elektronskog bankarstva obuhvata finansijske transakcije preduzete korištenjem mobilnog uređaja. Mobilno bankarstvo je fenomen koji se nedavno pojavio, posebno u zemljama u razvoju, potaknut rastućom potražnjom za mikro-plaćanjem (Fiedler, 2013). Mobilna plaćanja obavljaju se korištenjem različitih protokola te telekomunikacijski operateri djeluju kao finansijski posrednici između klijenta i poslovnih subjekata, odnosno klijenta i finansijske institucije (Filipkowski, 2008). Mogućnost kupovine SIM kartice bez provjere identiteta omogućava anonimnost osobe koja vrši mobilno plaćanje što koriste „perači" novca (Villasenor, Bronk i Monk, 2011). Pitanja o kojima se često raspravlja kada je riječ o mobilnom bankarstvu odnose se na pitanje autentičnosti, poznavanja klijenata, autorizacije i integriteta transakcije, praćenja iznosa koje pojedinci imaju na raspolaganju kao i onih koje šalju (Bamoriya, 2016).

Korespodentno bankarstvo

Članom 3. Zakona o sprečavanju pranja novca i finansiranju terorističkih aktivnosti pod k) propisano je "korespondentni odnos je odnos između domaće banke ili druge finansijske institucije i strane banke ili druge finansijske institucije koji nastaje otvaranjem računa strane banke ili druge finansijske institucije kod domaće banke ili druge finansijske institucije ili uspostavljanjem bilo kojeg drugog poslovnog odnosa, kao i kada domaća banka ili druga finansijska institucija otvara račun kod strane banke ili druge finansijske institucije ili uspostavlja bilo koji drugi poslovni odnos." Osnovna ideja korespondentnog bankarstva proizlazi iz nedostatka unutrašnje umreženosti respondentne banke, a obuhvaća: međubankarske depozitne aktivnosti, međunarodne elektronske transfere

[473] Karding (carding) predstavlja kombinaciju visokotehnološkog i sajber kriminala i uključuje skup tehnika pomoću kojih kriminalci prikupljaju informacije o kreditnim karticama i drugim informacijama vezanih za plaćanje te način korištenja tih informacija od strane istih (Meijerink, 2013).
[474] Fišing (phishing) je vrsta socijalnog inžinjeringa koji omogućava dobijanje ličnih podataka od strane korisnika računara (Ollman, 2004).

sistema, upravljanje gotovinom, cheque clearing[475] i usluge uplate, naplatu, procesuiranje uplata strankama (u domaćoj i stranoj valuti) te transfere putem payable-through accounts (Esoimeme, 2015, str. 93).

Poslovanje putem korespondentnog bankarstva podrazumijeva poslovnu saradnju prilikom koje banka primatelj nije obavezna raspolagati tačnim ili potpunim podacima o porijeklu novčanih sredstava koja su predmet uplate. (Weisman, 2014, str. 6). Vrsta poslovanja kojom posluje respondent, kao i tržište na kojem prodaje svoje usluge, korespondentu ukazuju na visinu rizika koji mu respondent predstavlja (Cindori i Petrović, 2016, str. 769).

Problem predstavljaju korespondentni odnosi s visoko rizičnim bankama koje imaju manjkavu pravnu regulativu, nepouzdani (ili korumpirani) menadžment, a samim time i lošu preventivnu strategiju suzbijanja pranja novca i finansiranja terorizma. U visoko rizične strane banke mogu se ubrojiti (Porobić, Bajraktarević, 2012, str. 92):

- *shell* banke – koje fizički ne postoje niti u jednoj zemlji;
- *offshore* banke – kojima je licenca ograničena na poslovanje samo s osobama izvan teritorija te zemlje ili joj je onemogućeno poslovanje s lokalnom valutom;
- banke koje se nalaze unutar države koja ne primjenjuje odgovarajuće standarde ili ne sarađuje u međunarodnim nastojanjima sprečavanja pranja novca i finansiranja terorizma.

Shell banke (fiktivne banke) se članom 3. stav 1. tačka 10. Treće direktive definiraju kao kreditne institucije ili institucije za obavljanje istovjetnih poslova, inkorporirane u nadležnost države u kojoj nisu fizički prisutne (uključujući autentičnost i menadžment), a nisu povezane niti sa zakonski regulisanom finansijskom grupom. U skladu sa principima Wolfsberg grupe, banke imaju obavezu odbiti uspostavu ili nastavak korespondentnog bankarstva s bankom koja je osnovana u jurisdikciji u kojoj nije fizički prisutna i povezana s normativno uređenom finansijskom grupom, poput *shell* banke (Esoimeme, 2015, str. 93).

Termin ofšor (engl. offshore) je iz engleskog prava, odnosno *common law* pravnog sistema, a prevodi se kao eksteritorijalno područje. Ovaj oblik poslovanja obavljao se na ostrvima izvan teritorije Velike Britanije, te je tako i nastao sam termin, a važio je za sva područja koja finansijskim institucijama nude specijalne pogodnosti, te se iste ogledaju u liberalnim ekonomskim i poreskim propisima. „Kako navode (Čudan i Fijat, 2015, str. 62)

[475] S obzirom na to da su međunarodni elektronski transferi pod povećanim nadzorom, „perači" novca mijenjaju oblik novca koristeći gotovinske čekove kao djelotvornu alternativu. Cheque clearing je transferiranje čeka iz banke u kojoj je položen do banke kod koje je podignut, dok se kretanje novca odvija u suprotnom smjeru (Weisman, 2014., str. 5–6).

ofšor centri su se počeli osnivati za vrijeme velike ekonomske krize 30-ih godina prošlog vijeka i to uz pomoć američkog organiziranog kriminala."

Razlog koji se najčešće navodi za osnivanje ofšor finansijskih centara jeste pružanje određenih „finansijskih pogodnosti" pravnim i fizičkim licima koja koriste njihove usluge, a te pogodnosti se najčešće koriste za legalizaciju ili skrivanje nelegalno stečenih sredstava (Bošković, 2005, str. 48). „Kako navodi Banović (2002) ovi finansijski centri imaju nekoliko osnovnih karakteristika:

- višestruki niz finansijskih transakcija,
- korištenje posrednika za njihovo izvođenje,
- razvijenost međunarodne mreže, takozvanih *shell* kompanija, uključujući i specijalizovane *off-the-shell* varijacije koje se gase odmah po završetku transakcije, kao i
- korištenje više ofšor centara za jednu operaciju pranja novca."

Prema Zirojeviću (2017) priroda korištenja korespondentskih računa stvara indirektan odnos u kojem korespondentska banka pruža bankarske usluge pravnim i fizičkim licima za koja ne postoje informacije o potvrdi identiteta. Pri tome se korespondentska banka oslanja na informacije respondentske banke. Uspostavljeni odnos se usložnjava u sljedećim slučajevima (Bošković, 2005, str. 39-40):

- kada se kao respondentska banka javlja ofšor finansijska institucija,
- kada je nemoguće procjeniti kvalitete mehanizama sprečavanja pranja novca iako postoji legislativa koja važi u respondentskoj banci,
- kada nije moguće nadgledati pojedinačne transakcije koje su uključene u velike transakcije između korespondentskih računa zato što banka nije u vezi sa pošiljaocem ili korisnikom tih transakcija i
- u slučajevima kada postoje podrespondenti, kada respondentska banka nudi korespondentske usluge.

Zaključak

Pranje novca predstavlja djelatnost koja obuhvata poduzimanje različitih aktivnosti s ciljem prije svega, prikrivanja nezakonito stečenih novčanih sredstava, a potom integraciju istih u legalne finansijske tokove. Dakle, pranje novca je proces koji se sastoji od tri faze, od plasmana „prljavog" novca do integracije istog. Radi postizanja navedenog koriste se različite tehnike od strane osoba koje se bave aktivnostima pranja novca. Pranje novca u sajber okruženju se vrši stvaranjem komplikovanih shema za prijenos novčanih sredstava koje je teško otkriti. Pojava elektronsko i korespondentno bankarstvo uticala je na razvoj novih pojavnih oblika pranja novca.

Elektronsko bankarstvo je dostupno stanovništvu putem elektronskih distributivnih kanala što omogućava obavljanje transakcija brzo i jednostavno. Takva vrsta poslovanja ima niz benefita kako za klijente koji na taj način mogu obavljati transakcije od kuće, tako i za banke koji pružanjem novih usluga postaju konkurenti na tržištu. Međutim, elektronsko bankarstvo može biti korišteno za aktivnosti pranja novca na različite načine, što zahtijeva procjenu rizika od strane finansijskih institucija te upravljanje istim.

Pranje novca korištenjem elektronskog bankarstva se ostvaruje na osnovu takozvanih „novac mazgi" koje predstavljaju osobe čije bankovne račune kriminalci upotrebljavaju s ciljem prijenosa novca koji je stečen na nezakonit način. Bankovni računi izloženi su sajber napadima s ciljem dobijanja ličnih podataka. Obavljaju više transakcija manjeg iznosa sa različitih računa na više različitih računa što otežava otkrivanje tih nezakonitih aktivnosti. Pored toga, mogućnost kupovine SIM kartice bez provjere identiteta kupca može uticati na korištenje mobilnog bankarstva radi pranja novca.

Korespondentno bankarstvo predstavlja oblast poslovanja koja omogućava pružanje usluga prijenosa novca sa računa jedne na račun druge banke uz određenu naknadu. Isto je izloženu riziku od pranja novca jer omogućava poslovanje sa rezidentnom bankom bez tačnih i pouzdanih informacija o porijeklu novčanih sredstava. Posebno su rizični korespondentni odnosi sa *shell* bankama koje fizički ne postoje niti u jednoj zemlji te bankama čije poslovanje je ograničeno samo na osobe u drugim zemljama. Stvaranjem tih ofšor centara je omogućeno skrivanje nezakonitih novčanih sredstava. U slučaju kada se kao rezidentna banka javlja ofšor finansijska institucija dolazi do usložnjavanja odnosa koji je uspostavljen u okviru korespodetnog poslovanja.

Literatura

1. Antonić, J. (2012). Abuse of Modern Technology of Money Laundering. *Economic outlook/Ekonomski pogledi,* 3, 66-79.
2. Bank safe online. (2008). Payment advice. Helpful information from the UK payments association.banke Money Mules. http://www.banksafeonline.org.uk/documents/money_mules_advice_guide_final.pdf pristupljeno 26.06.2019. godine.
3. Banović, B., (2002). *Obezbeđenje dokaza u kriminalističkoj obradi krivičnih dela privrednog kriminaliteta*, Beograd,Viša škola unutrašnjih poslova.
4. Baselski odbor za nadzor banaka, (2011.), *Dobre prakse za upravljanje operativnim rizikom i nadzor nad njim*, Banka za međunarodne namire.
5. Bamoriya, P. (2016). Issues in Mobile Banking in India with references to Regulations. *Journal of Accounting & Management,* 6 (1), 17-34.
6. Bejatović, M i Kovačević, M. (2009), Elektronsko bankarstvo- EFT, *Pravo - teorija i praksa*, 26 (9-10), str. 36-43.
7. Bjelopoljak, A. (2012). *Pranje novca Sumnjive transakcije i Off shore zone*. JU „Gradska biblioteka“ , Kakanj
8. Bošković, G., (2005). *Pranje novca*. BeoSing, Beograd
9. Cindori, S. i Petrović, T. (2016). Indikatori rizičnosti bankarskog sektora u okvirima prevencije pranja novca. *Zbornik PFZ*, 66, (6) 761-784.
10. Cindori, S. (2010). Procjena stupnja rizika poreznih savjetnika u sustavu sprječavanja pranja novca. *Zbornik Pravnog fakulteta Sveučilišta u Rijeci* 31 (2). str. 809-827.
11. Council of Europe, (2012). Moneywal report: criminal money flows on the internet: methods, trends and multi-stakeholder counteraction
12. Čudan, A. i Fijat, A., (2015). *Rizici i prevencija pranja novca – monografija,* Subotica, Printex, str. 62.
13. Daniali, G. (2014). E- money laundering Prevention. *New Marketing Research Journal*, 4, 29-38.
14. Direktivom 2005/60/EC Evropskog Parlamenta i Savjeta od 26. oktobra 2005 o sprečavanju korištenja finansijskog sistema u svrhu pranja novca i finansiranja terorizma.
15. Esoimeme, E. E., *The Risk-Based Approach to Combination Money Laundering and Terrorist Financing*, Eric Press, New York, 2015.
16. Fiedler, I. (2013). *Online gambling as a game changer to money laundering*? OnlineGamblingasaGameChangertoMoneyLaundering.pdf pristupljeno 27.06.2019.godine.
17. Filipkowski, W. (2008). Cyber laundering: an analysis of typology and techniques. Int. *J. Crim. Justice Sci*. **3** (1), 15–27
18. Gilmor, V. S., (2006). *Prljav novac, Razvoj međunarodnih mjera za borbu protiv pranja novca i finansiranja terorizma.* Prevod Mates, V., Izdanje Savjeta Evrope, „Plus“ Beograd.

19. Krivični zakon Bosne i Herceogivne Krivični zakon Bosne i Hercegovine (Službene glasnik Bosne i Hercegovine br. 03/03, 32/03, 37/03, 54/04, 61/04, 30/05, 53/06 i 55/06, 8/10, 47/14, 22/15, 40/15, 35718),
20. Leko, V. (1998.). Financijsko okruženje marketinga, materijal za izučavanje na disciplini "Financijsko okruženje marketinga", Zagreb: Ekonomski fakultet Sveučilišta u Zagrebu, Specijalistički poslijediplomski studij "Upravljanje poslovnim-industrijskim marketingom"..
21. Madinger, J. (2012). *Money Laundering: Guide for Criminal Investigator.* Third Edition, CRC Press, Boca Raton.
22. Madsen, F. G. (2009), *Transnational organised crime*, Oxon: Routledge.
23. Meijerink, T. J. (2013). *Carding Crime Prevention Analysis.* Netherlands Police Agency, Universiteit Twente.
24. Meštrović, D., (2002), Legalizacija nelegalno stečenog kapitala. *Policija i sigurnost* 11 (2002), 1-3, str. 147.
25. Odluci o upravljanju informacionim sistemom u banci (2017). Agencije za bankarstvo Federacije Bosne i Hercegovine
26. Ollman, G. (2004). The Phishing Guide – Understanding and Preventing.*White Paper, Next Generation*. Security Software Ltd.
27. Polman, E, Effron, D. A. i Thomas, M. R. (2018). Other people's Money: Money's Perceived Purchasing Power is Smaller for Others for the Self. *Journal of Consumer Research,* 45 (1), 109-125.
28. Porobić, M i Bajraktarević, M. (2012). Cyber kriminal, pranje novca i finansijske istrage. Jačanje tužilačkih kapaciteta u sistemu krivičnog pravosuđa.
29. Savona, E. (2004), *Responding to Money Laundering: International Perspectives*, Harwood Academic Publishers, London, str. 153-154.
30. Savić, B. (2016). Money Laundering and Ways of Suppressing It In The Public Sector *Безбједност - Полиција* - Грађани, година XII број 1–2/16.
31. Siwi, Y. E, (2018) Mafia, money-laundering and the battle against criminal capital: the Italian case. *Journal of Money Laundering Control, Vol. 21 Issue:* 2, 124-133,
32. Vuksanović, E. (2006). *Elektronsko bankarstvo*, Beograd, Beogradska bankarska akademija, str. 218.
33. Yubin, M. (2003). *E-Banking: Status, Trends, Challenges and Policy Issues. CRBC Seminar*, The Development and Supervision of e-banking, Shangai.
34. Weaver, S. (2005). Modern day money laundering: does the solution exist in an expansive system of monitoring and record keeping regulations? Annu. Rev. Bank. *Law Financ. Law* **24**, 443–465
35. Weisman, M. F. 2014. *Money laundering legislation, regulation and enforcement,* American Bar Association, Chicago, , str. 5 – 6.
36. Villasenor, J., Bronk, C. i Monk, C. (2011). *Shadowy figures: tracking illicit financial transactions in the murky world of digital currencies, peer-to-peer networks, and mobile device payments.* Paper, The Brookings Institution and the James A. Baker III Institute for Public Policy

http://bakerinstitute.org/media/files/Research/d9048418/ITP-pub FinancialTransactions-082911.pdf pristupljeno 30.06.2019.godine

37. Zakon o sprečavanju pranja novca i finansiranja terorističkih aktivnosti "Službeni glasnik BiH" br. 46/16.
38. Zirojević, A. (2017). Specifičnosti pranja novca u bankarskom sektoru. *PRAVO – teorija i praksa*, 7-9, 16-26.

Kriminalističke teme
Zbornik radova
Godina XIX, Broj 5, 2019.
ISSN 1512-5505

Panel 8

CYBER SIGURNOST: UMJETNOST NEVIDLJIVOSTI I ESTETIKA DE-CEPCIJE

Kriminalističke teme
Zbornik radova
Godina XIX, Broj 5, 2019.
ISSN 1512-5505

SVEOBUHVATNI PRISTUP NATO-A SAJBER ODBRANI
NATO'S COMPREHENSIVE APPROACH TO CYBER DEFENSE

Pregledni naučni rad

Sergej Cvetkovski[476]
Vancho Kenkov[477]

Sažetak

Inspiracija za rad i problem (i) koji se radom oslovljava (ju): U eri dominacije informacione tehnologije, sajber prostor je postao značajan sigurnosni problem za vlade koje su prisiljene poduzeti dodatne mjere za poboljšanje sajber sigurnosti.
Ciljevi rada (naučni i/ili društveni): U situaciji povećane upotrebe informacionih tehnologija u današnjem globaliziranom svijetu, cyber odbrana postaje veliki prioritet ne samo za pojedine zemlje, već i za njihove kolektivne mehanizme.
Metodologija/Dizajn: Ovaj rad bavi se problemima NATO kibernetičke odbrane i sajber bezbjednosti i mogućim poraznim efektima i posljedicama cyber napada. U tom cilju autori će koristiti dostupnu stručnu literaturu i online publikacije na ovu temu, na kojima će se primijeniti kvalitativna analiza sadržaja. Teret istraživanja bit će na strateškim i operativnim mjerama sigurnosti i obrane Saveza, jer postoji ograničena dostupnost informacija o mjerama taktičkog nivoa koje su povjerljive.
Ograničenja istraživanja/rada: Autori rada nastoje da razrade koordinirani i sveobuhvatni pristup NATO-a u postizanju efektivne sajber odbrane i sigurnosti komunikacionih i informacionih sistema za članice Saveza i njihove partnere.
Rezultati/Nalazi: Pitanja koja se pojavljuju su: koliko NATO savez ozbiljno razmatra rizike cyber napada, na koji način to odražava promjene u politici odbrane i strateškim konceptima Alijanse, koji je pristup rješavanju ovog novog sigurnosnog izazova i koje su obaveze na nivou Saveza?!
Generalni zaključak: Odgovor je da se fokus NATO-a u narednoj deceniji mora odnositi na razvoj sajber-moći.
Opravdanost istraživanja/rada: Tehnologija je u srcu naših čvrsto povezanih društava. Oslanjanje modernih društava na informacionih tehnologija podrazumijeva očigledne bezbjednosne probleme. Cyber prijetnje i napadi postaju sve češći, sofisticiraniji i štetniji. Čak i vojske i službe bezbjednosti koje se u velikoj mjeri oslanjaju na sajber prostor za obavljanje svojih misija nisu imune na takve napade.

[476] Associated Professor. Institute for Security, Defense and Peace - Faculty of Philosophy, Skopje, sergej@fzf.ukim.edu.mk
[477] PhD Professor. Institute for Security, Defense and Peace - Faculty of Philosophy, Skopje, vancok@fzf.ukim.edu.mk

Ključne riječi
sajber prostor, sajber napadi, sajber odbrana, NATO, sveobuhvatnost

Abstract
Reason for writing and research problem (s): In the era of domination of information technology, cyber space has become a significant security issue for governments that are forced to take additional measures to enhance cyber security.
Aims of the paper (scientific and/or social): In a situation of increased use of information technology in today's globalized world, cyber defense is becoming a high priority not only for individual countries, but also for their collective mechanisms.
Methodology/Design: This paper addresses the problems of NATO cyber defense and cyber security and the possible defeating effects and consequences of cyber attacks. To this end, the authors will use the available expert literature and online publications on this subject, on which a qualitative analysis of the content will be applied.
Research/Paper limitation: The authors of the paper make an attempt to elaborate NATO's co-ordinated and comprehensive approach in achieving effective cyber defense and security of communication and information systems for Alliance members and their Partners.
Results/Findings: The burden of the research will be on the strategic and operational security and defense measures of the Alliance because there is limited availability of information on tactical level measures that are kept confidential. The issues that arise are: how much does the NATO Alliance seriously consider the risks of cyber attacks, in which way it reflects the changes in the defense policy and strategic concepts of the Alliance, what is the approach to tackling this new security challenge and what are the commitments at the level the alliance to further improve security in cyber space?!
General Conclusion: The answer is that NATO's focus in the next decade must be on the development of cyber power.
Research/Paper Validity: Technology is at the heart of our tightly knit societies. Modern societies' reliance on information technology implies obvious security problems. Cyber threats and attacks are becoming more common, sophisticated and harmful. Even the military and security services that rely heavily on cyberspace to carry out their missions are not immune to such attacks.

Keywords
cyber space, cyber attacks, cyber defense, NATO, comprehensiveness

Uvod

Tehnologija je u srcu naših čvrsto povezanih društava. Oslanjanje modernih društava na informacionih tehnologija podrazumijeva očigledne bezbjednosne probleme. Cyber prijetnje i napadi postaju sve češći, sofisticiraniji i štetniji. Čak i vojske i službe bezbjednosti koje se u velikoj mjeri oslanjaju na sajber prostor za obavljanje svojih misija nisu imune na takve napade. Vlade širom svijeta počele su da razvijaju procedure i aktivnosti za zaštitu sajber prostora od sajber napada, a ta sposobnost je postala od suštinskog značaja za ostvarivanje sajber odbrane. Mnoge vlade priznaju da se sajber bezbjednost može postići samo kroz međunarodnu saradnju i partnerstvo. Ali posljedice od sajber napada ne utiču samo na pojedinačne vlade, već i na velike međunarodne

organizacije i saveza kao što je NATO savez, pri čemu su napadnuti komunikacijski i informacioni sistemi ovog saveza, tako da i NATO savez primjenjuje koordinirani pristup zaštite ključne informacione i komunikacijske infrastrukture.

Nakon događaja u Estoniji u maju i aprilu 2007. godine, kada je napadnuta informacijska infrastruktura zemlje, NATO je počeo kontinuirano razvijati i poboljšavati zaštitu svojih komunikacijskih i informacionih sistema od napada i neovlaštenog pristupa. Alijansa je također usmjerila svoje aktivnosti na podršku individualnih napora za zaštitu informacione infrastrukture svake države članice. U samom NATO-u u Lisabonu 2010. godine, sajber odbrana je predstavljena kao jedan od najvažnijih izazova Saveza u budućnosti. Posebno je naglašen značaj zaštite informacione i komunikacione infrastrukture NATO-a.

Danas se NATO i njegovi saveznici oslanjaju na jaku i elastičnu kibernetičku odbranu kako bi ispunili ključne zadatke Alijanse za kolektivnu odbranu, upravljanje krizama i sigurnosnu saradnju. NATO savez bi trebao nastaviti da bude spreman da brani svoje mreže i operacije protiv sve veće sofisticiranosti sajber prijetnji i napada s kojima se suočava. Glavni fokus u sajber odbrani NATO-a, pored zaštite mreža koje uključuju operacije i misije, jeste jačanje sajber otpornosti među svim državama članicama saveza.

1. Kiberprostor - novi predmet zaštite

1.1 Novi prostor rata

Prema međunarodnom pravu, postoji opšta saglasnost između država da sajber prostor podleže principima suvereniteta i nadležnosti, jednako kao i zabrana mješanja u poslove drugih država i upotrebe sile. U sajber prostoru države imaju pravo da koriste "kontra-mjere" kako bi uspostavile pravnu situaciju ili de-eskalirale nezakonitu situaciju. Tipično, takve mjere su obično fizičke operacije blokiranja i operacije odbijanja u području, na primjer, kako bi se spriječilo slijetanje ili prelet zrakoplova. U kibernetičkom prostoru, država može legalno preuzeti čin negiranja/odbijanja kao protumjere protiv zlonamjerne sajber aktivnosti sve dok ne dobije naknadu za nanesenu štetu.

Države se ohrabruju da istraže kako primijeniti međunarodno pravo u cyber domenu, u smislu da li su postojeći zakoni dovoljni. Postavlja se pitanje da li su svi cyber napadi kršenje međunarodnog prava?! Možemo nagađati da velike sajber sile ne žele da razgovaraju o crvenim linijama ofanzivnih sajber aktivnosti, što rezultira pozivima na različite napore usmjerene na jačanje političkih apetita za akciju.

U tom pravcu, i Crveni krst je prilično zabrinut zbog humanitarnih troškova sajber napada, ističući da organizacija koristi sajber prostor za komunikacije i logistiku i podložna je brojnim sajber napadima. Države se moraju tačno složiti o tome šta je okarakterizirano kao napad i da li su napaduti podaci zaštićeni međunarodnim humanitarnim pravom

(MHP). U tom smislu, Medjunarodni komitet crvenog krsta MKCK (ICRC) se zalaže za široko tumačenje pojma "napad" unutar MHP, koji također uzima u obzir slučajeve kao što su špijunaža i smetnje. Brisanje ili promjena podataka također može prouzrokovati više štete za civile nego fizičko uništenje nekih objekata, i stoga Međunarodni komitet crvenog krsta (MKCK) smatra podatke kao objekat zaštićen od MHP.

Sajber prostor je prioritetna tema za raspravu u UN-u. Međunarodno pravo također treba da se primjenjuje na sajber prostor, tako da će nauka, aktivnosti i pojedinci imati koristi, što će rezultirati odgovornim ponašanjem država u sajber prostoru kako bi se garantovala sloboda izražavanja i ideja, kao i bezbjedno okruženje za korisnike. Veći fokus je na miroljubivoj upotrebi sajber-prostora uz predanost da će se razviti novi ili primijenjeni postojeći mehanizmi za povećanje povjerenja među državama članicama UN-a o cyber mogućnostima i namjerama. Primjer je pokušaj Organizacije američkih država da implementira norme protiv proliferacije u kibernetskom prostoru, uključujući određivanje lokalnih kontakt tačaka za cyber sigurnost u svakoj državi članici i kroz razvoj nacionalnih planova za kibernetičku sigurnost (Jabbari 2018).

Sajber prostor je oblast informacionog okruženja koja se sastoji od nezavisne mreže informacione infrastrukture, uključujući Internet, telekomunikacione mreže, računarske sisteme i ugrađene procesore i kontrolore (Kissel, 2011). Sajber prostor nema zajedničku definiciju i ovaj termin se koristi za opisivanje ne-fizičkog prostora koji se sastoji od više komunikacijskih i informacionih sistema koji su povezani sa globalnom mrežom. Termin se koristi za opisivanje virtuelnog svijeta informacionih sistema gdje se predmet u sajber prostoru odnosi na pakete informacija koji protiču kroz kompjuterski sistem ili mrežu. Sa pojavom Interneta, sajber prostor sada obuhvata globalnu mrežu kompjutera.

Sajber prostor, koji se smatra petim prostorom ratovanja (nakon kopna, mora, vazduha i svemira) sastoji se od svih kompjuterskih mreža u svetu i svega što one povezuju i kontrolišu preko kablove, vlakna i bežične veze. Što se tiče mreže, sajber prostor nije samo Internet, već i mnoge druge mreže koje ne bi trebalo da budu dostupne preko interneta (Schreier, Weekes i Winkler 2011, str. 8). Sajber prostor je medij koji se sastoji od velikog broja učesnika sa sposobnošću interakcije i je domen koji karakteriše upotrebu elektronskog i elektromagnetnog spektra za skladištenje, modifikovanje i brisanje podataka putem mrežnih sistema i povezane fizičke infrastrukture (Baykal, 2013, str. 7). U eri informacionih tehnologija i povezivanja ljudi kroz komunikacione i informacione sisteme, sajber prostor postaje jedna od kritičnih oblasti nacionalne bezbjednosti, jer je ranjivost država na sajber kriminal značajan bezbjednosni rizik.

Sve veći naglasak se stavlja na razmatranja da se čini da rat prelazi u sajber prostor. Realizacija potencijalnog rata u sajber-prostoru dovešće do formiranja novih organizacija, koncepata i elemenata sukoba koji su paralelni, ali još uvijek različiti od konvencionalnih načina ratovanja (Moran, 2009, str. 138-139).

Uz sve veću ovisnost o informacijskoj tehnologiji, sve vitalne infrastrukture u državi su osjetljive na neku vrstu vanjskog napada. Aktivnosti koje se koriste za prijetnju vladama i međunarodnim organizacijama smatraju se sajber terorizmom i kao takve oslabljuju vladine ili vojne komunikacijske i informacione sisteme. Pojedinci, nacionalne grupe i cijele vlade koriste sajber prostor za ostvarivanje interesa kroz zlonamjerne aktivnosti. Terorističke grupe se regrutuju, obučavaju i djeluju kroz interneta. Kroz Internet organizuju se i kriminalne organizacije, kradu se i koriste se finansijski podaci sa profitom koji prelazi onaj trgovine drogom. Obavještajne službe također kradu poslovne i državne tajne putem interneta (Reveron, 2012, str. 3).

Čak i ako se stručnjaci ne slažu oko obima i prirode prijetnje, države još uvijek moraju usvojiti određene mjere za jačanje zaštite informacionih sistema. Ona bi trebala uključivati blisku saradnju među državama, izraženu kroz zajedničke vježbe kroz koje će se provoditi simulacija i modeliranje sposobnosti za razumijevanja utjecaja mogućeg napada na međusobno povezane i međusobno ovisne informacijske infrastrukture. To će doprinijeti razvoju novih mogućnosti za otkrivanje i identifikaciju mogućih negativnih implikacija na informacionu infrastrukturu. Poduzete mjere kategorizirane su kao kibernetička sigurnost, sajber obrana i informacijska sigurnost.

1.2 Sajber bezbjednost i sajber odbrana

Sigurnost sajber prostora danas predstavlja značajan izazov za nacionalnu sigurnost. Sajber bezbednost se odnosi na tehnologije, procese i prakse koji su dizajnirani da zaštite mreže, računare, programe i podatke od napada, od oštećenja ili od neovlašćenog pristupa. U kontekstu sajber bezbjednosti, vlada treba da implementira određene mjere kao što su dizajniranje sigurnih i otpornih mreža, sigurni komunikacijski i informacijski sistemi, te korištenje sigurnosnih politika, standarda i održivih sigurnosnih mehanizama. Sajber prostor postaje prilično dinamično okruženje koje prelazi državne granice i uvijek stvara nove dimenzije nesigurnosti kao rezultat pojave višestrukih centara moći u sajber prostoru, vladinog ili nevladinog. U ovim okolnostima, gore pomenuti akteri će oblikovati događaje u sajber prostoru koji će biti višestruko ciljani i uticati na komunikacijske i informacione sisteme sa katastrofalnim posljedicama.

Sajber bezbjednost ili sposobnost da se zaštiti i odbrani upotreba sajber prostora od sajber napada je osnova sajber odbrane. Obezbjeđivanje društva od sajber bezbjednosti postalo je jedan od najvećih prioriteta, i u tu svrhu vlade moraju energično braniti mreže i sisteme prijetnji unutrašnjim i spoljašnjim prijetnjama. Prema Bajkalu (Baykal, 2013, str. 13-14) u opsegu sajber obrane su štetne radnje ili prijetnje (moguće ili stvarne). Sajber odbrana se fokusira na štetne radnje koje su izvorno izvedene iz sajber prostora. Svrha sajber odbrane je da obezbijedi trajnost usluga sajber prostora za korisnike.

Sajber odbrana predstavlja sposobnost da zaštiti i zaštiti sajber prostor od mogućih sajber napada. Sajber napad je napad na sajber prostor u cilju ometanja, onemogućavanja, uništavanja i kontrole računarske infrastrukture ili uništavanja integriteta podataka i informacija ili njihove krađe.

Cyber odbrana danas predstavlja veliki izazov za vlade i može se postići samo kroz međunarodnu saradnju i partnerstvo. Vlade moraju podsticati koherentan odgovor na osiguranje sajber prostora, a na nacionalnom nivou to je zajednička odgovornost svih ministarstava i vladinih agencija, privatnog sektora i građana. Na regionalnom i međunarodnom nivou, ovo uključuje saradnju i koordinaciju sa svim relevantnim partnerima. Također zahtijeva izbor najbolje kvalifikovanog osoblja koje će voditi ove napore (Schreier, Weekes & Winkler, 2011, str. 14). Korišćenje, upravljanje i odbrana kritične informacione strukture je mnogo lakše kada se odgovornost dijeli i kada postoji međunarodna saradnja i partnerstvo.

1.3 Informacijska sigurnost

Sigurnost informacija ili kako i da nazovemo ovo područje koje se bavi sve većim poremećajima u povjerljivosti, dostupnosti i integritetu informacija, je glavni imperativ informacione sigurnosti (Information Security), osiguranja informacija (Information Assurance) i kibernetičke odbrane (Cyber Defense). Svi navedeni termini imaju više sličnosti nego razlike u načinu na koji se percipiraju sigurnost informacija i sigurnost informacijskih sustava. Sve se one međusobno preklapaju i dijele zajednički izazov, sigurnost informacija.

Međutim, postoje i pokušaji da se predstave kao odvojene discipline. Naime, informacijska sigurnost je predstavljena kao podskup informacijske bezbjednosti. Ali, i informaciona bezbjednost je predstavljena kao podskup sajber odbrane, tj. Sajber bezbjednosti i obrnuto. Mogućnost konfuzije proizlazi iz sličnosti i činjenice da je sajber bezbjednost relativno nova disciplina (Withman & Mattord, 2011). Stoga, ona želi da prihvati mišljenje da sajber odbrana pokriva samo sajber prostor, ili da je sajber odbrana u stvari bezbjednost informacija plus bezbjednost mreža. Međutim, povećana opasnost od napada informacijske sigurnosti prisilila je vlade da uzmu u obzir i rizike takvih napada na njihove komunikacijsko-informacijske sustave i druge kritične infrastrukture. Pažnja je također posvećena uključivanju država u informacijski rat i mogućnost kolapsa komunikacione infrastrukture ako se ona ne brani (Pindar i Rigelsford, 2011).

U tom pravcu, pored nacionalnog izazova za zaštitu informacija, zaštita NATO informacionog sistema je sastavni dio funkcionisanja Alijanse.

2. NATO-ov pristup sajber odbrani

Suština debata i aktivnosti sajber odbrane je u trci između napadača i branilaca, oko toga koji će prvi otkriti sljedeću slabost protivnika. Efekti sajber napada mogu biti prilično neočekivani i štetni. NATO je vojno-politički savez sa 70 godina zajedničkog cilja za sprečavanje sukoba i očuvanje mira i stabilnosti za oko 1 milijardu ljudi u evroatlantskom području. NATO, kao Savez od 29 zemalja članica Sjeverne Amerike i Evrope, nastoji to ostvariti obećavajući da će se članice braniti međusobno suglasno frazi: svi za jednoga, jedan za sve - obaveza poznata kao kolektivna odbrana.478 Oni prepoznaju rizik od sajber napada. Isti princip kolektivne odbrane odnosi se na pristup NATO-a sajber prostoru. NATO-ovo razmišljanje o sajber odbrani napreduje posljednjih godina. Sajber odbrana se više ne smatra čisto tehničkim pitanjem, već je dobila politički i strateški značaj. Široko rasprostranjeni sajber napadi koji su poremetili vladine i bankarske sisteme u Estoniji 2007. godine jasno su ukazali na evoluciju percepcije potencijalnih ranjivosti u našim srodnim i digitaliziranim društvima. Od napada u Estoniji, sajber odbrana je postala suštinski prioritet Alijanse.

2.1 Politika u oblasti sajber odbrane i hronologija obaveza

U aprilu 2008. godine, NATO je odobrio Politiku kibernetičke odbrane kao zajednički koordinirani pristup čiji je cilj zaštita ključnih informacijskih i komunikacijskih sistema i jedini odgovor na sajber napade. Prateći prioritete, osnovan je Organ za upravljanje sajber odbrane CDMA (Cyber Defence Management Authority), sa ovlašćenjem da upravlja krizom u sajber odbrani i da reaguje u slučaju sajber napada na svoje članove. CDMA je imala zadatak da sprovede sajber odbranu NATO informacione i komunikacione infrastrukture. Politika sajber odbrane naglašava potrebu da se zaštiti ključni informacioni sistem Saveza i da se pruži mogućnost da se zemljama članicama, na njihov zahtev, pomogne da zaustave sajber napad. Infrastruktura unutar NATO-a je neizbježno povezana. Ona prelazi nacionalne granice i ono što se dešava u jednom dijelu mreže može vrlo brzo utjecati na drugu, uzrokujući potencijalno katastrofalne rezultate (Hartmann, 2009, str. 186-187).

Na samitu NATO-a u Lisabonu, sajber bezbjednost je prikazana kao novi bezbjednosni izazov sa kojim se NATO mora suočiti u narednim godinama, a NATO je identifikovao sajber odbranu kao važan prioritet. U takvim okolnostima, Alijansa mora pomoći državama članicama da razviju sposobnosti koje se mogu brzo koristiti u skladu sa misijama Alijanse. Za "manje" članice Alijanse biće lakše razviti zajedničke odgovore na kibernetičke prijetnje, umjesto da djeluju samostalno u tom smjeru. NATO kao organizacija može pomoći i dati savjete o tome kako zaštititi kritičnu informacijsku infrastrukturu. Također, izgradnja bliskih veza sa privatnim sektorom, koji ima veliku ekspertizu, od posebne je važnosti. Neophodno je pronaći bolje načine kroz javno-

[478] Član 5. Severnoatlantskog ugovora.

privatna partnerstva kako bi se istražio vojni potencijal novih tehnologija, ali sa pažljivim aktivnim uključenjem javnog sektora u ove studije.

Strateški koncept NATO-a iz 2010. godine izražava potrebu da se zaštite informacioni i komunikacioni sistemi NATO-a kao rezultat brzog razvoja i sve veće sofisticiranosti sajber napada. Strateški koncept izražava zabrinutost da sajber napadi postaju sve učestaliji, organizovaniji i izazivaju veliku štetu javnim upravama, preduzećima, ekonomijama i potencijalnim transportnim i snabdjevenim mrežama, kao i drugim kritičnim infrastrukturama. Potencijalna šteta od ovih napada može da dostigne prag koji ugrožava nacionalni i evroatlantski prosperitet, bezbjednost i stabilnost (NATO, 2010).

U 2011. godini usvojena je revidirana politika NATO-a za sajber odbranu, sa jasnom vizijom napora u oblasti kibernetičke odbrane, kao i Akcionog plana za njenu implementaciju. Svrha ove revidirane politike je bila da se ponudi koordinirani pristup sajber odbrani u Savezu, sa fokusom na sprečavanje sajber napada i da se sve strukture NATO-a podvrgnu centralizovanoj zaštiti. Politika je također naglasila saradnju sa partnerskim zemljama, međunarodnih organizacija, privatnim sektorom i akademskom zajednicom. NATO-ova politika sajber odbrane i prateći Akcioni plan jasno su pokazali da je fokus NATO-a na zaštiti svojih komunikacionih i informacionih sistema. Osnovni principi politike zasnivaju se na prevenciji, izdržljivosti i ne-dupliciranju. Ključ efektivne sajber odbrane je koordinirana odbrana između članica Saveza i mreža NATO-a. Pored toga, postoji obaveza da će NATO pružiti koordiniranu pomoć ako su saveznik ili saveznici žrtve sajber napada i traže pomoć (Hunker, 2013).

Pokušaj da se poboljša sajber odbrana NATO potvrđen je na samitu u Čikagu u maju 2012. godine. Postavljanje svih mreža NATO-a pod centralizovanu zaštitu predstavljeno je kao osnovni zadatak. Daljnja reforma, kao dio tekućeg procesa reforme Alijanse, bila je uspostava NATO-ove Agencije za komunikacije i informacije (Agencija NCI) u julu 2012. godine, kako bi se cjelokupna struktura NATO-a dovela pod centraliziranu zaštitu. Glavni cilj NCI-ja je pružanje C4ISR tehnologije (za komandu, kontrolu, komunikacije, računare, obavještavajne, nadzor i izviđanje) i usluge i sposobnosti za komunikacija i informacijske sustave (CIS) za misije Alijanse, uključujući nove prijetnje i izazove kao što su sajber odbrana i raketna odbrana. Agencija također pruža kooperativnu razmjenu informacija između Alijanse, promovirajući potrebu za interoperabilnošću. Agencija je izvršno tijelo NATO-ove Organizacije za komunikacije i informacije (NCIO), koja ima za cilj pružanje sigurnih CIS usluga. NATO je prepoznao potrebu za pružanjem sveobuhvatnih usluga kibernetičke odbrane NATO-u, jer je cijela NATO struktura povezana sa istom mrežom i sve članice suočavaju se sa istim sajber prijetnjama. Prihvatanjem svih mreža NATO-a pod centraliziranom zaštitom, virtualne granice se mogu lakše definirati i izbjeći dupliranje napora i financijskih troškova.

Ofanzivne sposobnosti za sajber napade koje su razvili državni ili nedržavni akteri mogu lako uticati na NATO-ove usluge CIS-a. Da bi postigao efikasnu kibernetičku odbranu i pružio usluge CIS-a, NATO se mora fokusirati na novu dimenziju sajber prostora, sajber-

moć. Prema Hunkeru, (Hunker, 2013) u izgradnji bezbjednosnog prisustva u sajber prostoru, NATO se mora fokusirati ne samo na sprečavanje sajber napada, već i na to kako bi nacije i nedržavni akteri mogli koristiti svoje prisustvo u sajber prostoru da utiču na događaje, sa drugom riječju da izvrši moć. On kaže da se sve rasprave o sajberu u kontekstu Saveza odnose na odbranu, a još manje na rat. Jedan fokus na razvojne doktrine NATO-a treba staviti na posljedice sajber- moći, a ne samo na borbu protiv sajber rata ili odbranu sajber-napada. On predlaže da sajber-moć može poslužiti kao okvir za događaje koji će oblikovati okruženje NATO-a 2030. godine.

Potvrda ozbiljnog pristupa NATO-a sajber odbrani dolazi godinu dana kasnije, 2014, kada su saveznici NATO-a istakli da uticaj sajber napada "može biti štetan za moderna društva, baš kao i konvencionalni napad" (NATO, 2014).

Na samitu NATO-a u Varšavi 2016. godine, lideri saveznika NATO-a obećali su da će ojačati svoju nacionalnu kibernetičku odbranu kao dio Posvećenosti sajber odbrani. Od tada, oni su izveštavali o razvoju nacionalnih sajber strategija, kako su organizovani za sajber odbranu, kakve investicije vrše - i u pogledu finansija i u ljudske resurse, kao i o programa obuke i obrazovanja vezanih za sajber. Na ovom samitu, saveznici su prepoznali sajber prostor kao novi operativni domen u kojem se NATO mora efikasno braniti isto kao što to radi u zraku, na kopnu i na moru. Takvo priznavanje olakšava integraciju dobrovoljnog suverenog nacionalnog sajber doprinosa u misije i operacije NATO-a.

Da bi se efikasno omogućile integracije sajber-sposobnosti u komandnu strukturu NATO-a, na samitu u Briselu 2018. godine, saveznici su se dogovorili da osnuju Cyber Space Center, koji se nalazi u Monsu, u Belgiji. Centar bi trebao biti odgovoran za pružanje svijesti o situaciji, koordinaciju sajber napora i centralizirano planiranje za operacije i misije i predviđa se da će u potpunosti biti operativan do 2023. godine (Brent, 2019).

2.2 Ostvarivanje NATO-ovih prioriteta u sajber odbrani

NATO-ov mandat za sajber odbranu je dvostruk: da zaštiti svoje mreže i ojača sajber-otpor u Savezu od 29 zemalja. Pored stručnjaka za kibernetičku odbranu, NATO ima i timove za brzo reagovanje (RRT) koji se mogu rasporediti kako bi odgovorili na potencijalne sajber napade na mreže NATO-a ili na pomoć NATO saveznicima na njihov zahtjev. Razmjena informacija je neophodna za bolju informiranost i bolju spremnost za rješavanje kibernetičkih prijetnji. U tom cilju, NATO ima na raspolaganju nekoliko instrumenata, kao što je Platforma za razmjenu informacija o zlonamjernom softveru, koja omogućava razmjenu informacija u realnom vremenu. Da bi se osiguralo da su vještine u skladu sa tehnologijom, NATO ima programe obrazovanja, obuke i vježbe koji se i dalje razvijaju.

NATO također prilagođava način na koji funkcioniše, tako da može biti efikasan u sajber domenu kao što je to i u fizičkom svetu. U 2016. godini, saveznici su prepoznali

kibernetski prostor kao domen operacija - baš kao i zrak, kopno i more. To će omogućiti vojnim strukturama NATO-a da bolje zaštite misije i operacije od sajber-prijetnji. Ta orijentacija obezbjeđuje okvir za upravljanje resursima, vještinama i sposobnostima, istovremeno osiguravajući da se sajber odbrana u potpunosti odražava u vježbama, aktivnostima obuke i mjerama odgovora na krizu. Važno je napomenuti da priznavanje sajber prostora kao domena operacija ne mijenja misiju ili mandat NATO-a koji ostaju defanzivni. Na sastanku ministara odbrane NATO-a u novembru, saveznici su se složili oko okvira političkih i pravnih principa čiji je cilj usmjerivanje integracije dobrovoljnih sajber doprinosa država članica. Okvir osigurava da bilo koji savezni angažman u sajber prostoru poštuje NATO-ov odbranbeni mandat, politički nadzor i poštivanje međunarodnog prava. Ovo je također u skladu sa savezničkom podrškom razvoju normi i mjera za izgradnju povjerenja za sigurnost i stabilnost u kibernetičkom prostoru (Ducaru, 2018). Ovo odražava pristup "promjene u igri" u smislu integracije sajbera kroz strategiju i taktiku, obuku i vježbe, kao i u vojno planiranje u svim operativnim domenima.

Unutar NATO-a, veliki naglasak je na razvoju "digitalnog IQ" savezničke vojske.

- U Portugalu je uspostavljena NATO akademija za sajber i komunikacione informacione sisteme, a sajber-otpornost je sada uključena u nastavnim planova za koordinirano obučavanje u svakoj državi članici NATO-a.
- NATO-ov Centar za savršenstvo kibernetičke odbrane u Tallinnu, Estonija, je akreditovana institucija za istraživanje i obuku koja se bavi edukacijom o sajber odbrani, konsultacijama, naučenim lekcijama, istraživanju i razvoju. Iako nije dio NATO-ove komandne strukture, Centar nudi priznatu stručnost i iskustvo u sajber odbrani. Centar za savršenstvo u Estoniji organizuje dvije sajber vježbe godišnje. Prva, „Sajber koalicija“, testira procedure i politike za spremnost i odgovor Alijanse u situacijama rasprostranjenih, stalnih sajber napada. Druga vježba, pod bannerom „Zaključani štit“, testira vještine cyber-stručnjaka u scenarijima ratnih igara crvenih/plavih timova.
- Škola NATO-a u Oberammergauu u Njemačkoj također provodi edukaciju i obuku za sajber-odbranu kao podršku operacijama, strategiji, politici, doktrini i procedurama Saveza.
- Koledž odbrane NATO-a u Rimu, Italija, podstiče strateško razmišljanje o političko-vojnim pitanjima, uključujući pitanja vezana za sajber odbranu.

Godine 2018. ministri odbrane saveznika dogovorili su se da uspostave Centar za kibernetičku operaciju kao dio nove NATO-ove komandne strukture NATO-a, prvog sajber-orijentiranog entiteta u komandnoj strukturi NATO-a. Ovo je prvi korak ka integraciji sajber-sposobnosti u planiranje i operacije NATO-a. U fizičkom području kopna, zraka i mora, operativno planiranje se odnosi na prikupljene/isporučene fizičke snage ili sposobnosti. U sajber-domenu, integracija će se fokusirati na efekte generisane dobrovoljnim nacionalnim sajber-doprinosima, a ne na same sposobnosti, budući da je većina sajber instrumenata jedinstvena i diskretna (Ducaru, 2018).

U kontekstu sajber bezbjednosti, svaki od 29 saveznika NATO-a mora poboljšati sajber odbranu na svojim nacionalnim mrežama i infrastrukturama. Savez je jak koliko i njegova najslabija karika, tako da je podizanje nivoa sajber pripremljenosti i zaštite na nacionalnom nivou važan zadatak. Saveznici izvještavaju da je Zalog za sajber odbrane važan alat za podizanje svijesti kod višeg rukovodstva o važnosti sajber odbrane, što zauzvrat može pomoći u određivanju prioriteta ulaganja u ovoj oblasti. Ona također pomaže da se olakša koordinacija među različitim nacionalnih uključenih strana - od aktera za sigurnost i odbranu, preko onih koji primjenjuju zakon, pa sve do operatere kritične infrastrukturne. Dakle, privatni sektor je ključni igrač u kiberprostoru. Tehnološke inovacije i stručnost iz privatnog sektora su od ključnog značaja kako bi se omogućilo NATO i saveznim zemljama da podignu efikasnu sajber odbranu. Kroz NATO-ovo sajber partnerstvo sa industrijom (NICP), NATO i njegovi saveznici rade na jačanju njihovih odnosa sa industrijom. Ovo partnerstvo se oslanja na postojeće strukture i uključuje entitete NATO-a, nacionalne kompjuterske timove za reagovanje u vanrednim situacijama (CERTs) i predstavnike industrije iz članica NATO-a. Aktivnosti za razmjenu informacija i vježbi, obrazovanja i obuke samo su neki od primjera područja u kojima NATO i industrija rade zajedno. Kibernetička sigurnost podrazumijeva stvarni pristup čitavog društva, od korisnika tehnologije, programera i operatera pa sve do vladinog rukovodstva na kojeg se oslanjamo da bi se sprovodile politike koje nam pomažu da koristimo pogodnosti i ograničavamo rizike u sajber prostoru.

Pošto se sajber prijetnje ne zaustavljaju na državnim granicama niti na granicama organizacija, NATO mora sarađivati sa relevantnim zemljama, organizacijama i privatnim sektorom kako bi poboljšao međunarodnu sigurnost. Između ostalog, NATO sarađuje sa Evropskom unijom (EU), Ujedinjenim nacijama (UN), Savetom Evrope i Organizacijom za bezbjednost i saradnju u Evropi (OEBS). U februaru 2016. godine, NATO i EU potpisali su o Tehnički sporazum o sajber odbrani kako bi pomogli objema organizacijama da bolje spriječe i odgovore na sajber napade. Ovaj tehnički aranžman pruža okvir za razmjenu informacija i razmjenu najboljih praksi među timovima za odgovor u vanrednih situacija (NATO, 2016).

3. Zaključak

Sajber prostor kao novo sigurnosno pitanje može se smatrati petim prostorom ratovanja. U ovom međuzavisnom svetu postoji stalna opasnost od sajber napada na komunikacione i informacione sisteme i infrastrukturu. Poslednjih godina, sajber napadi su bili dio hibridnog rata. Bezbjednost i odbrana ključnih informacionih sistema i infrastrukture postali su prioritet za vlade koje vide efikasnost u njegovoj realizaciji u razvoju zajedničkog odgovora na sajber napade u međunarodnim bezbjednosnim organizacijama.

Alijansa se suočava sa složenom kompleksnom prijetnjom. NATO-ovi informacioni sistemi svakodnevno bilježe brojne sumnjive incidente. Kod većine njih suočavanje se obavlja automatski, ali postoje i one koje zahtijevaju dodatnu analizu i odgovor od stručnjaka. NATO kao međunarodna bezbjednosna organizacija naglašava sajber odbranu kao ključnu sposobnost Alijanse i njenih članica. Zaloga za poboljšanju NATO sajber odbranu je proces koji je u toku, a cilj sajber odbrane Alijanse je da garantuje održive i sigurne komunikacije i informacione sisteme (CIS). NATO saveznici zagovaraju stajalište da se međunarodno pravo, uključujući međunarodno humanitarno pravo i Povelja UN, primjenjuju na sajber prostor. NATO kontinuirano jača svoje sposobnosti za sajber obrazovanje, obuku i vježbe.

Bibliografija

- Baykal N. (ed.) (2013). Lectures Notes: Hands-on Cyber Defence Training Course for System/Network Administrators of The Republic of Macedonia. Ankara: Informatics Institute.
- Brent, L. (2019). NATO's Role in Cyberspace. ,NATO Review. Accessed May 12, 2019.
- http://nato.tagomago.be/files/Pages/2019/Also-in-2019/natos-role-in-cyberspace-alliance-defence/EN/index.htm
- Cyrus Jabbari. (2018). The Application of International Law in Cyberspace: State of Play. October 25h. Accessed May 06, 2019. https://www.un.org/disarmament/update/the-application-of-international-law-in-cyberspace-state-of-play/
- Ducaru, S. (2018). NATO advances in its new operational domain: cyberspace. Accessed February 02, 2019. https://www.fifthdomain.com/opinion/2018/07/05/nato-advances-in-its-new-operational-domain-cyberspace/
- Hartmann, U. (ed.) (2009). Connecting NATO: NCSA Under the Leadership of Lieutnant General Ulrich H.M.Wolf. Berlin: Hartmann Miles-Verlag.
- Hunker, J. (2013). NATO and cyber security. In Herd, P. G. & Kriendler, J. (eds.). Understanding NATO in the 21 st century: Alliance strategies, security and global governance. New York: Routledge.
- Kissel R. (ed.) (February 2011). Glossary of Key Information Security Terms. Accessed May 12, 2019. http://csrc.nist.gov/publications/nistir/ir7298-rev1/nistir-7298-revision1.pdf
- NATO. (2010). Active Engagement, Modern Defence. Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organisation adopted by Heads of State and Government. Lisbon, Portugal. Accessed May 1, 2019.
- https://www.nato.int/cps/ua/natohq/official_texts_68580.htm
- NATO. (2014). Wales Summit Declaration. Heads of State and Government participating in the meeting of the North Atlantic Council. Wales. Accessed April 2, 2019.
- https://www.nato.int/cps/ic/natohq/official_texts_112964.htm
- NATO. (2016). Nato Cyber Defence. Fact Sheet. Accessed March 03, 2018. https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160627_1607-factsheet-cyber-defence-eng.pdf
- Pindar, J. & Rigelsford, J. (2011). Cyber security and Information Assurance. The University of Sheffield.
- Reveron S. D. (ed.) (2012). Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World. Georgetown University Press.
- Schreier F., Weekes B., Winkler H. T. (2011). Cyber Security: The Road Ahead. DCAF Horizon 2015 Working Paper Series (4). Accessed March 04, 2016. http://www.dcaf.ch/Publications/Cyber-Security-The-Road-Ahead

- Withman E. M. & Mattord J. H. (2012). Principles of Information Security Fourth Edition. Boston: Course Technology, Cengage Learning.
- Моран, Д. (2009). Географија и стратегија. Во Бејлис, Џ., Вирц, Џ., Греј, К., & Коен, Е. (Eds., 2007), Стратегија во современиот свет, Второ издание (с. 122-139). Скопје: Нампрес.

Kriminalističke teme
Zbornik radova
Godina XIX, Broj 5, 2019.
ISSN 1512-5505

METODOLOŠKA ISTRAŽIVANJA U POLITICI I SIGURNOSTI KAO DIO KOMPJUTERSKE MANIPULACIJE PODACIMA U KREIRANJU SIGURNOSNE PERCEPCIJE JAVNOSTI

Stručni rad

Vanredni profesor dr Oliver Andonov[479]
Vanredni profesor dr Toni Georgiev[480]
Mr sc. Monika Andonova[481]

Sažetak

Uobičajeno kad govorimo o sajber sigurnosti (prevedeno kao kompjuterska sigurnost sa uticajem u sajber prostoru), mislimo na hakerske napade na kompjuterske sisteme ili na sigurnost podataka, pojedinih informacija, ličnih podataka i informacija.

U ovom radu naš cilj je da otvorimo jedno uslovno rečeno novo pitanje sajber sigurnosti, a koje se odnosi na metodologiju istraživanja političkih i sigurnosnih pojava sa aspekta naučnog pristupa i korišćenje suvremene kompjuterske tehnologije u kreiranju percepcije javnosti. Svakako da kreirana percepcija javnosti jeste i kreriranje javnog mnjenja, a to utiče na kretanje u društvu, ili kreiranje sigurnosne politike.

Pristup metodologije istraživanja političkih i sigurnosnih nauka i njihovo prevođenje u praksi veoma često se svodi na političku pragmu sa kojom se manipuliše u okviru naučne zasnovanosti prikazanih rezultata o društvenim kretanjima ili najviše u odnosu na percepciju sigurnosnih prijetnji i izazova. Jedan takav primer uslovljavanja kreiranja sigurnosne politike jeste „sekuritizacija" sigurnosnih problema kroz stvaranje percepcije javnosti kao uslov sekuritizacije. Sigurno da se ova percepcija ne može isključiti u odnosu na kreiranje javne komunikacije ili medija, ali smatramo da osnov upravo potkrepljivanja takvih stavova i percepcija jeste naučna potpora dobivenih rezultata.

Veoma interesantan pristup koji ćemo pokušati da otvorimo kao dilemu u ovom radu, jeste pristup u mjerenju laži u politici povezanih sa realnosti sigurnosnih ugrožavanja društva. Upravo prikazivanje ove realnosti i poticanje lažnih informacija jeste deo kreiranja javne percepcije o sigurnosti, a tome pridonosi sajber prostor kao glavni medij suvremenih društava i kreiranju percepcije građana o sigurnosti na svim nivoima.

Ovaj rad nema tendenciju da uradi cjelosnu elaboraciju i naučno istraživanje koje će u potpunosti determinirati korišćenje metodologije naučnog istraživanja i kreiranja željenih naučnih podataka radi stvaranja uticaja kroz sajber prostor na percepciju javnosti o sigurnosti i politici, već da pored tradicionalnih pogleda na sajber sigurnost u suvremenom svijetu i izazovima sajber sigurnosti pokušamo da pionirski otvorimo jedno novo

[479] Vojna akademija „General Mihailo Apostolski" –Skopje, andonov.oliver@yahoo.com
[480] Vojna akademija „General Mihailo Apostolski" – Skopje,tonigjorgiev@yahoo.co,uk
[481] Skopje, monika92andonova@gmail.com

poglavlje u kome je sajber sigurnost dio uticaja na društvena kretanja i kreiranju sigurnosne politike na svim nivoima.

Ključne reči
sajber prostor, metodologija političkih i sigurnosnih nauka, laži u politici, sigurnosna politika, percepcija javnosti

Uvod

Pisati znanstveni rad o sajber sigurnosti u vremenu razvijene informatičke tehnologije i dostupnosti informacija i pri tome se ograničiti isključivo na sajber terorizam ili upade u kompjutorske sigurnosne mreže jeste uobičajeni pristip ovom sigurnosnom problemu.

Upravo ovaj rad će pokušati da prezentuje jedan drugačiji pristup sajber sigurnosti u svjetlu sigurnosti građana i države, odnosno cjelokupnog društva. Korišćenje kompjuterskih tehnologija, informacionih sistema i tehničkih dostignuća u odnosu na ugrožavanje sigurnosti ne odnosi se uvijek i samo na tehničko-tehnološkom nivou ugrožavanja sigurnosti. Više nego ikada sajber sigurnost se ugrožava suptilnim korišćenjem znanstvenih dostignuća u cilju kreiranja javnog mnjenja i usmjeravanja političkih tokova i donošenja odluka.

Ovakav pristup ugoržavanja sigurnosti i to na državnoj razini (možemo da govorimo o državnoj sigurnosti) u svakom njenom segmentu, a da pri tome ne mislimo isključivo na zaštitu državnosti od direktnih ugrožavanja, jeste izraženo prisutan u suvremenim izvorima ugrožavanja sigurnosti.

Vidljivo je da akter ugrožavanja primenjuje suptilne metode i instrumente ugrožavanja objekta sa jedinstvenim ciljem da ostvari svoje interese, odnosno tradicionalno pitanje zaštite – „sigurnost od koga i od čega“ jeste poticaj za otvaranje različitog pristupa prema izvoru ugrožavanja.

Ciljevi koje izvor ugrožavanja želi da postigne u suvremenim okolnostima nisu puno različiti od onih povjesnih, odnosno zavladavanje ili potčinjavanje države i naroda. Različne su metode i pristipu koji su takoreći manje nasilni, ali ne imanje pogubni za napadnutu državu ili društvo. Jedan od isključivo važnih pristupa jeste ovladavanje političkom sferom uticaja države, a to se može pokriti demokratskim izborom građana te države koji na osnovu dobivenih informacija glasaju na izborima i na taj način na vlast dovode političku strukturu koja rukovodi državom. Ubjeđeni u najbolji izbor i vjerujući svemu rečenom i pretstavljenom kao i prikazanim „istraživačkim“ prikazima o tendencijama ko je u prednosti, raznim lažnim vijestima i kreiranim informacijama, potpuno i metodički pristupajući kroz sajber prostor kreira se javno mnijenje koje u datom trenutku donosi odluku koju upravo izvor ugrožavanje želi da bude donesena. Pri tome sve je to izraz demokarcije i volje naroda.

Da bi ovaj izraz demokracije i da bi ta i takva volja naroda mogli da budu obezbjeđeni i verifikovani, kretorima javnog mnijenja potrebni su mnogi elektronski obrađeni podaci koji imaju statističku osnovu i koji služe za obradu terena. Neizostavni dio te zloupotrebe podataka jeste i korišćenje ličnih podataka, a sa ciljem praćenja individualnih aktivnosti na socijalnim mrežama i u sajber prostoru i sprovođenje anketa i testiranja javnog mnijenja po opredjeljenim pitanjima oko kojih će se izraditi strateški pristup za kreiranje osnovnog javnog mnijenja.

U osnovi ovih operacija jeste poznavanje metodologije političkih znanosti i upotrebi sajber prostora u prikupljanju i slanju informacija prema strateškoj procjeni izvora ugrožavanja. Ovaj rad neće obuhvatiti metode suprotstavljanja već samo sistem metodološkog pristupa istraživanja u politici i pri tome zloupotrebe ličnih podataka i aktivnosti na socijalnim mrežama. Ovakav pristup radu daje karakter preglednog rada u klasifikaciji znanstvenih radova, ali nadamo se da će u budućnosti prouzrokovati interes za konkretno znanstveno istraživanje.

1. Sajber prostor i mogućnosti njegove zlouporabe

U zavisnosti od različitih perspektiva i društveno socijalnih gledišta, ne postoji jedinstvena ili unificirana definicija o tome što predstavlja sajber proctor. Sama riječ smatra se nasljednikom riječi kibernetika (cybernetic), a koja što semantički potiče od grčke riječi "kybernetes", koju prvi put spominje Norbert Winner prilikom njegovog rada sa elektronskim komunikacijama i avtomatizacijom. Sajber prostor kao pojam je najviše povezan sa informatičkim i telekomunikaciskim tehnologijama. Svakako njihovim razvojem godinama je mijenjana percepcija o tome što obuhvata sajber prostor kao pojam.

Jedna od većinom definicija o sajber prostoru daje Internacionalna Telekomunikacijska Jedinica (International Telecommunication Union – ITU), koja je specijalizirana agencija Ujedinjenih naroda namjenjena za informaciske i komunikaciske tehnologije. Prema definisanju ove Agencije, sajber prostor predstavlja: „skup korisnika, mreža, uređaja, softverskih procesa, informacija koji su sačuvani ili koji su u tranzitu, aplikacija i sistema koji mogu direktno ili indirektno da se povežu na mreži".[482]

Još jednu definiciju daje Talinski priručnik, koji pomoću međunarodnih zakona daje legalnu i nepolitičku perspektivu rješavanja sajber konflikata. U osnovi priručnik predstavlja pravni kodeks, uređen sa strane međunarodne grupe pravnih stručnjaka. Pri tome, sajber prostor se definiše kako: „sredina oformljena od fizičkih i abstraktnih

[482]International Telecommunication Union: **"Series X: Data networks, open system communications and security: overview of cybersecurity"**, 2008, str. 2

komponenata, koja se karakterizuje upotrebom kompjutorskih i elektronskih komponenata, sa ciljem očuvanja, modifikovanja i razmjene podataka upotrebom kompjutorskih mreža".[483]

Potrebno je napraviti distinkciju između poima internet i sajber prostor, koji su sasvim različiti ali su tijesno povezani. Sam internet i svi njegovi elementi (web strane, aplikacije) su komponente koje između ostalog formiraju sajber prostor gdje se odvija ogromna razmjena informacija. Sve većim porastom upotrebe interneta, povećava se sajber prostor koji se stalno puni podacima i informacijama svakakvog sadržaja. Ovakvim pristupom, sajber prostor ulazi u sve aspekte današnjeg društva i svakodnevnog života, a porastom njegove kompleksnosti raste i opasnost od njegove zlouporabe.

Prateći zadnju definiciju sajber prostora, možemo zaključiti da kada postoji sajber prostor postoje i sajber konflikti, a samim tim i različiti oblici napada i narušavanja ove sredine, odnosno razni načini njene zlouporabe posebno za nelegalna i protuzakonita dejstva.

Sajber napad predstavlja: „neovlaščeni pokušaj otkrivanja, krađe, pristupa do podataka, informacija ili kompjutorskih sustava i mreža, a najčešće sa malicioznim ciljem. Pre nego što klasifikujemo sajber napade, uradićemo pregled klasifikacije prijetnji u sajber prostoru. Pretnje mogu da budu slučajne ili namjerne i aktivne ili pasivne.

Slučajne prijetnje su rezultat ne namjernog pronalaženja defekata u softveru ili sustavu. Namjerno - planirane prijetnje, klasifikuju se različito od slučajnih upotrebom ureda za monitoring, pa sve do napada koji uključuju ozbiljna poznavanja sustava. Namjerne ili planirane prijetnje tretiraju se kao sajber napadi.

Pasivne prijetnje su one koje ukoliko se realizuju neće rezultirati nikakvim promjenama u sustavu, softveru ili te podataka sačuvanih u samom sustavu. Aktivne prijetnje uključuju promjenu informacija koje sadrži sustav ili promjenu u načinu rada samog sustava.

Prilikom dizajniranja sustava i produkta koje mogu biti cilj sajber prijetnji, potrebno je utvrditi mesta u sustavu kdje može doći do ovakvih napada i adekvatno ih zaštititi. Ipak moramo biti svjesni toga da uvjek postoji mogućnost i pored zaštite, sustavi i softveri da postanu žrtve sajber prijetnji, ali se ipak ovim pristupom zaštite smanjuju posljedice za realizaciju prijetnje.

Kada govorimo o sajber napadima, u zavisnosti od cilja koji se želi realizovati, mogu se klasifikovati u napade koji imaju za cilj da onemoguće rad napadnutog sustava, ili napad

[483]Michael N. Schmidt: **"Tallinn Manual on the International Law applicable to cyber warfare"**, Cambridge University Press, New York, str. 278

sa ciljem pristupa podacima koji su skaldirani u sustavu koji je napadnut ili dostup drugim informacijama, administratorskih prava i slično.

Postoji više tipova sajber napada koji se često nadopunjavaju i mijenjaju posebno razvojem tehnologije i samim tim se međusobno isprepliću pri čemu ne postoje koncizne granice. Postoji nekoliko njih i neke ćemo da objasnimo.

Malware – kovanica engleskog pojma malicious software ili takozvani „zlunamjerni softver". Bez obzira na to kakav je softver i kako je upravljan i dizajniran, ukoliko je cilj nanošenja štete targetovanom sustavu taj softver se smatra malicioznim, zlunamjernim. Ovim softverom može se napravite šteta funkcionalnosti sustava, mreže ili izvršilac napada se može ugnjezditi u korjen sustava odakle će moći da kontroliše cijeli sustav sa daljine.

Phishing – Fišing je tehnika kojom sajber kriminalci šalju mail poruke pokušavajući da obmanu subjekat. Subjekat koji je primio poruku može biti obmanut i sam izvrši skidanje malicioznih datoteka koje će uništiti rad sustava. Veoma često u ovakvim mailovima postoje linkovi do web sajtova koji traže podatke, senzitivne informacije, passworde, korisnička imena, bakovne račune ili nude anketne upitnike u vezi neke aktualne društvene teme. Ove informacije napadači kasnije koriste za opredjeljene ciljeve. Uobičajeno ovi email napadi se šalju ljudima slučajnim izborom, ali često su ljudi i grupa unaprijed targetirani sa ciljem sondaže terena ili dobijanja neke informacije koju ta grupa ljudi ima ili je važna za ostvarivanje ciljeva.

Negiranje usluge – Ovaj napad se upotrebljava da bi se zaustavio pravilan rad nekih internet usluga. Naprimjer, šalje se ogromna količina zahtjeva na neki web sajt ili na neku bazu podataka čime se opterećuje sustav i dovodi do toga da usluga bude nedostupna za sve korisnike. Vrlo često prilikom ovakvih napada upotrebljava se veliki broj kompjutora koji prije toga su napadnuti malicioznim softverima i stavljeni su pod kontrolom sajber kriminalaca radi preusmjeravanja saobraćaja sa svih prema ciljanom sustavu.

Čovjek u sredini – jeste metod kada se napadač tajno umiješa između korisnika i web usluge kojoj korisnik pristupa. Kao primjer može se uzeti zlouporaba wi-fi mreže gdje sajber kriminalac imitira mrežu na kojoj ukoliko se korisnik konektuje, napadač može da pristupi do sve informacije koje korisnik ispraća ili prima, uključujući passworde, bankovne i lične podatke.

Cryptojacking – je specijalizirani napad pri čemu se uzima neki kompjuter koji treba da generira kriptovalute za potrebe napadača (proces nazvan „mining" ' rudarenje). Napadač instalira maliciozni softwere u kompjuter žrtve ili startuje kod u Java skript koji se realizuje u pretraživaču žrtve.

SQL injection – napadač preko eksploatacije neke slabe točke u bazi podataka ili sustava preuzima cjelu bazu podataka žrtve napada. Najveći broj data baza su dizajnirane da reaguju na komande napisane strukturnim jezikom za pretragu (Structured Query Language), a ogromni broj web strana koje na bilo kakav način uzimaju određene podatke od svojih korisnika šalju te podatke u SQL bazi podataka. U ovakvim tipovima napada, napadač može da napiše nekoliko komandi u web formatu gdje može tražiti određene informacije kao što su imena, prezimena, adrese i drugo. Ukoliko baza podataka i web strana nisu adekvatno programirani i zaštićeni, ovakve komande može da daje i napadač i samim tim da dođe do podataka i ličnih informacija korisnika.

Danas, kada sajber prostor predstavlja našu svakodnevicu, napadi i zlouporaba su sve češći i razvijeniji. Pored standardnih ekonomskih, financiskih ili obavještajno-sigurnosnih ciljeva napada u kojima nerijetko učestvuju i vladine službe, sve je češća pojava da svaka individua postaje cilj sajber zlouporabe. Sve većim tempom razvoja znanosti povezanih za podatke – Data Science, svako od nas pojedinačno postaje potencijalna žrtva. Svakidašnjem korišćenjem socijalnih mreža i uopšte internet pristupa i internet tehnologija svi podaci koje slučajno ili namjerno unesemo u sajber prostor mogu biti zlopuptrebljeni za različite ciljeve.

Jedan od veoma čestih ciljeva zlouporabe ličnih podataka jeste i istraživanje u cilju kreiranja javnog mnijenja za političke ciljeve, odnosno odrešivanja ciljnih grupa i interesnih zajednica.

2.Uticaj na kreiranje javnog mnjenja za političke ciljeve kroz upotrebu kompjuterskih instrumenata metodologije znanstvenih istraživanja

2.1. Analiza, konstrukcija instrumenata, navođenje na željene odgovore, obrada podataka i njihova upotreba

Prilikom istraživačkih postupaka u cilju stvaranja relevantnih rezultata sasvim je normalno da se pojave greške. Ove greške mogu biti nenamerne, i njihovo odstranjivanje jeste permanentni zadatak istraživača ukoliko nam je tendencija da dobijemo znanstveno relevantne, potvrđene i proverljive rezultate istraživanja.

Upravo kao znanstvena suprotnost ovakvog pristupa, imamo tendencioznu pojavu grešaka koje kao posljedica projektiranja i realizacije istraživanja prouzrokuju namjerne sistematske „pogreške“ u istraživanju.

Ovakve namerne greške u okvirima potrebe sprovođenja istraživanja sa ciljem stvaranja lažne slike i kreiranja percepcije javnog mnijenja najčešće nisu rezultat neznanja, već namerno pogrešno konstruisanog teoriskog koncepta istraživanja, unapred određenog cilja rezultata istraživanja, pri čemu se neprimjenjuju pravila modela istraživanja, metodskih

postupaka, upotreba instrumenata i što je najvažnije, nepoštovanje etičkih načela u istraživanju. Ovo je rezultat unapred određenih „neophodnih" istraživačkih rezultata, a greške su katastrofalne i tendenciozno se izbegava logička analiza i ukrštanje podataka, već se upravo usmjerava ceo proces ka kreiranju istraživačkih podataka odnosno rezultata istraživanja. Ovakav pristup istraživanju jeste uvod ka stvaranju rezultata „željenih odgovora" i time otvaranje mogućnosti da se kroz pseudo znanstvene podatke i metodološki koncept prezentuju „relevantni" rezultati koji će imati uticaj na kreiranju javnog mnijenja u politici.

Nakon uvoda u istraživanje i tendenciozno stvaranje sistematske greške kroz ekspoloataciju pogrešnog teoriskog koncepta i samim tim i pogrešnog metoda i instrumenata dolazi do obrade dobivenih rezultata.

Obrada podataka se determinira „konzistentan sistem logičkih, epistemioloških, statističkih (matematičkih) i tehničkih postupaka kontrole, klasifikacije, grupisanja, prikazivanja, upoređenja, povezivanja, ukrštanja i kombiniranja podataka svih vidova u suglasnosti sa osnovnom idejom predmeta istraživanja i prema odredbama pravila istinskog mišljenja, dokazivanja i provjeravanja".[484]

Upravo polazeći od premise istinosti i znanstvene relevantnosti istraživanja druga faza istraživačkog procesa nakon sređivanja dobivenih podataka jeste analiza podataka. Cilj ove faze jeste izvođenje analize kao misaonog procesa u kome trebamo razlučiti istinitost i kvalitet istraživanja posebno preko provjere postavljenih hipoteza i upotrebe analitičkih tehnika. Ovo je u suštini faza u kojoj je veoma lako doći do istine, odnosno utvrditi validnost dobivenih podataka koje bi trebalo da se prezentuju u javnosti i prikazati kao javno mnijenje u vezi neke društvene pojave, rejting političkih stranaka ili stav građana o nekom događaju u društvu. Interesantno je što najčešće zbog tendencije stvaranja javnog mnijenja i pored dobro postavljenih hipoteza korektne obrade podataka i dobivenih rezultata, u ovoj fazi analize, postoji isključivo velika mogućnost namještanja podataka, odnosno njihovog prepravljivanja u okvirima korišćenja softverskih rešenja za obradu podataka. U praksi ovo znači vraćanje unatrag u prethodnoj fazi pri čemu analiza podataka utiče direktno na sređivanje podataka, izbegavanje njihove logičke kontorle i karaktera podataka. Pri tome, veoma je lako staviti bilo koje podatke u okvirima tabela, grafikona, dijagrama i slično koristeći bilo koji kompjuterski sistem za obradu podataka (MS Excel, SPSS, Statistica, StatGraf i sl.). Iskusne istraživačke agencije za mjerenje javnog mnijenja I stavova građana u politici još tokom sakupljanja podataka na terenu znaju da na osnovu konstrukcije istraživačkih instrumenata mogu sukcesivno i simultano da prate trend odgovora ispitanika, pri čemu se faze istraživačkog procesa uopšte ne moraju dijeliti već se u nekim momentima koriste zajedno. Informacije prikupljene istraživačkim

[484]Cane T.Mojanoski, **"Metodologija na bezbednosnite nauki-analitički postapki"**, Kosta Abraš, Ohrid-Skopje, 2015, str.31

instrumentima (anketni list, ček lista, intervju, protokol o osmatranju pojava i slično), unose se u kompjuterski sistem kroz izabrano softversko rješenje, ali te podatke unosi istraživački tim koji ima uvid u hipoteze i prije svega u cilj istraživanja, tako da sistematska-katastrofalna greška se prilagođava potrebama rezultata istraživanja, odnosno političkih ciljeva. Ovde se ne izvode logički zaključci o mogućim greškama, već se greške prilagođavaju željenim rezultatima, a time se stvara pogrešna slika o javnom mnijenju građana ili se na osnovu prikazanih rezultata kreira pogrešno javno mnijenje. Možemo uzeti primjer upotrebe sekuritizacije nekog sigurnosnog problema za potrebe kreiranja sigurnosne politike i kreiranja prijetnji od nekih izvora ugrožavanja koji ne mora da su upravo aktuelni ili direktno ugrožavajući.

Da bi se cijela ova operacija sprovela i ista izgledala logično posebno za javnost, neophodno je da se kreiraju adekvatni istraživački instrumenti koji bi sugerisali željene odgovore ispitanika. Na ovaj način kreiranje lažnih znanstvenih istraživačkih podataka biće olakšano jer će kroz instrument istraživanja i poticanje očekivanih odgovora ispitanika biti lakše unositi podatke u softverski sistem bez logičke kontrole. Teži put je da se nakon korektno realizovanog istraživanja bukvalno falsifikuju dobiveni podaci da bi se u javnosti prikazao željeni rezultat i time uticalo na kreiranje javnog mnijenja u politici.

Rezultata ovoga jeste upotreba simulacije, prije i za vrijeme istraživanja, a u pravcu političkih očekivanja ispitanika po određenom društvenom pitanju pri čemu je upotreba suvremenih kompjuterskih tehnologija neophodna.

2.2. Simulacija političkih očekivanja i kreiranje javnog mnijenja

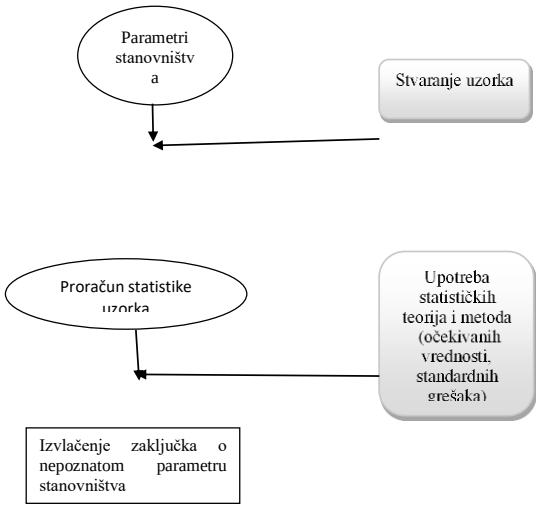
Politička očekivanja su sublimirana u dobivenim efektima reklamiranja političkih kampanja i kroz njih kreiranju javnog mnijenja. Reklame mogu imati i veoma slab efekat na populaciju, ali upravo zato kreiranje lažnih vjesti ili cjelih informacija, a posebno kreiranje kvazi znanstvena istraživanja i njihovi rezultati mogu preusmjeriti javno mnijenje i cjelovite rezultate političke kampanje. Upravo ovakvi ciljevi traže simulaciju mogućih odgovora ispitanika i njihovo usmjeravanje ka istima. Kako doći do željenih rezultata upravo definiše simulacija političkih očekivanja. Svakako da ova simulacija u osnovi ima realno i kvalitetno znanstveno istraživanje i točne proračune statističkih podataka, ali upravo zato sljedeći korak jeste manipulisanje podacima i opet simulacija podataka. U tome kontekstu jedan od najznačajnih istraživačkih ciljeva jeste: „istražiti vezu između karaktera kampanja i tendencije glasanja“, a pri tome se u osnovi nalazi tonalitet kampanja, a sve to ovisi od legitimiteta kritike u javnim medijima što je istraživački zaključak Kana i Kenedija.[485] Upravo zbog ovakvog mogućeg ponašanja ispitanika možemo modelirati ili maksimizirati (subjektivno ili psihološki) korisnost dobivenih odgovora ili ponašanja ispitanika

[485]Jannet Buttolph Johnson and H.T.Reynolds, **“Political Science Research Methods”**-Sixth Edition, Akademski pečat, Skopje, 2012, str.39-40

u korist našeg cilja istraživanja, što svakako nije etički a ponajmanje metodološki i istraživački ispravno. Supstituirajući modeliranje upotrebljavamo simulaciju mogućnosti i uticaja odgovora ispitanika i korišćenju njihovih ličnih podataka, a u čemu potpuno zavisimo od upotrebe kompjuterskih odnosno sajber znanja i tehničkih mogućnosti.

Simulacija jeste reprezent sistema kroz koji se povremeno studira sam sistem i njegovo ponašanje. Jadinice analize nisu diskretne individue, a fundament interesa jeste proces ili struktura kao što je to partička struktura ili društvo, koja što sadrži nekoliko ili mnoštvo komponenata. Do onog momenta kada individue ulaze u simulaciju, njihovo ponašanje kao kolektiv jeste glavni interes. Osnovno sredstvo istraživanja jeste kompjuterski program sa raznim i velikim mogućnostima, a što omogućava istraživaču da vidi kako se komponente sustava odnose i mjenjaju.[486] Osnovni faktor simulacije jeste vrijeme koje ističe dinamične interakcije unutrašnjih elemenata i njihovu kauzalnost prije svega recipročnu. Posebno je važno i cjelokupna tendencija simulacije jeste utvrđivanje mogućnosti da li sustav izlazi iz kontrole. Ovo je ustvari i glavni faktor koji utiče na intenzitet i veličinu kreiranja lažnih podataka, lažnih vijesti ili drugih tendencioznih informacija koje trebaju biti predstavljene javnosti i uticati na kreiranje javnog mnijenja.

Slika br. 1 Proces donošenja zaključaka na osnovu istraživačkog uzorka



[486]Ibid, str.192

Upravo zbog ostvarenje cilja uticaja na javno mnijenje i njegovo kreiranje u procesu simulacije mora se izabrati pravi ili istiniti primjerak istraživanja, a da bi ukazivalo na istinitost i znanstvenu istinitost istraživanja. Kreiranje javnog mnijenja traži donošenja zaključaka na osnovu iskorišćenog istraživačkog uzorka. Ovo donošenje zaključka jeste proces koji prikazujemo na slici br.1.

Upravo nam ova slika pokazuje kako se stvara primjerak istraživanja kao uzorak odabira onog djela stanovništva kroz koji hoćemo da nametnemo svoje stanovište i kreiramo javno mnijenje, a da u cjelome kontekstu imamo znanstvenu podlogu istraživanja.

Ovakav pristup izvlačenja zaključaka traži od kreatora lažnih vjesti ili lažnih istraživanja prije nego što krenu u simulaciju da imaju dostupnost do baze ličnih podataka ispitanika kako bi lakše opredijelili primjerak uzorka (N). Ovu bazu podataka mogu obezbijediti u državnim sustavima baze podataka (svakako ako se radi o vlasti) ili u vlastitim stranačkim bazama podataka. Svakako da ovi podaci mogu biti zlouporabljeni pa čak i sami kreirani u nekim segmentima koji direktno utiču na istraživačke rezultate.

3. Zaštita ličnih podataka u sajber prostoru i objavljivanje lažnih vijesti kao dio zloupotrebe kompjuterskog prostora

Proces koji nas okupira novom erom digitalizacije i digitalnog čuvanja podataka sve više postaje ozbiljan problem ne samo sa sigurnosne točke gledišta već i sa pravnog aspekta zaštite podataka. Zaštita ličnih podataka predstavljaju formalno-pravni i društveni fundament svakog fizičkog i pravnog lica, a u isti vrijeme predstavlja i sve vaća opasnost zbog otežavajuće kontrole mogućnosti da ovi senzitivni podaci dođu u nečije ruke i kako će i u koje svrhe biti upotrijebljeni. Formiranje državnih agencija za zaštitu ličnih podatka, prosljeđeno zakonski uređenim nadležnostima nije dovoljno, posebno gledano sa stanovišta njihovog postojanja kao čuvari. Potrebno je napraviti korak dalje u oblasti izvještavanja, ranog upozorenja i uzbunjivanja na nivou brze reakcije da je izvršen upad (bez obzira na razlog istog) u bazu ličnih podataka.[487]

U tom širokom prostoru zlouporabe ličnih podataka jeste i kreiranje lažnih profila koji se u strogo određenim ciljevima upotrebljavaju u okvirime socijalnih mreža, upravo koriste pravnu prazninu tipa neregulisane legislative, a to je ozbiljan problem koji omogućava zlouporabu ličnih podataka za krieranje politički motivisanog javnog mnijenja. Na račun sigurnosti, lišavamo se privatnosti, što postavlja dilemu „gdje je pravo privatnosti ili građanske i ljudske slobode“? Upravo zlouporaba ličnih podataka jeste pravni problem ne samo fizičkih već i pravnih lica i pitanje „od čega se trebaju oni odreći da bi sačuvali svoju sigurnost“? Samim ovim pitanjem ulazimo u sferu ekonomske sigurnosti, sigurnosti

[487] B. Pavišić, **„Kazneno pravo Vijeca Europe, Izvori, komentari, praksa”**, Golden marketing, Tehnička knjiga, Zagreb, 2006, str. 58

tržišta i jednakih mogućnosti, a svakako da biznis sektor ima veliki uticaj na politiku i političke odluke i stavove glasača. Ovo nas uvodi u razmišljanje da se lični podaci u cilju kreiranja javnog mnijenja veoma uspješno mogu upotrebiti i kriz podatke pravnih lica i to u biznis sektori i svakako u svim sektorima u zavisnosti od ciljane grupe.

Zbog svega što smo nabrojali i naveli kao mogućnost zloupotrebe ličnih podataka, postavlja se još jedan problem, a to je zaštita ličnih podataka pravnih lica, ne samo u okviru njihove elektronske korespodencije ili prava inovacija i industriskog vlasništva, transakcija već i intelektualna prava. Svakako da je velikim dijelom zaštita svih ovih aspekata regulisana u međunarodnom kompjuterskom pravu i zaštita žigova i drugih oblika elektronskog vlasništva, ali zaštititi podatke od zlouporabe za političke ciljeve je veoma teško.

Pravni pristup sajber kriminalu se uglavnom svodi na krađu kao definisani i krivično-pravni prekršaj učinjen sa strane jednog ili više lica, radi ostvarivanja određenog cilja, ali korišćenje podataka u okvirima istraživanja ili kvazi znanstvenog istraživanja koji mogu biti izmišljeni ili djelomično tačni nije pravno regulisano u okvirima sajber kriminala i samim tim se teško sankcioniše. Možemo govoriti o krađi podataka, ali to ne mora da bude direktno i potpuno obavljeno i vidljivo iskorišćeno, tako da je samim tim i teško utvrditi osnov kazneno-pravnog djela koje bi bilo kaznivo sankcionisano.

Jedan takav primjer zlouporabe ličnih podataka u cilju „istraživanja“ jeste lažno reklamiranje u ime T'mobila, pri čemu se telefon vrijednsoti 500 eura prodaje za samo 1 euro, ali prije toga se treba odgovoriti na desetak pitanja koja imaju za cilj ulaz u lične podatke financiske prirode.

Kao rezultat upravo jednog ovakvog primjera možemo zakjučiti da pravo ne može samo da reguliše već da preveniše i usaglasi nacionalno i međunarodno pravo.

Zaključak

Kroz rad koji smo prezentirali možemo da sagledamo nekoliko aspekata uticaja na sajber sigurnost i mogućnost kaznenih djela kako sa strane kazneno-pravnog aspekta, tako i sa strane isključivo stručnih postupaka i determiniranih načina upada u sajber prostor radi nanošenja štete i preuzimanja podataka.

Postojanje čvrste povezanosti zaštite ličnih podataka i njihovo korišćenje u cilju političke manipulacije i metodologije političkih istraživanja i stvaranja javnog mnijenja jeste vidljivo i pručavanjem podataka u jednom preglednom znanstvenom radu kao što je ovaj.

Zlouporaba ličnih podataka, upadanje u kompjutorski sustav, neregulisane pravne procedure i posebno ne tretiranje ovog tipa manipulacija kao krađa zbog ostvarivanja

imovinsko-financiske koristi, predstavlja ozbiljan problem sankcionisanja ovakvog tipa zlouporabe podataka. U suštini, radi se o korišćenju kompjutorskih tehnika i sajber prostora da bi se njima manipulisalo sa ciljem ostvarivanja političkih ciljeva, a sve to pokriveno znanstvenim (pseudo znanstvenim) istraživanjem.

Suvremena stvarnost je isključivo podložna ovakvom manipulacijom sajber prostora i znanstvenih istraživanja. U nekim slučajevima to su takozvane lažne vijesti, ali glavni cilj metodološke manipulacije u sajber prostoru jeste da se takozvanim znanstvenim autoritetom može manipulisati javnim mnijenjem i u isto vrijeme vršiti uticaj na njega, odnosno kreirati ga u pravcu ostvarenja vlastitih političkih ciljeva i to najčešće samo u datom trenutku i na kratkom periodu.

Postavlja se jednostavno pitanje. „Kako se odupreti ovoj pojavi i zlouporabi“? Odgovor je višeslojan i nalazi se u rješenju kazneno-pravnih regulativa ne samo u krađi ličnih podataka ili imovinsko-financiske koristi počinioca djela, već i u bilo kakvom obliku (makar i šaljivom) uzimanja tuđih ličnih podataka bez saglasnosti, zabrane kreiranja lažnih profila na socijalnim mrežama iako je to teško utvrditi, ali nije nemoguće pronaći ih i blokirati, ojačati kontrolu i zaštitu sustava u domenu sajber prostora od nanošenja štete upadima.

Ipak najvažnija je etika znanstvenika i njihova istraživačka djelatnost bazirana na točnim metodološkim postupcima i prezentiranju točnih znanstveno izdržanih podataka koji su lako provjerljivi. Svakako da je i ovo teško u realnosti ostvarljivo, jer ovaj tip pseudo znanstvenih istraživanja najčešće rade ljudi koji nisu u znanosti ili ljudi iz znanosti kojima je važnije ostvarivanje političkih ciljeva koje podržavaju.

Sukob etike u znanosti i želja za ostvarivanje vlastitih političkih ciljeva i interesa je uvjek prisutan i tako će i ostati. Ostaje na svima nama koji smo prisutni u sajber prostoru i koji smo “bombardovani“ informacijama potkrepljenih znanstvenim istraživanjem da provjerimo verodostojnost ovih informacija, mišljenja, stavova i anketa javnog mnijenja i da nakon toga donesemo vlastiti sud o društvenoj temi koja se obrađuje u sajber prostoru.

Bibliografija

1. Branislav Pavišić, „Kazneno pravo Vijeca Europe, Izvori, komentari, praksa", Golden marketing, Tehnička knjiga, Zagreb, 2006.
2. Cane T.Mojanoski, "Metodologija na bezbednosnite nauki-analitički postapki", Kosta Abraš, Ohrid-Skopje, 2015.
3. Jannet Buttolph Johnson and H.T.Reynolds, "Political Science Research Methods"-Sixth Edition, Akademski pečat, Skopje, 2012 .
4. Michael N. Schmidt: "Tallinn Manual on the International Law applicable to cyber warfare", Cambridge University Press, New York 2013.
5. International Telecommunication Union: "Series X: Data networks, open system communications and security: overview of cyber security", 2008.

Kriminalističke teme
Zbornik radova
Godina XIX, Broj 5, 2019.
ISSN 1512-5505

MEDIJSKA I INFORMACIJSKA PISMENOST U SISTEMU CYBER SIGURNOSTI

MEDIA AND INFORMATION LITERACY IN CYBER SECURITY SYSTEM

Pregledni naučni rad

Emir Vajzović[488]

Sažetak

Inspiracija za rad i problem (i) koji se radom oslovljava (ju): Činjenica da se informacijska, komunikacijska, medijska, obrazovna i sigurnosna okruženja mijenjaju, stvara nove mogućnosti i izazove modernim društvima.
Ciljevi rada (naučni i/ili društveni): Kvaliteta primljenih informacija uveliko utječe na naše odluke i postupke koji iz njih slijede, ali jednako predstavlja sigurnosni izazov u kontekstu dezinformacija, utjecaja raznih aktera na demokratske i sigurnosne procese.
Metodologija/Dizajn: Tehnološki napredak podstaknuo je, kvalitativno i kvantitativno, razvoj medija i drugih dobavljača informacija od kojih građani stiču različita znanja i primaju brojne i značajne informacije, uz mogućnost da ih dalje obrađuju i distribuiraju, ali i da donose odluke od sigurnosnog i nacionalnog značaja.
Ograničenja istraživanja/rada: Rad je analizirao relevantnu akademsku literaturu.
Rezultati/Nalazi: Od tri komponente za razmatranje nivoa cyber sigurnosti jedne države: tehnologija, procedura i ljudskih resursa - ovi posljednji (ljudski resursi) predstavljaju možda i najizazovniju komponentu za unapređenje nacionalne sigurnosne politike i doktrine.
Generalni zaključak: Razvoj i podizanje nivoa medijske i informacijske pismenosti postaje nezaobilazno u podizanju nivoa nacionalne sigurnosti, kao i ostvarivanju pravaca i ciljeva postavljenih u strategijama cyber sigurnosti.
Opravdanost istraživanja/rada: Uz digitalnu transformaciju društva, te razvoj novih generacija u digitalnom okruženju - medijska i informacijska pismenost postaje sve važniji element za preispitivanje obrazovnog sistema, cjeloživotnog učenja, demokratskih društava i aktivnog građanstva, ali i cyber sigurnosti svih država.

Ključne riječi

medijska i informacijska pismenost, informacijska i cyber sigurnost, digitalna transformacija društva, nacionalna sigurnost

[488] Docent, Odsjek sigurnosnih i mirovnih studija, Fakultet političkih nauka Univerziteta u Sarajevu. emir.vajzovic@fpn.unsa.ba.

Abstract

Reason for writing and research problem (s): The information, communication, media, educational and security environments are changing which is also creating new opportunities and challenges for modern societies.
Aims of the paper (scientific and/or social): The quality of the information received greatly influences our decisions and the procedures that follows, but equally presents a security challenge in the context of disinformation and the influence of various actors in democratic and security processes.
Methodology/Design: Technological advances have encouraged, both qualitatively and quantitatively, the development of media and other information providers from which citizens acquire diverse knowledge and receive numerous and meaningful information with the opportunity to further process and distribute it, but also to make decisions of security and national importance.
Research/Paper limitation: The paper analyzed the relevant academic literature.
Results/Findings: Of the three components for considering a country's cyber security level: technology, procedures and human resources - the latter are perhaps the most challenging component for development within national security policy and doctrine.
General Conclusion: The development of media and information literacy is becoming increasingly important for national security and cyber security strategies, but also a feasible opportunity for all countries to actively and effectively work on a viable and sustainable model for raising cyber security levels and awareness.
Research/Paper Validity: With digital transformation of society and the development of new generations in the digital environment, media and information literacy are becoming increasingly important elements for considering the education system, lifelong learning, democratic societies and active citizenship, and cyber security in all countries.

Keywords

Media and Information Literacy, Information and Cyber Security, Digital Transformation of Society, National Security.

1. Digitalna transformacija društva i sigurnosti

Ideal informisanog i obrazovanog aktivnog građanina jest osnov demokratske utopije društva koje teži prosperitetu, visokom stepenu ostvarivanja ljudskih prava i sloboda, životu dostojnom čovjeku i sve to u mirnom i sigurnom okruženju. Takav ideal implicira građanina koji ima razvijeno kritičko mišljenje i otpornost na manipulacije (primarno političko-ekonomske), unutrašnje i vanjske. Takvo društvo ima pretpostavke da je izraz slobodne volje čovjeka autonomno razvijen i realizovan kao izraz nosioca suvereniteta u demokratskom društvu kojem je zagarantovana sigurnost (vidi: Rousseau, 1950).

Pretpostavka za razvoj društva, kao i osnov za reprodukciju, multiplikaciju i akumulaciju znanja, jest komunikacija. Komunikacija je prošla svoj dug i daleki put od pećinskog crteža do TCP/IP-a, digitalnih metapodataka i podataka, razvoja umjetne inteligencije, algoritamskih kapija i mašinskog učenja (vidi: Crawford i Joler 2018; Perkov 2017a; 2017b; 2017c).

S druge strane, imajući u vidu da je digitalna transformacija društva donijela velike izazove u informisanju i obrazovanju, pa time i u razvoju kritičkog mišljenja - osjetljivost građana (pa i cijelog društvenog sistema) na hibridne asimetrične distorzije[489] i napade (vanjske i unutrašnje) proporcijalno se povećala, te su i izazovi za sigurnost postali značajniji (vidi: Podumljak, 2018). U nekom prethodnom periodu prije Zuckerberg ere, društvo je bilo organizovano na način da su se znali *gatekeeperi*[490] koji imaju ulogu da društvo razvijaju i usmjeravaju na društeno prihvatljiv i očekivan način. U to se ubrajaju, prije svega, mediji kao čuvari demokratije (mainstream, profesionalni – kao glavni posrednici u informisanju, pa i obrazovanju, ali i zabavi), zatim obrazovni sistem i biblioteke (kao ekskluzivni tumači, vlasnici i donosioci znanja), te vojska i policija, preko kojih država upravlja jedinim legitimnim aparatom za prisilu (kao ekskluzivni alati za unutrašnju i vanjsku sigurnost, održavanje mira, ali i, po potrebi, alati za napad i odbranu).

Međutim, uslijed apomedijacije u složenom medijskom, informacijskom, obrazovnom i sigurnosnom okruženju, tradicionalni *gatekeeperi* gube svoju pretpostavljenu ili očekivanu ulogu, te većinu tereta poimanja društveno-političke zbilje, pa i sigurnosne kulture (i u tom kontekstu cyber higijene), preuzimaju na sebe sami građani. Tako se onda pojavljuju akteri koji u kontekstu digitalnih medija zamjenjuju posrednike između korisnika i usluga (dakle informacija koje korisnici traže), što znači da sada stoje uz njih, osiguravajući dodatnu vrijednost izvana kao apomedijatori (Eysenbacha 2008). Drugim riječima kazano, „apomedijacija“ „tradicionalnu ulogu kao čuvara i posrednika odvodi prema ulogama vodiča, savjetnika i facilitatora (podržavatelja)“ (Kulenović 2018). Na taj se način život modernih informacijskih društva sve više integriše u cyber prostor, a samim time i sigurnosni izazovi sve više proizlaze iz istog domena. Ima li se to na umu, jasno će biti zašto se otpornost jednoga društva, države, političkog, ekonomskog i sigurnosnog sistema, medijska i informacijska pismenost sve očitije percipira kao jedna od ključnih kompetencija - i svakoga građanina pojedinačno i društva u cjelini.

U vezi s tim, u Deklaraciji o značaju medijske i informacijske pismenosti u Bosni i Hercegovini491, ističe se da: „Medijska i informacijska pismenost (MIP) jest preduslov održivog razvoja otvorenih, pluralnih, inkluzivnih i participativnih društava znanja, te

---

[489] Distorzija označava iskretanje, izvijanje, iskrivljenje; izopačenje, izobličenje; promjena izvornoga oblika tijekom manipulacije. U ovom kontekstu distorzija označava namjerno djelovanje na društveno-politički i sigurnosni sistem, sa ostvarivanjem političkog cilja. Npr. Podumljak (2018) navodi: „8. novembra 2016. Donald J. Trump osvojio je izborni koledž sa 304 glasa, u usporedbi s 227 glasova Hillary Clinton. Dok je Clinton pobijedila u glasanju naroda - 65,84 milijuna protiv 62,98 milijuna za Donalda Trumpa – Trump je taj koji je postao 45. predsjednik Sjedinjenih Država. Robert Mercer je još jednom postigao mega ***distorziju*** tržišta kao rezultat svog utjecaja na političko ponašanje. Ovaj je put osvojio još veću nagradu: s Trumpom na vlasti šansa da utječe na još mnogo političkih događaja i na mnoge igre u isto vrijeme“ (str. 35). (…) „Njegov fond zaradio je milijarde od referenduma o Brexitu i njegove prve "kontrolirane" tržišine ***distorzije“*** (str. 37).

[490] Gatekeeper: *engl.* Vratar, čuvar vrata ili ključeva; osoba ili stvar koja kontrolira pristup nečemu.

[491] Deklaracija dostupna na:
https://www.onlinepeticija.com/deklaracija_o_znaaju_medijske_i_informacijske_pismenosti_u_BiH
i na: http://fpn.unsa.ba/b/medijska-i-informacijska-pismenost/

građanskih institucija, organizacija, zajednica i pojedinaca koji čine ta društva.". Navedena se postavka u Deklaraciji nudi i kao šira, preciznija definicija:

„Medijska i informacijska pismenost odnosi se na kognitivne, tehničke i socijalne vještine i sposobnosti građanki i građana da pristupaju, kritički ocjenjuju, koriste i doprinose informacijskim i medijskim sadržajima putem tradicionalnih i digitalnih informacijskih i medijskih platformi i tehnologija, uz razumijevanje kako te platforme i tehnologije djeluju, kako da prilikom njihovog korištenja upravljaju vlastitim pravima i poštuju prava drugih, kako da prepoznaju i izbjegnu štetne sadržaje i usluge, da svrsishodno koriste informacije, medijske sadržaje i platforme da bi zadovoljili svoje komunikacijske potrebe i interese kao pojedinci i kao pripadnici svojih zajednica, te da bi prakticirali aktivno i odgovorno učešće u tradicionalnoj i digitalnoj javnoj sferi i u demokratskim procesima" (Deklaracija 2019).

Važno je, međutim, podcrtati da razvojem tehnike i tehnologije, cyber prostora i novih informacijskih i medijskih kanala, alata i platformi, te ulaskom u informacijsko društvo u digitalnom okruženju - sigurnosne prijetnje i izazovi izlaze iz okvira tradicionalnog poimanja međunarodnopravno definisanog i razumijevanog koncepta ratova (sukoba, konflikta), te ulazi u sferu hibridnih asimetričnih sigurnosnih izazova i ratova (Schmitt, 2017).

Pri tome, svakako, valja imati u vidu i da je „znanstveno-tehnološka racionalnost postindustrijske ere utkana u neprozirnu infrastrukturu mašinski upravljane društvenosti", te da je ta, „samokolonizacija neuromedijima" (Hibert 2018: 17) distribuirana kroz pametne uređaje građana koji su, praktično, u isto vrijeme: korisnici usluga i sadržaja, proizvođači sadržaja i metapodataka, pa i sam proizvod u situaciji i vremenu kad je informacija (tj. podatak/data) postala vrednija od nafte (Economist, 2017). Ta je okolnost ne samo „izmijenila način organizacije naših života već je i postala prepreka kognitivnoj autonomiji" (Lynch, 2016 u Hibert, 2018). Tako su građani, zapravo, postali ključni element, ali i najslabija karika u sektoru sigurnosti i, prirodno, jedno od mogućih doluznih oruđa ili očiglednih meta napada. Ipak, „informacijsko-komunikacijske tehnologije nisu puki alati već sile novog ekosistema koje utječu na našu percepciju sebe, interakcije i međusobne odnose, kao i predstavu stvarnosti" (Floridi, 2014 u Hibert, 2018), ali su oni i novi kanali pristupa do građana kojim se mogu kreirati distorzije stvarnosti, javnog mnijenja, volje, pa i manipulacije i stimulacije za djelovanje. Shodno tome, možemo pretpostaviti da se na sve to može odgovoriti jedino adekvatnim sistemskim, dugoročnim, izvodljivim i održivim pristupom medijskoj i informacijskoj pismenosti, jer je očigledno da su ostali demokratski mehanizmi već „hakirani" (vidi: Amer, 2019).

Medijska i informacijska pismenost je krovna kompetencija za: definisanje i artikulaciju informacijskih potreba; lociranje i pristup informacijama; procjenu informacija; organizovanje informacija; etično korištenje informacija; prenošenje informacija; korišćenje vještina IKT za obradu informacija; poznavanje uloge i funkcija medija u

demokratskim društvima; shvatanje uslova pod kojima mediji mogu vršiti svoje funkcije; kritičko vrednovanje medijskih sadržaja, s obzirom na predviđene funkcije medija; korištenje medija za samoizražavanje i demokratsko učešće; vještine prikazivanja (uključujući IKT), potrebne za kreiranje korisničkih sadržaja (Wilson i sar., 2015: 18; Grizzle, A. i Torras Calvo, M., 2013).

Sve su navedene kompetencije važne, građaninu potrebne da ga osnaže kako bi se nosio sa novom ulogom gatekeepera u digitalnom okruženju, pa i ključnog elementa cyber sigurnosti – individualne, institucionalne, državne, ali i međunarodne, jer sam „status tehnološke akceleracije, koji nerijetko ostaje izvan domašaja razumijevanja i kontrole netizena (Hauben i Hauben, 1997 u Hibert, 2018), dodatno pogoduje ambijentu internalizacije digitalnog zagađenja“ (dezinformacije, manipulacije, itd.) „amplificiranog algoritamskim upravljanjem i reorganiziranjem ljudskog kapitala (pažnje, podataka i privatnosti).“ (Hibert, 2018: 19).

U konačnici, pred građaninom, ali i društvom, državom i sektorom sigurnosti - postavljeni su izazovi za koje uglavnom nije dorastao (vidi: Bartlett 2018; Rees 2018; Bostrom 2014) i to, prije svega, zbog neadekvatnog sistemskog odgovora obrazovnog i sigurnosnog sektora na digitalnu transformaciju, u ovom kontekstu u segmentu cyber sigurnosti.

2. Strategije cyber sigurnosti

Sama digitalna transformacija društva učinila je velike pomake u razvoju nauke i tehnologije, kao i u procesima učenja i komunikacije, ali i doprinijela da čitavo sigurnosno poimanje svakodnevnice, pa i njezino izučavanje ili razumijevanje, postane značajno kompleksnije. Prenošenjem većine društvenih, ekonomskih i političkih sfera u cyber prostor, i sigurnost biva izložena novim izazovima, rizicima, pojavnim oblicima, što neminovno zahtijeva i prilagođene strateške, operativne i taktičke sigurnosne odgovore.

Neizbježan razvoj cyber-sigurnosne nauke, kao primijenjene i interdisciplinarne djelatnosti, razvija holistički pristup razumijevanju novih okolnosti i izazova u digitalnom okruženju, dakle pristup koji ima svoje poveznice sa onima iz analognog svijeta u razumijevanju, razvoju i praksi cyber sigurnosti (vidi: Dykstra 2016: 1-15).

Termin „cyber sigurnost“ treba u datom terminosistemu razumijevati kao složen pojam koji ove dvije riječi spaja u navedenu sintagmu: Cyber se odnosi na ljude, stvari, politike, pojmove i ideje povezane sa računarskim uređajima i računarskim mrežama, a posebno Internetom i informacijskim tehnologijama (OSCE 2019), dok termin Sigurnost ima korijene u starolatinskom izrazu securus (bezbrižan, pouzdan, siguran; Klaić, 1985 u Beridan, 2007) što u „znanosti, i u političkoj praksi (...) podrazumijeva dva svoja osnovna aspekta: – znači istodobno: a) funkciju, djelatnost države, društva i pojedinca, a potom i b) stanje u odnosima među državama, stanje unutar jedne države, među ljudima, odnosno stanje u prirodi i kosmosu spram života općenito“ (Beridan 2007: 100).

Na osnovu Beridanove izvedbe definicije sigurnosti (2007: 101), može se reći da sigurnost „općenito podrazumijeva stepen zaštićenosti ljudi od različitih oblika ugrožavanja, zaštitu materijalnih i kulturnih dobara u ličnoj i društvenoj svojini, zaštitu društva i njegovih vrijednosti, cjelovitu zaštitu naroda, nacije, države“ i međunarodnih odnosa, pa i na kosmičkom i planetarnom nivou života općenito, ljudskoga roda u cjelini „od svih vidova ugrožavanja“. Sigurnost podrazumijeva stepen zaštićenosti od ugrožavanja, uz naglasak da ne postoji apsolutna i potpuna sigurnost, već možemo govoriti o većem ili manjem stepenu sigurnosti.

U tom kontekstu moguće je zaključiti da cyber sigurnost jest stanje i praksa zaštite infrastrukture, informacijsko-komunikacijskih sistema, mreža, uređaja i informacija od ugrožavanja, u cilju zaštite ljudi, materijalnih i kulturnih dobara u ličnoj i društvenoj svojini, zaštitu društva i njegovih vrijednosti, cjelovitu zaštitu naroda, nacije, države i međunarodnih odnosa.

Prijetnje kojima se suprotstavlja cyber sigurnost, jesu brojne, ali ih, radi jednostavnijeg razumijevanja, prije svega potrebno posmatrati kao cilj ili kao sredstvo (1) u cyber kriminalitetu, (2) u politički motivisanim cyber napadima i (3) u cyber terorizmu.

1. Cyber kriminalitet uključuje pojedince ili grupe koji „ciljaju“ IKT sisteme za finansijsku protupravnu dobit ili za pravljenje (društvene, ekonomske, političke, sigurnosne) disrupcije. Ovdje govorimo o obliku kriminalnog ponašanja kod kojega se korištenje IK tehnologije i sistema upotrebljava kao sredstvo ili cilj izvršenja, čime se ostvaruje neka krivično-pravno relevantna posljedica. Kompjuterski kriminalitet je, također, protivpravna povreda imovine kod koje se računarski podaci s predumišljajem mijenjaju (manipulacija računara), razaraju (računarska sabotaža) ili se koriste zajedno s hardverom (krađa).492

2. Cyber napadi često uključuju politički motivisano prikupljanje informacija i/ili onesposobljavanje ključne / kritične infrastrukture, pa čak i stvaranje distorzija u društveno-političkom životu zajednice. Sve češće su prikriveni vidovi specijalnog informacijskog ratovanja koji su teško prepoznatljivi u dinamično digitalnom medijskom okruženju. Razvoj moći i kapaciteta visokotehnoloških kompanija, prikupljanje podataka i metapodataka, te njihova dostupnost onome ko je spreman platiti - razvija i nove modele specijalnog asimetričnog hibridnog informacijskog ratovanja, koji uključuju i pomoć algoritamski determinisanih društvenih mreža, dezinformacijsko-propagandne kampanje i intimno poznavanje individualnih građana na osnovu akumuliranih podataka (data points) i digitalnog traga. (vidi: Crawford i Joler 2018; Perkov 2017a; 2017b; 2017c)

[492] Vidi: Krivični zakon Federacije Bosne i Hercegovine "Službene novine Federacije BiH", br. 36/2003, 21/2004 - ispr., 69/2004, 18/2005, 42/2010, 42/2011, 59/2014, 76/2014, 46/2016 i 75/2017: gl. XXXII

3. Cyber terorizam ima za cilj da smišljenom upotrebom napada (ili prijetnje) na IKT sisteme izazove strah, te da se, s namjerom prisiljavanja ili zastrašivanja vlasti ili društva, postignu ciljevi koji su općenito politički, vjerski ili ideološki. Uz to, teroristi i terorističke organizacije jednako efikasno koriste cyber prostor za propagandu, regrutovanje novih kadrova, kao i komunikaciju sa javnostima i medijima (vidi: Babić, 2015).

Načelno, cyber sigurnost gledamo sa aspekta sposobnosti države da odgovori na prijetnje, incidente, i organizuje adekvatnu otpornost sigurnosnog sistema i elemente: snage, mjere, funkcije i aktivnosti sistema nacionalne sigurnosti (vidi: Beridan 2007).

U tu svrhu se izrađuju državne strategije cyber sigurnosti. U okruženju cyber prijetnji (koje je promjenljiva kategorija), države moraju imati fleksibilne i dinamične strategije cyber sigurnosti. Državna strategija za cyber sigurnost jest plan mjera namijenjen poboljšanju sigurnosti i otpornosti infrastruktura i usluga; njome se određuje niz nacionalnih ciljeva i prioriteta koji bi se trebali postići u određenom vremenskom okviru.

Osim rješavanja izazova cyber sigurnosti, strategije se temelje na saradnji – unutrašnjoj i vanjskoj ili međunarodnoj. Neke od najvažnijih postavki za poboljšanje saradnje između sudionika jesu razmjena informacija i stvaranje javno-privatnog partnerstva.493 S obzirom na okruženje rizika i prijetnji koje mutiraju, razvijaju se, konvergiraju i mimikriraju, sigurnost u stanju statičnosti nije adekvatno rješenje u cyber okruženju. Cyber sigurnost je proces (pa čak se može reći i životna filozofija, stanje uma) koji se odnosi na ljude, stvari, politike, pojmove i ideje povezane sa računarskim uređajima i računarskim mrežama, posebno sa internetom i informacionim tehnologijama. U tom kontekstu cyber prostor je više nego internet, jer „uključuje ne samo hardver, softver i informacione sisteme, već i ljude i društvenu interakciju u okviru ovih mreža“ (OSCE 2019: 34).

Tri ključna elementa cyber sigurnosti, potrebna za sveobuhvato poimanje, jesu: tehnologija, procedure i ljudski resursi.

U pogledu tehnologije, koliko god se taj aspekt cyber sigurnosti na prvi pogled činio kompleksnim, u većini slučajeva postoje (polu)gotova hardwerska i softwerska rješenja koja se kupuju od specijaliziranih kompanija (vidi: Microsoft, Cisco, itd). Samo manji broj država ima kapacitete da razvijaju vlastitu tehnologiju, hardware, software, alate, pa i cyber oružja. Tako, naprimjer, Sjedinjene Američke Države kao vodeća država po ulaganju u sigurnost i oružane snage, kontinuirano i sve više ulažu u cyber sigurnost, pa je tako trenutno (za 2020.) za federalne institucije iz budžeta planirano 17,5 milijardi USD, odnosno, ukupno je procijenjenih 66 milijardi USD koje se u SAD ulažu u cyber sigurnost (Forrest 2016; The White House, 2019; Statista, 2019).

---

493 Više na: The European Union Agency for Cybersecurity (ENISA): https://www.enisa.europa.eu/

Drugi element cyber sigurnosti jesu procedure, uglavnom zasnovane na konceptima sistema informacijske sigurnosti (npr. ISO/IEC 27000 grupa standarda), a one jasno propisuju da kroz uspostavljanje i upravljanje tim sistemom, javna uprava (ali i komercijalni sektor, i sami građani) dosljedno izvršava svoju ulogu u izgradnji informacionog društva (vidi: Calder i Watkins, 2015).

Menadžment informacijske sigurnosti posebno je bitan za javne institucije, što znači da „razvojem sistema informacijske sigurnosti javna uprava uspostavlja preventivne mjere i stvara organizaciono-tehničke preduvjete za sistemski razvoj zaštitnih i represivnih mjera u okviru informacijskog društva. Ti procesi ne mogu se uspješno sprovoditi bez uspostavljanja konzistentnog sistema informacijske sigurnosti (…) Pod politikom upravljanja informacijske sigurnosti podrazumijeva se hijerarhijski uređen skup dokumenta koji predstavlja osnovu za implementaciju sistema upravljanja informacijske sigurnosti.“494

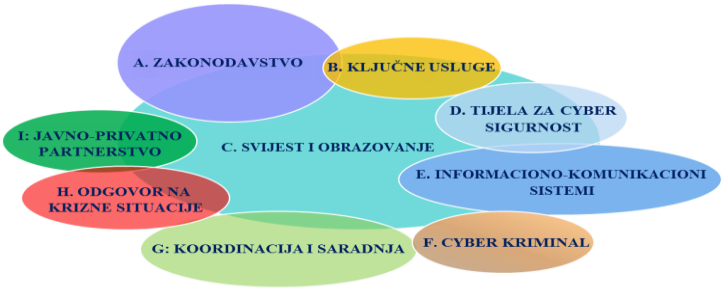
Na kraju, ljudski resursi koji su možda i najvažniji segment ekosistema cyber sigurnosti. Ljudske resurse treba posmatrati dvojako: 1) kao relativno mali broj visoko kvalifikovanih stručnjaka (uglavnom u oblasti IKT), te 2) kao širu grupu ostalih uposlenika, ali i ukupno građanstvo kao aktivne ili pasivne sudionike u cyber prostoru. Prvi su stručnjaci koji su završili obrazovanje za rad u cybersigurnosnom okruženju i koji su toliko traženi da ih je sve teže zadržati na radu u državnom / javnom sektoru. Za druge je (praktično sve ostale građane) prije svega potreban skup kompetencija koje se mogu objediniti pod konceptom medijske i informacijske pismenosti. Izostanak takvih kompetencija proporcionalno povećava sigunosni rizik, jer građanin, zaposlenik u firmi koji ima pristup mreži, javni službenik, pa i agent sigurnosnih službi bez medijske i informacijske pismenosti nedvojbeno jest najslabija karika u cyber sigurnosti. Najčešće cyber napadi ciljaju upravo najslabije tačke (Symantec, 2019), tj. ljude koji su sigurnosno interesantni i nedovoljno medijski i informacijski pismeni.

Medijska i informacijska pismenost zauzima značaj segment obrazovanja i pismenosti današnjice (Vajzović 2017; Vajzović i sar., 2018; Vajzović i sar., 2019). Kompetencije ljudi u segmentu građanske pismenosti postale su ključne u vremenu kada je, zbog postepenog gubljenja sistemske uloge gatekeepera, teret donošenja odluka više nego ikada na pojedincima. Tradicionalni mediji, obrazovni sistem, sigurnosni sistem, pa i porodica, sve više i sve očitije gube bitku u dominaciji naspram interneta i cyber okruženja.

[494] Vidi: Politika upravljanja informacijskom sigurnošću u institucijama Bosne i Hercegovine, za razdoblje 2017 - 2022. godine. Službeni glasnik Bosne i Hercegovine br. 2017/38

U pogledu holističkog sagledavanja izazova, jasno definisani strateški ciljevi cyber sigurnosti pomažu cjelokupnom društvu da razvije adekvatnu cyber sigurnost, kao što je izloženo u grafikonu 1.

Grafikon 1. *Strateški ciljevi cyber sigurnosti*



Izvor: Smjernice za strateški okvir cyber sigurnosti u Bosni i Hercegovini (2019).[495]

Iz grafikona 1. jasno je vidljivo da je razvijanje svijesti o cyber sigurnosti i obrazovanje u toj oblasti značajan i povezujući element za sve ostalo, što se navodi u cilju C (Podizanje nivoa svijesti i znanja o cyber sigurnosti i podciljevima), C1 (Podizanje svijesti o cyber sigurnosti) i C2 (Jačanje programa treninga i obrazovanja). Iz tih je razloga posebno važno „Podržavati procese uključivanja medijske i informacijske pismenosti u formalno i neformalno obrazovanje.“, te „Uvoditi teme vezane za cyber sigurnost i medijsku i informacijsku pismenost u nastavne planove svih nivoa obrazovanja“ (OSCE 2019: str. 13-14).

3. Osnaživanje građana kroz MIP kao strateško opredjeljenje cyber sigurnosti

Cyber sigurnost je izazov za međunarodno (humanitarno) pravo, međunarodne organizacije, multinacionalne korporacije i pojedinačne države, za društvo i za pojedinca. Iz te okolnosti proizlazi da je koncept cyber sigurnosti i značaj osnaživanja te vrste sigurnosnih pitanja kroz medijsku i informacijsku pismenost važno i nužno razumijevati i

[495] Smjernice za strateški okvir cyber sigurnosti u Bosni i Hercegovini je dokument koji je izradila neformalne radna grupa stručnjaka iz javnih, privatnih i akademskih institucija, pod okriljem Misije OSCE-a u Bosni i Hercegovini, a na poziv Ministarstva sigurnosti Bosne i Hercegovine.

pratiti na tri osnovna nivoa: individualnom, institucionalnom, te državnom i međunarodnom nivou.

1. Individualni nivo – gdje je značajna cyber sigurnosna higijena, ali i suštinsko razumijevanje informacija, sadržaja i medija u digitalnom okruženju, kao i shvatanje kompleksnosti infrastrukture i arhitekture dezinformacija i moći ubjeđivanja građana koji nisu medijski i informacijski mudri i osnaženi (vidi: Car, 2015). Praktično to znači da više ne govorimo samo o Clickbaitu[496] i farmama portala ili naloga na društvenim mrežama za potrebe pribavljanja imovinske koristi[497], već govorimo o smjenama vlada, izborima izvršne i zakonodavne vlasti, promjeni ustava, okupacijama ili strateškim ubjeđenjima širokih narodnih masa, pa i podrški za „konvencionalno" ratovanje – šta god to danas značilo u doba dronova, autonomnih oružanih sistema, umjetne inteligencije u i slično (vidi: Giles, 2016).

2. Institucionalni nivo – gdje upravljanje sistemima informacijske sigurnosti, sa bazom u medijskoj i informacijskoj pismenosti na nivou organizacijskih jedinica / kompanija, postaje ključan element sigurnosti kolektiva (vidi: Armerding, 2018).

3. Državni i međunarodni nivo – gdje je fokus na saradnji i izgradnji povjerenja, a medijska i informacijska pismenost značajna, kao strateško opredjeljenje, za podizanje digitalne sigurnosne kulture, za obrazovanje i podizanje svijesti, te za jačanje otpornosti cijelog društva na hibridne asimetrične napade i distorzije u demokratskim društvima.

Brojni su primjeri narušavanja cyber sigurnosti, distorzije društveno-političkog sistema i hibridnih asimetričnih napada koji se odnose na sva tri nivoa, kao što su, primjerice:

1. Estonija[498] - Od 27. aprila 2007. svakodnevnicu u Estoniju čine cyber-napadi, informacijsko ratovanje, lažne vijesti. Te 2007. godine su je pogodili i cyber-napadi velikog obima koji su u nekim slučajevima trajali sedmicama. Internetske usluge estonskih banaka, medijskih kuća i državnih tijela su srušeni sa neviđenim nivom internetskog prometa. Uzastopni valovi napada spamovima od botnete i ogromne količine automatiziranih internetskih zahtjeva preplavile su servere. Rezultat je za građane Estonije bio da su bankomati i internetske bankarske usluge bile sporadično van funkcije; Vladini zaposlenici nisu bili u mogućnosti komunicirati jedni s drugima putem e-pošte; a novine i televizijske stanice iznenada su otkrile da ne mogu isporučiti vijesti.
2. Ukrajina (Brantly, Cal i Winkelstein: 2017) - Otkako su političke krize započele 2014. godine, u Ukrajini je više nego u bilo kojem drugom sukobu, uključivale širok spektar metoda: konvencionalnu taktiku, cyber operacije, elektroničko

[496] Engl. Clickbait - izraz kojim se opisuju senzacionalistički naslovi članaka koji čitateljima web portala navodno nude ekskluzivan ili nesvakidašnji sadržaj. Izraz je složenica engleskih riječi *click* (klik) i *bait* (mamac).
[497] Više na: https://raskrinkavanje.ba/analiza/farme-portala-sarajevo-grad
[498] Vidi: https://www.bbc.com/news/39655415

ratovanje i informacijsko ratovanje. Kombinirani izazovi neprekidnog sukoba, nejasnih boraca i raznolike primjene fizičke, informacijske, elektroničke i cyber sile prema zvaničnim ukrajinskim snagama duž crte razgraničenja, ali i ukrajinskim građanima širom zemlje predstavljaju novu upotrebu moći radi postizanja političkih ciljeva. Tu se ističu i cyber napad na elektroenergetsku mrežu u decembru 2015. godine i niz snažnih cyber napada s zlonamjernim softverom Petya iz 2017. godine.

3. Gruzija (Cornell i Starr, 2009) - U augustu 2008. Rusija je optužena da je koristila cyber uz oružane napade protiv Gruzije: napad na vladine web resurse sa ciljem nanošenja štete ugledu; ugašeni su mediji, forumi i blogovi u Gruziji sa rezultatom da ljudi nisu mogli dobiti prave informacije, uz istovremeno dezinformacije o stvarnim činjenicama od strane ruskih medija; blokirani i prekinuti su gruzijski internetski resursi: Internet komunikacija je bila nemoguća u zemlji i van nje.
4. Cambridge Analitika sa projektima Brexit i Trump499 (Podumljak, 2018; Amer, 2019) - Tvrtka za analizu podataka koja je radila s izbornim timom Donalda Trumpa i pobjedničkom kampanjom Brexit sakupila je milijune Facebook profila birača, u jednom od najvećih tehnoloških kršenja ikada, i koristila ih za izgradnju moćnog softverskog programa za predviđanje i utjecaj na izbore. Steve Bannon 2014. godine - tada izvršni predsjedavajući „ultra desničarske" informativne mreže Breitbart i Robert Mercer, američki milijarder hedge fondova i republikanski donator, bili su kreatori i investitori u Cambridge Analitika. Njihova ideja je bila da spoje „big data" i društvene mreže/medije u poznate vojne metodologije - „informacijskih operacija" - a zatim je iskoriste za američke izbore.

Činjenica da se o hibridnim napadima u novije vrijeme sve češće razmišlja i sve više govori, potvrđuju i riječi ljudi „od struke". Tako generalpukovnik Senad Mašović, načelnik Zajedničkog štaba Oružanih snaga BiH upozorava na nužnost da „kao država prepoznamo module hibridnog rata. Iako ne postoji dogovorena definicija hibridnog ratovanja», smatra da „za ono što je uobičajeno u posljednjih desetak godina, ta djelovanja možemo prepoznati i na našim prostorima", te podsjeća „da su asimetrične prijetnje stalno prisutne, da imaju za cilj sprječavanje funkcionisanja državnih institucija, stvaranje političke i ekonomske nesigurnosti, stvaranje negativnog mišljenja i nezadovoljstva kod stanovništva, kao i nepovoljnih ekonomskih prilika. Posebno je ova problematika izražena u stvaranju negativne slike koja dovodi do masovnog odlaska mladih ljudi koji ne vide perspektivu u svojoj državi, što se dalje negativno odražava na cjelokupno stanje" (Čavčić 2019).

Za državu je i za cyber sigurnost postojanje dobro organizovanih CERT / CSIRT500 ključno u smislu adekvatnih odgovora na incidente i prijetnje, kao i u pogledu njihove aktivne

[499] Za više informcija, dostupno na: https://www.theguardian.com/news/series/cambridge-analytica-files
[500] CSIRT (Computer Security Incident Response Team) - tim za odgovor na računarske sigurnosne incidente

uloge u saradnji sa drugim državama i međunarodnim organizacijama. Njihova saradnja na platformama poput FIRST-a501 kao međunarodnog foruma timova za odgovor na računarske sigurnosne incidente, posebno je značajna za globalnu sigurnost. Okupljajući timove osposobljene za odgovore na različita pitanja i izazove računalne sigurnosti iz vladinih, poslovnih i obrazovnih organizacija, FIRST promovira suradnju i koordinaciju u prevenciji incidenata, inicira brzu reakciju na incidente i podržava razmjenu informacija među članovima i zajednicom u cjelini.

4. Zaključni osvrt

Vidjeli smo da je digitalna transformacija društva donijela velike izazove u informisanju i obrazovanju, pa time i u razvoju kritičkog mišljenja. Život modernih informacijskih društva sve više integriše u cyber prostor, a samim time i sigurnosni izazovi sve više proizlaze iz istog domena. Osjetljivost građana (pa i cijelog društvenog sistema) na hibridne asimetrične distorzije i napade (vanjske i unutrašnje) proporcijalno se povećala, te su i izazovi za sigurnost postali značajniji. Kako smo naveli, uslijed apomedijacije u složenom medijskom, informacijskom, obrazovnom i sigurnosnom okruženju, tradicionalni gatekeeperi gube svoju pretpostavljenu ili očekivanu ulogu, te većinu tereta poimanja društveno-političke zbilje, pa i sigurnosne kulture (i u tom kontekstu cyber higijene), preuzimaju na sebe sami građani. Iz svega je vrlo jasno zašto se (za otpornost jednoga društva, države, političkog, ekonomskog i sigurnosnog sistema) medijska i informacijska pismenost sve očitije percipira kao jedna od ključnih kompetencija - i svakoga građanina pojedinačno i društva u cjelini.

Na kraju je, umjesto zaključka, važno još jedanput ukratko potcrtati da bi kao temelj daljnjeg razvoja i podizanja nivoa cyber sigurnosti, trebalo biti podizanje nivoa medijske i informacijske pismenosti, kao strateškog opredjeljenja opšteg razvoja cyber-sigurnosnog domena, te usavršavanja otpornosti na hibridne asimetrične specijalne informacijske napade i ratovanja. Na taj bi se način dugoročno i značajno osnažila nacionalna sigurnost i istovremeno olakšao posao sigurnosnim snagama u suočavanju sa novim dinamičnim izazovima cyber sigurnosti. Na individualnom planu, stvarali bi se uvjeti da građanin prestane učiti na vlastitim greškama koje nerijetko preskupo koštaju i njega samoga, ponekad i zajednicu u kojoj živi i radi.

Kako je navedeno, okruženje rizika i prijetnji mutira, razvijaja se, konvergira i mimikrira, te sigurnost u stanju statičnosti nije adekvatno rješenje u cyber okruženju. Cyber sigurnost je proces koji se odnosi na ljude, stvari, politike, pojmove i ideje povezane sa računarskim uređajima i računarskim mrežama, posebno sa internetom i informacionim tehnologijama i sadrži navedena tri ključna elementa cyber sigurnosti, potrebna za sveobuhvato poimanje: tehnologija, procedure i ljudski resursi. S obzirom da je ljudski

[501] Vidi na: www.first.org

faktor često i najslabija karika, medijska i informacijska pismenost je zasigurno možda i najznačajni segment u sistemu cyber sigurnosti.

Bibliografija:

1. Amer, K., Noujaim, J. & Amer, K., Barnett, E., Kos, P. (2019) The Great Hack. SAD
2. Armerding, T. (20.12.2018.). The 18 biggest data breaches of the 21st century. Dostupno: https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html.
3. Babić, V. (2015) Cyber terorizam – suvremena sigurnosna prijetnja. Novi Travnik
4. Bartlett, J. (2018). The People vs Tech: How the internet is killing democracy (and how we save it). London. Ebury Press.
5. Beridan, I (2007) Politika i sigurnost – sadržaj i obilježja pojmova. Godišnjak 2007 Fakultet političkih nauka Sarajevo.
6. Bostrom, N. (2014). Superintelligence: Paths, Dangers, Strategies. Oxford. Oxford University Press
7. Brantly, A. F., Cal, N. M., i Winkelstein, D. P. (2017) Defending The Borderland: Ukrainian Military Experiences with IO, Cyber, and EW. The Army Cyber Institute at West Point
8. Calder, A., & Watkins, S. (2015). IT governance: an international guide to data security and ISO 27001/ISO 27002. KoganPage.
9. Car V., ur. (2015). Medijska pismenost - preduvjet za odgovorne medije. Zbornik radova sa 5. regionalne znanstvene konferencije "Vjerodostojnost medija", Sarajevo: Fakultet političkih nauka
10. Crawford, K and Joler, V. (2018) Anatomy of an AI System: The Amazon Echo As An Anatomical Map of Human Labor, Data and Planetary Resources. AI Now Institute and Share Lab, (September 7, 2018) https://anatomyof.ai
11. Čavčić, I. (19.11.2019.) „General Senad Mašović: Asimetrične prijetnje su stalno prisutne, Oružane snage ih znaju prepoznati“. Klix.ba. Dostupno na: https://www.klix.ba/vijesti/bih/general-senad-masovic-asimetricne-prijetnje-su-stalno-prisutne-oruzane-snage-ih-znaju-prepoznati/191119015
12. Deklaracija o značaju medijske i informacijske pismenosti u Bosni i Hercegovini, Sarajevo, 28.1.2019. dostupna na: http://fpn.unsa.ba/b/wp-content/uploads/2019/06/Deklaracija-o-znacaju-MIP-u-BiH_final_310119.pdf
13. Dykstra, J. (2016). Essential cybersecurity science: build, test, and evaluate secure systems. OReilly.
14. Eysenbach, G. (2008). Credibility of Health Information and Digital Media: New Perspectives and Implications for Youth. In M. J. Metzger, & A. J. Flanigan (Eds.), Digital Media, Youth, and Credibility (pp. 125-154). Cambridge, MA: MIT Press.
15. Farme portala: "Sarajevo grad". (n.d.). Dostupno na: https://raskrinkavanje.ba/analiza/farme-portala-sarajevo-grad.
16. Forrest, Conner „Obama seeks $19B for cybersecurity in 2017, a 36% increase“. TechRepublic. Objavljeno 9 Februar, 2016. dostupno na: https://www.techrepublic.com/article/obama-seeks-19b-for-cybersecurity-in-2017-a-36-increase/

17. Giles, K. (2016). Handbook of Russian information warfare. Rome, Italy: NATO Defence College Research Division.
18. Grizzle, A., Torras Calvo, M. (2013) Media and Information Literacy Policy and Strategy Guidelines. United Nations Educational
19. Hibert, M. (2018) Digitalni odrast i postdigitalna dobra: krtičko bibliotekarstvo, disruptivni mediji i taktičko obrazovanje. Zagreb. Multimedijalni institut i Institut za političku ekologiju. Dostupno na:
20. http://lida.ffos.hr/2018/datoteke/abstracts_2018/LIDA_2018_Kulenovic_paper_68.docx
21. Krivični zakon Federacije Bosne i Hercegovine "Službene novine Federacije BiH", br. 36/2003, 21/2004 - ispr., 69/2004, 18/2005, 42/2010, 42/2011, 59/2014, 76/2014, 46/2016 i 75/2017: gl. XXXII
22. Kulenović, F. Strategies of Apomediation in Complex Information Surounding, Abstract. 15. juni 2018. Konferencija: LIBRARIES IN THE DIGITAL AGE (LIDA) 2018, University of Zadar, Croatia, 13 - 15 June 2018. Dostupno na: http://lida.ffos.hr/2018/program/
23. OSCE (2019) Smjernice za strateški okvir cyber sigurnosti u Bosni i Hercegovini. Dostupno na: https://www.osce.org/bs/mission-to-bosnia-and-herzegovina/438386?download=true
24. Perkov, B. (01.08.2017.). Političko-informaciono ratovanje: kratko uputstvo. Dostupno: https://labs.rs/sr/politicko-informaciono-ratovanje-kratko-uputstvo/.
25. Perkov, B. (04.08.2017). Nematerijalni rad i prikupljanje podataka. Dostupno: https://labs.rs/sr/nematerijalni-rad-i-prikupljanje-podataka/.
26. Perkov, B. (17.08.2017.). Istraživanje metapodataka: Haking Tim. Dostupno: https://labs.rs/sr/istrazivanje-metapodataka-haking-tim/.
27. Podumljak, M. (2018) TRUMP'S CODE: Making Money on Populist Disorder. Partnership for Social Development (PSD), Zagreb. ISBN: 978-953-55446-6-1
28. Politika upravljanja informacijskom sigurnošću u institucijama Bosne i Hercegovine, za razdoblje 2017 - 2022. godine. Službeni glasnik Bosne i Hercegovine br. 2017/38)
29. Rees, M. (2018) On the Future Prospects for Humanity. Princeton & Oxford. Princeton University Press
30. Rousseau, J.-J. (1950) The Social Contract and Discourses. trans. G. D. H. Cole. New York: E. P. Dutton. Pristupion na: http://www.questia.com/read/4795085/the-social-contract-and-discourses.
31. Schmitt, M. N. (2017). Tallinn manual 2.0 on the international law applicable to cyber operations. Cambridge University Press.
32. Statista (2019) Spending on cybersecurity in the United States from 2010 to 2018. dostupno na: https://www.statista.com/statistics/615450/cybersecurity-spending-in-the-us/
33. Symantec (2019) ISTR. Dostupno na: https://www.symantec.com/content/dam/symantec/docs/reports/istr-24-2019-en.pdf

34. The Economist (06.05.2017.) The world's most valuable resource is no longer oil, but dana: The data economy demands a new approach to antitrust rules. Dostupno na: https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data
35. The European Union Agency for Cybersecurity (ENISA). Dostupno na: https://www.enisa.europa.eu/topics/national-cyber-security-strategies?tab=details
36. The Guardian. The Cambridge Analytica Files. Dostupno na: https://www.theguardian.com/news/series/cambridge-analytica-files
37. The White House. 2019. "Cybersecurity Funding". dostupno na: https://www.whitehouse.gov/wp-content/uploads/2019/03/ap_24_cyber_security-fy2020.pdf
38. Vajzović E., Džihana A., Hibert M., Ibrahimbegović-Tihak V., Bakić S., Kulenović F. (2018). Pregledna studija o politikama i strategijama medijske i informacijske pismenosti u Bosni i Hercegovini. Sarajevo: Fakultet političkih nauka.
39. Vajzović, E. (2017). Informacijsko društvo i demokratija: građanska pismenost za digitalno doba. U D. V. Nedeljković & D. Pralica (Authors), Digitalne medijske tehnologije i društveno-obrazovne promene 7 (pp. 268-278). Novi Sad: Filozofski fakultet, Odsjek za medijske studije. UDC 321.7:004.738.
40. Vajzović, E., Turčilo, L., Cerić, H., Osmić, A., Silajdžić, L. (2019) Uvođenje medijske i informacijske pismenosti u obrazovni sistem – procjena kompetencija nastavnika za podučavanje medijske i informacijske pismenosti u Kantonu Sarajevo. Sarajevski žurnal za društvena pitanja. Godište VIII. Broj 1-2. 2019. str.137-172. Fakultet političkih nauka Univerzitet u Sarajevu
41. Wilson, C., Grizzle, A., Tuazon, R., Akyempong, K., Cheung, C.K.. (2015) Medijska i informaciona pismenost: Program obuke nastavnika. Nacionalna biblioteka Crne Gore "Đurđe Crnojević".

Zaključci konferencije

ZAKLJUČCI KONFERENCIJE

1. Generalno, postoji potreba za javno-privatnim partnerstvom u implementiranju aktivnosti povezanih sa cyber sigurnosti. Bosna i Hercegovina i države u regionu ne raspolažu, u dovoljnoj mjeri, kapacitetima za adekvatnu borbu protiv prijetnji koje egzistiraju u cyber prostoru, pa je jedno od rješenja partnerski odnos sa privatnim sektorom u uspostavljanju što boljih sistema zaštite. Postoji i potreba konstantne edukacije u oblasti cyber sigurnosti kako stručnjaka tako i javnosti da bi se smanjio prostor za ugrožavanje ovog oblika sigurnosti. Uvođenje jasnih procedura u operiranju na deepweb i darkwebu, bez obzira na zloćudnost naziva su sastavni dio sistema na koji se svi korisnici oslanjaju u svojim operacijama i aktivnostima. Potrebno je aktivno raditi na podizanju svijesti javnosti o tome šta je cyber sigurnost i kako se efikasno zaštiti od prijetnji koje su prepoznate. Dodatno, konstantno informiranje o vrstama prijetnji i načinima njihovog izvođenja tako da potencijalne mete mogu prepoznati zloupotrebu i kontaktirati agencije za provedbu zakona ili druge agencije koje se bave sprečavanjem ovih zloupotreba.
2. Problem seksualnog iskorištavanja i zlostavljanja djece u BiH je izuzetno prisutan, iako to ne pokazuju zvanične statistike. Nedostatak ekspertize među naučnicima i stručnjacima o ovoj temi, upozorava nas potrebu za kontinuiranim istraživanjima i unapređenjem znanja. Trenutni zakonski okvir ne omogućava adekvatnu reakciju na seksualno iskorištavanje i zlostavljanje djece u BiH, pa se analize i izmjene nameću kao prioritet.
3. Podaci o korisnicima zdravstvenih usluga, posebno o djeci, smatraju se posebno osjetljivim podacima pa je u cilju njihove zaštite donijeto niz međunarodnih i evropskih standarda kao i zakonskih propisa u oblasti zaštite podataka o ličnosti kojima se ti podaci štite. Ti standardi se moraju koristiti ne samo od organa za provedbu zakona već i od šire javnosti od značaja.
4. Uslijed nedovoljne zaštite okoliša neophodno je unapređenje sistema upotrebom savremenih tehnologija uključujući i informacione sisteme. Kada govorimo o ekonomskim štetama i rizicima treba istraknuti da je korespondentno bankarstvo u Bosni i Hercegovini je izloženo riziku od pranja novca jer u cyber prostoru omogućava poslovanje sa rezidentnim bankama bez pouzdanih i tačnih informacija o porijeklu novčanih sredstava.
5. Kada govorimo o vještačenju digitalnih dokaza postoje određeni problemi razumijevanja i vjerodostojnosti! Potreban je jedinstven i ujednačen zakonski okvir, kvalitetnija obučenost kadrova za vještačenje i formiranje jedinstvene agencije na nivou BiH za istragu cyber kriminala! U postupanju sa digitalnim dokazima u praksi policijskih tijela u BiH postoje različite prakse što doprinosi kreiranju pravne nesigurnosti i neizvjesnosti sudskih postupaka. Pored toga, potrebno je istražiti načine smanjenja očekivanih nagrada koje počinitelj može imati od

činjenja krivičnih djela u cyber prostoru. Iako je teorijska logika ovoga stava razumna, ostaju dva izazova za buduća akademska istraživanja cyber kriminala: koja sredstva koristiti za smanjenje opaženih koristi od činjenja krivičnih djela u cyber prostoru? Kako da testiramo učinkovitost svih predloženih mjera za smanjenje percepcije visokih koristi od činjenja krivičnih djela u cyber prostoru? Ovo je prvi korak u traženju inovativnih pristupa kako bi nadopunili postojeći niz tehnika protiv cyber kriminala i akademskih znanja vezanih za cyber prostor.

6. Udio računalnog kriminaliteta u ukupnom kriminalitetu u Republici Hrvatskoj je sve veći. Statistika računalnog kriminaliteta (registrovani kriminalitet) nije objektivna jer istraživanja pokazuju visoku stopu tamne brojke. Naime, neprijavljivanje kaznenih djela u značajnoj je mjeri povezano sa nepovjerenjem prema policiji, osjećajem da ne mogu uraditi ništa, birokraciji i slično. Stoga, to ukazuje na potrebu stalne edukacije korisnika različitih sustava, što uključuje policiju, vojsku, tužilaštvo i kaznene sudove. Može se pretpostaviti da je slična situacija u Bosni i Hercegovini i drugim zemljama regiona. Više istraživanja u ovoj oblasti je potrebno, ali i treninga/edukacije lica kojima je povjerena sigurnost građana/ki i njihove imovine.
7. Za istraživače cyber kriminala potrebne su edukacije kako bi se razvio osjećaj i primijenili etički principi u istraživanju društveno-političkih procesa i spriječila zloupotreba cyber prostora, naprimjer ličnih podataka. Vrijedi dodati da je medijska informacijska pismenost ključna komponenta cyber sigurnosti, zbog čega je potrebno raditi na osvještavanju šire javnosti o sadržajima koji se nalaze u cyber prostoru.
8. Cyber prostor je prostor u kojem se vode ratovi. Međunarodno humanitarno pravo se primjenjuje i na cyber prostor, a fokus sigurnosnih institucija, uključujući i NATO mora biti usmjeren na razvoj cyber moći. Međutim, vrijedi istaknuti da je vrlo vjerovatno da nikada neće postojati međunarodno pravo cyber prostora u klasičnom smislu pravne nauke, ali je moguće da će biti dio neke pravne oblasti ili forme. Ostaje otvoreno pitanje kako riješiti međunarodne (pravne) standarde i njihovu implementaciju u domaćim kontekstima. Bosna i Hercegovina predstavlja egzemplarnu studiju, jer se u Bosni i Hercegovini u protekle dvije godine aktivno vode hibridni ratovi protiv države i njenih stanovnika. Glavni akteri su razne interesne skupine, radi se naprimjer o srpskim separatističko-nacionalističkim skupinama koje uživaju podršku Rusije i njenih posrednika. U svakome slučaju, cyber aktivnosti povezane sa terorizmom i separatizmom predstavljaju generičku prijetnju za mir i sigurnost Bosne i Hercegovine i njenih stanovnika.
9. Kako bi riješili brojne probleme i zloupotrebe koje se dešavaju u cyber prostoru neophodna je bolja i slobodnija saradnja između privatnog i javnog sektora u otkrivanju i dokazivanju krivičnih djela, naprimjer krijumčarenja ljudi. Efikasna primjena komercijalne tehnologije može olakšati otkrivanje i dokazivanje krivičnih djela. Za rješavanje krivičnih djela povezanih sa cyber prostorom potrebno je uvezati „cyber" kapacitete u Bosni i Hercegovini. Ljudi predstavljaju kritični resurs u cyber prostoru, a javnost je idealan partner u uspostavljanju cyber sigurnosti.

10. Zaštita kritične infrastrukture u cyber prostoru predstavlja uslov za održavanje stabilnosti društva i države. Iz tog razloga, između ostalih, zakonodavna tijela moraju hitno donijeti zakon o kritičnoj infrastrukturi Bosne i Hercegovine. To zahtijeva sistemski pristup i rješavanje (upravno-)pravne regulative.