Vićentije Darijević*

UDK 343.533::004
004.738.5.056.53

DOI: 10.5937/MegRev2102257D
Stručni članak
Primljen 15.04.2021.
Odobren 22.04.2021.

SAJBER KRIMINAL KAO BEZBEDNOSNI RIZIK NA INTERNETU**

Sažetak: *Razvoj interneta utiče dvojako na ljudsko društvo: omogućava napredak društva i ugrožava bezbednost. Platforme kojima se pristupa, putem interneta, olakšavaju poslovanje, edukaciju i kontakte. S druge strane, pojedinci koji pristupe virtuelnim platformama izlažu svoju privatnost i svoju imovinu riziku od sajber napada. Nažalost, stiče se utisak da zakonska regulativa ne može da drži korak sa tehnološkim napretkom tako da mnogi zločini počinjeni na internetu ostanu nesankcionisani. U ovom radu se ukazuje na karakteristike sajber kriminala, daje se pregled međunarodnih dokumenata kojima je cilj da se uspostavi sajber sigurnost. Daje se i popis domaće zakonodavne regulative kojima Republika Srbija nastoji da reši probleme koje izaziva sajber kriminal. Takođe se ukazuje na karakteristike ove vrste kriminala koje direktno utiču na nemogućnost globalne regulative i zaštite korisnika interneta.*

Ključne reči: *internet, sajber prostor, zakoni, globalno regulisanje.*

* Pravni fakultet, Megatrend univerzitet, Beograd, Srbija; vdarijevic@yahoo.com

** Ovaj rad je rezultat projekta FPMIRS – Znanjem do integrisanja u društvene i ekonomske tokove. Projekat je pokrenut sporazumom Pravnog fakulteta sa Međunarodnim institutom za romološke studije.

1. Uvod

Sajber kriminal razvojem interneta postaje ozbiljna pretnja savremenom društvu. Tehnološki razvoj je brži od promene zakonskih propisa, a osim toga zakonodavac se suočava sa mogućim povredama prava korisnika interneta, kao što su lična prava na privatnost i slobodu govora i integritet javnih i privatnih mreža. Drugi evidentan problem je međunarodna priroda današnjih mreža, tako da nijedna zemlja pojedinačno ne može doneti zakone za efikasno rešavanje problema u vezi sa sajber zločincima, bez saradnje na globalnom nivou.

Trenutna definicija sajber kriminala koja je uglavnom u upotrebi potiče od Centra za istraživanje računarskog kriminala i po njoj sajber kriminal je zločin koji je počinjen na internetu uz korišćenje računara kao alata. Zakonodavstvo, suočeno sa brojnim kontroverzama koje ova vrsta kriminala izaziva, i dalje pokazuje nesnalaženje u otklanjanju ove vrste pretnji, naročito u odnosu na efikasnost krivičnog gonjenja počinilaca sajber kriminala.[1]

Sajber prostor, kao mesto izvršenja sajber kriminala, u suštini predstavlja paralelni urbani prostor,[2] u kome se razmenjuju iskustva, rešavaju problem socijalnog nesnalaženja i socijalne isključenosti. Neretko se u ovom prostoru odvijaju socijalno-ekonomski sukobi i geografske podele.[3]

Ne može da se ospori pozitivna uloga interneta, kada je u pitanju komunikacija koju ostvaruju korisnici ovog prostora, kao i neiscrpnost potencijala za traženje informacija ili za elektronsko poslovanje. Internet i digitalna tehnologija na taj način pozitivno utiču na život ljudi.[4] Međutim, digitalni medijski prostor i društvene medijske aplikacije mogu izazvati i zavisnost kod korisnika.[5]

Internet je globalno rasprostranjen, što znači da se u virtuelnom prostoru susreću učesnici koji dolaze iz svih slojeva društva i kultura,[6]koji se izlažu povredi prava na privatnost. „Privatnost je jedno od osnovnih ljudskih prava koje je posebno ugroženo pojavom novih informacionih tehnologija. Internet je omogućio praćenje komunikacija, analizu fotografija, pristupanje ličnim podacima korisnika i njihovo dalje distribuiranje bez saglasnosti i znanja osobe čiji su

1 Aghatise E. Joseph, *Cybercrime Definition*, Computer Crime Research Center (June 28, 2006), http://www.crime-research.org/articles/joseph06/.

2 Kneale, J. (1999): The Virtual Realities of Technology and Fiction: Reading William Gibson's Cyberspace, in Crang, M. et al (eds.): Virtual Geographies: Bodies, Space and Relations, pp. 205-221; Routledge: London.

3 Rheingold, H. (2002). *Smart mobs: The next social revolution.* Cambridge, MA: Perseus Publishing.

4 :Mossberger, K., Tolbert, C. J., & McNeal, R. S. (2008). *Digital citizenship: The Internet, society, and participation*. Cambridge, MA: MIT Press.

5 Alter, Adam. 2017. Irresistible: The Rise of Addictive Technology and the Business of Keeping Us Hooked. Penguin Random House.

6 Rheingold, H. (2002). *Smart mobs: The next social revolution.* Cambridge, MA: Perseus Publishing.

podaci. Otkrivanjem ličnih podataka korisnici sami doprinose stvaranju digitalnih zapisa o njima. Tako ostavljene informacije i podaci sa korisničkog profila mogu biti zloupotrebljeni na različite načine. Podaci mogu da se iskoriste za pričinjavanje štete korisnicima i eventualnu ucenu, krađe identiteta, sajber nasilje i slične oblike zloupotreba."[7]

2. Sajber kriminal

Pojam *sajber* podrazumeva računarsku mrežu, pomoću koje se može obavljati bilo koja aktivnost u virtuelnom prostoru. Sajber kriminal predstavlja činjenje prevare, trgovinu dečjom pornografijom i intelektualnom svojinom, krađu identiteta ili kršenje privatnosti korišćenjem digitalnih podatka iz računarskih sistema i drugih elektronskih uređaja.

Val (Wall) tvrdi da, kako bismo definisali sajber kriminal, moramo da razumemo uticaj informacionih i komunikacionih tehnologija na naše društvo i kako su ove tehnologije transformisale naš svet. Sajber kriminal stvara nove mogućnosti kriminalcima da vrše krivična dela putem njegovih jedinstvenih karakteristika.[8]

Karakteristike koje Val izdvaja kao najznačajnije za određenje sajber kriminala odnose se na sledeće:

- „Globalizacija", koja dovodi do toga da počinioci nisu ograničeni državnim granicama;
- „Distribuirane mreže", predstavljaju nov prostor pogodan za traženje žrtava;
- „Sinopticizam i panoptizam", koji omogućavaju nadzor nad uključenjem žrtve na daljinu;
- „Tragovi podataka", koje korisnici mreža ostavljaju prilikom priključenja na internet i olakšavaju sajber kriminalcima izvrše krađu identiteta.9

U ovom radu prihvatamo podelu sajber kriminala koju je dao Jar (Yar). On je sajber kriminal podelio na četiri kategorije:

- „Sajber-upad: prelazak sajber granica i upad u tuđe računarske sisteme i prostore gde ljudi imaju pravo vlasništva i gde se uzrokuje šteta, npr. hakovanje i virus distribucija;

[7] Vesna Baltezarević**,** Radoslav Baltezarević (2017):*Zaštita privatnosti na internetu-evropski model*, Megatrend Review Vol. 14 (1). Beograd: Univerzitet "Džon Nezbit, ISSN 1820-3159; COBISS.SR-ID 116780812. UDK 004.738.5316.774, p. 244.

[8] Wall, D., 2007. Hunting Shooting, and Phishing: New Cybercrime Challenges for Cybercanadians in The 21st Century. The ECCLES Centre for American Studies. http://bl.uk/ecclescentre, 2009.

[9] Wall, D.S., 2005. The internet as a conduit for criminal activity. In: Pattavina, A. (Ed.), Information Technology and the Criminal Justice System. Sage Publications, USA, ISBN 0-7619-3019-1.

- Sajber-obmane i krađe: različite vrste činjenja štete koje se mogu odvijati unutar sajber prostora. Na jednom nivou leže tradicionalni obrasci krađe, kao što je lažna upotreba kreditnih kartica i (sajber) novca. Postoji posebna zabrinutost da će se u perspektivi ovaj tip kriminala povećavati zbog povećanja broja onlajn bankovnih računa, kako elektronsko bankarstvo postaje sve popularnije;
- Sajber-pornografija: predstavlja kršenje zakona o razvratnosti i nepristojnosti;
- Sajber-nasilje: nasilni uticaj sajber aktivnosti drugih na individualno, socijalno ili političko grupisanje. Iako takve aktivnosti nemaju direktnu manifestaciju, žrtva ipak oseća nasilje i može da doživi dugoročne psihološke posledice.

Ovde navedene sajber aktivnosti kreću se u rasponu od sajber-progona i govora mržnje do tehnoloških razgovora.

Pored navedenog, Jar je dodao i novu vrstu aktivnosti koju je nazvao „zločin protiv države", opisujući ga kao one aktivnosti koje krše zakone koji štite integritet nacionalne infrastrukture, poput terorizma, špijunaže i obelodanjivanja službenih tajni."[10]

Gordon i Ford (Gordon & Ford) pokušali su da stvore konceptualni okvir zakona koji proizvođači mogu da koriste prilikom kreiranja pravnih definicija koje su značajne i iz tehničke i iz društvene perspektive.[11]

3. Nastojanje da se uspostavi sajber sigurnost

Nacionalna inicijativa za karijeru i studije o sajber sigurnosti (NICCS), definiše sajber sigurnost kao aktivnost ili proces, sposobnost ili kapacitet, bilo države u kojoj se informacijski i komunikacioni sistemi i informacije sadržane u njima štite od i/ili brane od oštećenja, neovlaštene upotrebe, modifikacije ili eksploatacije.[12]NICCS je glavni mrežni resurs (na području SAD) za obuku o sajber bezbednosti. Sjedinjene Države nastoje da razviju radnu snagu efikasnih profesionalaca za uspostavljanje sajber bezbednosti. "Značajne investicije koje su SAD uložile u programe poput NICCS-a pomažu građanima da se obrazuju i da steknu veštine koje su im potrebne za napredovanje u karijeri i uklanjanje nedostataka u veštinama radne snage u sajber-bezbednosti."[13]

[10] Yar, M., 2006. Cybercrime and Society. Sage Publication Ltd, London.

[11] Gordon, S., Ford, R., 2006. On the definition and classification of cybercrime. J. Comput. Virol. 2 (1), 13–20.

[12] NICCS, Official website of the Cybersecurity and Infrastructure Security Agency (2021).'Explore Terms: A Glossary of Common Cybersecurity Terminology,' https://niccs.us-cert.gov/glossary.

[13] Ibid

Na međunarodnom evropskom nivou borba za ostvarivanje sajber sigurnosti odvija se donošenjem različitih međunarodnih akata:

- Konvencija o visokotehnološkom kriminalu, doneta je 23. novembra 2001. godine u Budimpešti. „Konvencija o visokotehnološkom kriminalu je osmišljena u cilju sprečavanja dela koja su usmerena protiv integriteta, poverljivosti i dostupnosti kompjuterskih sistema, mreža i podataka, a samim tim i sprečavanja zloupotrebe tih sistema, mreža i podataka tako što će se pokrenuti kaznene mere za takvo delovanje kao što je opisano u Konvenciji i pri čemu će se primeniti kazne za efikasnu borbu protiv krivičnih dela, i na taj način će se na unutrašnjem i međunarodnom nivou olakšati otkrivanje, istraga i gonjenje za izvršena krivična dela i omogućiti da se obezbede uslovi za brzu i pouzdanu međunarodnu saradnju.“[14]
- Dodatni protokol uz Konvenciju o visokotehnološkom kriminalu koji se odnosi na inkriminaciju dela rasističke i ksenofobične prirode izvršenih preko računarskih sistema (2003);
- Konvenciju Saveta Evrope o zaštiti dece od seksualnog iskorišćavanja i seksualnog zlostavljanja (tzv. Lanzarot konvencija – Savet Evrope 2007. godine, stupila na snagu 2010. godine i ratifikovana iste godine od strane Republike Srbije);
- Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, Strasbourg, 28.I.2003, Art.1;
- Odluku Saveta Evropske unije o suzbijanju dečije pornografije na internetu 2000/375/JHA;
- Direktivu Evropskog parlamenta o borbi protiv seksualne zloupotrebe, seksualne eksploatacije i dečije pornografije 2011/92EU;
- Direktivu 2013/40/EU Evropskog parlamenta i Saveta EU o napadima na informacione sisteme i zameni Okvirne odluke Saveta 2005/222/JHA;
- Bezbednosnu agendu Evropske unije za period od 2015. do 2020. Godine;
- Strategiju sajber bezbednosti Evropske unije iz 2013. godine – „Otvoren, bezbedan i zaštićen sajber prostor”;
- IOCTA (Internet organised crime threat assessment 2017) – Procena pretnje od Internet organizovanog kriminala.15

Ovi dokumenti predstavljaju osnov za borbu protiv sajber kriminala i istovremeno polaznu bazu za dalju konkretizaciju zakonodavstva u Republici Srbiji. Usaglašavanje sa komunitarnim pravom, sa regulativom koja je do sada doneta u okviru Evropske unije, omogućava da se adekvatno reaguje na sve vrste sajber kriminala a da se ne uspori razvoj informacionih tehnologija.

[14] Strategija za borbu protiv visokotehnološkog kriminala za period 2019–2023. godine, str. 6.

[15] Ibid, str. 6-8.

Republika Srbija borbu protiv visokotehnološkog kriminala nastoji da reši donošenjem određene zakonske regulative.

Krivični zakonik[16] „propisuje sledeća krivična dela protiv bezbednosti računarskih podataka: oštećenje računarskih podataka i programa (član 298), računarska sabotaža (član 299), pravljenje i unošenje računarskih virusa (član 300), računarska prevara (član 301), neovlašćeni pristup zaštićenom računaru, računarskoj mreži i elektronskoj obradi podataka (član 302), sprečavanje i ograničavanje pristupa javnoj računarskoj mreži (član 303), neovlašćeno korišćenje računara ili računarske mreže (član 304), pravljenje, nabavljanje i davanje drugom sredstava za izvršenje krivičnih dela protiv bezbednosti računarskih podataka (član 304a). Za navedena krivična dela krivično gonjenje je u isključivoj nadležnosti Posebnog tužilaštva za borbu protiv visokotehnološkog kriminala. Takođe, u Krivičnom zakoniku se definiše značenje pojedinih izraza od važnosti za oblast visokotehnološkog kriminala."[17]

Zakonik o krivičnom postupku[18] „propisuje niz posebnih dokaznih radnji koje se mogu primeniti u krivičnim postupcima protiv učinilaca krivičnih dela iz stvarne nadležnosti Posebnog tužilaštva za borbu protiv visokotehnološkog kriminala. i u ovom zakoniku se definiše značenje izraza od važnosti za oblast visokotehnološkog kriminala."[19]

Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala[20] „definiše okvir za otkrivanje, krivično gonjenje i suđenje za krivična dela protiv bezbednosti računarskih podataka, intelektualne svojine, imovine, privrede i pravnog saobraćaja, kod kojih se kao objekat ili sredstvo 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 2.000 ili nastala materijalna šteta prelazi iznos od 1.000.000 dinara; krivična dela protiv sloboda i prava čoveka i građanina, polne slobode, javnog reda i mira i ustavnog uređenja i bezbednosti Republike Srbije, koja se zbog načina izvršenja ili upotrebljenih sredstava mogu podvesti pod visokotehnološki kriminal."[21]

Zakon o elektronskim komunikacijama[22] „uređuje uslove i način za obavljanje delatnosti u oblasti elektronskih komunikacija, nadležnosti državnih organa u oblasti elektronskih komunikacija, zaštitu prava korisnika i pretplatnika, bezbednost i integritet elektronskih komunikacionih mreža i usluga, tajnost elek-

16 „Službeni glasnik RS", br. 85/05, 88/05 – ispravka, 107/05 – ispravka, 72/09, 111/09, 121/12, 104/13, 108/14 i 94/16.

17 Strategija za borbu protiv visokotehnološkog kriminala za period 2019–2023. godine, str. 6.. 11-12.

18 Službeni glasnik RS", br. 72/11, 101/11, 121/12, 32/13, 45/13 i 55/14)

19 Strategija za borbu protiv visokotehnološkog kriminala za period 2019–2023. godine, str. 12.

20 „Službeni glasnik RS", br. 61/05 i 104/09

21 Strategija za borbu protiv visokotehnološkog kriminala za period 2019–2023. godine, str 13.

22 „Službeni glasnik RS", br. 44/10, 60/13 – US i 62/14

tronskih komunikacija, zakonito presretanje i zadržavanje podataka, nadzor nad primenom ovog zakona, mere za postupanje suprotno odredbama ovog zakona, kao i druga pitanja od značaja za funkcionisanje i razvoj elektronskih komunikacija u Republici Srbiji." [23]

Zakon o informacionoj bezbednosti[24] „uređuje mere zaštite od bezbednosnih rizika u informaciono-komunikacionim sistemima, odgovornost pravnih lica prilikom upravljanja i korišćenja informaciono-komunikacionih sistema i određuju se nadležni organi za sprovođenje mera zaštite, koordinaciju između činilaca zaštite i praćenje pravilne primene propisanih mera zaštite." [25]

Prema podacima kojima MUP raspolaže, kada je u pitanju ova oblast kriminala, ukazuje se na to da je više od 90% sajber napada počinjeno na istovetan način: fišing kampanjom. „Najčešće se vrše krivična dela prevare, krivična dela protiv polne slobode prema maloletnim licima, prikazivanje, pribavljanje i posedovanje pornografskog materijala i iskorišćavanje maloletnog lica za pornografiju, proganjanje, ugrožavanje sigurnosti, neovlašćen pristup zaštićenom računaru, računarskoj mreži i elektronskoj obradi podataka, računarska prevara, računarska sabotaža i drugo – kažu za eKapiju iz MUP-a." [26]

4. Sajber kriminal kao specifično kriminalno delo

„Visokotehnološki kriminal je po mnogim svojstvima specifičan u odnosu na vršenje drugih krivičnih dela. Pre svega, reč je o relativno novoj pojavi. Do pre nekoliko godina zakonodavstva država nisu adekvatno reagovala na njegovu pojavu; danas su različita dela koja se mogu počiniti upotrebom računara deo mnogih pravnih sistema. Ipak, među rešenjima koja su upotrebljena ne postoji konzistentnost, a često ni minimum potrebne komplementarnosti kako bi se neko delo uspešno procesuiralo. Sa druge strane, visokotehnološki kriminal ima veoma izraženu nadnacionalnu dimenziju – dela te vrste se po pravilu vrše u međunarodnom prostoru, odnosno uključuju na direktan ili posredan način više država."[27]

Specifičnosti karakteristične za ovu vrstu kriminala utiču na otežano regulisanje ove materije i problem u procesuiranju izvršilaca. Sajber kriminal najčešće prevazilazi granice jedne države, a samim tim i granice važećeg teritorijalnog zakonodavstva. Najčešće se izvršenje dela rasprostire na teritoriju više država zbog čega se postavlja pitanje konkretne nadležnosti za procesuiranje izvršilaca.

[23] Strategija za borbu protiv visokotehnološkog kriminala za period 2019–2023. godine, str. 13.

[24] „Službeni glasnik RS", br. 6/16 i 94/17.

[25] Strategija za borbu protiv visokotehnološkog kriminala za period 2019–2023. godine, str. 13-14.

[26] https://www.ekapija.com/news/3044298/visokotehnoloski-kriminal-u-srbiji-vise-od-90-sajber-napada-zapocinje-fising-kampanjom

[27] Lidija Komlen Nikolić et al. (2010) Suzbijanjevisokotehnološkog kriminala. Beograd: Udruženje javnih tužilaca i zamenika javnih tužilaca Srbije, str. 135.

Iluzija beskonačne slobode na internetu, koju mnogobrojni korisnici prihvataju kao bezuslovnu, jer smatraju da je internet medij bez cenzure, često može da dovede izvršioce dela u zabludu. Surfovanjem po sajber prostoru učine krivično delo a da nemaju svest o tome da su radnje koje su preduzeli sankcionisane, smatrajući da svojim radnjama nisu imali nameru da steknu protivpravnu imovinsku (ili drugu) korist.

Problem koji posebno izaziva različite kontroverze odnosi se na kontrolisanje korisnika interneta pri čemu postoji bojazan od ugrožavanja pravana privatnost pojedinca.

Međunarodno pravo još uvek nije dalo adekvatan odgovor za borbu sa sajber kriminalom. Ne postoji globalno prihvaćena regulativa, već nasuprot tome, šaroliko zakonodavstvo unutar konkretnih država. Sporost međunarodnih organa i usaglašavanja država koje se najčešće usmerava na bilateralne sporazume, ili na rešavanja na usko regionalnim nivoima, omogućava sajber kriminalu da se nesmetano rasprostire i da ugrožava korisnike društvenih mreža.

5. Zaključak

Istraživanjem dostupne literature i zakonskih dokumenata iz oblasti sajber kriminala stiče se utisak da sajber kriminal nezadrživo prodire i razara sve sfere društva i pored svih napora koji se čine na domaćem i međunarodnom nivou da se obezbedi zaštita korisnika interneta. Kako se znanje i veštine sajber kriminalaca povećavaju, tako se povećava potreba za efikasnijom prevencijom i otkrivanjem ovih kriminalnih aktivnosti. Sporost pravnog sistema, dugotrajne procedure međunarodnih usaglašavanja, obezbeđuju prostor učiniocima krivičnih dela u sajber prostoru da neometano deluju. Daleko od toga, da zakonodavci ne reaguju. U polju sajber sigurnosti postoji niz novih modela, sistema i alata koji imaju za cilj da otkriju i spreče napade na pojedince koji koriste digitalne tehnologije. Danas postoje zakoni širom sveta kojima se teži ka odvraćanju sajber kriminalca od zločina u sajber prostoru i procesuiranju počinioca na adekvatan način. Međutim, stiče se utisak da generalni pristup sprečavanja sajber kriminala, koji treba da bude u zaštiti pojedinaca, mora biti usaglašeniji. Samo na taj način može biti od koristi za rešavanje problema kriminala na mreži. Nameće se pitanje: Kako poboljšati borbu protiv sajber kriminala na globalnom nivou? Ovde je problematika znatno kompleksinija. Bilateralni i regionalni sporazumi za rešavanje problema sajber kriminala ne predstavljaju problem. Problem se pojavljuje kada je globalna regulacija u pitanju. Prepreke koje onemogućavaju donošenje globalnog akta za sankcionisanje ove vrste kriminala, ne postoji, niti će moći da budu donete u dužem vremenskom periodu. Do tada najbitnije je za sprečavanje sajber kriminala, stvaranje svesti o ugroženoj bezbednosti, kod korisnika interneta i usaglašeno globalno delovanje, bez obzira na različite pristupe pojedinih država rešavanju ovog problema.

Literatura:

- Aghatise E. Joseph (2006): *Cybercrime Definition*, Computer Crime Research Center, http://www.crime-research.org/articles/joseph06/.
- Alter, Adam. (2017): *Irresistible: The Rise of Addictive Technology and the Business of Keeping Us Hooked*. Penguin Random House.
- Baltezarević, V., Baltezarević, R. (2017):Zaštita privatnosti na internetu-evropski model, *Megatrend Review* Vol. 14 (1), 241-251.
- Kneale, J. (1999): The Virtual Realities of Technology and Fiction: Reading William Gibson's Cyberspace, in Crang, M. et al (eds.): Virtual Geographies: Bodies, Space and Relations, 205-221; Routledge: London.
- Komlen Nikolić L. et al. (2010):*Suzbijanjevisokotehnološkog kriminala*. Beograd: Udruženje javnih tužilaca i zamenika javnih tužilaca Srbije.
- Mossberger, K., Tolbert, C.J., & McNeal, R.S. (2008): *Digital citizenship: The Internet, society, and participation*. Cambridge, MA: MIT Press.
- NICCS Official website of the Cybersecurity and Infrastructure Security Agency (2021): 'Explore Terms: A Glossary of Common Cybersecurity Terminology,' https://niccs.us-cert.gov/glossary
- Rheingold, H. (2002): *Smart mobs: The next social revolution*. Cambridge, MA: Perseus Publishing.
- „Službeni glasnik RS", br. 85/05, 88/05 – ispravka, 107/05 – ispravka, 72/09, 111/09, 121/12, 104/13, 108/14 i 94/16.
- Službeni glasnik RS", br. 72/11, 101/11, 121/12, 32/13, 45/13 i 55/14)
- Strategija za borbu protiv visokotehnološkog kriminala za period 2019–2023. godine, str. 12.
- „Službeni glasnik RS", br. 61/05 i 104/09
- „Službeni glasnik RS", br. 44/10, 60/13 – US i 62/14
- „Službeni glasnik RS", br. 6/16 i 94/17.
- Strategija za borbu protiv visokotehnološkog kriminala za period 2019–2023. godinehttp://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/vlada/strategija/2018/71/1/reg
- Wall, D., (2007): *Hunting Shooting, and Phishing: New Cybercrime Challenges for Cybercanadians in The 21st Century*. The ECCLES Centre for American Studies. http://bl.uk/ecclescentre.
- Wall, D.S., (2005): The Internet as a conduit for criminal activity. In: Pattavina, A. (Ed.), Information Technology and the Criminal Justice System. Sage Publications, USA, 77-98.
- Yar, M., (2006): *Cybercrime and Society*. Sage Publication Ltd, London.
- Gordon, S., Ford, R., (2006): On the definition and classification of cybercrime. *Journal in Computer Virology* 2 (1), 13–20.
- https://www.ekapija.com/news/3044298/visokotehnoloski-kriminal-u-srbiji-vise-od-90-sajber-napada-zapocinje-fising-kampanjom

Vićentije Darijević

UDC 343.533::004
004.738.5.056.53

DOI: 10.5937/MegRev2102257D
Expert article
Received 15.04.2021.
Approved 22.04.2021.

CYBER CRIME AS A SECURITY RISK ON THE INTERNET

Summary: *The development of the Internet affects human society in two ways: it enables society to progress and endangers security.Online access platforms facilitate business, education and contacts.On the other hand, individuals who access virtual platforms expose their privacy and their assets to the risk of cyber attacks.Unfortunately, one gets the impression that legislation cannot keep pace with technological advances so that many crimes committed on the internet remain unsanctioned. This paper points out the characteristics of cybercrime, gives an overview of international documents aimed at establishing cyber security.A list of domestic legislative regulations by which the Republic of Serbia seeks to solve the problems caused by cybercrime is also given.It also points out the characteristics of this type of crime that directly affect the impossibility of global regulation and protection of Internet users.*

Keywords: *Internet, Cyberspace, Laws, Global regulation.*