DOI: 10.5937/vojdelo1803128D

ORGANIZOVANI VISOKOTEHNOLOŠKI KRIMINAL – POJAM, RAZVOJ I OSNOVNE KARAKTERISTIKE

Anđelija Đukić
Univerzitet u Beogradu, Fakultet bezbednosti

U radu se razmatra visokotehnološki kriminal (VTK) kao savremeni oblik organizovanog kriminala. Dat je kratak pregled istorijskog razvoja VTK, kao i njegove transformacije u organizovani oblik. Prikazan je uticaj najznačajnijih faktora, pre svega interneta i globalizacije, koji su postavili osnov da ovaj kriminal preraste u organizovan kriminal na transnacionalnom nivou. Razmatrana su ključna pitanja, da li je to organizovani VTK ili je VTK koji se realizuje na organizovan način, odnosno, da li je tehnološki napredak samo olakšao izvršenje tradicionalnih oblika kriminala ili je došlo do stvaranja novog talasa tradicionalnog, virtuelnog i organizovanog kriminala. Izdvojene su i opisane četiri najvažnije karakteristike organizovanog VTK: sofisticiranost, komercijalizacija, organizovanost i transnacionalnost. Istraživanja organizovanosti VTK sugerišu da je onlajn kriminalno umrežavanje omogućeno internetom upravo jedan od najvećih istorijskih preobražaja kriminala. U radu je korišćena literatura, koja je, prema autoru, najznačajnija za ovu oblast, tako da popis literature predstavlja i svojevrsnu bibliografiju po pitanju organizovanog VTK (izuzimajući posebnu celinu: kriminalne grupe, forume i onlajn kriminalnu ekonomiju).

Ključne reči: *organizovani visokotehnološki kriminal, internet, sofisticiranost kriminala, transnacionalnost kriminala, kriminalne mreže*

Uvod

Globalizacioni procesi, nagli razvoj interneta i stalno povećanje broja njegovih korisnika (na početku 2018. godine bilo je preko četiri milijarde korisnika), pored svih dobrobiti za ljudsko društvo, stvorili su nove mogućnosti za visokotehnološki kriminal[1] (VTK) i druge zlonamerne aktivnosti u sajber prostoru; time je postavljen osnov da VTK preraste u organizovan kriminal na transnacionalnim nivou. Rast i razvoj sajber prostora kao međusobno zavisne mreže infrastrukture informacionih tehnologija koje uključuju i internet, telekomunikacione mreže i računarske sisteme, doprinosi i naglom porastu broja zloupotreba IKT, kao što su

[1] U Srbiji se koriste izrazi sajber ili kiber (*cyber*) kriminal, kompjuterski kriminal i visokotehnološki kriminal. Termin visokotehnološki kriminal je široko prihvaćen u akademskim radovima domaćih autora, pre svega onih koji su povezani sa borbom protiv ove vrste kriminala. Ovaj izraz je prihvaćen i u domaćem zakonodavstvu i strategijskim dokumentima kojima se uređuje oblast borbe protiv VTK, pa se koristi i u ovom radu.

VTK, špijunaža, terorizam i sajber ratovanje. Savremeni globalizacioni procesi pomeraju granice lokalnih, regionalnih i međunarodnih kriminalnih aktivnosti [1] i stvaraju nove mogućnosti povezivanja kriminalaca i organizovanih grupa, a računarske mreže postaju mesto, meta, cilj i sredstvo izvršenja kriminalnih aktivnosti, dok je, sa druge strane, odgovor bezbednosnih organa na pretnje u virtuelnom prostoru još uvek više reaktivan nego proaktivan [2, 3, 4]. Povećanje broja i sofisticiranosti uređaja i objekata povezanih na internet, korišćenje novih usluga zasnovanih na računarstvu u oblacima (*Cloud computing*) kao modula za povećanje računarske snage i prostora za skladištenje podataka i informacija i razvojem VoIP (*Voice over Internet Protocol*), stvoren je moćan alat i kao mete napada organizovanog VTK fokusirani su značajni ciljevi sa velikim finansijskim i drugim resursima.

Tokom proteklih četvrt veka, od ranih devedesetih godina XX veka i komercijalizacije interneta, VTK se promenio i dostigao nivo nacionalnih prioriteta i prioriteta međunarodne politike [5:531]. Sofisticiranost i organizovanost VTK izazivaju velike gubitke nacionalnih i globalne ekonomije, koji se ne mogu ni utvrditi u realnom iznosu. Procene globalne štete od VTK za 2015. godinu bile su u rasponu od 400 do 500 milijardi dolara. Globalna šteta tokom dve godine (2013-2015) je učetvorostručena, a procenjuje se da će globalna šteta u 2019. godini biti oko 2,1 hiljade milijardi dolara ($2{,}1*10^{12}$ dolara). Ove procene nisu obuhvatile neka krivična dela, poput industrijske špijunaže, kao ni gubitke koji postoje a nisu prijavljeni iz različitih razloga. Zbog povećanja broja, kvaliteta, uspešnosti i dobiti od krivičnih dela VTK, javlja se i reakcija na tržištu proizvoda namenjenih za zaštitu i procenjuje se rast sa oko 75 milijardi dolara u 2015. na oko 175 milijardi dolara u 2020. godini [6].

Organizovani VTK se može smatrati i naj organizovanijim delovanjem kriminalaca, gde stručnjaci svoja znanja primenjuju na kriminalne aktivnosti, bilo da deluju u konvencionalnim kriminalnim grupama koje su počele da koriste digitalnu tehnologiju ili u novim kriminalnim mrežama osposobljenim za delovanje u sajber prostoru. Iako postoje dileme oko toga u kojoj meri su tradicionalne kriminalne organizacije uključene u VTK i kakva je struktura i način funkcionisanja novih kriminalnih grupa koje su svoje delovanje usmerile na sajber prostor i internet, zbog velikog broja indikatora koji potvrđuju organizovano delovanje pri izvršenju dela VTK, sve je više tvrđenja da je isti globalan i organizovan. Potvrdu takvih tvrđenja daju istraživanja ilegalnih društvenih foruma i funkcionisanja kriminalnih globalnih onlajn ekonomija koje su u kontinuiranom razvoju i napretku. Nesporna je činjenica da su organizovane kriminalne grupe (OKG) glavni organizator i nosilac aktivnosti nelegalnih onlajn tržišta, koja postaju sve razvijenija i organizovanija i sa velikim brojem članova čiji broj je teško proceniti.

Porast rasprostranjenosti i uticaja organizovanog kriminala u virtuelnom svetu, sve više se odražava i na svakodnevni život ljudi, a dovodi i do sve veće zastupljenosti ovog fenomena u naučnim i stručnim radovima i sve veće zainteresovanosti akademske zajednice. Porast broja radova na ovu temu ne znači da je ovaj fenomen u potpunosti istražen, jer još uvek postoje problemi u njegovom potpunom razumevanju [7, 8, 9, 10, 11]. U naučnim i stručnim radovima pojavljuju se i neosnovane pretpostavke i neargumentovani izveštaji iz tehnoloških kompanija o ovom obliku kriminala, dok je vrlo malo empirijskih istraživanja [12, 13, 14, 15, 16].

Težište ovog rada biće osnov, razvoj i tendencije razvoja organizovanog VTK, dok će se u manjem obimu razmatrati kriminalne grupe za delovanje u sajber prostoru.[2] Rad je za-

[2] Zbog ograničenog prostora, ovaj rad ne obuhvata analizu struktura, unutrašnjih odnosa i funkcionisanje kriminalnih grupa VTK, onlajn kriminalnih foruma i kriminalnih tržišta (ekonomija) na internetu.

snovan na traženju odgovora u dostupnoj i izabranoj literaturi na pitanja o povezanosti VTK i transnacionalnog organizovanog kriminala, kao što su: u kojoj meri je VTK postao organizovan i da li je nastao novi oblik organizovanog kriminala, i obratno, šta je uzrokovalo nagli i veliki prodor VTK u transnacionalni organizovani kriminal; kako je to uticalo na razvoj novih metoda i tehnika izvršenja kriminalnih radnji u sajber prostoru kada je izvršenje krivičnih dela VTK od hakera – pojedinaca preuzela organizacija ili kriminalna mreža; kako se to odrazilo na bezbednost pojedinaca, kompanija, država, međunarodnih institucija, i uopšte, na globalnu bezbednost; i, kakav razvoj organizovanog VTK se može očekivati u budućnosti.

Pojam organizovanog visokotehnološkog kriminala

Pojam povezanosti organizovanog kriminala i VTK odražava dinamičnu prirodu i brzinu promena transnacionalnog kriminala [7: 107]. Iako su empirijska istraživanja o VTK još uvek oskudna, teorijska saznanja o uslovima njegovog nastanka i napredne hipoteze u literaturi, daju osnov za izvođenje zaključka da internet transformiše kriminal i da VTK postaje organizovan i obiman sa sve prisutnijom podelom poslova unutar OKG. Povezivanje VTK i tradicionalnog organizovanog kriminala i viktimizacija na mreži (internetu), imaju za posledicu sve veće preklapanje u pojedinim vrstama kriminala. Tradicionalni tipovi kriminala su transformisani korišćenjem računara i drugih IKT, što je dovelo do povećanja rizika koji zahvataju mnoge aspekte društvenog života (finansijske transakcije, seksualno nasilje, uznemiravanje i pretnje, komercijalne štete i poremećaji poslovanja). VKT obuhvata širok spektar aktivnosti i ponašanja, počevši od zločina koji uključuju ugrožavanja lične ili korporativne privatnosti (ugrožavanje integriteta informacija koje se čuvaju u digitalnom obliku, krađa identiteta i upotreba nezakonito pribavljenih digitalnih informacija za ucenu firmi ili pojedinaca); preko dela kakva je prevara, dečija pornografija, digitalna piraterija, pranje novca i falsifikovanje; pa sve do aktivnosti koje za cilj imaju da ometaju rad samog interneta, kao što su spam poruke, haking ili DoS napadi [17: 154].

Tačne dimenzije VTK su nepoznate. Sudske osude za VTK, u odnosu na druge vrste kriminala, relativno su retke, iako to ne znači da ova vrsta kriminala nije preovladavajuća. Zbog virtuelnosti i „nevidljivosti", složenosti digitalnih tragova i otežane ili onemogućene saradnje žrtava zbog straha od narušavanja ugleda, postoji velika „tamna brojka" neotkrivenih, neprijavljenih, neistraženih ili nerešenih slučajeva [18: 738]. Sa druge strane, sadržaje objavljenih brojnih statistika o računarskim incidentima, posebno o fišingu, virusima i drugom zlonamernom softveru, treba prihvatati veoma kritički, jer takve statistike uglavnom potiču od kompanija koje se bave proizvodnjom i plasmanom anti virusnog softvera i ti sadržaji su direktno povezani sa njihovim poslovnim interesima, tako da „stvarnost nije problem onoliko koliko mislimo – ali mi zaista nemamo dobar način za njenu kvantifikaciju" [19: 15].

Uprkos velikoj medijskoj zastupljenosti i istraživačkim izveštajima o stepenu korišćenja interneta (u zemljama zapadne Evrope), nije zabeležen veliki broj slučajeva u kojima je internet imao presudnu ulogu pri izvršenju dela organizovanog kriminala. Nedostatak pouzdanih podataka može se pripisati činjenici da su jedinice koje su angažovane u borbi protiv organizovanog kriminala razdvojene od jedinica zaduženih za borbu protiv VTK, tako da se fenomen organizovanog VTK ne može sagledati u celini. Situacija je slična i sa naučnicima, jer većina naučnika izučava organizovani kriminal i VTK – nezavisno [20: 155].

Neki od glavnih problema koji doprinose nedovoljnom razumevanju VTK usled nedostatka empirijskih pokazatelja su: (a) nedostaci mehanizama za precizno razlikovanje onlajn i oflajn krivičnih dela; (b) nepotpuno prijavljivanje VTK od strane poslovnih organizacija, državnih institucija i pojedinaca; (c) nedoslednost u merenju i definisanju VTK u značajnim istraživanjima; (d) informacije o VTK iz industrijskih izvora su često neuporedive sa podacima iz drugih oblasti, npr. oblasti bezbednosti; (e) istraživanja sa anketiranjem žrtava često su zasnovana na malim i ne reprezentativnim uzorcima iz kojih se ne mogu donositi zaključci za širu populaciju; (f) zbog globalne karakteristike VTK i kako nije ograničen nacionalnim granicama, veoma su otežana precizna merenja kriminala, kao i identifikacija i privođenje počinilaca; (g) VTK se može preduzeti u velikoj meri i istovremeno prema većem broju žrtava, što stvara veliki broj naizgled nezavisnih incidenata, tako da se time usložava postupak prikupljanja podataka i njihovo povezivanje [21].

Organizovani VTK ili VTK koji se realizuje na organizovan način [20, 22, 23], predstavlja i ključno pitanje u razmatranju organizovanog VTK: da li je tehnološki napredak samo olakšao izvršenje tradicionalnih oblika kriminala ili je došlo do stvaranja novog talasa tradicionalnog, virtuelnog i organizovanog kriminala [7: 107].

Razvoj organizovanog visoko tehnološkog kriminala

Pojava i razvoj VTK može se pratiti od početka kompjuterske ere i podeliti na dva perioda: prvi period obuhvata vreme od pojave prvog računara do 1990. godine (odnosno do početka komercijalne upotrebe interneta), nakon čega nastupa vreme značajnih mogućnosti i inovacija zasnovanih na ekspanziji interneta [22, 24, 25]. Proučavanje kriminala koji se na neki način povezuje sa računarima i/ili mrežama, a kasnije i sajber prostorom i internetom, počelo je početkom 60-tih godina XX veka, kada su se pojavili naučni radovi o kriminalu zasnovanom na manipulaciji računarima, sabotaži, špijunaži i drugoj nezakonitoj upotrebi računarskih sistema. Prve empirijske studije o kompjuterskom kriminalu objavljene su 70-tih godina, što je dovelo i do donošenja određenih zakona koji su se odnosili na kompjuterski kriminal, odakle potiču i prva određenja da je to: svaka namerna manipulacija računarima u privatnom, državnom, institucionalnom ili korporacijskom vlasništvu, u svrhu planiranja ili izvršenja prevara ili nezakonitog pribavljanja novca, imovine ili usluga [26: 161].

U vreme kada su, 60-tih i 70-tih godina XX veka, računari počeli da se koriste u poslovne i druge svrhe, nastao je i VTK, prvenstveno u finansijskoj sferi i uz isključivu podršku insajdera. Ograničena upotreba računara i nedostatak veza sa drugim računarima smanjivali su mogućnosti izvršenja kompjuterskih zločina, a ako su se isti i izvršavali – bili su u vezi sa ograničenim brojem računara (ili samo jednim računarom) i ograničenim brojem ljudi [25: 259]. Zajedničko svim kriminalnim delima izvršenim u ovom periodu jesu žrtve, koje su, po pravilu, bile velike kompanije ili vladine agencije, s obzirom na to da su jedine koristile *mainframe* računare. Pored toga, zastupljena je bila i manipulacija telefonskim sistemima (*phone phreaking*) i socijalni inženjering [22: 10-13]. Poslovni, ekonomski i kriminal „belih okovratnika" brzo su se menjali u sredinama u kojima su računari bili uključeni u proces rada, što je dovelo do promene potrebnih znanja i veština u ovoj oblasti, tako da su u kriminalne radnje uključivani kompjuterski programeri i operateri i inženjeri elektronike. Zločini koji su se dešavali u stvarnom, dešavali su se i u računarskom okruženju. Bitno se menjaju

i metodi, tehnike i oblici izvršenja kriminalnih aktivnosti, kao i potrebno vreme direktnog izvršenja koje se meri vremenom izvršenja računarskih instrukcija, a geografska ograničenja su postala nevažna i nisu ograničavajući faktor kriminala [27: 21-22]. Ovi faktori su uticali na to da organizacije, vladine agencije i institucije nisu bile adekvatno pripremljene ili motivisane da se bave suzbijanjem ove vrste kriminala.

U sferi istraživanja VTK sedamdesetih godina prošlog veka, istraživači povezani sa univerzitetima i vladinim agencijama u SAD, dali su nekoliko važnih studija o zloupotrebama računara, kriminalu povezanom sa računarima i VTK. Rezultati istraživanja su pomogli društvu da sagleda novu pojavu koja se danas naziva visokotehnološki ili sajber kriminal [28: 158]. Među prvim istraživačima u ovoj oblasti bio je Don Parker (Donn Parker) koji je proučavao različite oblike zloupotrebe računara, sa konstatacijom da je broj zloupotreba u porastu i da je otvorena budućnost razvoja VTK u kojoj će mlađe generacije korisnika imati velike neprilike i trpeti znatne štete [29].

Nove mogućnosti za razvoj VTK stvorene su 80-tih godina XX veka razvojem interneta i personalnih računara koji su bili pogodna sredina za delovanje hakera, pre svega radi zabave i dokazivanja vlastite inteligencije i znanja. Štetan (maliciozan) softver (malveri: virusi, crvi, trojanci) pojavio se 90-ih godina prošlog veka i koristeći slabosti računara, vršio je njihovo ometanje ili prekidanje radne funkcije. Nagli razvoj kriminala podržanog računarima i mrežama beleži se posle 90-tih godina XX veka evolucijom hakovanja (haking – *hacking*) koji prerasta u profitni kriminal; dolazi do pojave prodaja brojeva kreditnih kartica, njihovog falsifikovanja i krađa novca od banaka na ovakav način [22: 23]. Ovaj period je karakterističan i po ekspanziji malvera, a kasnije i njegove podvrste poznate kao ransomver, namenjenog za smanjenje ili prekid radnih funkcija računarskih sistema, ucene vlasnika i prodavanja šifri za „otključavanje“. Kao krivična dela u oblasti VTK, pored krađa i proganjanja, razvija se i pornografija na internetu. Posebno su za kriminalce bili atraktivni bankarski računarski sistemi kao sredstva za pranje novca, gde su ukinute mnoge barijere klasičnog bankarstva usled primene novih tehnologija, a posrednik u transakcijama novca je postao internet [30: 87]. Istraživanja u oblasti kompjuterskog kriminala u periodu do kraja XX veka bila su nedovoljna da bi se ova pojava adekvatno opisala i razumela, a osnovni razlozi, pored nedovoljnog finansiranja, bili su: (a) fokusiranost organa za borbu protiv kriminala na tradicionalne oblike kriminala koji ne uključuju internet i uređaje IKT; (b) nerazvijen sistem statističkog izveštavanja o izvršenom kompjuterskom kriminalu; (c) uzdržanost i nevoljnost finansijskih institucija i drugih organizacija da izveštavaju o novčanim gubicima i gubicima podataka iz straha od gubitka klijenata, potrošača ili investitora; (d) relativno mali broj istraživača je bio zainteresovan ili obučen u poznavanju IKT, kako bi se uspešno bavio problemima kompjuterskog kriminala [28: 161].

Početkom XXI veka VTK postaje veliki biznis na globalnom nivou, kao što je to i danas. Korišćenje računarske i druge visoke tehnologija nije ograničeno na hakovanje i malvere, nego se obilato koristi i za izvršenje tradicionalnih zločina (prevare, krađe, iznuđivanja, krađe intelektualne svojine) na nove načine, manjim rizikom kriminalaca i znatno većim dobicima [31]. Dalji razvoj IKT povećao je broj računara, mobilnih telefona i drugih mobilnih uređaja i broj Internet stvari (*Internet of things* – IoT), a uvođenje bežičnog interneta (*Wireless Internet*) je znatno olakšalo komunikaciju [32: 26]. Razvijeno je računarstvo u oblacima (*cloud*) i *Voice over Internet Protocol* – VoIP. *Cloud* računarstvo je, pored već iskorišćene digitalne i umrežene tehnologije, stvorilo nove kriminalne mogućnosti

za upotrebu softverskih aplikacija, skladišnog prostora za podatke, informacije i druge digitalne zapise i za jeftinu upotrebu infrastrukture provajdera; povećalo je računarsku snagu i smanjilo troškove kriminalaca, čime je olakšan kriminal preko *botnet* mreža i kriminal koji zahteva veliku računarsku snagu (kao što je dešifrovanje lozinki) [5: 538].

Povezivanje VTK i organizovanog kriminala uočeno je još sedamdesetih godina XX veka (u SAD je tada bilo oko 100 hiljada računara), kada su istražni kriminalistički organi SAD oglasili da „postoje jaki dokazi koji ukazuju na to da je organizovani kriminal ušao u područje kompjuterskog kriminala“, a kao osnovne kategorije kriminala identifikovane su samo one u kojima je kriminal podržan računarima, ali se može izvršavati i bez njihovog korišćenja, kao što su krađe, pronevere, krađa imovine i usluga, krađa podataka i informacija i plaćanja nepostojećim organizacijama [33: 9-14]. Pristupi računarima telefonskih kompanija omogućili su kriminalcima da pristupe i manipulišu telefonskim sistemima (*phone phreaking*) i dele svoje znanje širom sveta, smatrajući to samo vidom lepe zabave [22: 12-13].

Osamdesetih godina XX veka raste broj računarskih sistema kao potencijalnih meta napada, što je rezultiralo razvojem hakovanja i kriminala oblika softverske piraterije i krađe patenata. Mogućnosti koje su pružile računarske mreže, doprinele su bržem širenju zlonamernog softvera, prvenstveno sve većeg broja računarskih virusa [34: 302]. Popularizacija hakovanja, kao profitabilne aktivnosti, rezultat je pojave personalnih računara i jačanja interneta, kada je računarstvo prestalo da bude aktivnost stručnjaka, a slika kreativnih i dobroćudnih hakera je izbrisana [35: 38].

Početkom XXI veka Fil Vilijams (Phil Williams) je ustanovio da postoji nekoliko aspekata na koji način organizovane kriminalne grupe koriste internet: kako bi olakšale izvršenje tradicionalnih krivičnih dela (kao što su velike prevare i krađe sa fokusom na elektronsko bankarstvo i trgovinu), kako bi širile delovanje na različite oblike kriminala na internetu (na primer, kriminal poznat kao „kriminal belih okovratnika“), za vršenje ucena korišćenjem interneta ili da bi upotrebom kompjuterskih virusa dobile pristup lozinkama u bankama i finansijskim institucijama. Međutim, razmatrajući budućnost organizovanog VTK Vilijams je smatrao: da „organizovani kriminal i sajber kriminal nikad neće biti sinonimi“; da će većina organizovanog kriminala nastaviti da funkcioniše u stvarnom a ne u virtuelnom svetu; da će većinu VTK činiti pojedinci a ne kriminalne organizacije; i, da će se stepen preklapanja između ova dva fenomena verovatno povećavati narednih godina [36: 22]. Kasnija istraživanja i analize pokazale su da je velikim delom VTK postao organizovan, tako da se predviđanja koja je dao Vilijams, očito nisu u potpunosti ostvarila.

Naglim razvojem interneta i uvođenjem *WWW* sistema za bolju komunikaciju devedesetih godina XX veka, povećana je brzina razmene informacija u kriminalnoj sredini na trans nacionalnom nivou. U prvoj deceniji XXI veka dominirali su novi i visoko sofisticirani metodi izvršenja kriminalnih aktivnosti poput fišinga i botnet napada, upotrebljavana je nova tehnologija koja otežava rad organa za borbu protiv VTK kao što su internet telefonska tehnika – VoIP i *cloud* računarstvo [37]. Iako se postavljalo pitanje o postojanju organizovanog kriminala u sajber prostoru, nekoliko studija iz tog perioda [38, 39, 40], sugeriše da je VTK postao integralni deo trans nacionalne pretnje i da nesumnjivo postoje kriminalni elementi koji rade u onlajn okruženju: kriminalne grupe koje su organizovane na mreži, a ne tradicionalne organizovane grupe koje rade na mreži. Tada nije bilo jasno da li tradicionalne OKG deluju i koliko su angažovane u sajber okruženju, ali je verovatno da se one neće „udaljavati“ od sajber prostora, jer na taj način olakšavaju svoj rad,

prikrivaju nezakonite prihode i fizičke zločine u stvarnom svetu, pri čemu primenjuju malvere ili botnet mreže radi izvođenja DDoS napada i iznuđivanja ili koriste onlajn bankarstvo radi pranja novca [40: 16].

Računari i internet su postali okosnica za sve aspekte modernog života, a društvene mreže su uobičajeno sredstvo komunikacije velikog broja ljudi, što je kao pojava doprinelo i razvoju i širenju organizovanog VTK, posebno podzemnih kriminalnih ekonomija. Komercijalizacija interneta, kao i svaka druga tehnološka promena, modifikovala je okruženje u kome deluje kriminal i stvorila je širok opseg novih mogućnosti i novu dinamiku kriminalnih aktivnosti, bilo da su one potpuno nove (zlonamerni softver, lažiranje i krađa podataka) ili su kriminalci samo promenili neke aspekte već postojećih aktivnosti [40: 35].

Sve veće korišćenje interneta, globalizacija kao svetski proces i posledice koje je ostavila ekonomska i finansijska kriza 2007. godine i kasnije, smatraju se značajnim događajima koji imaju veliki uticaj na društvo, tako da su verovatno uticali i na stvaranje spektra novih mogućnosti za delovanje OKG, kao i nove trendove tog delovanja [41: 10]. Kriminal kao deo društva nije imun na ove promene i zato ne iznenađuje činjenica da su pogodnosti interneta za izvršenje kriminala, osim kriminalaca, privukle i pažnju kriminologa. Postoji veliki stepen saglasnosti kod kriminologa i lica koja se bave borbom protiv VTK da je internet ponudio mnoštvo novih mogućnosti za kriminalce, uključujući i za organizovani kriminal [18, 20, 42, 43, 44]. Velike zarade u kombinaciji sa malim rizicima učinili su digitalne mreže atraktivnim okruženjem za različite vrste aktivnosti, a jednostavnost komunikacija, anonimnost i dostupnost alata i ilegalnih operacija – transformisali su VTK u globalnu, brzo rastuću i profitabilnu industriju [45].

Globalizacija kao svetski proces[3] značajno je uticala na razvoj VTK kao savremenog oblika organizovanog kriminala i to u njegovoj trans nacionalnoj formi. Kada globalizacioni procesi nisu u dovoljnoj meri praćeni svesnim upravljanjem, javljaju se stanja koja pogoduju nastanku svetskih ekonomskih kriza, čemu odgovara koncept „refleksivne globalizacije" koji označava fenomen samo organizovanja, samo praćenja, samo regulacije i samo proizvodnih procesa, onako kako se procesi pojavljuju u društvenim sistemima koji se nalaze u društveno-ekonomskim krizama. Sa haotičnim stanjem refleksivnih finansijskih sistema koji nisu regulisani, stvaraju se povećane mogućnosti za delovanje trans nacionalnog organizovanog kriminala i VTK kao njegovog oblika [1: 54]. Transformacije u umrežavanju, prenošenju informacija i globalizaciji, doprinele su radikalnim promenama u organizaciji kriminala, podeli kriminalnog rada i povećanju kriminalnih prilika [47: 39]. Pored toga, procesi globalizacije su doveli do novih pretnji kao što su: (a) pojave prenosa međunarodnih kontradikcija u informacioni prostor, upotreba informacionog oružja i informaciono ratovanje; (b) mogućnosti nastanka novih vrsta katastrofa zbog grešaka ili zloupotreba globalnih IKT mreža; (c) mogućnost stvaranja novih globalnih informacionih infrastruktura kriminalnih i terorističkih organizacija koje je teško kontrolisati; i (d) stvaranje novih oblika VTK, uključujući i organizovani VTK [48: 1-2]. Velika svetska finansijska kriza pokrenuta u leto 2007. godine, pored toga što je poučna sa aspekta razmatranja nestabilnosti globalnog kapitalističkog tr-

[3] Po pitanju kako definisati koncept globalizacije, postoji mnogo sugestija i debata, a od nekoliko ponuđenih opcija od strane UNESCO izabrane su dve karakteristične definicije: (a) globalizacija se može smatrati procesom (ili skupom procesa) koji odražava transformaciju prostorne organizacije društvenih odnosa i transakcija; (b) globalizacija se odnosi na sve one procese kojima se narodi sveta inkorporiraju u jedno jedinstveno svetsko društvo – globalno društvo [46].

žišta, pokazala je skup društvenih i tehnoloških uslova koji su olakšali globalizaciju kriminalnih aktivnosti. Iako je finansijska kriza u mnogim državama uticala na većinu društvenih aktivnosti, na organizovani kriminal taj uticaj je bio znatno manji, jer su se OKG brzo prilagodile novim zahtevima tržišta u realnoj ekonomiji [49: 12-13].

Obeležja globalizacije kao što su neuređenost međuzavisnih odnosa političkih i ekonomskih aktera u svetu, globalna digitalna povezanost i deteritorijalizacija država, ujedno predstavljaju i osnovne uslove za razvoj globalnog kriminala [40], kao što su:

– globalni domet trenutnih digitalnih komunikacionih tehnologija: internet, World Wide Web, video konferencije, multimedijalne digitalizacije, računarstvo u oblacima;

– globalizacija ili pojava globalnog umreženog društva (informaciono društvo) u kome su umrežene informacije, društveni odnosi, usluge i institucije (era sajber prostora ili globalna telekomunikaciona povezanost);

– radikalno prikupljanje i obrada podataka sa lokalnih i regionalnih prostora i njihovo objedinjavanje na globalnom nivou (stvaranje baza podataka o nacionalnom i globalnom stanovništvu i formiranje eksteritorijalnog policijskog i nadzornog sistema);

– rastuća povezanost i pokretljivost proizvodnje, trgovine i finansijskog kapitala, što doprinosi interesu globalnih sila za potražnjom nepotrebne robe (komodifikacija i konzumizam);

– širenje digitalnih masovnih medija, posebno novinarstva, koji su stalno uključeni u izveštavanja, po sistemu 24/7 (24 časa dnevno – 7 dana nedeljno); i

– „zamagljivanje“ tradicionalnih normativnih granica između dozvoljenih i nedozvoljenih aktivnosti, što je postalo normalno ponašanje u političkom i ekonomskom svetu.

Kriminalci koji se bave VTK uspešno koriste postojanje distribuirane informacione strukture kao osnovnog tehničkog i materijalnog sredstva u sajber prostoru. Digitalne komunikacione mreže i stvorene opšte prisutne multi medije, pogoduju onlajn kriminalu omogućenim novim informacionim mrežama. Sklop ovih uslova formira okruženje za „globalizaciju kriminala u doba kapitalističke sajber kulture“ [1: 39-43].

Internet je na početku na kriminal i/ili štetno ponašanje uticao na tri osnovna načina: *prvo,* postao je sredstvo za komunikaciju kojim se podržava postojeći obrazac štetne aktivnosti kao što su trgovina drogom, govori mržnje, uhođenje i slično; *drugo*, stvorio je trans nacionalno okruženje koje pruža nove mogućnosti za štetne aktivnosti, kao što su prevare i pedofilija; *treće*, priroda virtuelnog okruženja je stvorila potpuno nove forme štetnih aktivnosti koje ne poznaju granice, kao što su povrede autorskih prava i druge [24: 3]. Internet je tada omogućio nove kriminalne oblike kao što su *spam* poruke (zloupotreba elektronskih sistema u svrhu slanja masovnih poruka) i zlonamerni softver i olakšavao izvršenje tradicionalnih krivičnih dela. U početnom periodu komercijalne upotrebe Interneta (posle 1990. godine), bio je u porastu broj izvršenih krivičnih dela i naneta je šteta državama koje nisu imale odgovarajuće zakone i/ili su posedovale male ljudske i materijalne kapacitete za njihovo sprovođenje. Internet je korišćen za pranje novca putem međunarodne trgovine, a razvijena je i komunikacija između hakera i malih kriminalnih grupa sa organizovanim kriminalom [36: 24]. Kao elemenat sajber prostora, pored ostvarivanja pozitivnih efekata, internet je viđen kao „kriminalni problem“, ali i kao stvarni kanal za protok kriminalnih aktivnosti [50: 88]. U vreme kada je upotreba interneta postala rutinska aktivnost u svakodnevnom životu, zadatak kriminologije, krivičnog prava i politike je da uključe Internet i VTK u vlastite rutinske aktivnosti, jer internet po svojim karakteristikama predstavlja ogromnu, globalnu i otvorenu mrežu koja omogućava trenutnu ko-

munikaciju i koja transformiše društvene i ekonomske procese, pa se može očekivati da transformiše i kriminal [51].

U kriminologiji i krivičnom pravu internet zaslužuje posebnu pažnju zbog svojih glavnih odlika kao što su globalni karakter, trenutna dostupnost i neograničenost, digitalan je i omogućava automatsku obradu podataka. To pruža posebne mogućnosti za izvršenje dela VTK u kojima su računarske mreže cilj i značajan alat. Internet omogućava interakciju između kriminalaca i kriminalnih organizacija, a funkcionisanjem kriminalnog tržišta informacijama i finansijskim korisničkim kredincijalima olakšavaju se prevare, krađe i druge kriminalne aktivnosti [18: 737].

Karakteristike interneta kao globalne računarske mreže, a posebno, da omogućava trenutne veze u mrežnoj decentralizovanoj strukturi i da se zasniva na digitalnim informacijama, sačinjavaju osnov za međusobno povezivanje i pojedinačno važnih faktora rizika koji olakšavaju aktivnosti organizovanog VTK [1, 9, 18, 47, 52], među kojima su najznačajniji:

– Zbog globalnog dometa, omogućeno je kriminalcima da traže najranjivija mesta u mreži (računari, računarske mreže i žrtve) bilo gde u svetu i bez napuštanja svog prebivališta.

– Nema ograničenja državnim granicama, tako da je VTK, u velikom broju slučajeva, postao međunarodna aktivnost, što zahteva i prekograničnu saradnju organa za borbu protiv njega.

– Omogućeno je stvaranje i funkcionisanje decentralizovanih i fleksibilnih (labavih) mreža kao organizacione strukture kriminalnih grupa, u kojima one vrše podelu poslova i razmenu veština, znanja i alata.

– Olakšana je anonimnost izvršilaca kriminala ako se upotrebljavaju odgovarajući alati (*remailers, torrent networks*), kada su izvršioci „na većoj udaljenosti“ od *IP* broja, e-adrese ili *Facebook* profila.

– Omogućena je produžena interakcija počinilaca i žrtava i uklanjaju se eventualne društvene barijere sa kojima se suočavaju počinioci, posebno u početnoj fazi komunikacije.

– Znatno je olakšana manipulacija podacima, informacijama i softverima sa minimalnim pratećim troškovima.

– Automatizacija pojedinih kriminalnih procesa omogućava da se neki oblici nelegalno instaliranog zlonamernog softvera brzo umnožavaju, napadaju milione računara istovremeno u dužem vremenskom periodu i sa ponavljanjem napada.

– Izaziva znatno veće štete nego što su uloženi napori kriminalaca i daleko veće štete nego što bi se sličnim postupcima postiglo bez posredstva interneta.

– Omogućava agregiranje malih dobitaka u jedan veliki dobitak kriminalaca – iskorišćava se veliki broja žrtava sa relativno malim gubicima (metod seckane salame – *salami method/salami-slice strategy*).

– Stvaraju se mogućnosti za formiranje informacione ekonomije sa informacijama kao vrednom imovinom, kako na pravom tržištu (muzika, filmovi, knjige, softver), tako i na „crnom“ tržištu gde se, radi prevara i krađa, trguje ličnim informacijama, lozinkama i brojevima kreditnih kartica, ali i znanjima, veštinama, elementima infrastrukture i softverom za kriminalne aktivnosti.

– Veoma brze izmene inovacionih ciklusa i razvoj novih tehnika i alata za izvršenje kriminalnih aktivnosti u kratkom vremenskom periodu, imaju za posledicu proširenje mogućnosti za zaobilaženje kontra mera sigurnosnih sistema.

Karakteristike interneta navode na zaključak da je komunikacija na svetskoj računarskoj mreži neposredna i trenutna, individualna, dinamična, produbljena, interaktivna, anonimna, ne cenzurisana, jeftina i dalekosežna, što je čini superiornijom u odnosu na mogućnosti drugih medija [53]. Tradicionalne trans nacionalne prepreke organizovanom kriminalu sa kojima su se suočavale bivše generacije kriminalaca, srušene su i prevaziđene u onlajn svetu, omogućavajući im slobodan pristup na svaku željenu virtuelnu lokaciju [54: 14].

Rizici bazirani na internetu ušli su u delokrug rada državnih bezbednosnih službi zbog problema sajber terorizma i sajber ratovanja, što je rezultiralo preduzimanjem onlajn prevencija, kontrola, otkrivanja i krivičnog gonjenja. Pojačan nadzor i praćenje korisnika interneta i nemogućnost provajdera da zadrže podatke o korisnicima, predstavljaju značajnu pretnju privatnosti. Pored državnih institucija i mnoga komercijalna preduzeća nezakonito prikupljaju podatke o korisnicima interneta i njihovom ponašanju radi ciljanog oglašavanja i marketinga ili prodaje podataka trećem licu za komercijalne i druge namene [55: 5-6]. Zbog mogućnosti modifikacija, gubitaka ili krađa,[4] opasnost po bezbednost informacija postoji i kod organa koji su ovlašćeni za njihovo prikupljanje, čuvanje i obradu. Krađa identiteta i preuzimanje akreditiva ili ličnih podataka drugog lica sa namerom da se upotrebe u kriminalne svrhe, jedna je od glavnih pretnji daljoj upotrebi i razvoju e-uprava i drugih vidova elektronskog poslovanja [57: 2].

Nove i ozbiljne pretnje prate rast informacionog društva i sve veću primenu IKT, posebno u oblasti kritičnih infrastruktura, kao što su snabdevanje električnom energijom, vodom, gasom, nuklearna postrojenja, vojna infrastruktura i drugi objekti, čije je upravljanja i funkcionisanje bazirano na primeni IKT i veoma osetljivo na računarske napade. Napadi na informacione infrastrukture i internet servise imaju nove mogućnosti da nanesu štetu društvu na nove načine i sa veoma velikim posledicama [57: 2].

Internet nema samo značaj kao dobar komunikacioni kanal, već je stvorio mogućnost postojanja i delovanja mešovitih kriminalnih mreža i sadrži potencijal da na značajan, ako ne i presudan način, utiče na kriminalno tržište [41: 12]. Otvoren je put za formiranje nelegalnih foruma, skladišta i tržišta različitih roba i usluga, gde se mogu sresti mnogi zainteresovani kupci i prodavci, koji za oglašavanje roba i usluga, pored sakrivenih, koriste i obične veb stranice (mogu se naći na legalnim pretraživačima), jer su, zbog drugih karakteristika Interneta, veoma male šanse da oglašivači budu otkriveni [58: 4].

Nove kriminalne pretnje u sajber prostoru stvorene su razvojem *cloud* računarstva [5, 32, 59]. Kao i drugi tehnički napreci, to je privuklo čitav kriminalni ekosistem, od pojedinaca do organizovanih grupa koje imaju za cilj da preuzmu kompletnu globalnu računarsku mrežu (internet) [60]. Zbog povećane moći (snage) računara povećavan je i učinak botnet mreža, DDoS napada i prevara putem spam poruka, čime su postignuti bolji efekti i smanjeni rizici kriminalaca.

Karakteristike organizovanog visoko tehnološkog kriminala

Koncept VTK nije radikalno drugačiji od koncepta konvencionalnog kriminala. Oba uključuju ponašanje koje se sastoji u činjenju ili nečinjenju koje uzrokuje kršenje prava i podleže sankciji [61: 241]. Sa tog aspekta, karakterističan pristup u razmatranju pove-

[4] „Lični podaci i ne-javne informacije o gotovo 60 posto građana SAD-a dostupni su na mreži zbog neispravne baze podataka. Više od 191 miliona zapisa američkih birača otkrili su na Internetu istraživači bezbednosti“ [56].

zanosti organizovanog kriminala i VTK, a na osnovu njihovih osnovnih karakteristika, može se sagledati iz radova ruskih autora [45, 48, 49, 62, 63, 64, 65, 66]. Ovi autori, uglavnom, u određivanju koncepta organizovanog kriminala, kao činjenice, navode sledeće stavove: postoje lica, organizovane kriminalne formacije, organizovane kriminalne grupe i zajednice organizovanih kriminalnih grupa koje stabilno funkcionišu, stalno vrše kriminalne aktivnosti i na taj način obezbeđuju stalan prihod i druge koristi. Pored toga, kao svojstva organizovanog kriminala ističu se: organizovanje grupa za vršenje kriminalnih aktivnosti u dužem ili kraćem periodu; centralizacija moći u rukama jednog ili više članova grupe; specijalizacija grupe za vršenje određenih kriminalnih aktivnosti i raspodela funkcija unutar grupe; korupcija i stvaranje veza sa predstavnicima državnog aparata; i, ustanovljavanje discipline i poštovanje utvrđenih pravila ponašanja [65]. Upoređujući karakteristike organizovanog kriminala sa tipičnim odlikama sadašnjeg VTK, uprkos specifičnog distributivnog okruženja (interneta) i neophodne specijalizacije izvršilaca kriminalnih aktivnosti, ovakav kriminal se „može sa uverenošću nazvati organizovani visokotehnološki kriminal (ruski: киберпреступность организованной преступностью)“ [49: 187].

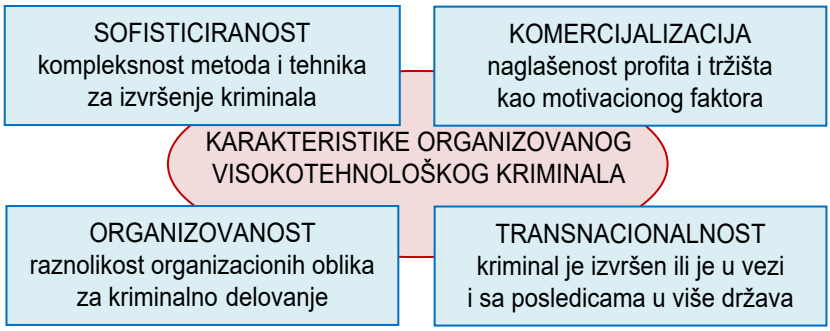
Kod pojedinih autora se kao osnovne karakteristike organizovanog VTK navode: anti društvena ideologija, prisustvo hijerarhijske strukture, transnacionalni karakter, prisustvo stručnjaka sa specijalnim informatičkim znanjima i veštinama, i eksploatacija pornografije [49, 67].

Sa aspekta promenljivog tehnološkog okruženja koje je izmenilo i prirodu samog kriminala [5: 532], osnovne odlike organizovanog VTK su:

1) *Organizovani VTK se odvija u sajber prostoru*: ponašanje na društvenim mrežama je, posredstvom digitalnih i umreženih tehnologija, pretvoreno u mreže komunikacija koje su stvorile globalno, informaciono i rasprostranjeno ponašanje. Iako je ovaj prostor delom „imaginaran“, posledice kriminalnih radnji u sajber prostoru imaju stvarne posledice u fizičkom svetu [5: 532]. Neograničenost i anonimnost sajber prostora omogućavaju uspostavljanje društvenih odnosa i onlajn veza (Facebook, Twitter, YouTube), gde se identiteti u sajber prostoru formiraju na osnovu pruženih informacija od strane korisnika i ne moraju biti istiniti. Digitalizacija na internetu omogućava skoro trenutni prenos informacija korišćenjem mobilnih uređaja na trans nacionalnom nivou, a pored ostalog, omogućava prenos i distribuciju virusa i zlonamernog softvera [1: 44].

2) *VTK je omogućen tehnologijom,* istom onom koja stvara sajber prostor i koja transformiše kriminalno ponašanje. Razvoj IKT je učinio da kriminal postane globalan, informacioni i rasprostranjen, stvarajući nove kriminalne mogućnosti.

3) *VTK je automatizovan*, a stepen automatizacije se svakodnevno povećava, jer digitalne i umrežene tehnologije postaju naprednije i sve sofisticiranije. Ovaj proces pozitivno utiče na većinu kriminalnih aktivnosti jer ih čini jeftinijim i manje zahtevnim za veštinama izvršilaca koje su apsorbovane automatizacijom. Sa druge strane, za kontrolu istih tehnologija i novih procesa, zahtevaju se nova znanja i dodatno učenje. Činjenica da je za kontrolu izvršenja kompletnog kriminalnog postupka potrebno jedno do dva lica, što je ranije zahtevalo mnogo više lica i setove različitog znanja, ima duboke posledice za razumevanje organizovanog VTK. Nepromenljivost umnoženih informacija od originala, bez obzira na broj kopija, pogoduje krađama identiteta, drugih podataka, informacija i intelektualne svojine [1: 44-45].



Slika 1 – *Karakteristike organizovanog visokotehnološkog kriminala*

Kao osnovna obeležja organizovanog VTK u XXI veku (slika 1), mogu se izdvojiti: sofisticiranost, komercijalizacija i organizacija (različitost organizacionih formi) [32: 15]. Ovome treba dodati i transnacionalni karakter organizovanog VTK, koji je omogućen globalizacionim procesima i globalnom IKT strukturom i internetom [68, 69].

Sofisticiranost organizovanog visokotehnološkog kriminala

Pod sofisticiranošću organizovanog VTK podrazumeva se kompleksnost metoda i tehnika kojima se izvršava kriminal. Napredak sofisticiranosti organizovanog VTK može se videti poređenjem najvećih procenjenih pretnji u određenom vremenskom periodu. Na primer, mogu se porediti 2012. i 2016. godina. Najveće pretnje u 2012. godini poticale su od: primene trojanaca tehnikama socijalnog inženjeringa; softvera za eksploataciju neotkrivenih ranjivosti (ranjivost nultog dana) i eksploataciju veb stranica (*Unpatched Software*), fišinga, mreža u kojima se nalaze i cirkulišu razne vrste računarskih crva i napredne uporne pretnje (*Advanced Persistent Threats*). Pretnje u 2016. godini bazirane su na rasprostranjenoj upotrebi novih tehnologija kao što su *cloud* računarstvo, skladištenju velikih količina podataka i masovnoj upotrebi mobilnih uređaja. Dve tehnološke novine bile su najznačajnije za pokretanje pretnji: Internet stvari – stvari koje se povezuju na internet ili druge mreže; i, veoma velike količine uskladištenih podataka. Time je redosled pretnji promenjen i najizraženije pretnje su u obliku: napredne uporne pretnje, fišing, trojanci, botnet mreže, ransomveri, DDoS napadi, napadi posebnim malverima za brisanje hard diskova (*Wiper Attacks*), krađa intelektualne svojine, krađa novca, špijunski malveri, tehnika „čovek u sredini“ (*Man in the Middle – MITM*), zlonamerno oglašavanje (*malvertising*), preuzimanje softvera i baza podataka (*Drive-by downloads*), lažni softver (na primer kao anti virusi) sa prilogom malvera (*Rogue software*) i softvera za eksploataciju ranjivosti [70].

Pored postojećih malicioznih softvera i njihove stalne nadgradnje i usavršavanja tehnika primene, menjale su se i naglo razvijale i botnet mreže (mreže „zombi“ računara).[5] Ove mreže

[5] Botnet (*Botnets*) ili mreža zombi računara predstavlja skup umreženih kompromitovanih računara koji su daljinski upravljani iz jednog centra, a koristi se za obavljanje raznih aktivnosti, uključujući slanje spam poruka, širenje malvera, pokretanje DDoS napada i podržavanje nelegalnih veb stranica [14: 47]. Početkom 2017. godine na društvenoj mreži Tviter (*Twitter*) otkriveno je oko 350 hiljada lažnih naloga i svi oni su bili deo jedne botnet mreže, ali su pronađeni i drugi nalozi manjih botnet mreža, što je ukupno činilo preko pola miliona lažnih naloga [106: 62].

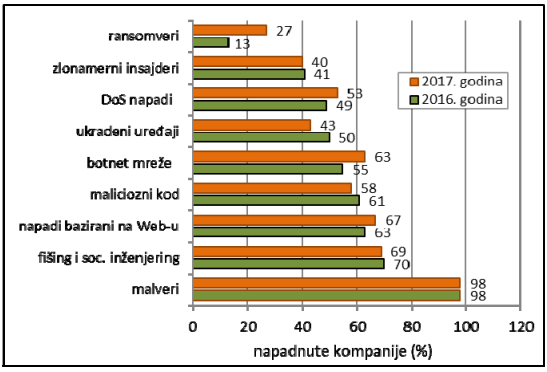
mogu da sadrže stotine i hiljade zaraženih računara, a procene stručnjaka su da je 16-25% svih računara povezanih na internet deo neke botnet mreže [71: 378]. Ovakve mreže mogu da vrše nelegalne aktivnosti poput krađe informacija i krađe identiteta, DoS i DDoS napada, slanja neželjenih poruka (spam poruke) i širenje malvera radi izvršenja finansijskog kriminala.

Napadi ransomvera postaju sve više ciljani, prvenstveno na finansijske institucije, radi trenutne velike dobiti, umesto do sada primenjivanih masovnih napada sa manjim dobicima. Napadi ransomvera, kao posebne vrste malvera, tokom 2017. godine su iznenada i spektakularno prošireni na poslovne organizacije sa zahtevanom velikom otkupninom. Novina u upotrebi ransomvera je njihovo dizajniranje za uništavanje podataka, a ne samo za sprečavanje pristupa fajlovima i finansijsku korist napadača. Troškovi žrtava u samo tri velika napada u 2017. godini iznosili su stotine miliona dolara [72].

Stvaranjem „peer-to-peer" (P2P) botnet mreža, u kojima kompromitovani kompjuteri komuniciraju međusobno pre nego sa centralnom komandnom lokacijom, povećana je rezistentnost (otpornost) mreže. Trojanci koji postoje već više od tri decenije, dostigli su visok nivo sofisticiranosti, tako da su postali prilagodljiviji navikama žrtve, prikupljajući podatke iz njenog računara [32: 15-17]. Dostupnost i „otvorenost" digitalnih informacija ili softvera, čini ga pogodnim za modifikacije uz minimalne troškove, što omogućava kriminalcima njegove izmene i prilagođavanja vlastitim potrebama [1: 44-45].

Kvalitativni napredak u razvoju sajber prostora učinjen je razvojem modela poznatog kao *cloud* računarstvo koji omogućava jednostavan pristup velikim računarskim resursima u mrežnom okruženju (mrežni serveri, skladišta, aplikacije i usluge), uz minimalne napore korisnika i bez korišćenja servisa provajdera. Koncept računarstva u oblacima se zasniva na deljenju resursa na mreži, najčešće na internetu. Model se sastoji od tri servisa koji pružaju mogućnosti korisniku da koristi provajderove softverske aplikacije, platforme za smeštanje svojih podataka ili aplikacija, kao i namensku infrastrukturu kojom raspolaže provajder [73: 1-2], a koju korisnici ne moraju da održavaju [59: 84]. Uprkos kontradiktornih stavova koji postoje oko računarstva u oblacima, činjenica je da su njegova pojava i razvoj znatno uticali na povećanje računarske snage, povećanje mogućnosti skladištenja elektronskih zapisa i vršenje drugih računarskih usluga, uz znatno smanjene troškove pojedinačnih korisnika, što je olakšalo izvršenje složenih i zahtevnih kriminalnih aktivnosti [5: 529].

Potreba za međusobnim povezivanjem uređaja preko interneta dovela je do razvoja pametnih uređaja, kućne automatizacije i Interneta stvari (IoT). Ovaj fenomen se pojavio nakon 2009. godine, a sa padom cena mnogih naprednih tehnologija, bilo je moguće izgraditi složenu računarsku mrežu u koju su uključene sve vrsta objekata i uređaja, kao što su personalni i mobilni računari, automobili, medicinski instrumenti, geološka oprema, avioni, oružja, kamere i kućni aparati. Veliki deo ovih mreža može da bude ranjiv i predstavlja dobru metu za kriminalne eksploatacije [74: 1-2]. Internet stvari mogu se definisati kao svet u kome su fizički objekti integrisani u informacionu mrežu i oni postaju aktivni učesnici u poslovnim procesima, a dostupne usluge mogu da komuniciraju sa ovim "pametnim objektima" preko interneta [75: 1]. Predviđa se da će, ionako složen softver za upravljanje IoT na sadašnjem nivou, biti najbrže rastući tehnički segment za IoT sa zahtevima da obezbedi poseban softverski ekosistem, praćen softverom za povezivanje, za analitiku i IoT platforme i sigurnosnim softverom. Procenjuje se da je globalna potrošnja na IoT u 2017. godini bila 674 milijarde dolara, a da će u 2021. godini dostići vrednost od 1.100 milijardi dolara [76].



Slika 2 – *Najzastupljeniji tipovi napada i eksploatacije visoko tehnološkog kriminala na kompanije, prema [77]*

Prema istraživanju Ponemon instituta (Ponemon Institute) [77] kojim je obuhvaćeno 254 kompanija iz osam najrazvijenijih država u svetu u različitim oblastima delatnosti (industrijska proizvodnja, finansije, usluge, zdravstvo i druge delatnosti), a koje su imale od 1.050 do 259.000 aktivnih računarskih priključaka na internet (prosečan broj priključaka je oko 8.500 po kompaniji), najzastupljeniji napadi na računarske sisteme, preuzimanje kontrole i eksploatacija njihovih sadržaja u 2017. godini, mogu se klasifikovati u osam osnovnih tipova ili metoda: malveri, fišing i socijalni inženjering, napadi bazirani na Web-u, maliciozni kod, napadi preko botnet mreža, DoS napadi, zlonamerni insajderi i ransomveri. Kao poseban vid nanošenja gubitaka, pod napadima se podrazumevaju i krađe uređaja – elemenata infrastrukture. Iz prikaza na slici 2 vidljivo je da su skoro sve kompanije pretrpele napade malvera (virusi, crvi i trojanci), da je broj napada ransomvera u 2017. godini udvostručen u odnosu na prethodnu godinu, da je oko 70% kompanija pretrpelo napade oblika fišinga i drugih oblika socijalnog inženjeringa, a 67% kompanija je imalo napade na veb stranice u bilo kom obliku. Napadi zlonamernog softvera (malveri, ransomveri) prikazani su odvojeno od napada malicioznim kodom, iako su usko povezani, zato što su kao zlonamerni kod klasifikovani oni zlonamerni napadi koji su uspešno infiltrirali zlonamerni softver u mrežu organizacije [77].

Komercijalizacija organizovanog visokotehnološkog kriminala

Naglašenost profita i tržišta kao motivacije za izvršenje kriminala osnovna je karakteristika komercijalizacije organizovanog VTK. Eksponencijalni rast i razvoj digitalnih tehnologija i elektronskog poslovanja omogućili su povećanje kriminala na internetu, prvenstveno krađa. Sama tehnologija VTK je postala komercijalna: moguće je angažovati hakere ili besplatno preuzeti potrebne softverske alate sa uslužnih servisa, dok se posebno dizajnirani maliciozni softver može kupiti ili iznajmiti. Kriminalna komercijalizacija botnet mreža, od njihovog nastanka 2004. godine, jedna je od najvažnijih karakteristika organizovanog VTK. Najnovije varijante botneta koje omogućavaju povezivanje sa uslužnim servisima (*Crimeware-as-a-service*), takođe su predmet prodaje na servisima interneta

[44: 76]. Drugi primer komercijalizacije ogleda se u otkrivanju i prodaji neotkrivenih mana u kompjuterskim kodovima, koji kriminalcima donose veliku dobit, ali sa druge strane, mogu da nanesu značajne štete žrtvama [32, 78].

Komercijalizacija organizovanog VTK ogleda se prvenstveno u nelegalnom ostvarivanju dobiti kriminalnih organizacija koje deluju u sajber prostoru, a koje ostvaruju delovanjem protiv finansijskih, privrednih, uslužnih i drugih organizacija i državnih institucija. Činjenica da je internet razvijan i dizajniran prvenstveno za vojne potrebe tako da se zaobiđu spoljašnji uticaji i kontrole, ostavila je prostor za mnoge zloupotrebe. Koristeći takve pogodnosti nastale su brojne kriminalne ekonomije u veoma kratkom vremenskom periodu [79: 201]. Naglom širenju organizovanog VTK doprinelo je i funkcionisanje onlajn ilegalnih tržišta čije je finansijske transakcije teško proceniti.

Prema navedenom istraživanju Ponemon Instituta, troškovi sajber bezbednosti za 2017. godinu porasli su u obimu od oko 23% u odnosu na 2016. godinu. Sajber bezbednost je tokom godine prosečno za jednu kompaniju narušavana oko 130 puta, a prosečni gubici su bili 11,7 miliona dolara po kompaniji (najveći gubitak je iznosio 77,1 milion dolara). Troškovi su varirali u odnosu na države, veličine kompanija, sektore delatnosti, vrste sajber napada i efikasnosti zaštite, a odnosili su se na: troškove usled gubitka ili krađe informacija; troškove prekida poslovanja; troškove oštećenja opreme; i, gubitak profita. Najveći obim troškova bio je na aktivnostima otkrivanja i otklanjanja posledica napada VTK (oko 55%), a zatim na troškove usled prekida poslovanja i istrage (oko 32%); prosečni troškovi po jednom računarskom mestu bili su četiri puta manji za velike kompanije (436$) nego za manje kompanije (1.736$). U odnosu na tip napada i učestalost incidenata, najveće troškove izazivaju napadi malvera, fišing i socijalni inženjering i napadi bazirani na Web-u. Ukupni godišnji troškovi po tipu napada su najveći za napade malverima, zatim za napade bazirane na Web-u i za DoS napade [77].

Organizovanost visoko tehnološkog kriminala

Još na početku XXI veka, kada je pojmu visokotehnološki kriminal pripisan pojam organizovani kriminal, među kriminolozima su nastala neslaganja i konfuzija oko toga da li je takav kriminal derivacija tradicionalnog organizovanog kriminala ili predstavlja evoluciju kriminala u onlajn prostoru [36, 39, 50, 68, 80]. Iako je postojalo nekoliko prijavljenih slučajeva organizovanog VTK, generalno nije bilo indicija da će VTK dostići nivo organizovanih bandi, ali je ostavljana mogućnost da će posebne forme organizacija delovati na granici između stvarnog i virtuelnog sveta. Pri tome nije bilo jasno da li će se i kako postojeće tradicionalne organizacije prilagoditi novim uslovima [39: 24-26]. Prema nekim autorima ova dilema još uvek nije razrešena, jer različite statistike ukazuju da se internet previše koristi za kriminalne aktivnosti, počevši od delovanja običnih prevaranata do krađa velikih količina novca, što predstavlja jedan od glavnih problema da se identifikuju izvršioci i upozna način njihovog organizovanja [11, 44]. Nekoliko studija koje su istraživale prisustvo tradicionalnih OKG i novoformiranih kriminalnih grupa u sajber prostoru [10, 20, 81, 82], svoja istraživanja zasnivala su na sekundarnim podacima, pri čemu je primenjivana veoma široka radna definicije organizovanog kriminala sa ekstremno niskim standardima, kako bi se različite forme organizovanja podvele pod ovu kategoriju kriminala

[11: 175]. Iako predstavljaju grupu koju čine tri ili više lica, izvršioci određenih krivičnih dela VTK ne mogu se po svim elementima "uklopiti" u koncepciju "organizovane kriminalne grupe" prema *Konvenciji UN protiv trans nacionalnog organizovanog kriminala* iz 2000. godine [83], posebno u delu koji se odnosi na „postojanje u određenom vremenskom periodu", jer pojedini izvršioci mogu u aktivnosti biti uključeni samo kratko vreme, dok drugi mogu biti angažovani u različitim vremenskim periodima.

Međutim, veliki broj istraživača organizovanog VTK, kao i institucija namenjenih za borbu protiv VTK, saglasni su da i tradicionalne kriminalne grupe usmeravaju svoje delovanje prema internetu koji im omogućava nove načine za vršenje kriminala [80, 84, 85, 86]. Tradicionalni koncept organizovanog kriminala, zasnovan na monolitnim, hijerarhijski i etnički baziranim grupama koje teže ostvarivanju profita oslanjajući se na podmićivanje i nasilje, može se smatrati zastarelim. Digitalna tehnologija je uslovila mrežne oblike organizacije i druge tipove kolektivnih akcija u sajber prostoru [12, 14, 87].

Mnogi kriminalci VTK nisu organizovani na tradicionalan način, već deluju kao labave onlajn mreže i deo su globalnog onlajn tržišta. Kriminalne grupe u sajber prostoru deluju u određenom vremenskom periodu, imaju labavije organizacione strukture i veću fleksibilnost, trans nacionalne su i imaju tendenciju da se sastoje iz manjeg broja članova [87: 40-41].

Onlajn kriminalno umrežavanje koje je omogućio internet je jedan od najvećih preobražaja kriminala, jer onlajn kriminalne društvene mreže predstavljaju osnov za pojavu globalne onlajn podzemne ekonomije [10: 54]. U organizovanju VTK značajnu ulogu imaju nelegalni društveni forumi na kojima se ostvaruju kontakti, vrši razmena znanja i veština između kriminalaca, organizuju kriminalne grupe i, kao osnovno, izvršava tržišna funkcija [13, 14, 88, 89]. Poseban oblik organizovanja VTK ispoljava se kroz delovanje na ilegalnim onlajn tržištima, koja ponekad predstavljaju i čitave kriminalne ekonomije, gde kriminalni proces može da obuhvata sve potrebne aktivnosti, od izvršenja inicijalnih kriminalnih dela do prenosa novca kriminalnoj organizaciji [12, 16, 90].

Specifičan oblik organizovanosti, iako ne predstavlja organizaciju ljudi, čine mreže zombi računara (botnet). One su najznačajniji novi oblik organizovanja kriminala, iako mogu da ih kreiraju pojedinci ili organizovane grupe; same po sebi ove mreže su oblik organizovanog kriminala kada se upotrebljavaju za nezakonite aktivnosti [32, 91].

Trans nacionalnost organizovanog visoko tehnološkog kriminala

Transnacionalni organizovani kriminal je pretnja za međunarodnu, nacionalnu i ljudsku bezbednost: na međunarodnom nivou vrši negativan uticaj na međunarodne institucije i norme kojima se održava međunarodni sistem; na nacionalnom nivou destabilizuje jedinstvo države, elemente vlasti i sistem bezbednosti; i, ima dubok uticaj na ljudsku bezbednost, a opasnosti su izloženi i mnogi pojedinci u svetu; to je fenomen koji se stalno menja i prilagođava spoljašnjim faktorima i tehnološkim i geopolitičkim promenama [92, 93].

Zabrinutost policijskih i drugih organa za borbu protiv kriminala zbog ekspanzije trans nacionalnog organizovanog kriminala, počela je tokom 90-tih godina XX veka kada su kriminalne aktivnosti u velikoj meri počele da prelaze državne granice [94: 205]. Lokalni i regionalni karakter kriminalnih grupa menja se u međunarodni ili transnacionalni karakter, što se vremenski preklopilo sa nekoliko značajnih međunarodnih događaja: spora-

zum o slobodnoj trgovini između severne Amerike i Evropske unije (1986); počeci primene sistema World Wide Web za povezivanje dokumenata na internetu (1990); raspad SSSR (1991) i komercijalizacija Kine (uključno i prijem Hong Konga od Velike Britanije, 1997). Ovi događaji, ali i njihovo kombinovanje sa drugim, manje značajnim događajima, podstakli su nastanak novih trans nacionalnih kriminalnih grupa, koje ulaze u strateške saveze sa drugim kriminalnim grupama radi dobijanja pristupa novim tržištima i korišćenja jedinstvenih kriminalnih veština [30: 6-7]. Slika o organizovanim grupama koje su stalno pokretne i racionalno deluju na međunarodnom nivou, u poslednje vreme je u mnogome promenjena, tako da je verovatnije da je njihovo delovanje usmereno na lokalni nivo (država, region), a da je umrežavanje i saradnja između grupa na preko graničnom i globalnom nivou postao njihov glavni oblik delovanja [95, 96, 97].

Prema Konvenciji UN iz 2000. godine [83] pod delovanjem trans nacionalnog organizovanog kriminala podrazumeva se da su krivična dela učinjena u više država, ili su u vezi i proizvode bitne posledice u više država i da je delo izvršila grupa za organizovani kriminal. Zbog toga što se niz kriminalnih aktivnosti može vršiti trans nacionalno i na organizovan način, da se tokom vremena menjaju lokalni i globalni uslovi i pojavljuju nove forme kriminala, Konvencija UN ne daje preciznu definiciju trans nacionalnog organizovanog kriminala, načina delovanja ili strukturu kriminalne grupe niti precizira zločine koji bi spadali pod organizovani kriminal, već samo navodi aktivnosti kriminalne grupe koje države treba da inkriminišu nacionalnim zakonima [79]. Međutim, definicija organizovanog kriminala, prema Konvenciji, ne opisuje u celini složenu i fleksibilnu prirodu moderne mreže organizovanog kriminala i delovanje OKG u kriminalnim ekonomijama u kojima su diktirani zakoni ponude i potražnje, sa tolerancijom društva na određene vrste kriminala kao što su prodaja falsifikovane robe i specifične prevare usmerene na javnu vlast ili velike kompanije [98: 13].

Postoje nastojanja da se na osnovu određenja trans nacionalnog organizovanog kriminala u Konvenciji UN, izvede i definicija trans nacionalnog organizovanog VTK: transnacionalni organizovani VTK je svaka kriminalna aktivnost koja je namerno učinjena od strane tri ili više lica sa zajedničkom namerom da se ostvari materijalna korist, stekne moć ili ostvare drugi nematerijalni interesi, pri čemu je izvršeno više od jednog krivičnog dela, a članovi grupe deluju zajednički u produženom vremenskom periodu; kao sredstvo se koriste IKT, a cilj može biti internet ili uređaj povezan sa internetom ili se internet upotrebljava kao instrument za izvršenje krivičnog dela koje je izvršeno ili je u vezi sa dve ili više država [69]. Ova definicija je „usamljena“, jer vodeći istraživači u ovoj oblasti ne daju konkretnu definiciju, već pažnju posvećuju kriminalnim grupama, njihovoj strukturi i karakteristikama delovanja [15, 39, 44, 99].

Transnacionalni karakter organizovanog VTK uočen je još početkom XXI veka, jer je na organizovani kriminal uticala trans nacionalnost postojeće infrastrukture IKT i Interneta, stvarajući pogodan ambijent za kriminalne aktivnosti. Ovakav ambijent OKG koriste prvenstveno za ciljane napade na žrtve u bogatim regionima, kada ostvaruju i znatno veće dobitke nego što bi ih ostvarili u sopstvenoj državi. Trans nacionalnosti VTK doprinose i velike razlike u zakonskom, regulatornom i političkom odnosu u različitim državama, kao i nedostatak višeg stepena međunarodne saradnje u procesuiranju i sprečavanju kriminala [100: 6-7]. Globalna proširenja interneta novim informacionim tehnologijama praćena su i širenjem različitih i geografski nepovezanih oblika kriminalnih aktivnosti [1: 44-45]. Osim jezika

i pojedinih adaptera za napajanje, računarska tehnologija u osnovi je ista u celom svetu: postoji veoma mala razlika između računara i mobilnih uređaja koji se prodaju u Americi, Evropi, Aziji ili Africi, a analogna situacija je i na internetu, gde standardizacija omogućava korisnicima širom sveta da pristupe istim sadržajima i uslugama [101].

Karakteristike organizovanog VTK proističu i iz uticaja drugih faktora koji olakšavaju ili na drugi način doprinose izvršenju, a koji nisu nužno sami po sebi kriminalne aktivnosti. Time se u aktivnosti VTK uključuju sadržaji povezani sa komunikacijama, finansiranjem, enkripcijom, Internetom stvari i socijalnim inženjeringom [102].

Kategorije krivičnih dela prema ulozi računara, mreža i interneta

Danas u istraživačkim krugovima postoje prihvaćeni stavovi o upotrebi IKT za izvršenje organizovanog VTK s obzirom na svrhu i način upotrebe računara i interneta u pripremi i izvršenju kriminalnog dela: pojedini autori navode dve kategorije [1, 20, 21], drugi autori smatraju da se krivična dela VTK, po ovom kriterijumu, mogu klasifikovati u tri kategorije [44, 55, 103]; dok se kod nekih autora javlja i klasifikacija na četiri kategorije krivičnih dela VTK [78]. Ovakva podela na kategorije krivičnih dela ima korene i u istorijskom razvoju VTK, kada su u pojedinim vremenskim periodima mogle da budu korišćene samo mogućnosti koje je pružao dostignuti nivo razvoja IKT.

Prema prvoj grupi autora, pojam visokotehnološki kriminal predstavlja tzv. „kišobran" termin koji se upotrebljava da opiše dve različite, ali ipak blisko povezane kriminalne aktivnosti: (a) kriminal omogućen sajber prostorom (*syber enabled crimes*); (b) kriminal zavisan od sajber prostora (*syber dependent crimes*) [21, 104]. Neki autori, navodeći kategorije organizovanih grupa koje eksploatišu napredak IKT, pored navedene dve kategorije kriminalnih aktivnosti, razmatraju i aktivnosti organizovanih grupa koje se sastoje od ideološki i politički motivisanih pojedinaca [105: 270].

Druga grupa autora smatra da postoji i među kategorija kada se tradicionalna krivična dela izvršavaju na novi način, tako da krivična dela razvrstavaju na tri kategorije: (a) tradicionalna krivična dela koja su izvršena na tradicionalan način u kojima se IKT upotrebljavaju samo kao pomoćna sredstva; (b) tradicionalna krivična dela izvršena upotrebom računarske mreže i na novi način; i (c) krivična dela koja se u pravom smislu reči mogu smatrati delima VTK, jer ih karakteriše automatizovana i široko rasprostranjena upotreba sajber prostora i Interneta [103: 45-49].

Treća grupa autora uvažava postojeću podelu na tri kategorije dodajući i novu kategoriju krivičnih dela koja su usmerena na platforme – računare i sisteme, kao što je distribucija botneta, koji olakšavaju izvršenje drugih krivičnih dela, ali direktno ne donose novac kriminalcima [78: 1].

Prema ulozi tehnologije u izvršenju krivičnog dela VTK, odnosno u zavisnosti od toga da li se internet koristi u izvršenju dela kao pomoćno sredstvo, a delo može biti izvršeno i bez njega uz upotrebu nekih drugih sredstava ili je internet neophodan za izvršenje kriminalne aktivnosti i bez njega takav zločin ne bi postojao, krivična dela se mogu razvrstati u dve osnovne kategorije [9: 10]:

Prvu kategoriju krivičnih dela čine ona dela koja su bila rasprostranjena i pre postojanja interneta sa današnjim sadržajem i mogućnostima i čije izvršenje nije direktno uslovljeno njegovim postojanjem niti upotrebom. To su tradicionalna krivična dela za čije izvršenje se koriste računari i mreže za komunikaciju ili prikupljanje informacija, a koja bi mogla biti izvršena i bez njihove podrške, kao što su: različiti oblici prevare (npr: prodaja nepostojeće, neispravne, falsifikovane robe ili robe koja ne zadovoljava standarde); krađa novca putem kreditnih kartica i bankarske prevare; investicione prevare (piramidalne šeme i lažne humanitarne i druge akcije); ugrožavanje intelektualne svojine, uključujući i neovlašćeno deljenje sadržaja zaštićenih autorskim pravima (filmovi, muzika, digitalizovane knjige, slike i računarski softver); objavljivanje, deljenje i/ili prodaja nepristojnih i zabranjenih seksualnih sadržaja; i, uznemiravanje, proganjanje, nasilje i različiti oblici iskazivanja mržnje i/ili klevete. Nove IKT pružaju nove mogućnosti za širenje kriminalnih aktivnosti u velikom obimu, gde je presudan veliki domet Interneta, automatsko umnožavanje sadržaja i velike mogućnosti prikrivanja i/ili prikazivanja lažnog identiteta izvršilaca dela [5: 10]. U ovu kategoriju se mogu uključiti i krivična dela koja su generalizovana i radikalizovana upotrebom novih elektronskih medija (pranje novca, krijumčarenje narkotika, onlajn kockanje), ali koja se mogu izvršiti i bez upotrebe Interneta.

Drugu kategoriju krivičnih dela čine dela koja su fokusirana na računar i čija meta su hardver i softver (elektronska infrastruktura) i mogu biti učinjena samo uz upotrebu računara, računarskih mreža ili drugih IKT. To su dela VTK zavisna od sajber prostora ili „čist" VTK koji obuhvata osnov samog interneta. Krivična dela su usmerena na računarske sisteme i računarske mreže i njihove baze podataka [1: 46], kao što su distribucija zlonamernog softvera (virusi, crvi, trojanci), DoS i DDoS napadi i različiti oblici izmena vizuelnog izgleda legitimnih veb stranica (*Website defacement*) [21: 4]. Kao specifičan oblik izvršenja krivičnih dela javljaju se ona dela koja su omogućena postojanjem botnet mreža, jer je njihov razvoj, kao mreža kompromitovanih računara koji pokreću programe pod eksternom kontrolom, transformisao neke vrste VTK, poput fišinga, u svetski podzemni ekosistem kojim upravlja organizovani kriminal, a trgovina botnetom je postala aktivnost sa visokim prihodima [45]; ove mreže su dostupne i na uslužnim servisima nelegalnih foruma i mogu se iznajmljivati. Botnet mreže se uspešno koriste i za distribuciju ransomvera (*ransomware*)[6] kada su napadi usmereni na više kompanija ili državnih institucija. Zajednica botnet mreža koristi najkvalitetnije računarske sisteme koji su vlasništvo korporacija, vladinih institucija i univerziteta.

Budući razvoj organizovanog visoko tehnološkog kriminala

Pored proizvodnje, distribucije i prodaje droga, imovinskog kriminala, trgovine ljudima i krijumčarenja migranata, jedna od najvećih budućih pretnji je i organizovani VTK, posebno nelegalno onlajn trgovanje dobrima i uslugama [98: 7]. Elektroenergetske mreže,

[6] Ransomveri (*ransomware*), zbog rasprostranjenosti i destruktivnosti, postali su jedna od najopasnijih pretnji VTK. Dostupni su na uslužnom servisu RaaS (*Ransomware-as-a-Service*) gde se prodaju ili izrađuju po zahtevu. U toku 2016. godine je detektovano 98 familija ransomvera [107]. Broj napada na privatne korisnike je smanjen, a povećan je na kompanije i to prvenstveno na finansijske institucije. Vrednost otkupa šifara je i do više milona dolara. Od aprila 2016. do marta 2017. godine, ransomverom je napadnuto oko 2,5 milona korisnika [72].

gasovodi, svi servisi (policija, hitna pomoć, vatrogasna služba), berza, kontrole letenja, snabdevanje vodom za piće, bolnice, ulična rasveta i drugo, zavisni su od IKT i funkcionisanja Interneta. Živi se u svetu bez granica gde pravosuđa ne poznaju nematerijalne „otiske prstiju i DNK" i gde je stopa uspešnosti detekcije pretnji 5%, a vreme detekcije stalno raste Kako će se u budućnosti države i vlade truditi da kontrolišu trans nacionalne mreže i osiguraju njihovu bezbednost za legitimnu upotrebu, tako će i novi kriminalci pokušavati da manipulišu i zloupotrebljavaju ove mreže za nezakonite ciljeve [54: 21-26].

Neke procene su da će godišnji troškovi nastali usled delovanja VTK, a koji uključuju nastalu štetu i uništene podatke, ukradeni novac, izgubljenu produktivnost, krađu intelektualne svojine, krađu ličnih i finansijskih podataka, pronevere, prevare, povratak na normalno poslovanje, forenzičke istrage, brisanje i obnavljanje hakovanih podataka i sistema i povreda reputacije, sa tri hiljade milijardi dolara u 2015. godini porasti na šest hiljada milijardi dolara u 2021. godini i da će globalna potrošnja na zaštitu i odbranu od VTK premašiti iznos od milijardu dolara godišnje [108]. Iako je 2017. godine dostignut rekord u investicijama za informacionu bezbednost, dogodili su se raznoliki napadi VTK, ugrožavanja podataka i gubitaka informacija, a za budućnost se ne mogu dati garancije da će povećani nivoi odbrane i troškova uspešno smanjiti nivoe izloženosti napadima VTK [105: 8].

Dva osnovna razloga zbog kojih se u budućnosti može očekivati povećanje broja krivičnih dela i pričinjene štete zbog VTK, a posebno organizovanog VTK, su: *prvo*, tehnologija VTK je postala pristupačna i potrebni alati za izvršenje kriminalnih aktivnosti su dostupni širokom spektru ljudi, a ne samo informatičkim stručnjacima, što daje mogućnost OKG da za neposredno izvršavanje kriminalnih aktivnosti angažuju veliki broj nekvalifikovanih pojedinaca; *drugo,* broj korisnika interneta u nerazvijenim regionima sveta je u stalnom porastu, a broj potencijalnih bogatih žrtava u razvijenim regionima je uglavnom nepromenljiv, što će izazvati povećan broj napada na njih, kada će svaki novi prestupnik imati mogućnosti da eksponencijalno poveća broj napada kroz sve veću automatizaciju koju omogućavaju novi alati i Internet [79: 203-204]. Opšte tendencije organizovanog VTK, pored ostalog, biće izražene kroz [109: 7-8]:

a) dalji razvoj ilegalnih onlajn tržišta;

b) rasprostranjene DDoS napade uslovljene prelaskom sa botneta na cloud infrastrukturu i korišćenje velike distributivne moći;

c) korišćenje bezbednih servera i neprobojnih sistema zaštite vlastitih resursa kriminalaca;

d) sukobljavanje velikih kriminalnih grupa organizovanog VTK;

e) povećanje broja napada baziranih na socijalnom inženjeringu;

f) elektronski napadi na kritičnu infrastrukturu kao što je snabdevanje, transport i usluge prenosa podataka;

d) hakovanje uređaja povezanih sa internetom sa direktnim fizičkim uticajem (na primer: komunikacija među automobilima).

Prema predviđanjima pretnji VTK do 2020. godine [109: 6-7], najefikasnije pretnje bi mogle da se svrstaju u nekoliko kategorija: (a) napadi za ostvarivanje novčane i druge koristi; (b) napadi radi špijunaže; (c) manipulacija podacima i mrežama; (d) uništavanje podataka; (e) zloupotreba procesne moći; (f) napadi alatima i tehnikama utaje. Žrtve kriminalnog delovanja će obuhvatati širok opseg, od pojedinaca, malih i srednjih preduzeća i kompanija, do kritičnih infrastruktura i odbrambenih sistema, a motivacija će se kretati u

rasponu od obične zabave do profitiranja stvaranjem komercijalnih i tehnoloških prednosti. Većina navedenih pretnji je prisutna i sada, ali će se pojaviti i novi izazovi kao što su pretnje protiv infrastrukture i trgovanja ljudskim organima, kao i nanošenje šteta stvarima povezanim na Internet.

Informaciono-komunikacione tehnologije: Prema prognozama koje je dao Mark Gudman (Marc Goodman), u budućnosti se može očekivati veliki napredak u razvoju i primeni IKT, što će dovesti do većeg nadzora pojedinaca i organizacija od strane moćnih kompanija i vlada, kao i stvaranje boljih mogućnosti za kriminalne aktivnosti: „budućnost VTK će biti eksponencijalna, automatizovana i trodimenzionalna" [54: 506]. Na razvoj organizovanog VTK u budućnosti mogla bi uticati tri ključna oblika tehnološkog razvoja: (a) mrežne tehnologije će se verovatno širiti i razvijati u bočne ogranke; (b) samobrišuće komunikacije omogućavaće veću anonimnost kriminalaca i brisanje dokaza kriminala; (c) upotreba kriptovaluta (Bitcoin, Robocoin, Dodgecoin, Litecoin i posebno Zerocoin) razviće alternativne sisteme za njihovu razmenu. Uticaj ovih tehnologije vremenom će se pojačavati korišćenjem *cloud* računarstva, jer povećanje računarske snage, povećanje kapaciteta skladištenja i smanjenje troškova, doprineće da kriminalci lakše izvršavaju složene i komplikovane zadatke sa velikim dobicima koji će se dalje povećavati, posebno pri primeni ransomvera i iznuđivanju [5: 336-338]. 3D štampanje će do kraja 2018. godine rezultirati sa preko 100 milijardi dolara gubitaka intelektualne svojine, a veštačka inteligencija bi mogla dostići nivo ljudske inteligencije do 2029. godine. Bio tehnologija, nano tehnologija, kvantna fizika i svemirska tehnologija su sledeće generacije bezbednosnih pretnji [54].

Softver: Taktika malvera, vektori napada i zlonamerna infrastruktura su u stalnoj transformaciji [106: 8]. U buduće, napadi ransomvera biće usmereni na finansijske institucije, za koje se procenjuje da će imati enormne gubitke. Ransomveri će se i dalje ubrzano razvijati, pretpostavlja se da bi mogli da budu korišćeni u novoj sferi – za podrivanje tržišta kriptovaluta, sa ciljem dugotrajnog izvlačenja dobiti. Takođe se pretpostavlja da će u primeni ransomvera biti uključeno više OKG i da će se povećati korišćenje insajdera u izabranim kompanijama i državnim institucijama [72]. Broj familija ransomvera se svake godine povećava, čemu ide u prilog i nastajanje novog servisa 2016. godine (*Ransomware-as-a-Service*). Nastanak i razvoj novog servisa uključuje i napredovanje programera malvera koji usavršavaju komplete alata za kreiranje i prilagođavanje novih familija ransomvera [107: 63]. Širok opseg imejlova koji sadrže maliciozni softver i razrađena tehnika velikih napada u vidu spam kampanja, kao i profit koji ovakav vid delovanja donosi napadačima, verovatno će se nastaviti i u buduće [106].

Internet stvari (IoT): Nove tehnologije će povećati broj uređaja povezanih na internet, broj komunikacijskih tokova i količinu podataka radi upravljanja „pametnim stvarima". To će pružiti mogućnost povećane eksploatacije od strane kriminalaca [5: 337]. Treba očekivati da će Internet stvarima biti dodeljene IP adrese i da će biti transformisane u informacione tehnologije, što će omogućiti daljinsku kontrolu bilo kog objekta na Zemlji. Procenjuje se da će razvoj interneta i pratećih tehnologija do 2020. godine dovesti do 50 milijardi stvari koje su povezane sa internetom (2013. godine bilo je oko 13 milijardi onlajn uređaja) [54]. Povećanje broja IoT i sve veća sofisticiranost njihovog sistema upravljanja, izazivaju troškove koji se za 2017. godinu procenjuju na 674 milijardi dolara. Usluge vezane za IoT biće druga po veličini kategorija tehnologije, praćena softverom i povezivanjem. Razvoj softvera biće usmeren na aplikativni softver zajedno sa softverom za anali-

tiku, IoT platformama i sigurnosnim softverom. Softver će biti najbrže rastući tehnološki segment za IoT i do 2021. godine očekuje se da će više od polovine investicija za projekte IoT biti uloženo u softver i usluge [75].

Kriptovaluta brzo postaje atraktivan cilj za kriminalce. Značaj kriptovaluta će se povećavati kako se povećava broj kriminalaca, koji će dobro razvijen sistem pranja novca primenjivati i u sajber prostoru [98: 7]. Neke vrste kriminala su već ustaljene, poput krađe novca pri e-plaćanju promenom adrese na koju se novac upućuje, kao i krađa sa kreditnih kartica. Može se očekivati povećan broj primene rasomvera radi blokade datoteka sa kriptovalutama i traženje otkupa, kao i napadi na veb stranice radi krađe kriptovaluta (zlonamerni „rudari"). „Rudarenje" će se proširiti širom sveta i očekuju se napadi na kompanije radi proširenja aktivnosti, što će uključiti i zaposlene (rudari insajderi) koji će koristiti resurse kompanija (električna energija i snaga računara) [72].

Napadi na organizacije i institucije: Napadi na finansijske institucije, zdravstvene ustanove i druge organizacije beležiće dalji rast, sofisticiranost i povećanje gubitaka. Neke specifične pretnje su [72, 98, 106]:

– Napadi na finansijske institucije odvijaće se sa ciljem povlačenja velike količine novca. Pogodnost napada čine bankarske preko granične transakcije i stvorene mogućnosti povlačenja novca u bilo kojoj finansijskoj organizaciji u svetu. Broj napadnutih institucija se stalno proširuje, OKG su prodrle u bankarsku infrastrukturu, sisteme poslovanja elektronskim novcem, razmenu kriptovalutnih sredstava, fondove za upravljanje kapitalom, pa čak i kazina. Znatno je prošireno otuđenje novca iz bankomata, što je potpomognuto korišćenjem usluga posebnog servisa malvera (*malware-as-a-service*) i doprinelo je povećanju broja kriminalaca koji su velikom većinom – neprofesionalaci, a očekuje se automatizacija napada upotrebom posebnih mini-računara. Jedna od glavnih meta napada OKG biće nove bankarske institucije koje svoje poslovanje zasnivaju na digitalnom poslovanju i mobilnim uređajima korisnika i poslovanje proširuju po celom svetu, posebno u zemljama u razvoju. Povećaće se broj i poboljšati sofisticiranost napada na računarske sisteme kompanija koje se bave transakcijama kriptovalute, čiji bezbednosni sistema nisu potpuno ispitani. Radi obezbeđenja većih količina novca za državne potrebe, mogu se očekivati i napadi OKG podržani od strane vlada nekih država. Razlog tome je odsustvo tradicionalnog bankarstva, širenje poslovanja bez granica i specifičnost komunikacija između banaka i klijenata koje se realizuju putem mobilnih aplikacija, što izaziva veliku izloženost narastućeg broja klijenata bez mobilnog bankarskog iskustva.

– Napadi na zdravstvene ustanove razvijaju se usled rastućeg korišćenja povezanih uređaja i sistema u zdravstvu i koji mogu ponuditi napadačima pristup velikom obimu ličnih podataka, a isti su uglavnom minimalno zaštićeni. Napadi će se zasnivati na odbijanju usluge ili putem ransomvera, koji jednostavno uništavaju podatke i predstavljaju sve veću pretnju za sve digitalizovane zdravstvene ustanove. Očekuje se više incidenata vezanih za napade ransomverom sa ciljem enkripcije podataka kao i blokiranja medicinskih uređaja i opreme: povezana medicinska oprema je često skupa, a ponekad i životno potrebna, što je čini glavnom metom napada i iznuđivanja.

Značajne promene desiće se i u aktivnostima kriminalnih organizacija VTK, počevši od prilagođavanja postojećih struktura novim tehnološkim uslovima, povećanja anonimnosti, poboljšanja zaštite komunikacija i sigurnosti izvršilaca krivičnih dela, do smena na onlajn kriminalnim tržištima i razvoja novih metoda i tehnika napada i eksploatacije žrtava.

Organizovani VTK će se u budućnosti razvijati u skladu sa razvojem IKT i novim kriminalnim mogućnostima koje one pružaju. Pojava i velika upotreba računarstva u oblacima povećaće snagu računara i mogućnosti skladištenja velike količine podataka i informacija korišćenjem objedinjene infrastrukture, što će predstavljati novu i stalnu pogodnu metu organizovanog VTK, kao i dobro utočište radi zaštite od organa gonjenja. Eksplozivno rastući broj stvari, uređaja i elementa infrastrukture koji su povezani i zavisni od interneta, pružiće nove mogućnosti za kriminalne aktivnosti. Razvoju organizovanog VTK doprineće dalji razvoj botnet mreža i preuzimanje sve većeg broja računara za DDoS napade, sve viši nivo obrazovanja elitnih IT kriminalnih profesionalaca i razvoj potrebnih softverskih alata, pre svega malvera i ransomvera, kao i razvoj i sve veća sofisticiranost tehnika i metoda njihove upotrebe.

Zaključak

U ovom radu nije bilo moguće u celini sagledati komplesnost organizovanog VTK, tako da rad predstavlja samo pokušaj da se prikažu njegovi pojedini značajni elementi i karakteristike, bez bitnijeg razmatranja kriminalnih grupa VTK. I pored težnje da se da širok pregled literature aktuelne po pitanjima transformacije VTK u organizovani oblik, zbog obimnosti značajne literature, u popisu literature prikazani su samo najznačajniji radovi.

Kao globalni zaključak i odgovor na pitanje da li je VTK postao organizovan ili se pojedini njegovi oblici samo izvršavaju na organizovan način, moguće je samo konstatovati da među istraživačima postoje različiti stavovi. Kao polazni kriterijum za određenje šta je organizovani kriminal i OKG, uglavnom se prihvataju određenja data u *Konvenciji protiv trans nacionalnog organizovanog kriminala* koju su donele UN 2000. godine [83].

Slična dilema je prisutna i oko klasifikacije kriminalnih dela prema ulozi interneta u njihovom izvršenju: da li su kriminalna dela koja su postojala i pre korišćenja interneta, a sad se izvršavaju na efikasniji način korišćenjem interneta kao pomoćnog alata ili sredstva, dela VTK, ili su dela VTK samo ona dela za koje je internet alat, sredstvo i meta izvršenja, kada se takav kriminal može smatrati *čistim* VTK.

Postoje obrazloženi stavovi da je internet promenio i samu prirodu kriminala, jer posmatrano sa tehnološkog aspekta, organizacija kriminala se odvija u sajber prostoru, kriminal je omogućen visokom tehnologijom i postignut je visok stepen automatizacije kriminalnih aktivnosti. Organizaciji i uspešnosti realizacije dela VTK, značajan doprinos dali su i razvijeni novi moduli interneta kao što su *WWW* sistem za komunikaciju, internet telefonska tehnika – VoIP i cloud računarstvo. Usled uticaja interneta i globalizacionih procesa, pojavile su se i nove pretnje u vidu informacionog oružja, novih vrsta katastrofa zbog grešaka ili zloupotreba globalnih IKT mreža i novih kriminalnih dela VTK, bilo da se ona izvršavaju pojedinačno ili organizovano.

Nedostatak pouzdanih empirijskih podataka o VTK i dalje doprinosi njegovom nedovoljnom razumevanju. Takođe su i dimenzije VTK malo poznate, uglavnom zbog virtuelnosti i „nevidljivosti" kriminala, složenosti digitalnih tragova i otežane ili onemogućene saradnje žrtava, kao i ograničenosti delovanja organa zakona u otkrivanju i gonjenju počinilaca, što stvara veliku tamnu brojku neotkrivenih, neprijavljenih, neistraženih ili nerešenih slučajeva.

Prognoze eksperata i međunarodnih bezbednosnih agencija ukazuju da se može očekivati dalji razvoj organizovanog VTK, prvenstveno zbog sve veće pristupačnosti tehnologija širokom spektru ljudi i mogućnosti da se za kriminalne aktivnosti angažuje veliki broj nekvalifikovanih pojedinaca, kao i zbog povećanog broja napada koji će biti posledica velike automatizacije koju omogućavaju alati i internet. Opšte tendencije organizovanog VTK biće izražene kroz dalji razvoj ilegalnih onlajn tržišta, rasprostranjenost DDoS napada korišćenje cloud infrastrukture, korišćenje bezbednosnih servera kriminalaca, povećanje broja napada baziranim na socijalnom inženjeringu, povećanje elektronskih napada na kritičnu infrastrukturu (snabdevanje, transport, prenos podataka) i hakovanje uređaja povezanih sa internetom. Postoje procene da će gubici usled delovanja VTK, pojedinačno ili kroz različite organizacione forme, u 2021. godini dostići šest milijardi dolara.

Literatura

[1] Sandywell, B. (2010). On the globalisation of crime: the Internet and new criminality. In Y. Jewkes, & M. Yar, (Eds.). *Handbook of Internet crime*. US, Portland: Willan Publishing, 38-66.

[2] Broadhurst, R. (2006). Developments in the global law enforcement of cyber-crime. *Policing: An International Journal of Police Strategies & Management*, *29*(3), 408-433.

[3] Savona, E. U., & Riccardi, M. (2015). (Eds.) *From illegal markets to legitimate businesses: the portfolio of organised crime in Europe. Final Report of EU co-funded Project OCP*. Organized Crime Portfolio. Milan: Transcrime.

[4] Wang, Q. (2016). A Comparative Study of Cybercrime in Criminal Law: China, US, England, Singapore and the Council of Europe. (Dissertation). Rotterdam: Erasmus Universiteit Rotterdam. Pristupljeno 28.05.2018. na https://repub.eur.nl/pub/94604/.

[5] Wall, D. S. (2017). Towards a Conceptualisation of Cloud (Cyber) Crime. In *International Conference on Human Aspects of Information Security, Privacy, and Trust*. Springer, Cham. 529-538.

[6] Forbes. (2017). Cyber Crime Costs Projected To Reach $2 Trillion by 2019. Pristupljeno 10.02.2018. na https://www.forbes.com/sites/stevemorgan/2016/01/17/ cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#7608d16a3a91.

[7] McCusker, R. (2012). Organised cybercrime: myth or reality, malignant or benign? In S. Manacorda (Ed.) *Cybercriminality: finding a balance between freedom and security* Milano, Italy:ISPAC, 107-116.

[8] McGuire, M. (2012). Organised crime in the digital age. *London: John Grieve Centre for Policing and Security*.

[9] Yar, M. (2013). *Cybercrime and society*. London: Sage Pubications Ltd.

[10] Lusthaus, J. (2013). How organised is organised cybercrime? *Global Crime*,*14*(1), 52-60.

[11] Lavorgna, A., & Sergi, A. (2016). Serious, therefore Organised? A Critique of the Emerging"Cyber-Organised Crime" Rhetoric in the United Kingdom. *International Journal of Cyber Criminology*, *10*(2), 170.

[12] Motoyama, M., McCoy, D., Levchenko, K., Savage, S., & Voelker, G. M. (2011). An analysis of underground forums. In *Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference*. *ACM*, 71-80.

[13] Yip, M., Shadbolt, N., Tiropanis, T., & Webber, C. (2012). The digital underground economy: A social network approach to understanding cybercrime. *Digital Futures.* Pristupljeno 13.04.2018. na https://eprints.soton.ac.uk/343351/1/yip_de2012_ submission.pdf.

[14] Ablon, L., Libicki, M. C., & Golay, A. A. (2014). *Markets for cybercrime tools and stolen data: Hackers' bazaar*. Rand Corporation.

[15] Leukfeldt, E. R. (2015). Organised Cybercrime and Social Opportunity Structures. A Proposal for Future Research Directions. *The European Review of Organised Crime*, *2*(2), 91-103.

[16] Holt, T. J., Smirnova, O., Chua, Y. T., & Copes, H. (2015). Examining the risk reduction strategies of actors in online criminal markets. *Global Crime*, *16*(2), 81-103.

[17] Broadhurst, R., & Choo, K. K. R. (2011). *Cybercrime and online safety in cyberspace* (Doctoral dissertation, Routledge).

[18] Koops, B. J. (2011), The Internet and its Opportunities for Cybercrime. *Tilburg Law School Legal Studies ResearchPaper Series No. 09/2011*, 715-754.

[19] Viega, J. (2012). Ten years on, how are we doing? (Spoiler alert: We have no clue). *IEEE Security & Privacy*, *10*(6), 13-16.

[20] Lavorgna, A. (2015). Organised crime goes online: realities and challenges. *Journal of Money Laundering Control*, *18*(2), 153-168.

[21] McGuire, M., & Dowling, S. (2013). Cyber crime: A review of the evidence. *Home Office Research report*, *75.*

[22] Brenner, S. W. (2010). *Cybercrime: criminal threats from cyberspace*. USA, Santa Barbara: An Inprint ABC-CLIO, LLC.

[23] Leukfeldt, E. R., Lavorgna, A., & Kleemans, E. R. (2017). Organised Cybercrime or Cybercrime that is Organised? An Assessment of the Conceptualisation of Financial Cybercrime as Organised Crime. *European Journal on Criminal Policy and Research*, *23*(3), 287-300.

[24] Wall, D. S. (2003). Cybercrimes and the internet. In D. Wall (ed.) *Crime and the internet*. London: Routledge.

[25] Николаева, А. Б., & Тумбинская, М. В. (2014). Киберпреступность: история развития, проблемы практики расследования. У*ТРУДЫ SORUCOM-2014. Третья Международная конференция Развитие вычислительной техники и ее программного обеспечения в России и странах бывшего СССР: история и перспективы,* 259-264.

[26] Goodman, M. D., & Brenner, S. W. (2002). The emerging consensus on criminal conduct in cyberspace. *International Journal of Law and Information Technology*, *10*(2), 139-223.

[27] Parker, D. B. (1989). *Computer Crime: Criminal Justice Resource.* Washington: National Institute of Justice.

[28] McQuade, S. C. (Ed.). (2009). *Encyclopedia of cybercrime*. London, Greenwood Press.

[29] Parker, D. B. (1976). *Crime by computer.* New York: Charles Scribner's Sons.

[30] Richards, J. R. (1999). *Transnational criminal organizations, cybercrime & money laundering: a handbook for law enforcement officers, auditors, and financial investigators [Elecrtonic version].* New York: CRC Press LLC.

[31] Lagazio, M., Sherif, N., & Cushman, M. (2014). A multi-level approach to understanding the impact of cyber crime on the financial sector. *Computers & Security*, *45*, 58-74.

[32] Grabosky, P. (2017). The evolution of cybercrime, 2006-2016. In T. J. Holt (Ed.), Cybercrime Through an Interdisciplinary Lens. NewJork: Routledge, 15-36.

[33] Bequai, A. (1978). *White-collar crime – a 20th crisis.* Lexington Books.

[34] Thackeray, G. (1985). Computer-related crimes: An outline. *Jurimetrics*, *25*(3), 300-318.

[35] Shea, T. (1984). The FBI goes after hackers. *Infoworld*, *6*(13), 38-39.

[36] Williams, P. (2001). Organized crime and cybercrime: Synergies, trends, and responses. *Global Issues*,*6*(2), 22-26.

[37] International Telecommunication Union (ITU). (2012). *Understanding cybercrime: Phenomena, challenges and legal response*. Pristupljeno 20.05.2018. na http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ Cybercrime%20legislation%20EV6.pdf

[38] Mann, D., & Sutton, M., (1998). >>NETCRIME: More Change in the Organization of Thieving. *British Journal of Criminology*, 38 (2), 201–229.

[39] Brenner, S. W. (2002). Organized cybercrime-how cyberspace may affect the structure of criminal relationships. *North Carolina, Journal of Law and Technology, 4*(1), 1-50.

[40] Lavorgna, A. (2013). *Transit crimes in the Internet age: How new online criminal opportunities affect the organization of offline transit crimes.* (Dissertation). University of Trento, Doctoral School of International Studies.

[41] Lavorgna, A., & Sergi, A. (2013). Types of organised crime in Italy. The multifaceted spectrum of Italian criminal associations and their different attitudes in the financial crisis and in the use of Internet technologies. *International Journal of Law, Crime and Justice*, *xx*, 1-17.

[42] Yar, M. (2012). Sociological en Criminological Theories in the Information Era. In E. R. Leukfeldt, & W. Ph. Stol (Eds.), *Cyber Safety: An Introduction* (pp. 45-55). Den Haag: Eleven International Publishing.

[43] Leukfeldt, E. R. (2014). Cybercrime and social ties. *Trends in organized crime*, *17*(4), 231-249.

[44] Wall, D. S. (2015). Dis-organised crime: Towards a distributed model of the organization of cybercrime. *The European Review of Organised Crime* 2(2), 71-90.

[45] Tropina, T. (2010). Cybercrime and Organized Crime. *Freedom from Fear Magazine*, *7*(3). Pristupljeno 20.05.2017. na http://f3magazine.unicri.it/?p=310.

[46] United Nations Educational, Scientific and Cultural Organization (UNESCO*). (2017). Globalisation*. Pristupljeno 01.05.2018. na http://www.unesco.org/new/en/social-and-human-sciences/themes/international-migration/glossary/globalisation/#topPage.

[47] Wall, D. S. (2007). *Cybercrime: The transformation of crime in the information age*. UK, Cambridge: Polity Press, 4.

[48] Леонов, А. П. (2005). *Актуальные проблемы информационной безопасности в контексте глобализации.* Pristupljeno 10.06.2018. na http://www.itsec.ru/doc/ leonov.doc.

[49] Леонов, А. П., и Черкасова, Т. В. (2004). О криминологических признаках организованной киберпреступности. Crime-research. ru А. Сухаренко (17.04.2004), 185-187. Pristupljeno 03.05.2018. na https://scholar.google.com.

[55] Wall, D. S. (2010). Criminalising cyberspace: the rise of the Internet as a'crime problem'. In Y. Jewkes, & M. Yar, (Eds.). *Handbook of Internet crime*. US, Portland: Willan Publishing, 88-103.

[51] Curran, J. (2010). Reinterpreting Internet history. In Y. Jewkes, & M. Yar, (Eds.). *Handbook of Internet crime*. US, Portland: Willan Publishing, 17-37.

[52] Franks, M. A. (2010). The Banality of Cyber Discrimination, or, the Eternal Recurrence of September. Denver Law Review Online, 87, 1-6.

[53] Weimann, G. (2004). *www.terror.net: How modern terrorism uses the Internet*. DIANE Publishing,United States Institute of Peace, 31.

[54] Goodman, M. (2015). *Future crimes: Everything is connected, everyone is vulnerable and what we can do about it*. Anchor. Pristupljeno 25.03.2018. na http://executivebookreview.com/wp-content/uploads/2017/04/Future-Crimes.pdf.

[55] Jewkes, Y., & Yar, M. (Eds.). (2010). *Handbook of Internet crime*. US, Portland: WillanPublishing.

[56] [Infowach. (2015). *191 million US voters' data exposed online.* Pristupljeno 20.13.2018. na https://infowatch.com/analytics/leaks_monitoring/5274]

[57] International Telecommunication Union (ITU). (2012). *Understanding cybercrime: Phenomena, challenges and legal response*.

[58] Felson, M. (2006). *The ecosystem for organized crime*. Helsinki: European Institute for Crime Prevention and Control, affiliated with the United Nations. HEUNI Paper No. 26, 1-20.

[59] Singh, J. (2014). Comprehensive solution to mitigate the cyber-attacks in cloud computing. *International Journal of Cyber-Security and Digital Forensics (IJCSDF)*, *3*(2), 84-92.

[60] Microsoft. (2018). Cybercrime: A story of vulnerability, deception, and security. Pristupljeno 03.04.2018. na https://www. microsoft. com/en-us/trustcenter/security/ cybercrime

[61] Dashora, K. (2011). Cyber crime in the society: Problems and preventions. *Journal of Alternative Perspectives in the Social Sciences*, *3*(1), 240-259.

[62] Гуров, А. И. (1992).Организованная преступность -не миф, а реальность.*Знание*, *79*.

[63] Gilinskiy, Y., & Kostjukovsky, Y. (2004). From thievish artel to criminal corporation: the history of organised crime in Russia. In C. Fijnaut & L. Paoli (Ed.) *Organised Crime in Europe: Concepts Patterns and Control Policies in the European Union and Beyond, Springer*. Netherlands: Springer, 181-202.

[64] Иванцов, С. В. (2009). Организованная преступность: системные свойства и связи (криминологическая оценка). (Автореферат диссертации). Москва: Российская академия правосудия.

[65] Шинкаренко, А. П. (2011). Организованная киберпреступность. Pristupljeno 02.06.2018. na https://scholar.google.com.

[66] Осипенко, А. Л. (2012). Организованная преступность в сети Интернет. *Вестник Воронежского института МВД России,* 3, 10-16.

[67] Grabosky, P. (2007). The internet, technology, and organized crime. *Asian Journal of Criminology*, *2*(2), 145-161.

[68] McCusker, R. (2006). Transnational organised cyber crime: distinguishing threat from reality. *Crime, law and social change*, *46*(4-5), 257-273. Pristupljeno 10.06.2018. na http://tees.openrepository.com/tees/bitstream/10149/115450/2/115450.pdf?origin= publication_.

[69] Li, Xianghia. (2015). Transnational Organized Crime in the Context of Internet. (Dissertation). Vienna: University of Vienna.

[70] Secureworks. (2017). Cyber Threat Basics, Types of Threats, Intelligence & Best Practices. Pristupljeno 03.04.2018. na https://www.secureworks.com/blog/cyber-threat-basics

[71] Silva, S. S., Silva, R. M., Pinto, R. C., & Salles, R. M. (2013). Botnets: A survey. *Computer Networks*,*57*(2), 378-403.

[72] Kaspersky Lab. (2017). An annual report by Kaspersky Lab. *Securelist*. Pristupljeno 10.04.2018. na https://securelist.com/ksb-review-of-the-year-2017/83338/

[73] Mell, P., & Grance, T. (2011). The NIST definition of cloud computing. Pristupljeno 03.05.2018. na http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145. pdf.

[74] Kebande, V. R., Karie, N. M., Michael, A., Malapane, S. M., & Venter, H. S. (2017). *How an IoT-enabled "smart refrigerator" can play a clandestine role in perpetuating cyber-crime.* In IST-Africa Week Conference (IST-Africa), 2017. IEEE, 1-10.

[75] Weber, R. H., & Weber, R. (2010). *Internet of things* (Vol. 12). USA, New York: NY, Springer.

[76] Internacional Data Corporation (IDC). (2018). FutureScape: Worldwide IoT Predictions. ICD. Pristupljeno 03.03.2018. na https://www.idc.com/getdoc. jsp?containerId= US43193617.

[77] Ponemon Institute. (2017). *Cost of cyber crime study*. USA, Traverse City: Ponemon Institute. Pristupljeno 03.05.2018. na https://www.accenture.com/us-en/insight-cost-of-cybercrime-2017.

[78] Anderson, R., Barton, C., Böhme, R., Clayton, R., Van Eeten, M. J., Levi, M., & Savage, S. (2012). Measuring the cost of cybercrime. Presented at the Workshop on the Economics of Information Security (WEIS), Berlin, Germany. Pristupljeno 25.04.2018. na http//weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf.

[79] United Nations Office on Drugs and Crime (UNODC). (2010). *The globalization of crime - A transnational organized crime threat assessment*. Vienna: United Nations publication.

[80] Tropina, T. (2012). The evolving structure of online criminality how cybercrime is getting organised. *Eucrim 4, 158-165.*

[81] Hutchings, A. (2014). Crime from the keyboard: organised cybercrime, co-offending, initiation and knowledge transmission. *Crime, Law and Social Change*, *62*(1), 1-23.

[82] Leukfeldt, E. R., Kleemans, E. R., & Stol, W. P. (2016). Cybercriminal networks, social ties and online forums: social ties versus digital ties within phishing and malware networks. *British Journal of Criminology*, *57*(3), 704-722.

[83] Narodna Skupština RS. (2001). Zakon o potvrđivanju konvencije Ujedinjenih nacija protiv transnacionalnog organizovanog kriminala i dopunskih protokola. Sl. list SRJ - MU, br. 6/2001.

[84] Choo, K. K. R., & Smith, R. G. (2008). Criminal exploitation of online systems by organised crime groups. *Asian journal of criminology*, *3*(1), 37-59.

[85] Broadhurst, R., Grabosky, P., Alazab, M., Bouhours, B., & Chon, S. (2014). Organizations and Cyber crime: An analysis of the nature of groups engaged in cyber crime. *International Journal of Cyber Criminology, 4*(1), 1-20.

[86] Europol. (2017). *Internet organized crime threat assessment*. Europol, EC3.

[87] Choo, K. K. R., & Grabosky, P. (2013). Cyber crime. In L. Paoli (Ed.), *Oxford Handbook of Organized Crime*. Oxford: Oxford University Press, 1-31.

[88] Samani, R., & Paget, F. (2013). Cybercrime Exposed Cybercrime-as-a-Service. *McAfee, Inc.* Pristupljeno 03.05.2018. na https://www.mcafee.com/us/resources/ white-papers/wp-cybercrime-exposed.pdf.

[89] Sui, D., Caverlee, J., & Rudesill, D. S (2015). The Deep Web and the Darknet: A Look Inside the Internet's Massive Black Box. USA, Washington: Wilson Center.

[90] Wehinger, F. (2011). The Dark Net: Self-regulation dynamics of illegal online markets for identities and related services. In *Intelligence and Security Informatics Conference (EISIC), 2011 European*. IEEE. 209-213.

[91] Chang, Y. C. (2012). *Cybercrime in the Greater China region: regulatory responses and crime prevention across the Taiwan Strait*. Edward Elgar Publishing.

[92] Lavorgna, A. (2003). Criminal Behavior in the Internet Age: The social organization of Transnational Organized Crime. *University of Torento–Italy*.

[93] Pikareli, Dž. T. (2012). Transnacionalni organizovani kriminal (567-583). U P. D. Vilijams (Ur.), *Uvod u studije bezbednosti*. Beograd: Službeni glasnik i Univerzitet u Beogradu - Fakultet bezbednosti.

[94] Albanese, J. S. (2007). *Organized Crime in Our Times (Fifth Ed),* New Jork: Anderson Publishing.

[95] Adamoli, S., Di Nicola, A., Savona, E. U., & Zoffi, P. (1998). *Organised crime around the world*. Helsinki: Heuni.

[96] Hobbs, D. (1998). Going down the glocal: the local context of organised crime. *The Howard Journal of Crime and Justice*, *37*(4), 407-422.

[97] Von Lampe, K. (2009). Transnational organised crime connecting Eastern and Western Europe: Three case studies. In K. Von Lampe (Ed.) *Crime, money and criminal mobility in Europe* (19-42). NL, Nijmegen: Wolf Legal Publishers.

[98] Europol. (2017). *European Union: Serious and Organised Crime Threat Assessment: Crime in the Age of Technology*. Europol*, EC3.*

[99] Lusthaus, J. (2012). Trust in the world of cybercrime. *Global crime*, *13*(2), 71-94.

[100] Sofaer, A. D., & Goodman, S. E. (2001). Cyber crime and security. The transnational dimension. *The transnational dimension of cyber crime and terrorism*, 1-34.

[101] Gercke, M. (2008). National, Regional and International Legal Approaches in the Fight Against Cybercrime. *Computer law review international*, (1), 7-13.

[102] Europol. (2017). *Internet organized crime threat assessment*. Europol, EC3. Pristupljeno 20.04.2018. na https://www.europol.europa.eu/iocta/2017/index.html

[103] Wall, D. S. (2008). Cybercrime, media and insecurity: The shaping of public perceptions of cybercrime. *International Review of Law, Computers & Technology*, *22*(1-2), 45-63.

[104] Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. *Journal in Computer Virology*, *2*(1), 13-20.

[105] Choo, K. K. R. (2008). Organised crime groups in cyberspace: a typology. *Trends in organized crime*, *11*(3), 270-295.

[106] European Union. (2018). *Threat Landscape Report 2017*. ENISA, European Union Agency For Network and Information Security.

[107] Symantec. (2017). *Internet Security Thteat Report*. Pristupljeno 28.03.2018. na https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf

[108] Cybersecurity Ventures. (2017). Cybercrime Report. Pristupljeno 10.04.2018. na https://cybersecurityventures.com/2015-wp/wp-content/uploads/2017/10/2017-Cybercrime-Report.pdf.

[109] Europol. (2017). *Project 2020 Scenarios for the Future of Cybercrime - White Paper for Decision Makers*. Europol, EC3.