Svetislav R. Lutovac*
Nikoleta S. Lutovac**

UDK 343.533::004

DOI: 10.5937/MegRev2202069L
Pregledni naučni članak
Primljen 15.04.2022.
Odobren 10.05.2022.

ULOGA DIGITALNIH TEHNOLOGIJA U ORGANIZOVANOM KRIMINALU***

Sažetak: *Sajber prostor je postao mesto u kome internet korisnici pored obavljanja svakodnevnih aktivnosti, kao što su komunikacija sa ostalim korisnicima, zabava ili obavljanje posla, vrlo lako mogu postati i žrtve različitih sajber kriminalnih aktivnosti. Kriminalci su unapredili i adaptirali svoje tradicionalne kriminalne metode i uz pomoć digitalnih tehnologija mogu nanositi štetu, kako lakovernim pojedincima tako i samim vladama. Za razliku od realnog prostora, u digitalnom okruženju, sajber kriminalci mogu ostati anonimni i izbeći sankcionisanje od strane nadležnih organa. Neretko su ovakve sajber kriminalne grupe organizovane i deluju na međunarodnom nivou, što još više otežava identifikovanje prestupnika. Cilj ovog rada je da informiše o metodama kojima se služe pojedinačni sajber kriminalci, ali i organizovane kriminalne grupe i sugeriše na neophodnost međunarodne zajedničke saradnje svih nadležnih organa, ali i na potrebu informisanja i usaglašavanja zakona iz ovog domena, kako bi se borba protiv ovakvih ilegalnih sajber aktivnosti efikasnije vodila.*

Ključne reči: *Sajber prostor, Internet korisnici, Sajber kriminal, Digitalne tehnologije, Organizovani kriminal*

* Docent, Pravni fakultet, Megatrend univerzitet, Beograd; lutovacsveto@gmail.com
** Asistent, Pravni fakultet, Megatrend univerzitet, Beograd; nlutovac@megatrend.edu.rs
*** Rad je rezultat Projekta FPPNT –Pravo i nove tehnologije.

1. Uvod

Digitalne tehnologije i pored svih prednosti koje obezbeđuju čovečanstvu, takođe se koriste i u svrhe kriminalnih aktivnosti. Procenat ovakvih sajber kriminalnih dela je u porastu poslednjih godina. Mnogo je teže suprotstaviti se kriminalu u sajber prostoru nego tradicionalnom, jer je kriminalcima omogućeno da u digitalnom svetu mnogo lakše ostanu anonimni. Sa druge strane, u prilog ovakvom tipu kriminalaca ide na ruku još uvek neusaglašena i konfuzna zakonska regulativa, ali i nedovoljan nivo digitalne globalne pismenosti korisnika.[1]

Pregledom literature je otkriveno da su hakeri jedan od primarnih tipova sajber-kriminalaca na koje su se fokusirale studije.[2] Međutim, sve je više organizovanih grupa koje sprovode svoje aktivnosti u sajber prostoru. Korišćenjem sijaseta digitalnih alata, njihove mete mogu biti pojedinci, ali i same države i sposobni su da izazovu čitav dijapazon kako emocionalnih, tako i materijalnih šteta.

Sajber kriminalci mogu delovati kao labave mreže, ali dokazi sugerišu da se članovi i dalje nalaze u neposrednoj geografskoj blizini čak i kada su njihovi napadi međunacionalni. Na primer, male lokalne mreže, kao i grupe koje uključuju rođake i prijatelje, značajni su akteri. Vruće tačke sajber kriminala sa potencijalnim vezama sa organizovanim kriminalnim grupama nalaze se u mnogim zemljama, međutim zemlje bivšeg Sovjetskog Saveza u tome još uvek prednjače.[3] Analiza je pokazala da su mreže koje su prvenstveno koristile onlajn forume za rast bile u stanju da izvrše međunarodne napade sa relativno malom grupom prestupnika.[4]

Pojedine zemlje nisu u situacijama otkrivanja sajber kriminalaca uvek kooperativne, a nedovoljna usaglašenost međunarodnih zakona o organizovanom sajber kriminalu doprinosi da problem ranog identifikovanja ovakvih aktivnosti ne bude efikasno rešen.

Program INTERPOL-a za sajber kriminal je svetao primer u međunarodnoj borbi protiv ove pojave. Ovaj program insistira na međunarodnoj razmeni informacija, organizuje radne grupe, kurseve obuke i konferencije i koordinira međunarodne operacije u borbi protiv ilegalnih sajber aktivnosti.[5]

---

1 Baltezarević, R.,Baltezarević, I. (2021): The Dangers and Threats that Digital Users Face in Cyberspace. *IPSI Transactions on Internet Research*, Vol. 17, No. 1, January 2021, pp. 46-52.

2 Silic, M., Lowry, P. B. (2019). Breaking bad in cyberspace: Understanding why and how black hat hackers manage their nerves to commit their virtual crimes. Information Systems Frontiers, pages 1–13.

3 Kshetri, N. (2013): Cybercrime and Cybersecurity in the Global South. Palgrave Macmillan.

4 Leukfeldt, E.R., E.R. Kleemans & W.Ph. Stol (2016): A typology of cybercriminal networks:From low tech locals to high tech specialists. Crime, Law and Social Change. DOI:10.1007/s10611-016-9646-2

5 United Nation Office on Drugs and Crime (2012): The use of the Internet for terrorist purposes. https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf (Pristupljeno: 20.05.2022).

2. Organizovani kriminal

Veliki deo konfuzije u debati o organizovanom kriminalu može se objasniti neuspehom da se shvati da postoje različiti načini da se konceptualizuje organizovani kriminal i da svaki pristup može dovesti do različitog razumevanja i procene iste situacije.[6] Analizom više od 100 definicija organizovanog kriminala, Federiko Vareze (Federico Varese) je ilustrovao kako su definicije organizovanog kriminala varirale tokom vremena, u rasponu od definicija koje naglašavaju kriminalne strukture sa jasnom hijerarhijom i centralizovanim vođstvom do definicija koje definišu organizovani kriminal kao kriminalne poduhvate uključene u nezakonite aktivnosti i definicije koje se fokusiraju na strukture kriminalnih mreža.[7]

Kresi (Cressey) je možda ponudio najpotpuniju definiciju i po njemu je organizovani kriminal jedinstven oblik kriminalne aktivnosti, koji je opisao kao svaki zločin počinjen od strane osobe koja zauzima, u utvrđenoj podeli rada, položaj dizajniran za izvršenje zločina, pod uslovom da takva podela rada takođe uključuje najmanje jednu poziciju za koruptivca, jednu poziciju za korumpiranu osobu i jednu poziciju za izvršioca.[8] Prema Albiniju (Albini) organizovani kriminal može se klasifikovati u četiri glavna oblika: politički — društveno organizovani (kao što su gerilci, terorističke organizacije i druge politički motivisane grupe), plaćenički (maloletničke bande i organizovanje pljački), orijentisan na grupe (motociklističke bande) i sindikati (mafija koja obezbeđuje nedozvoljenu robu ili usluge).[9] Organizovani kriminal ne podrazumeva samo zločine poroka, niti predstavlja deo dublje kriminalne zavere ili sredstvo za etničke grupe da postignu inače nedostižne ciljeve uspeha. Organizovani kriminal je prilično preduzetnički orijentisan i iako uključuje kršenje zakona, prvenstveno proširuje legitimne tržišne aktivnosti u zabranjenim područjima.[10] Abadinski (Abadinsky), smatra da političkim motivima nije mesto u definiciji organizovanog kriminala i gleda na organizovani kriminal kao na neideološki poduhvata koji uključuje određeni broj osoba u bliskoj društvenoj interakciji, organizovanih na hijerarhijskoj osnovi, sa najmanje tri nivoa/ranga, u cilju obezbeđenja profita i moći bavljenjem nelegalnim i legalnim aktivnostima.[11] Kada sažmemo pojam

6 von Lampe, K. (2016): *Organized Crime: Analyzing Illegal Activities, Criminal Structures, and Extra-Legal Governance*. US: SAGE Publications.

7 Varese, F. (2010). What Is Organized Crime? Pp. 1–35 in *Oranized crime: Critical Concepts in Criminology*, edited by F. Varese. Londonand New York: Routledge.

8 Cressey, D. R. (1969): *Theft of a Nation: The Structure and Operations of Organized Crime in America*. New York, NY.: Harper and Row.

9 Albini, J. L. (1971): *The American Mafia: Genesis of a Legend.* Appleton-Century-Crofts.

10 Smith, D. C. (1978): Organized Crime and Entrepreneurship. *International Journal of Criminology and Penology* 6(3):161–77.

11 Abadinsky, H. (1994): *Organized Crime*. 4th ed. Chicago: Nelson-Hall.

organizovanog kriminala, nalazimo tri različite perspektive. Prvo, organizovani kriminal se može odnositi na organizaciju kada ovaj pojam označava prisustvo više ili manje stabilnih i strukturiranih veza među prestupnicima. Drugo, organizovani kriminal se može odnositi na kriminalne aktivnosti koje karakteriše određeni nivo sofisticiranosti i kontinuiteta. Treće, može se odnositi na koncentraciju moći, kada je fokus na prisustvu sistemskog stanja u obliku vlade podzemlja ili saveza između kriminalaca i političkih i ekonomskih elita.[12] Dakle, organizovani kriminal se ne razlikuje samo ontološki od oportunističkih pojedinaca, već evocira i ideju interpersonalne i društvene pretnje i zbog toga predstavlja veću pretnju, jer ono što pojedinci mogu da urade, organizacije to mogu učiniti još bolje.[13]

3. Kriminalne aktivnosti u digitalnom okruženju

Mnoga krivična dela organizovanog kriminala oslanjala bi se na nove tehnologije kao što su mobilni telefoni, veb okruženje uključujući Deep Veb gadžete za poverljivu komunikaciju, neke računarske aplikacije za razmenu informacija, mnoge opreme za snimanje i tako dalje.[14] U ranim danima sajber kriminala, scenom su uglavnom dominirali mladi hakeri koji su ilegalno pristupali kompjuterskim sistemima i kršili mere bezbednosti samo iz zabave ili da bi pokazali svoje tehničke veštine. Sajber-kriminal je postepeno evoluirao od relativno malog obima zločina koji je počinio pojedinačni prestupnik specijalista do kriminala velikog obima poput organizovanog i industrijskog.[15] Sajber kriminal iskorišćava međunacionalne razlike u kapacitetima za sprečavanje, otkrivanje, istragu i krivično gonjenje takvih zločina, i brzo postaje sve veća globalna briga. Ovaj transnacionalni karakter pruža sajber kriminalcima, bilo da deluju kao pojedinci ili kao organizovane kriminalne grupe, potencijal da izbegnu protivmere, čak i kada ih osmisle i sprovode najsposobniji akteri.[16] Ono što pojedinačni prestupnici mogu učiniti, često i bolje, mogu i organizacije. Očigledno je da su mnoge, ako ne i sve vrste kriminalnih organizacija, sposobne da se bave

[12] von Lampe, K. (2008): Organized Crime in Europe: Conceptions and Realities. Policing, (2)1,7-17.

[13] Lavorgna, A. (2016): Exploring the cyber-organised crime narrative: The hunt for a new-bogeyman? In P.C. van Duyne et al. (Eds.), Organising fears, Crime & Law Enforcement-New horizons and trends in Europe & beyond. Oisterveijk: Wolf Legal Publishers.

[14] Peterson, M. (2005): *Intelligence-Led Policing: The New Intelligence Architecture*, Bureau of Justice Assistance.

[15] Anderson, R., Barton, C., Bohme, R., Clayton, R., van Eeten, M., Levi, M., & Moore, T.(2012): Measuring the Cost of Cybercrime. Presented at the Workshop on theEconomics of Information Security (WEIS), Berlin, Germany.

[16] Broadhurst, R., Chang, Y. C. (2013): Cybercrime in Asia: Trends and Challenges. In Asian Handbook of Criminology (pp. 49–64). Springer.

sajber kriminalom. Internet i srodne tehnologije savršeno su pogodne za koordinaciju širom disperzovanog područja. Organizovana kriminalna grupa može biti visoko strukturisana tradicionalna mafijaška grupa koja angažuje prestupne IT profesionalce (hakere). To može biti kratkotrajni projekat koji vodi grupa koja preduzima određeni onlajn zločin ili cilja određenu pojedinačnu žrtvu ili grupu. Umesto grupa, ovakav vid aktivnosti može uključiti i širu zajednicu koja je isključivo bazirana na mreži i bavi se digitalnom imovinom, kao što je trgovina ilegalnim softverom ili distribucija opscenih slika dece. Takođe se može sastojati od pojedinaca koji rade samostalno, ali su istovremeno povezani sa makro-kriminalnom mrežom.[17]

Poslednjih godina, pobunjeničke i ekstremističke grupe su koristile internet tehnologiju kao instrument krađe kako bi poboljšale svoju bazu resursa. Imam Samudra (Imam Samudra), osuđeni arhitekta bombaških napada na Baliju, navodno je pozvao svoje sledbenike na internetu da počine prevaru sa kreditnim karticama kako bi finansirali militantne aktivnosti.[18] Konvencionalni kriminalci i teroristi koriste internet kao medij komunikacije u podsticanju kriminalnih zavera. I, kao što je slučaj sa građanima koji poštuju zakon, digitalna tehnologija poboljšava kapacitete za čuvanje zapisa i drugih informacija, kao i za obavljanje finansijskih transakcija. U slučaju kriminalaca, takve transakcije mogu biti deo aktivnosti pranja novca. Sa druge strane, proizvođači nedozvoljenih supstanci oglašavaju i trguju receptima preko digitalnih tehnologija.[19]

Hačingsova (Hutchings) studija o kompjuterskim zločinima koji ugrožavaju podatke i finansijsku sigurnost sugeriše da su mnogi sajber prestupnici visoko umreženi, da sarađuju jedni s drugima u činjenju prekršaja i da uče svoje ponašanje od drugih. Rezultati, međutim, ne pokazuju da li treba da označimo ove grupe koje rade na mreži kao organizovane kriminalce.[20] MekGvajer (McGuire) je identifikovao tri glavna tipa organizovanih kriminalnih sajber grupa (tip I, II i III) i šest podtipova (roj, čvorišta, prošireni hibridi, klasterizovani hibridi, agregati i hijerarhije) i zaključio da je do 80 procenata sajber kriminala organizovani

[17] Spapens, T. (2010); Macro Networks, Collectives, and Business Processes: An IntegratedApproach to Organized Crime. European Journal of Crime, Criminal Law and Criminal Justice, 18(2), 185–215.

[18] Sipress, A. (2004): An Indonesian's Prison Memoir Takes Holy War Into Cyberspace: In Sign of New Threat,Militant Offers Tips on Credit Card Fraud. Washington Post. https://www.washingtonpost.com/archive/politics/2004/12/14/an-indonesians-prison-memoir-takes-holy-war-into-cyberspace/71edfe6f-5231-479f-8bab-2a3ce9944ccf/ (Pristupljeno: 20.05.2022).

[19] Schneider, J. L. (2003): Hiding in Plain Sight: An Exploration of the Illegal(?) Activities of a Drugs Newsgroup. The Howard Journal of Criminal Justice, 42(4), 374–389. doi:10.1111/1468-2311.00293

[20] Hutchings, A. (2014): Crime from the keyboard: organised cybercrime, co-offending,initiation and knowledge transmission. Crime, Law and Social Change, 62(1), 1–20.

kriminal. Prema izveštaju, određene ključne karakteristike tradicionalnih organizovanih kriminalnih grupa treba da se preispitaju kada grupe rade na mreži. Na primer, u sajber prostoru veličina grupe nije u korelaciji sa uticajem i obimom prekršaja i mnoga udruženja su veoma prolazna. Međutim, kako bi bilo odlučeno da li određena mreža prestupnika treba da bude označena kao organizovani sajber kriminal, treba se baviti ponavljajućim obrascima prestupnika i obimom aktivnosti, zanemarujući debate oko definicija organizovanom sajber kriminalu i usvajajući krovni termin ovoj pojma, kako bi se uključio širok spektar grupa koje izlažu neki stepen organizovanosti.[21]

Ko su zapravo osobe koje se bave sajber kriminalom pojedinačno ili u okviru organizovane grupe? Ajzenkova (Eysenck) teorija u pokušaju da objasni kriminalni profil osobe koja je sklona činjenju zločina predlaže trodimenzionalni model (PEN) ličnosti: psihoticizam (antisocijalan, agresivan i bezbrižan), ekstraverzija (traženje senzacija) i neuroticizam (nestabilnost).[22] Ove tri dimenzije ličnosti čine jedinstven skup karakteristika koje pojedinca čine podložnim kriminalnom ponašanju. Takođe, imajući u vidu značaj mračne trijade i tradicionalnog zločina, osobine psihoticizma, narcizma i makijavelizma takođe su povezane sa kriminalnim ponašanjem.[23]

Većina studija se fokusira na faktore kao što su obrazovna dostignuća, modus-operandi i mreže-saradnici.[24] Ovaj opšti pristup naglašava potrebu za ciljanijim istraživanjem kako bi se identifikovale razlike među različitim tipovima prestupnika, informišući o preventivnim aktivnostima organa za sprovođenje zakona. Drugi fokus u pregledanim člancima je i način na koji sajber kriminalci komuniciraju i grade poverenje. Nalazi ukazuju na to da karding forumi olakšavaju organizovani sajber kriminal jer nude hibridni oblik organizacione strukture koja je u stanju da se pozabavi izvorima neizvesnosti i minimizira transakcione troškove do mere koja omogućava da se pojavi konkurentno podzemno tržište. Stoga su neophodna dalja istraživanja o različitim karakteristikama članova foruma za karding, kao što su veštine, motivacija, ali i veze sa kriminalom van mreže.[25]

---

21 McGuire, M. (2012): Organised Crime in the Digital Age. London: John Grieve Centrefor Policing and Security.

22 Eysenck. H. (1964): Crime and Personality. London: Routledge and Kegan Paul, 1964

23 Seigfried-Spellar, L. D., Villacıs-Vukadinovic, KC (2017): Computer criminal behaviour is related to psychopathy and other antisocial behaviour. Journal of Criminal Justice, (51):67–73.

24 Lazarus, S., Okolorie, G. U. (2019) The bifurcation of the nigerian cyber-criminals: Narratives of the economicand financial crimes commission (efcc) agents. Telematics and Informatics, 40:14–26.

25 Yip, M., Webber, C., Shadbolt, N. (2013). Trust among cybercriminals? carding forums, uncertainty and implications for policing. Policing and Society, 23(4):516–539

4. Uloga tehnologija u prevenciji kriminala i međunarodna saradnja u borbi protiv sajber kriminala

Pregledom istorijskog razvoja napora u sprečavanju kriminala ističe se poenta da je tehnologija bila glavna pokretačka snaga koja je dovela do reforme strategija kontrole i prevencije kriminala, kako od strane pojedinaca, zainteresovanih grupa, tako i od strane zvaničnih policijskih agencija.[26] Tehnološki napredak tokom godina imao je dubok uticaj na način na koji razmišljamo o kriminalu i na napore koji se preduzimaju da se on spreči. Čvrste tehnologije (eng. hard technologies) za sprečavanje kriminala pokrivaju širok spektar primena u različitim kontekstima, uključujući detektore metala u školama, pregled prtljaga na aerodromima, neprobojne prozore u bankama i bezbednosne sisteme u kućama i preduzećima, zatvorene televizijske kamere i slično.[27] Međutim, postoje samo dve tehnološke inovacije koje imaju poznati uticaj na prevenciju kriminala: zatvorene televizijske kamere i poboljšano ulično osvetljenje. Za druge vrste tvrde tehnologije, neophodna istraživanja nisu još uvek sprovedena.[28] Sa druge strane, meke tehnologije (eng. soft technologies) se ubrzano razvijaju u pogledu dizajna, implementacije i uticaja mekih informacionih tehnologija u oblasti identifikovanja i prevencije kriminalnih aktivnosti.[29] Među najistaknutijim predstavnicima mekih tehnologija koji se koriste u prevenciji kriminala izdvajaju se sistemi za upravljanje dokumentima, mobilni terminali za podatke, kompjuterski podržani sistemi za otpremu, deljenje informacija putem interneta, kompjuterizovane analize kriminala, softveri za mapiranje zločina i sistemi ranog upozorenja odnosno rane intervencije prema nedoličnom ponašanju.[30]

Informaciona tehnologija, može povećati sposobnost skladištenja i obrade velikih količina podataka, poboljšavajući obaveštajne i istražne sposobnosti i obezbeđujući lak pristup krivičnim evidencijama i drugim vrstama relevantnih podataka.[31] Iako informacione tehnologije imaju potencijal da unaprede rad policije

[26] Harris, C. (2007): Police and Soft Technology: How Information Technology Contributes to Police Decision Making. In: Byrne, J. and Rebovich, D. (2007). *The New technologyof Crime, Law and Social Control,* Monsey, NY: Criminal Justice Press, p. 153-183.

[27] Marx, G. (2007): Engineering of Social Control: Intended and Unintended Consequences. P In: Byrne J. and Rebovich, D. (eds) *The New Technology of Crime, Lawand Social Control*, Monsey, NY: Criminal Justice Press, p 347-371.

[28] Hankin, A., Hertz, M., and Simon, T. (2011): Impacts of metal detector use in schools: insights from 15 years of research. *Journal of School Health*, 81(2), p. 100-106.

[29] Manning, P. (2008): A view of surveillance. In: Leman-Langlois, (ed) *Techno-Crime: Technology, Crime, and Social Control,* Willan Publishing: Collompton, Devon,p. 209-242.

[30] Harris, C. (2007): Police and Soft Technology: How Information Technology Contributes to Police Decision Making. In: Byrne, J. and Rebovich, D.(2007). *The New technologyof Crime, Law and Social Control,* Monsey, NY: Criminal Justice Press, p. 153-183.

[31] Reichert, K. (2001): Use of information technology by law enforcement. *Promising Approaches to Addressing Crime Series*. University of Pennsylvania, Jerry Lee Center of

i suštinski promene tradicionalnu policijsku praksu, malo je dokaza da je do takve promene i došlo i da je rad policije efikasniji u poređenju sa ranijim erama i usvajanjem telefona, dvosmernog radija i automobila. Međutim, može se zaključiti da je razvoj informacionih tehnologija u velikoj meri unapredio tradicionalne prakse.[32]

Razumevanje prevencije kriminala zahteva proučavanje namera, kao i posledica. Potrebno je razmotriti širok spektar mera izvan tradicionalnog broja krivičnih događaja ili prestupnika. Dodatni faktori uključuju količinu sprečene štete ili broj žrtava koje su oštećene (često i više puta).[33] Transnacionalna priroda sajber kriminala i teškoća u identifikaciji počinioca ili mesta izvršenja zločina stvorile su nekoliko prepreka i izazova za organe za sprovođenje zakona širom sveta u vezi sa pribavljanjem prekograničnih dokaza i izručenjem kriminalaca. Stoga je efikasna, brza i dobro funkcionišuća međunarodna saradnja između država u krivičnim stvarima od suštinskog značaja za unapređenje istraga i krivičnog gonjenja sajber kriminala koji je olakšan na globalnom nivou.[34] Policijska međunarodna saradnja podrazumeva razmenu podataka i informacija između policijskih organa različitih zemalja u cilju razmene kriminalističkih obaveštajnih podataka, sprovođenja istrage i hapšenja osumnjičenih. Takva razmena se može vršiti direktno ili preko jedne od međuvladinih organizacija kao što su Međunarodna organizacija kriminalističke policije (INTERPOL) i Evropska policijska kancelarija (EUROPOL) u cilju borbe protiv različitih vrsta zločina.[35] Program INTERPOL-a za sajber kriminal je važan alat u međunarodnoj borbi protiv ove pojave. Njegova glavna svrha je da podrži razmenu informacija među državama članicama kroz regionalne radne grupe i konferencije, pomogne i koordinira međunarodne operacije i ponudi kurseve obuke za razvoj i unapređenje profesionalnih standarda. Pored toga, igra važnu ulogu u stvaranju svetske liste službenika za kontakt za istrage sajber kriminala u svrhu pružanja pomoći zemljama članicama u slučaju sajber napada, identifikovanja novih pretnji i deljenja ovih obaveštajnih podataka, obezbeđujući siguran veb portal za pristup operativnim informacijama i dokumentima, kao i razvoj strateškog partnerstva sa drugim međunarodnim organizacijama i institucijama privatnog sektora.[36]

Criminology, Forum on Crime and Justice.

32 Harris, C. (2007): Police and Soft Technology: How Information Technology Contributes to Police Decision Making In: BYRNE, J. and REBOVICH, D.(2007). *The New technology-of Crime, Law and Social Control,* Monsey, NY: Criminal Justice Press, p. 153-183.

33 Sherman, L.W., Gottfredson, D.C., Mackenzie, D.L., Eck, J.E., Reuter, P., and Bushway, S.D. (1997): *Preventing Crime: What Works, What Doesn't, What'sPromising.* Washington, DC: National Institute of Justice, U.S. Department of Justice.

34 Verdelho, P. (2008): the effectiveness of international co-operation against cybercrime: examples of good practices 1, 4.

35 Lemieux, F. (2010): International police cooperation: Emerging issues, theory and Practice, Willan. ISBN 9781843927600

36 United Nation Office on Drugs and Crime (2012): The use of the Internet for terrorist purposes. https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.

5. Zaključak

Skoro polovina celokupne svetske populacije koristi internet i sajtove društvenih mreža, što je indikator činjenice da je virtuelno okruženje postalo nezaobilazno mesto u kreiranju stavova internet korisnika. Na žalost, iako su ljudi svakodnevno izloženi uticaju raznih digitalnih informacija, one se ne mogu uvek smatrati kredibilnim izvorom.[37] Studija koja je sprovedena 2021. godine je pokazala da potrošači više veruju elektronskoj komunikaciji od usta (eWOM), nego tradicionalnoj komunikaciji od usta do usta (WOM).[38] Ovo su činjenice koje idu na ruku pojedinačnim i organizovanim grupama koje se bave sajber kriminalom. Korisnici interneta su danas postali lake mete sajber prestupnika, pored činjenice da je do njih danas lako doći, nedovoljna digitalna pismenost na globalnom nivou jedan je od glavnih faktora koji omogućavaju sprovođenje sajber kriminalnih aktivnosti, jer takvi korisnici, često i nesvesno, postaju žrtve u okviru sajber prostora.

U rastućem svetu interneta, kako u ličnim tako i u internet preduzećima, sajber kriminal je sve veći problem. Kažnjavanje ovih aktivnosti postala je nova oblast u istrazi zločina i sprovođenju zakona. Sajber kriminal je odveo kriminalce preko granica i ograničenja od pojave interneta. Tamo gde su „virtuelna" vrata ostavljena otvorena, kriminalni element će pronaći svoj put. U ovom slučaju, vrata za zločin je sajber prostor. Sajber kriminal je ogroman po obimu. Kreće se od pojedinačnih kriminalaca do sve većeg prisustva međunarodnog organizovanog sajber kriminala. Prevare haraju internetom, pune foldere e-pošte i veb stranica, pokušavajući da namame nesuđene žrtve u svoje mreže obmane. Sajber kriminalci pokušavaju da pristupe njihovim osetljivim ličnim i poslovnim informacijama, da prikupe ono što mogu da pronađu i da te podatke iskoriste sa kriminalnim namerama.

Internet nije samo okupio ljude, već je spojio međunarodne agencije za borbu protiv kriminala u zajedničkom cilju. Jasno je da je sajber kriminal industrija koja raste na međunarodnom planu. Upravo zbog svoje međunarodne prirode, ovakvi zločini stvaraju mnoge političke i pravosudne probleme koji proizilaze iz neusklađenosti krivičnog zakona.Digitalne tehnologije imaju potencijal da dramatično poboljšaju i efikasnost i efektivnost prevencije i suzbijanja kriminalnih aktivnosti i sistema krivičnog pravosuđa. Međutim, pored pozitivnih aspekata mora se pomenuti da tehnološke inovacije ugrožavaju lične slobode i izazivaju povećano nepoverenje javnosti. Pronaći idealni balans biće neophodnost koja očekuje sve stručnjake iz ove oblasti u bliskoj budućnosti.

pdf (Pristupljeno: 20.05.2022).

37 Baltezarević, R.(2022):Uloga normativnog konformizma u digitalnom okruženju u kreiranju stavova potrošača prema luksuznim brendovama, *Megatrend revija,*Vol. 19, № 1, 177-188

38 Kwiatek, P., Baltezarević, R., Papakonstantinidis, S. (2021): The impact of credibility of influencers recommendations on social media on consumers behavior towards brands. *Informatologia.Vol. 54 No. 3-4,* 181-196

Literatura:

- Abadinsky, H. (1994): *Organized Crime*. 4th ed. Chicago: Nelson-Hall.
- Albini, J. L. (1971): *The American Mafia: Genesis of a Legend*. Appleton-Century-Crofts.
- Anderson, R., Barton, C., Bohme, R., Clayton, R., van Eeten, M., Levi, M., & Moore, T. (2012): Measuring the Cost of Cybercrime. Presented at the Workshop on the Economics of Information Security (WEIS), Berlin, Germany.
- Baltezarević, R.,Baltezarević, I. (2021): The Dangers and Threats that Digital Users Face in Cyberspace. *IPSI Transactions on Internet Research*, Vol. 17, No. 1, January 2021, pp. 46-52.
- Baltezarević, R.(2022):Uloga normativnog konformizma u digitalnom okruženju u kreiranju stavova potrošača prema luksuznim brendovama, *Megatrend revija*,Vol. 19, № 1, 177-188
- Broadhurst, R., Chang, Y. C. (2013): Cybercrime in Asia: Trends and Challenges. In Asian Handbook of Criminology (pp. 49–64). Springer.
- Cressey, D. R. (1969): *Theft of a Nation: The Structure and Operations of Organized Crime in America*. New York, NY.: Harper and Row.
- Eysenck. H. (1964): Crime and Personality. London: Routledge and Kegan Paul, 1964
- Hankin, A., Hertz, M., and Simon, T. (2011): Impacts of metal detector use in schools: insights from 15 years of research. *Journal of School Health*, 81(2), p. 100-106.
- Harris, C. (2007): Police and Soft Technology: How Information Technology Contributes to Police Decision Making In: BYRNE, J. and REBOVICH, D. (2007). *The New technologyof Crime, Law and Social Control,* Monsey, NY: Criminal Justice Press, p. 153-183.
- Hutchings, A. (2014): Crime from the keyboard: organised cybercrime, co-offending, initiation and knowledge transmission. Crime, Law and Social Change, 62(1), 1–20.
- Kshetri, N. (2013): Cybercrime and Cybersecurity in the Global South. Palgrave Macmillan.
- Kwiatek, P., Baltezarević, R., Papakonstantinidis, S. (2021): The impact of credibility of influencers recommendations on social media on consumers behavior towards brands. *Informatologia.Vol. 54 No. 3-4,* 181-196
- Lavorgna, A. (2016): Exploring the cyber-organised crime narrative: The hunt for a newbogeyman? In P.C. van Duyne et al. (Eds.), Organising fears, Crime & Law EnforcementNew horizons and trends in Europe & beyond. Oisterveijk: Wolf Legal Publishers.
- Lazarus, S., Okolorie, G. U. (2019) The bifurcation of the nigerian cyber-criminals: Narratives of the economic and financial crimes commission (efcc) agents. Telematics and Informatics, 40:14–26.

- Lemieux, F. (2010): International police cooperation: Emerging issues, theory and Practice, Willan. ISBN 9781843927600
- Leukfeldt, E.R., E.R. Kleemans & W.Ph. Stol (2016): A typology of cybercriminal networks: From low tech locals to high tech specialists. Crime, Law and Social Change. DOI: 10.1007/s10611-016-9646-2
- Manning, P. (2008): A view of surveillance. In: Leman-Langlois, (ed) *Techno-Crime: Technology, Crime, and Social Control,* Willan Publishing: Collompton, Devon,p. 209-242.
- Marx, G. (2007): Engineering of Social Control: Intended and Unintended Consequences. P In: Byrne J. and Rebovich, D. (eds) *The New Technology of Crime, Lawand Social Control*, Monsey, NY: Criminal Justice Press, p 347-371.
- McGuire, M. (2012): Organised Crime in the Digital Age. London: John Grieve Centre for Policing and Security.
- Peterson, M. (2005): *Intelligence-Led Policing: The New Intelligence Architecture*, Bureau of Justice Assistance.
- Reichert, K. (2001): Use of information technology by law enforcement. *Promising Approaches to Addressing Crime Series*. University of Pennsylvania, Jerry Lee Center ofCriminology, Forum on Crime and Justice.
- Schneider, J. L. (2003): Hiding in Plain Sight: An Exploration of the Illegal(?) Activities of a Drugs Newsgroup. The Howard Journal of Criminal Justice, 42(4), 374–389. doi:10.1111/1468-2311.00293
- Sherman, L.W., Gottfredson, D.C., Mackenzie, D.L., Eck, J.E., Reuter, P., and Bushway, S.D. (1997): *Preventing Crime: What Works, What Doesn't, What'sPromising*. Washington, DC: National Institute of Justice, U.S. Department of Justice.
- Seigfried-Spellar, L. D., Villacıs-Vukadinovic, KC (2017): Computer criminal behaviour is related to psychopathy and other antisocial behaviour. Journal of Criminal Justice, (51):67–73.
- Silic, M., Lowry, P. B. (2019). Breaking bad in cyberspace: Understanding why and how black hat hackers manage their nerves to commit their virtual crimes. Information Systems Frontiers, pages 1–13.
- Sipress, A. (2004): An Indonesian's Prison Memoir Takes Holy War Into Cyberspace: In Sign of New Threat, Militant Offers Tips on Credit Card Fraud. Washington Post. https://www.washingtonpost.com/archive/politics/2004/12/14/an-indonesians-prison-memoir-takes-holy-war-into-cyberspace/71edfe6f-5231-479f-8bab-2a3ce9944ccf/ (Pristupljeno: 20.05.2022).
- Smith, D. C. (1978): Organized Crime and Entrepreneurship. *International Journal of Criminology and Penology* 6(3):161–77.
- Spapens, T. (2010): Macro Networks, Collectives, and Business Processes: An IntegratedApproach to Organized Crime. European Journal of Crime, Criminal Law and Criminal Justice, 18(2), 185–215.

- United Nation Office on Drugs and Crime (2012): The use of the Internet for terrorist purposes. https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf (Pristupljeno: 20.05.2022).
- Varese, F. (2010). What Is Organized Crime? Pp. 1–35 in *Oranized crime: Critical Concepts in Criminology*, edited by F. Varese. Londonand New York: Routledge.
- Verdelho, P. (2008): the effectiveness of international co-operation against cybercrime: examples of good practices 1, 4.
- von Lampe, K. (2008): Organized Crime in Europe: Conceptions and Realities. Policing, (2)1,7-17.
- von Lampe, K. (2016): *Organized Crime: Analyzing Illegal Activities, Criminal Structures, and Extra-Legal Governance*. US: SAGE Publications.
- Yip, M., Webber, C., Shadbolt, N. (2013). Trust among cybercriminals? carding forums, uncertainty and implications for policing. Policing and Society, 23(4):516–539

Svetislav R. Lutovac
Nikoleta S. Lutovac

UDC 343.533::004

DOI: 10.5937/MegRev2202069L
Review scientific paper
Received 15.04.2022.
Approved 10.05.2022.

THE ROLE OF DIGITAL TECHNOLOGIES IN ORGANIZED CRIME

Abstract: *Cyberspace has become a place where Internet users, in addition to performing everyday activities, such as communicating with other users, having fun or doing business, can very easily become victims of various cybercriminal activities. Criminals have improved and adapted their traditional criminal methods and with the help of digital technologies, they can harm both gullible individuals and governments themselves. Unlike real space, in the digital environment, cybercriminals can remain anonymous and avoid sanction by the authorities. Such cybercrime groups are often organized and operate at the international level, which makes it even more difficult to identify criminals. The aim of this paper is to inform about the methods used by individual cybercriminals, but also organized criminal groups, and suggests the need for international joint cooperation of all competent authorities, but also the need to inform and harmonize laws in this domain, in order to combat such illegal cyber activities more effectively.*

Keywords: *Cyberspace, Internet users, Cybercrime, Digital technologies, Organized crime*