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.