UDK 343.9.02
Biblid: 0025-8555, 75(2023)
Vol. LXXV, br. 4, str. 667–684
DOI: https://doi.org/10.2298/MEDJP2304667P

Pregledni rad
Primljen 31. 8. 2023.
Odobren 30. 9. 2023.

Kriptografija u službi oganizovanog kriminala – izazov za nauku i praksu

Nenad PUTNIK[1], Milica BOŠKOVIĆ[2]

Apstrakt: Organizovani kriminal predstavlja ozbiljnu pretnju po bezbednost, ekonomiju, a nekada i pravni poredak zemlje. Kriminalne grupe koriste dostignuća informaciono-komunikacionih tehnologija (IKT) za širenje organizacije, komunikaciju i upravljanje aktivnostima i resursima, kao i za ulaganje u razvoj sopstvenih aplikacija za delovanje kroz nelegalne kanale. Najmoćnije organizovane kriminalne grupe imaju svoje IKT stručnjake čiji je cilj da štite komunikacione kanale, kao i da osmišljavaju nove načine „zaobilaženja" i neutralisanja policijskih mera i tehnika za otkrivanje i praćenje njihovog delovanja. Pripadnici organizovanih kriminalnih grupa koriste komunikacione aplikacije koje omogućavaju šifrovani prenos elektronskim uređajima pomoću odgovarajućeg operativnog sistema, omogućavajući instaliranje aplikacije i uspostavljanje veze sa internetom kako bi se omogućila potrebna zaštićena komunikacija. Postoje i aplikacije koje omogućavaju šifrovanje celog uređaja, što otežava pronalaženje njegovog sadržaja ili otkrivanje potrebnih informacija i dokaza. U radu su prikazane karakteristike organizovanog kriminala i načina njegovog izvršenja, sa akcentom na upotrebi kriptografskih tehnika. Obrađene su studije slučaja koje ilustruju veličinu i obim problema zloupotrebe enkripcije od strane organizovanih kriminalnih grupa, a zatim su identifikovani izazovi u suprotstavljanju zloupotrebi kriptografije sa tehničko-tehnološkog i pravnog aspekta i date smernice za unapređenje mehanizama suprotstavljanja organizovanom kriminalu.

Ključne reči: organizovani kriminal, međunarodna bezbednost, enkripcija, komunikacija, dokazne radnje.

---

[1] Redovni profesor, Fakultet bezbednosti – Univerzitet u Beogradu, nputnik@fb.bg.ac.rs, ORCID 0000-0002-6374-7270

[2] Redovni professor, Fakultet za diplomatiju i bezbednost, milica.boskovic@fdb.edu.rs, ORCID 0000-0002-3421-7107

Rad je nastao u okviru projekta koji finansira Fond za nauku Republike Srbije u okviru Programa "IDEJE" – Management of New Security Risks – Research and Simulation Development, NEWSIMR&D, #7749151.

Uvod

Organizovani kriminal je od ozbiljnog nacionalnog rizika početkom XXI veka prerastao u jedan od vodećih međunarodnih izazova bezbednosti. Kriminalni akteri prepoznaju svoje interese, povezuju se i sarađuju van nacionalnih granica, brže i efikasnije nego što to nekada uspevaju države na planu ekonomije i spoljne politike. Od početka ovog veka, organizovani kriminal doživljava bitne promene. Među njih možemo svrstati činjenicu da on prerasta u transnacionalnu pojavu i organizacije čiji članovi postoje i deluju u različitim zemljama. Osim toga, profit i moć ostvareni ovom vrstom kriminala se enormno uvećavaju, a raste i vaninstitucionalni uticaj organizovanih kriminalnih grupa na izvršnu vlast slabih država i donosioce političkih odluka (Bošković 2021, 28).

Organizovani kriminal, stoga, predstavlja ozbiljnu pretnju po bezbednost, ekonomiju, a nekada i pravni poredak zemlje. Povezivanjem i širenjem ovakvih grupa van nacionalnih granica, rizici i negativni uticaji se višestruko povećavaju. Brojne su posledice delovanja transnacionalnog organizovanog kriminala. Na individualnom nivou raste broj žrtava i nevinih ljudi koji trpe ozbiljne finansijske posledice, a neretko i trajne fizičke i psihičke traume. Osim ovoga, pogubnost po međunarodne tokove ogleda se i u prisustvu internacionalnih koruptivnih radnji, legalizaciji milijardi nelegalno stečenih dolara, namernom izazivanju konflikata među državama, devastiranju životne sredine i dr. Iako raznovrsne i međusobno katkad nepovezane, sve ove posledice proističu iz delovanja najzastupljenijih oblika organizovanog kriminala. Ilegalna trgovina oružjem, trgovina narkoticima, trgovina ljudima (trafiking), krijumčarenje (ljudi, kulturnih dobara ili retkih i zaštićenih životinjskih vrsta), najopasniji su, najčešći i najunosniji oblici (transnacionalnog) organizovanog kriminala (Bošković 2021, 31). Najveći nelegalni profit (koji se danas meri u milijardama dolara na godišnjem nivou) i najozbiljnije posledice ostavljaju trgovina narkoticima, oružjem kao i trgovina ljudima. Istovremeno, ovo su i oblici organizovanog kriminala koji su najbrže „napredovali" u prevazilaženju nacionalnih granica i širenju svog delovanja, čak i van kontinenata.

Nakon Drugog svetskog rata, pa čak i nakon završetka Hladnog rata, vladajući bezbednosni koncepti kao najvažnije vitalne vrednosti smatrali su teritorijalni integritet i ekonomski prosperitet države, a glavni stratezi nacionalne bezbednosti poticali su iz vojske. Međutim, u posthladnoratovskom periodu identifikovani su novi bezbednosni problemi, izazovi i pretnje koji su proizveli nove nesigurnosti, umesto nuklearnih ili ideoloških pretnji. Pitanja koja obično nisu povezivana sa bezbednošću tokom Hladnog rata sekuritizovana su, pošto se bezbednost proširila sa vojnog poimanja bezbednosti na širi osećaj opstanka u nizu bezbednosnih dimenzija (Castle 1997, 4). Najbolji primer za to možda daju studije ekološke

bezbednosti, gde se pretnje prirodnim vrstama identifikuju kroz degradaciju životne sredine, ali i kroz sukobe koji proističu iz tih pretnji, postavljajući se kao analogni tradicionalnijim opasnostima (Waever 1995). Narastajući socio-ekonomski problemi, recesija, klimatske promene i drugi, uslovili su promenu pogleda na međunarodnu bezbednost i prepoznavanje da nevojne pretnje mogu ozbiljno uzdrmati postojeće pravne okvire, ekonomske tokove, zajednice ali i međunarodnu i nacionalnu bezbednost. Štaviše, upozorenja kriminologa, pravnika i sociologa, da će enormne zarade i moć pripasti današnjim vodećim kriminalnim organizacijama i transnacionalnim mrežama, uvela su kriminal u nastavne programe političkih nauka i ekonomije (Castle 1997, 1). Kriminalne grupe deluju ilegalno kroz korupciju, eksploataciju, nasilje i trgovinu u cilju sticanja moći, uticaja i novčane dobiti (Tundis and Mühlhäuser 2020, 60). Zbog raznovsrnih oblika kriminala kojima se bavi, načina organizovanja i delovanja, teritorijalne (ne)određenosti, autori su dugo pokušavali da dođu do opšteprihvaćene definicije organizovanog kriminala. Definicije i karakteristike koje su najčešće u upotrebi čak potiču iz pojedinih ekonomskih teorija, što zapravo govori o suštini ovih grupa – organizovanju isključivo radi sticanja nelegalnog profita. Organizovani kriminal inkorporirao je mnoge uspešne principe koji postoje u legalnim poslovnim organizacijama (Weber 1947), a pre svih to su:

- Lanac izdavanja naredbi
- Jasan cilj rada i postojanja
- Specijalizacija u pojedinačnim zadacima i poslovima
- Podređeni ima(ju) kontakt samo sa nadređenim
- Standardi ulaska u organizaciju
- Čuvanje tajne (u slučaju kriminalnih grupa, takozvana omerta – zakon ćutanja) (Mallory 2012, 2).

Transnacionalni organizovani kriminal je obeležen da sledi ekonomsku logiku i instrumentalno rezonovanje preduzetnika (Vicenzo 2020, 4). Danas organizovani kriminal ima transnacionalni karakter, generiše milijarde dolara, a članovi su povezani istim finansijskim ili drugim motivima (kao što je sticanje političke moći), bez obzira kom društvu ili etničkoj grupi pripadaju, ili nekim drugim ličnim svojstvima (Bošković and Janković 2023, 18). Organizovani kriminal u Americi je „posao" koji donosi 500 milijardi dolara godišnje zarade, dobro je finansiran i visoko sofisticiran (Bequai 1997, 25-29). Okrutnost i strogi „zakon ćutanja" koji odlikuju pripadnike organizovanih kriminalnih grupa, uz posedovanje ogromnog profita i vršenje koruptivnih radnji, čime pojedini donosioci odluka na nacionalnom i međunarodnom nivou, na određeni način čine deo njihovih aktivnosti i potpomažu ih na političkom nivou, otežava otkrivanje i procesuiranje ovog vida kriminala.

Ozbiljnost i dubina problema koji organizovani kriminal predstavlja i za nacionalni, ali i za međunarodni pravni i mirovni poredak, na jezgrovit način ističe Kastl: „Ako su kriminalne organizacije uspešne u izbegavanju autoriteta u jurisdikcijama u kojima deluju, i u mogućnosti su da vode svoje različite operacije na profitabilan način, logično je pretpostaviti da će pre nego delujući kao destabilizujuća sila, ponašati se kao svaki profitabilan posao i nastojaće da podrže administrativni *status quo* pod kojim su napredovali" (Castle 1997, 5). Istovremeno, pored terorizma, transnacionalni organizovani kriminal privlači najveću pažnju i nacionalnih i međunarodnih bezbednosnih organizacija, ali i drugih institucija. Savet Evrope (2014), na primer, pokušao je da identifikuje društvenu i ekonomsku štetu koju izaziva ova vrsta kriminala, naglašavajući način na koji on upotrebljava određene pravne nedorečenosti, koristi sofisticirane metode za prikrivanje aktivnosti i prihoda stečenih kriminalom, zloupotrebljava prednosti globalizacije i informacionih i komunikacionih tehnologija (Vicenzo 2020, 4). Transnacionalni organizovani kriminal bio je ozbiljan problem tokom većeg dela XX veka, ali je tek krajem prošlog veka prepoznat kao pretnja svetskom poretku (Shelley 1995, 463).

Upotreba savremenih tehnologija od strane organizovanih kriminalnih grupa

Kriminal, odnosno njegovi nosioci i aktivnosti, dinamična su i prilagodljiva kategorija. Kako se društvo razvija, pojavljuje se širok spektar oblika kriminala, koji obuhvata i individualni i organizovani kriminal (Dela 2016, 55). Zbog velike količine novca kojim raspolaže i moći koju stiče korupcijom, organizovani kriminal ne samo da se najlakše prilagođava promenama i izazovima, već i vrlo uspešno preuzima inovacije i tehnološka rešenja koristeći ih u svom interesu. Poslednjih decenija, usled eksploatacije interneta i razvoja novih kompjuterskih tehnologija došlo je do povećane mogućnosti za vršenje kriminalnih aktivnosti, kao i za širenje pretnji i veličanje nasilja (Tundis and Mühlhäuser 2020, 60). Maksimu da „tehnologija znači efikasnost" prepoznali su ne samo nauka, privreda i društvo, već i kriminal (Vicenzo 2020, 5). Nastanak sajber prostora predstavljao je svojevrsnu prekretnicu u sferi vojnih aktivnosti ali i poimanja korporativne, nacionalne, regionalne i globalne bezbednosti (Putnik, Milošević and Bošković 2017, 176). Kriminalne grupe ne samo da koriste dostignuća informaciono-komunikacionih tehnologija (IKT), za širenje organizacije, komunikaciju i upravljanje aktivnostima i resursima, već i ulažu, preko tajnih i nelegalnih kanala u razvoj sosptvenih aplikacija koje će koristiti za svoje delovanje. Same organizovane kriminalne grupe, one najmoćnije, imaju svoje IKT

stručnjake čiji je cilj da, ne samo štite komunikacione kanale, već i osmišljavaju nove načine „zaobilaženja" i neutralisanja policijskih mera i tehnika za otkrivanje i praćenje njihovog delovanja. Ozloglašeni darkveb (DarkWeb) prerastao je nivo online „crnog tržišta" zabranjenih supstanci, oružja, inkriminišućih audio i video sadržaja i postao mesto ponude i tražnje inovacija u oblasti IKT koje prevazilaze postojeće mere praćenja, otkrivanja i dešifrovanja koje koriste službe bezbednosti. Pored toga, sajber prostor postao je idealno mesto transnacionalnim kriminalnim grupama za borbu protiv konkurencije, širenje tržišta, pronalaženje, profilisanje i vrbovanje novih žrtava, ali i izazivanje lokalnih konflikata, koji će im poslužiti za plasiranje svoje moći i ilegalnog oružja koje prodaju. Sajber prostor je postao savršeno okruženje za činjenje zločina, kao i za omogućavanje novih načina za vođenje organizovanog kriminala i upravljanje novim oblicima nadmetanja za uticaj (Dela 2016, 55). Sajber prostor i široko popularne i korišćene internet aplikacije, omogućavaju (prividnu) anonimnost, koju mnogi ljudi koriste za pretragu internet sadržaja, upoznavanje i promociju svojih ideja – tu mogućnost uveliko koriste i organizovane kriminalne grupe u potrazi za novim žrtvama (trafikinga), konzumentima (ilegalnih narkotika), kupcima (ilegalnog oružja, umetničkih dela), ali i za plasiranje lažnih medijskih sadržaja (takozvane „fake news"), kojima destabilišu društvo ili donosioce političkih odluka i čine sebi pogodno tlo za širenje i vršenje svojih aktivnosti i dalje uvećanje moći. Iz perspektive načina izvršenja ovih krivičnih dela mogu se razlikovati sajber-zavisni i sajber-omogućeni zločini. Dok se sajber-zavisni zločini mogu počiniti samo korišćenjem računara, sajber-omogućeni zločini su oni koji se mogu povećati u svom obimu ili dosegu upotrebom računara, računarskih mreža ili drugih oblika informaciono-komunikacione tehnologije (Bird et al. 2020, 1). Platforme i aplikacije društvenih medija, na primer, koje koristi 46% svetske populacije, postale su mreže „komandovanja i kontrole" po izboru za one koji se bave sajber kriminalom (Europol 2023). Čak su i destruktivne verske sekte svoje delovanje prenele u onlajn prostor, pre svega u aspektu promocije svojih „ideja i uverenja" i pronalaženja sledbenika. Sociopatološke pojave, poput kockanja, takođe se danas sve više odvijaju putem onlajn aplikacija. Na sve ove načine, ali i mnogo šire i opasnije, organizovane kriminalne grupe koriste dostignuća IKT. Ključni trend identifikovan u Evropolovoj godišnjoj internet proceni pretnji od organizovanog kriminala (IOCTA) je rastući „model kriminal kao usluga" u kome specijalizovani provajderi nude sajber usluge organizovanim kriminalnim grupama, što govori o tome da će sajber kriminal nastaviti da raste i da će se upotreba onlajn platformi i sajber alata u kontekstu uspostavljenih tržišta organizovanog kriminala i dalje širiti (Bird et al. 2020, 2).

Ne postoji oblik organizovanog kriminala, odnosno vrsta krivičnih dela, koje danas ne počivaju u velikoj meri na prednostima IKT. Informaciona tehnologija

predstavlja moćno i efikasno oruđe za kriminalce, za podršku kreiranju novih kriminalnih scenarija, pojednostavljivanje izvršavanja određenih nezakonitih radnji i smanjenje rizika od otkrivanja (Tundis et al. 2018).

Korišćenje sajber prostora, društvenih mreža i zaštićenih online komunikacija, u najvećoj meri je prisutno u slučajevima ilegalne trgovine narkoticima, trgovine ljudima, u kreiranju i distribuciji dečije pornografije. Uprkos činjenici da je Put svile (Silk Road), najpoznatiji sajt za ilegalnu prodaju droge na mreži, oboren 2013. godine, rast tržišta nije usporen. Prema jednoj proceni, prihod od ove prodaje se utrostručio od zatvaranja Puta svile 2013. do 2016. godine (RAND Europe 2016). Pre svega, finansijski pokazatelji upućuju na to koliko brzo onlajn crno tržište narkotika raste. RAND Europe[3] je procenio da je 2016. prihod na darknet tržištu za tu godinu bio između 12 i 20 miliona dolara, dok se procene globalne trgovine kreću između 425 i 625 milijardi dolara (Bird et al. 2020, 4). Studija iz 2018. godine o Abraxas-darknet tržištu identifikovala je 463 prodavaca i 3.542 kupaca nedozvoljenih droga i utvrdila da je više od polovine svih kupovina napravilo samo 10% kupaca, pri čemu je većina kupaca izvršila samo jednu kupovinu. Ovo bi moglo da ukazuje na pojavu da distributeri niskog nivoa kupuju zabranjene droge na mreži za dalju preprodaju (Norbutas 2018).

Trgovina ljudima, možda najperfidniji i najbrutalniji oblik organizovanog kriminala, jako brzo je poprimio transnacionalne razmere (i u pogledu organizatora, žrtava – njihovih zemalja porekla i „krajnjih" destinacija). Trgovina ljudima pogađa (posrednom ili neposrednom viktimizacijom) više od 40 miliona ljudi širom sveta – „71% njih su žene i devojke, a 25% deca, dok organizatori zarađuju 150 milijardi dolara godišnje" (Bird et al. 2020, 11). IKT su omogućile širenje i brže povezivanje tržišta („ponude" i „potražnje"), skriveniju komunikaciju u lancu trafikinga, ali i lakše dolaženje do žrtava, naročito zloupotrebom društvenih mreža. Na žalost, jedan od oblika trgovine ljudima i zločina koji najbrže raste zahvaljujući IKT jeste online seksualna eksploatacija dece. Ovo je jedan od zločina koji se najbrže prilagođavaju mogućnostima koje nudi tehnologija, brzo prelaze sa korišćenja usluga grupnog deljenja fajlova na sektorstvo (kategorisanje), onlajn „doterivanje" (grooming) i prenos seksualnih činova uživo za zatvorenu publiku (Bird et al. 2020, 11). Projekat Arachnid, koristeći automatizovani pretraživač web lokacija za skeniranje preko 230 miliona web-stranica, u periodu od šest nedelja tokom 2017. godine, otkrio je preko 5,1 milion pojedinačnih web stranica koje su zajedno hostovale preko 40.000 jedinstvenih slika koje prikazuju zlostavljanu decu (van der Bruggenand and Blokland 2021).

[3] Istraživačka institucija čiji je cilj da svojim rezultatima pomogne kreiranju javnih politika i donošenju odluka.

Ono što je organizovanim kriminalnim grupama olakšalo delovanje, upravljanje aktivnostima i dalji razvoj, a imajući u vidu primenu IKT, u najvećoj meri jeste zloupotreba znanja i dostignuća iz oblasti kriptografije. Aplikacije koje omogućavaju enkriptovanu (šifrovanu) komunikaciju, omogućile su članovima (transnacionalnih) kriminalnih grupa zaštićenu komunikacije bez potrebe za fizičkim sastajanjem i kontaktom, bezbednu razmenu poruka na vrlo udaljenim mestima i otežale istražnim organima da otkrivaju i prate komunikaciju između počinilaca krivičnih dela i to koriste kao dokazni materijal. Dvadeset evropskih zemalja evidentiralo je upotrebu softvera za šifrovanje od strane sajber kriminalaca da bi zaštitili svoje pohranjene podatke, dok je osam država članica posebno apostofiralo problem kodiranja (enkripcija i dekripcija) kao najveći izazov za istragu sajber kriminala (Pisarić 2020).

(Zlo)upotreba kriptografije od strane organizovanog kriminala

Kriptografija je značajna i važna naučna disciplina, koja izučava i produkuje načine zaštite tajnosti podataka, poruka i informacija. Time ona, pre svega, jeste od velike važnosti za bezbednosni sistem i privredu, u oblasti zaštite komunikacija (pisanih ili usmenih poruka i razgovora), državnih, vojnih ili poslovnih tajni. Kriptografija, ili „umetnost šifrovanja", stara je nekoliko hiljada godina. Jedna od prvih istorijski dokumentovanih upotreba specijalnih kodova u komunikaciji može se pratiti do starog Egipta, kada su nestandardni hijeroglifi korišćeni za prikrivanje sadržaja poruke (Vilím et al. 2021). Začetak šifrovanja podrazumevao je upotrebu pergamenta i alatke za pisanje, da bi se vremenom usavršavao, a za kodove i ključeve počele da se koriste matematičke formule. U XX veku, a naročito tokom Drugog svetskog rata, šifrovanje poruka je dobilo na naročitom značaju, kada počinju i da se razvijaju uređaji za šifrovanje, poput Nemačke mašine Enigma.

Enigma je koristila *simetrične* šifarske tehnike, što znači da je dešifrovanje podrazumevalo obrnut proces od šifrovanja. Tako je Enigma koristila određeni ključ za šifrovanje poruke, a na prijemu se za dešifrovanje koristila identična mašina sa istim ključem. Dakle, i pošiljalac i primalac imali su istu informaciju i obojica su koristili isti ključ za šifrovanje i dešifrovanje – njihov odnos je simetričan (Sing 2010, 324).

Savremene kriptografske tehnike zasnivaju se na *asimetričnom* šifrovanju. U asimetričnom sistemu, kao što mu ime kaže, ključ za šifrovanje i ključ za dešifrovanje nisu isti. Ovaj sistem je, dakle, zasnovan na paru različitih ključeva. Ključ za šifrovanje je svima dostupan i on se naziva *javnim ključem*, dok ključem za dešifrovanje raspolaže samo primalac poruke, i taj ključ se naziva *tajnim*

ključem. U asimetričnom sistemu komunikacija se odvija tako što pošiljalac poruke koristi javno dostupan javni ključ kojim šifruje poruku i šalje je primaocu. Primalac potom poruku dešifruje pomoću svog privatnog (tajnog) ključa. Jedna od najvećih prednosti asimetrične šifarske tehnike jeste u tome što se njome prevazilazi problem distribucije ključa koji je karakterističan za simetričnu šifarsku tehniku. Primalac poruke u asimetričnom sistema ne mora da u tajnosti preda pošiljaocu poruke javni ključ za šifrovanje – sasvim suprotno, sada može svima da ga otkrije. Njemu odgovara da njegov ključ za šifrovanje bude javno dostupan, jer na taj način svi mogu da mu šalju šifrovane poruke. Istovremeno, uprkos tome što je njegov javni ključ opšte poznat, niko ne može da dešifruje nijednu poruku koja je njime šifrovana, jer poznavanje javnog ključa nije ni od kakve pomoći pri dešifrovanju. Štaviše, čak ni pošiljalac poruke koji je poruku šifrovao javnim ključem primaoca, ne može da je dešifruje. To može da učini samo primalac koji ima privatan ključ (Sing 2010, 325-326). Otkrićem asimetrične šifarske tehnike značajno je unapređena kriptografija, koja je danas postala „igralište matematičara“ (Landau 2004).

Savremena enkripcija bazirana je na softverima koji koriste složene matematičke algoritme kako bi kreirali šifre i alatke za kodiranje. Stvaranje sofisticiranih alata za šifrovanje usko je povezano sa nastojanjem vojno-odbrambenih snaga zemlje i državnih organa da prikriju svoje komunikacije i strateške dokumente, koji su važni za funkcionisanje države, bezbednosnog sistema i zaštitu građana (Vilim et al. 2023). Međutim, kriptografija u rukama organizovanog kriminala otežava bezbednosnim službama da otkriju, prate i dokumentuju audio i pisanu komunikaciju, kako bi istražili izvršenje teških krivičnih dela. Takođe, funkcija kriptografije, pa i zloupotreba zavisi od toga da li se ona koristi za omogućavanje i očuvanje poverljivosti ili potvrdu identiteta i autentičnosti. Društvena pretnja se javlja prvenstveno sa uslugama poverljivosti – onime što nazivamo šifrovanjem (Denning and Baugh Jr. 1997, 2). Metode potvrde autentičnosti i identiteta, od koristi su za istražne radnje, jer služe osiguravanju tačnosti izvora podataka i integriteta (autentičnosti) razmenjenih poruka. Međutim, enkripcija se koristi kao alat za prikrivanje informacija u raznim zločinima, uključujući prevaru i druga finansijska krivična dela, krađu vlasničkih informacija, kompjuterski i sajber kriminal, drogu, dečju pornografiju, terorizam, ubistva, ekonomsku i vojnu špijunažu (Denning and Baugh Jr. 1997, 4). Kriminalne grupe sve više koriste šifrovane kanale, kao što su Telegram i Signal, kao metod komunikacije kako bi izbegli da ih bezbednosne službe razotkriju. Kriminalci koriste ove kanale da dela planiraju, izvršavaju i razgovaraju o svojim operacijama (Koomen 2021). Asimetrično šifrovanje, koje zahteva par povezanih javnih i privatnih ključeva (kodova) za pristup podacima između komunikanata, omogućava kriminalcima da potvrde da su

poruke koje su primili autentične, a ne od imitatora – neželjenog izvora poruke. Kriminalci, kao i teroristi, koriste šifrovanu komunikaciju da sakriju svoje transfere novca i zaštite se od tehnika hakovanja koje uključuju upotrebu malvera (malware) i rensomvera (ransomware) koji ciljaju njihovu finansijsku imovinu, kao i da obezbede tajnost „posla". (Napoleon et al. 2021). Rensomver predstavlja vrstu malvera, iz potkategorije ucenjivačkog malicioznog softvera, koji autorizovanom korisniku ograničava pristup računarskom sistemu ili u njemu pohranjenim podacima i traži otkupninu kako bi korisnik povratio pristup svom sistemu i/ili podacima (Fruhlinger 2020). Otkupnina se po pravilu traži i isplaćuje u kriptovalutama, najčešće u bitkoinu. Transakcijama u kriptovalutama je teško pratiti trag, te je njihovo korišćenje u funkciji očuvanja anonimnosti napadača (Putnik, Milošević and Cvetković 2022, 328). Neke vrste rensomvera mogu da blokiraju računar na način da se na ekranu pojavi ucenjivačka poruka koju korisnik ne može da skloni bez plaćanja otkupnine. Druge vrste ovog malvera mogu da šifruju pojedinačne ili sisteme datoteka u računaru. Ako je računar povezan sa lokalnom mrežom, rensomver se, takođe, može proširiti na druge računare ili uređaje za skladištenje na mreži ili u internet oblaku. U tom slučaju se od korisnika čiji je računar zaražen traži otkupnina u zamenu za otključavanje kriptovanih podataka (Putnik, Milošević and Cvetković 2022, 329).

Danas je upotreba komunikacionih aplikacija koje omogućavaju šifrovani prenos elektronskim uređajima pomoću potrebnog operativnog sistema, omogućavajući instaliranje aplikacije i uspostavljanje veze sa internetom postala opšteprihvaćeni standard kojim je omogućena zaštićena komunikacija. Postoje i aplikacije koje omogućavaju da se ceo uređaj šifruje, što otežava pronalaženje njegovog sadržaja ili otkrivanje potrebnih informacija i dokaza (Vilim et al. 2023).

Aplikacije za asimetričnu enkripciju šifruju kompletnu komunikaciju između pošiljaoca i primaoca poruke, uz upotrebu javnog i privatnog ključa, gde se dešifrovanje može izvršiti samo posedovanjem i primenom privatnog ključa. Telegram je bio jedna od prvih aplikacija za enkriptovanu komunikaciju, a danas je u opticaju veliki broj njih (poput aplikacija Viber, Wickr, WhatsApp). Sve one koriste takozvano „end-to-end" (E2EE) šifriranje. Enkripcija po principu „end-to-end" je način bezbednog komuniciranja koji onemogućava trećem licu da pristupi podacima dok se prenose sa jednog sistema ili uređaja na drugi (od pošiljaoca do primaoca). U E2EE enkripciji, podaci su šifrovani na sistemu ili uređaju pošiljaoca i samo primalac kome je namenjena poruka može da je dešifruje – provajder internet usluga, provajder, haker ili neka treća strana ne može poruku da pročita ili menja. U ovakvim slučajevima, jedino što bezbednosne službe mogu da iskoriste su metadpodaci – podaci koje provajder internet usluga može da pruži, a oni podrazumevaju identifikaciju uređaja sa kojih je komunikacija obavljena, vreme

ostvarivanja komunikacije i dužina trajanja razgovora (u slučaju audio komunikacije), bez mogućnosti uvida i dešifrovanja sadržaja koji je razmenjen.

Tako, na primer, Sinaola kartel, međunarodni narko kartel i jedna od najmoćnijih kriminalnih organizacija na svetu sa sedištem u Meksiku, bavi se krijumčarenjem narkotika – kokaina, heroina, metamfetamina i MDMA na američko tržište, a komunikacija unutar organizacije obavlja se kriptovanom komunikacijom. El Mencho, deo Sinaola kartela, sa vrhom organizacije komunicira putem WhatsApp aplikacije – korišćenjem E2EEE enkripcije. Za njih ovo predstavlja jednostavan, direktan i bezbedan način razmene poruka kroz celu hijerarhiju ove kriminalne organizacije (Bird et al. 2020, 11).

Kada je reč o trgovini ljudima, enkriptovane aplikacije koriste se za komunikaciju među članovima grupe, sa (potencijalnim) žrtvama, kao i sa klijentima (korisnicima seksualnih usluga, fizičkog rada ili zlostavljanja dece). Zainteresovane strane na tržištima trgovine ljudima (mreže trgovine ljudima, kupci/korisnici usluga) mogu anonimno i bezbedno da komuniciraju putem šifrovanih aplikacija za razmenu poruka, zatvorenih soba za ćaskanje (chat-rooms) i drugih foruma na deep ili dark vebu, gde pristupaju sa posebno šifrovanim, jedinstvenim pozivnicama (Bird et al., 2020, 14). Izveštaj Evropola iz 2021. godine – *Procena pretnje od ozbiljnog i organizovanog kriminala (SOCTA) 2021* – direktno opisuje bezbednosne rizike koji nastaju za bezbednost granica kada IKT koriste organizovane grupe koje krijumčare ljude preko granica, bilo kopnom, vazduhom ili morem (Napoleon et al. 2021).

Sofisticirane digitalne tehnologije i široko rasprostranjena upotreba enkriptovanih aplikacija za komunikaciju, organizovanim kriminalnim grupama omogućavaju gotovo potpuno zaštićenu i bezbednu razmenu poruka, upravljanje aktivnostima i širenje poslova, dok bezbednosnim službama i istražnim organima otežavaju bilo koji vid „digitalnog upada" u ove grupe, presretanje, praćenje i dešifrovanje komunikacije, a time i pravovremenog otkrivanja i dokazivanja krivičnih dela. Nova tehnologija nije stvorila samo nove pretnje već je i otežala identifikaciju aktera bezbednosnih pretnji i njihovog razlikovanja (Miljković and Putnik 2016, 164).

Sky ECC enkriptovana aplikacija naročito je popularna za upotrebu među kriminalnim grupama. Ovu aplikaciju razvila je i na tržište plasirala Kanadska kompanija Skajglobal (SKY Global), prvobitno kao deo Blekberi (Blackbery) telefona, a zatim i kao samostalni proizvod. Ova aplikacija doživela je ekspanziju kod kriminalnih grupa nakon „pada" platforme za enkriptovanu komunikaciju EnroChat 2020.godine. Evropska policija je nakon uspešne infiltracije na EnroChat platformu pronašla na milione šifrovanih poruka – rezultat toga bio je hapšenje 746 osumnjičenih, konfiskovanje 77 komada vatrenog oružja i oko dve tone droge

(Fisher 2020). Sky ECC bio je veći izazov za policiju i izražne organe, međutim „slaba karika" prepoznata je u serverima na kojima se zapisi o enkriptovanim porukama čuvaju. Naime, šifrovane poruke automatski se brišu 30 sekundi nakon što su pročitane, a ako je telefon bio van internet mreže (offline), poruka se čuvala do 48 sati pre brisanja. Međutim, stručnjaci za visokotehnološki kriminal zapadnoevropskih policija shvatili su da se poruke, iako izbrisane, čuvaju na serveru ove aplikacije. Sky ECC je prevashodno „pala", upadom policije i preuzimanjem podataka sa servera. Nakon toga, belgijska, holandska i francuska policija su „provalile" servis za šifrovanje poruka ove aplikacije, što im je omogućilo razotkrivanje 80 miliona poruka (The Brussels Times 2022). Na ovaj način, policija Belgije dobila je dokaze za pokretanje 276 istraga i zaplenu 90 tona droge. Prema podacima Minisarstva unutrašnjih poslova Srbije iz 2021. godine, oko 30% od 70.000 telefona koji koriste aplikaciju Sky bilo je u rukama kriminalaca sa Balkana (Milovanović 2022). Upotreba ove aplikacije evidentirana je i u Republici Srpskoj u decembru 2021. godine, kada je uhapšeno 19 lica zbog krijumčarenja droge i oružja u okviru akcije *„Storidž 2"*, na čelu sa Državnom agencijom za istrage i zaštitu (SIPA) i Ministarstvom unutrašnjih poslova Republike Srpske (Klix 2021). Ono što je Sky ECC aplikaciju činilo posebno atraktivnom za kriminalne grupe jeste postojanje opcije za takozvano „samouništenje", odnosno mogućnost unošenja posebne „panik" šifre koja bi obrisala sadržaj. Međutim, slabost sistema za koju kriminalci tada nisu znali jeste da se, iako izbrisane, poruke neko vreme čuvaju na serverima aplikacije, što je bilo ključno otkriće policije u borbi protiv brojnih organizovanih kriminalnih grupa.

Suprotstavljanje zloupotrebi kriptografskih tehnika kao izazov za nauku i praksu

Prethodno opisane studije slučaja govore u prilog tome da prvi korak u pokušaju otkrivanja i dokazivanja krivičnih dela organizovanih kriminalnih grupa jeste kreiranje sofisticiranih softvera koji će biti u stanju da na autonoman i automatizovan način presreću i dešifruju enkriptovanu komunikaciju, što predstavlja značajan tehničko-tehnološki izazov. Podaci koje pružaoci internet usluga mogu dati od značaja su, ali treba imati u vidu da se i sami mobilni uređaji, naročito oni koji su sistemski enkriptovani, bez obzira na druge aplikacije, mogu nabavljati pod lažnim identitetima, naročito na dark web-u.

Sa druge strane, kada je reč o legalnoj prodaji mobilnih uređaja, internet aplikacija i softvera, i praćenju i prisluškivanju njihovih korisnika, osetljivo je pitanje

i izazov sa stanovišta zaštite ljudskih prava i privatnosti. Razvoj digitalne tehnologije obesmišljava postojeće domaće ustavne i zakonske odredbe koje još uvek govore o „nadzoru i zapleni pisama i drugih pošiljki“ iako je svet već decenijama unazad sa pisama, razglednica i čestitki prešao na imejlove i digitalne čestitke, sa fiksnih telefona na mobilne, sa SMS poruka na internet komunikacione platforme poput Vibera, Votsapa (WhatsUp) i Telegrama, budući da su one poslednjih godina sve češće u upotrebi jer omogućavaju kriptovanu komunikaciju, kao i autonomni šifrovani uređaji koji garantuju tajnost i sigurnost komunikacije (Bajović 2020, 154).

SAD su razmatrale različite opcije pri donošenju odluka i daljih politika u pogledu korišćenja enkripcije i razvoja programa za oporavak kodova nakon narušavanja poverljivosti, u slučajevima ugrožavanja nacionalne bezbednosti. Dening i Bo (Denning and Baugh 1997) ističu da je šifrovanje kritično međunarodno pitanje koje zahteva partnerstvo između kompanija i vlade i međunarodnu saradnju. Jedan od uspešnih primera saradnje države, odnosno njenih bezbednosnih službi i privrede i to na međunarodnom nivou, jeste operacija koju je američki Federalni istražni biro (FBI) sproveo sa još 16 zemalja, a u kojoj su stvorili privatnu kompaniju ANOM, koja se bavila proizvodnjom kriptovanih telefona i aplikacija za komunikaciju. ANOM je na dark web-u prodao 12.000 enkriptovanih telefona, koje je kupilo preko 300 kriminalaca, članova transnacionalnih organizovanih grupa. ANOM je ciljao potencijalne kupce nudeći šifrovane komunikacione uređaje i objavljivajući ih na dark web-u, kako bi ih pripadnici kriminalnih grupa kupili. Na taj način bezbednosnim službama zemalja učesnica u ovoj operaciji omogućeno je da prisluškuju i presreću komunikaciju organizovanih kriminalnih grupa koje su koristile ove uređaje (Napoleon et al. 2021).

Slučajevi EncroChat i Sky ECC aktuelizovali su problematiku pribavljanja, prirode i ocene dokaza pribavljenih u inostranstvu. U vezi sa tim, postavlja se pitanje pravnog osnova za dostavljanje EncroChat i Sky komunikacije, njenog korišćenja u krivičnom postupku, ocene ovakvih dokaza od strane suda, kao i načina i mogućnosti njihovog izvođenja na glavnom pretresu (Bajović 2022, 158). Kada govorimo o korišćenju dokaza pribavljenih putem presretanja ili otkrivanja komunikacija, imajući u vidu široku akciju koja se odnosila na EnroChat i Sky ECC, kao gotovo jedini način razmene poruka bez fizičkog prisustva, ono što je najvažnije, jeste poštovati zakon i procedure za pribavljanje dokaza. Zakonik o krivičnom postupku Republike Srbije (Sl. glasnik RS 27/2021) zabranjuje donošenje presuda na osnovu dokaza koji su pribavljeni suprotno Ustavu republike Srbije. U suštini, kao i prilikom pribavljanja dokaza koji se tiču upotrebe metoda praćenja, prisluškivanja, narušavanja tajnosti pisama i slično i za „upad” u enkriptovane komunikacije potrebna je odluka suda.

Prema podacima iz zajedničkog izveštaja Europol/Eurojust, svega nekolicina evropskih država ima posebnu regulativu koja reguliše tajno pristupanje šifrovanoj elektronskoj komunikaciji i njeno dekodiranje (online nadzor, upad u računarski sistem, korišćenje tehničkih sredstava za pristup digitalnim dokazima i sl.) (Bajović 2022, 158). Naša normativa čak i ne reguliše posebno digitalne dokaze već ih podvodi pod isprave, propisujući da „računarski podatak koji je podoban ili određen da služi kao dokaz činjenice koja se utvrđuje u postupku predstavlja ispravu“ (čl. 2 st. 1 t. 26 ZKP) (Bajović 2022, 159). Mora se imati u vidu da „digitalni dokazi" često nisu jednaki ostalim oblicima fizičkih dokaza u odnosu na koje su osetljiviji i podložni menjanju strukture i sadržaja, te se prema njima treba posebno odnositi (Milanović and Milanović 2010).

Zaključak

Organizovane kriminalne grupe će, po svoj prilici, nastaviti da koriste asimetričnu enkripciju budući da ona nudi dodatnu zaštitu i poverljivost komunikacije. Bezbednosne službe i istražni organi će, shodno prepoznatim rizicima, morati da unaprede svoju metodologiju dešifrovanja kako bi se suprotstavili organizovanom kriminalu koji, za sada vrlo uspešno koristi mogućnosti IKT za svoje nezakonite potrebe i poslove. Sa druge strane, tužilaštvo i sudstvo, odnosno zakonodavstvo generalno, moraće da prilagode normative i procedure savremenim trendovima koje kriminalne grupe nedvosmisleno prate i putem njih olakšavaju sebi delovanje i ostajanje „ispod radara" zakonitog praćenja i pribavljanja dokaza. Nauka o digitalnim dokazima je standardizovana u ISO/IEC 270375 (prikupljanje i čuvanje digitalnih forenzičkih dokaza), kao i kroz SWGDE – Scientific Working Group on Digital Evidence i IOCE – International Organization on Computer Evidence. U okviru ovih dokumenata nalaze se preporuke za osnovne principe forenzičke analize digitalnih dokaza, kriterijumi, kao i standardne radne procedure za zaplenu računara, forenzičku akviziciju i analizu, čuvanje, kopiranje originalnih digitalnih dokaza i drugo (Milanović and Milanović 2010). Iako nauka i praksa razvijaju metode digitalne forenzike, organizovane kriminalne grupe ali i kompanije čiji je osnovni cilj komercijalizacija i profit, sa svoje strane, razvijaju takozvanu „digitalnu anti-forenziku". Ova nastojanja kriminalnih grupa Berinato (Berinato 2007) lakonski definiše maksimom „Otežajte im da vas nađu i onemogućite im da dokažu da su vas našli".

Na kraju, treba pomenuti da digitalni jaz nije izražen samo između država i organizovanih kriminalnih grupa, već i između tehnološki razvijenih i manje

razvijenih država. Zemlje sa dobro razvijenom IKT infrastrukturom i sofisticiranim odbrambenim sistemima u sferi sajber prostora, imaju tehnološku prednost u poređenju sa manje razvijenim zemljama (Dela 2016, 58). Nedovoljna razvijenost mera odbrane u sajber prostoru, kao i same IKT infrastrukture, kod zemalja u razvoju može se manifestovati u nemogućnosti bezbednosnih službi da adekvatno reaguju na delovanje organizovanih kriminalnih grupa, što može imati ne samo teške društvene posledice i narušenu nacionalnu, već i međunarodnu bezbednost. S obzirom na to da savremeni svet karakteriše asimetrija pristupa (kriptovanim) informacijama i da je on postao polje nesagledivog štetnog delovanja transnacionalnog organizovanog kriminala, međunarodna saradnja nacionalnih i nadnacionalnih institucija, pomoć u razmeni informacija i razvoju IKT, usaglašavanju nacionalnih normativa i mera koje će smanjiti zloupotrebu šifrovanih aplikacija i uređaja, ključna je za anuliranje prednosti koju, čini se, kriminal može steći nad bezbednosnim sektorom.

Bibliografija

Bajović, Vanja. 2022. „Encrochat i Sky ECC komunikacija kao dokaz u krivičnom postupku“. *Crimen* 13: 154–179.

Bequai, August. 1997. “Organized Crime: Manipulating Cyber-Space”. In: *A Transatlantic Agenda – final report*, edited by Ernesto U. Savona, Shawna Gibson and Daria Angelini, 25-29. Trento: European Commission.

Berinato, Scott. 2007. “The Rise of Anti Forensics”. Jun 08. https://www.csoonline.com/article/521254/investigations-forensics-the-rise-of-anti-forensics.html.

Bird, Lucia, Hoang Thi, Stanyard Julia, Walker Summer, and Haysom Simone. 2020. *Transformative Technologies – How digital is changing the landscape of organized crime*. Geneva: Global Initiative Against Transnational Organized Crime.

Boskovic, Milica and Jankovic Brankica. 2023. “Forced Migrations and the Risk of Human Trafficking”. In: *Handbook of Research on the Regulation of the Modern Global Migration and Economic Crisis,* edited by Emilia Alaverdov and Muhammad Waseem Bari, 18-36. Hershey, PA: IGI Global. https://doi.org/10.4018/978-1-6684-6334-5.ch002.

Bošković, Milica. 2021. „Žene u kriminalu”. *Diplomatija i Bezbednost* 2(4): 27-38.

Bruggen Madeleine van der, and Blokland Arjan. 2021. "A Crime Script Analysis of Child Sexual Exploitation Material Fora on the Darkweb". *Sexual Abuse* 33(8): 950–974.

Fisher, Christine. 2020. "European police hacked encrypted phones used by thousands of criminals". Jul 2. https://www.engadget.com/europe-uk-police-hacked-encrochat-encrypted-phones-144351998.html.

Castle, Allan. 1997. "Transnational Organized Crime and international Security". Working Paper No. 19, 1-17. *Institute of International Relations.* The University of British Columbia.

Dela, Piotr. 2016. "Cyberspace as the Environment Affected by Organized Crime Activity". *Connections* 15(3): 55-64.

Denning, Dorothy E., and Baugh Jr. William E. 1997. "Encryption and Evolving Technologies as Tools of Organized Crime and Terrorism". *Trends in Organized Crime* 3, 84–91. https://doi.org/10.1007/s12117-997-1149-1.

Koomen, Maria. 2021. "Encryption and Crime: The Case for a Transatlantic Encryption Alliance", *Center for European Policy Analysis*, June 2021, https://cepa.org/encryption-and-crime-the-case-for-a-transatlantic-encryption-alliance/.

Europol. 2016. "The relentless growth of cybercrime" September 27. https://www.europol. europa.eu/media-press/newsroom/news/relentless-growth-of-cybercrime.

Fruhlinger, Josh. 2020. "Ransomware explained: How it works and how to remove it" June 19. https://www.csoonline.com/article/563507/what-is-ransomware-how-it-works-and-how-to-remove-it.html.

Landau, Susan. 2004. "Polynomials in the Nation's Service: Using Algebra to Design the Advanced Encryption Standard". *The American Mathematical Monthly* 111(2): 89–117. https://doi.org/10.2307/4145212.

Lukáš, Vilím, Borut Eržen, and Monika Weber. 2023. "Cryptography – how modern technology plays into the hands of people smugglers and human traffickers". *International Center for Migration Policy Development,* https://www.icmpd.org.

Mallory, Stephen. 2012. *Understanding Organized Crime.* Second Edition. Jones & Bartlett Learning.

Milanović, Zoran, and Milanović Tanja. 2010. Digitalna anti-forenzika kao kriminogeno sredstvo zaštite kiber kriminala. *Naučno stručno savetovanje Ziteh 2010,* 1-10.

Miljković, Milan, and Nenad Putnik. 2016. „Aktivnosti savremenih obaveštajnih službi u kiber prostoru". *Vojno delo* 68(7):164-180.

Napoleon, Patrianna, Saturnia Owen, Shoesmith Michael, and Petrovitch Jonathan. 2021. "The Use of Encrypted Communications by Criminals" November 22. https://www.counterterrorismgroup.com/post/the-use-of-encrypted-communications-by-criminals.

Norbutas, Lukas. 2018. "Offline constraints in online drug marketplaces: An exploratory analysis of a cryptomarket trade network". *International Journal of Drug Policy* 56: 92–100.

The Brussels Times. 2022. "Operation Sky ECC: 888 suspects and €4.5 billion worth of drugs seized" March 10. https://www.brusselstimes.com/justice-belgium/210112/operation-sky-ecc-888-suspects-and-e4-5-billion-worth-of-drugs-seized.

Pisarić, Milana. 2020. "Encryption as a Challenge for European Law Enforcement Agencies". *Thematic Conference Proceedings of International Significance - Archibald Reiss Days,* Vol. 10: 391-416.

Putnik, Nenad, Milošević Mladen, and Cvetković Vladimir. 2022. „Rensomver kao pretnja bezbednosti – društveni i krivičnopravni aspekti". *Sociološki pregled* 56(1): 328-353.

Putnik, Nenad, Milošević Mladen, and Milica Bošković. 2017. „Strateško planiranje sajber odbrane – ka adekvatnijem pravnom okviru i novoj koncepciji procene rizika, izazova i pretnji". *Vojno delo* 69(7): 174-85.

RAND Europe. 2016. "The role of the 'dark web' in the trade of illicit drugs, Research brief". https://www.rand.org/content/dam/rand/pubs/research_briefs/RB9900/RB9925/RAND_RB9925.pdf.

Ruggiero, Vincenzo. 2020. *Organized Crime and Terrorist Networks*. Routledge.

Shelley, Louise I. 1995. "Transnational Organized Crime: An imminent Threat to the Nation-State? *Journal of international Affairs* 48(2): 463-489.

Sing, Sajmon. 2010. *Knjiga o šiframa*. Beograd: DN Centar i Plato.

Klix. 2021. "Sve otkrila aplikacija Sky: Na području RS-a već uhapšeno 19 osoba zbog krijumčarenja droga i oružja" December 08. https://www.klix.ba/vijesti/sve-otkrila-aplikacija-sky-na-podrucju-rs-a-vec-uhapseno-19-osoba-zbog-krijumcarenja-droga-i-oruzja/211208014.

Tundis, Andrea, and Mühlhäuser Max. 2020. "The Role of ICT in Modern Criminal Organizations". In: *Organized Crime and Terrorist Networks*, edited by Ruggiero Vincenzo, 60-78. Routledge.

Tundis, Andrea, Huber Florian, Jäger Bernhard, Daubert Jorg, Vasilomanolakis Emmanouil, and Mühlhäuser Max. 2018. "Challenges and Available Solutions

Against Organized Cyber-crime and Terrorist Networks". In: *WIT Transactions on the Built Environment*, 429–441. WIT Press.

Milovanović, Tanja. 2022. "Vulin: Od 70.000 Skaj telefona više od 30 odsto pripada ljudima sa Balkana", Nova, April 21. https://nova.rs/vesti/hronika/vulin-od-70-000-skaj-telefona-vise-od-30-odsto-pripada-ljudima-sa-balkana.

Waever, Ole. 1995. "Securitization and Desecuritization". In: *On Security*, edited by Ronnie D. Lipschutz, 46-86. New York: Columbia University Press.

Weber, Max. 1947. *The Theory of Social and Economic Organizations*. New York: Free Press.

Zakonik o krivičnom postupku. 2021. *Sl. glasnik RS*, br. 72/2011, 101/2011, 121/2012, 32/2013, 45/2013, 55/2014, 35/2019, 27/2021.

Nenad PUTNIK, Milica BOŠKOVIĆ

CRYPTOGRAPHY AT THE SERVICE OF ORGANIZED CRIME – A CHALLENGE FOR SCIENCE AND PRACTICE

Abstract: Organized crime represents a serious threat to the security, economy, and sometimes for the legal order of the country. Criminal groups not only use the achievements of information and communication technologies (ICT) for the expansion of the organization, communication and management of activities and resources, but also invest, through secret and illegal channels, to develop their own applications of their own applications that they will use for their activities. Organized criminal groups themselves, the most powerful ones, have their ICT experts whose goal is not only to protect communication channels, but also to devise new ways of "circumventing" and neutralizing police measures and techniques for detecting and monitoring their activities. Members of organized criminal groups to use those communication applications that enable encrypted transmission to electronic devices using the necessary operating system, enabling the installation of the application and the establishment of a connection to the Internet in order to enable the necessary protected communication. There are also applications that allow the entire device to be encrypted, making it difficult to find its contents or discover the necessary information and evidence. This paper presents the characteristics of organized crime and their operating modes, with an emphasis on the use of cryptographic techniques. Case studies are illustrating the size and scope of abuse of encryption by organized criminal groups, by data on cases which were processed, as well as challenges in opposing the abuse of cryptography from a technical-technological and legal aspect, after that we provided guideline for improving the mechanisms for reduction of organized crime.

Keywords: organized crime, international security, encryption, communication, evidence work.