DOI: 10.5937/vojdelo1807123D

# KRIMINALNE GRUPE ORGANIZOVANOG VISOKOTEHNOLOŠKOG KRIMINALA

*Anđelija* Đukić
Univerzitet u Beogradu, Fakultet bezbednosti

Globalizacioni procesi i razvoj Interneta omogućili su saradnju kriminalaca na globalnom nivou i stvaranje transnacionalnog organizovanog kriminala u sajber prostoru. Visokotehnološki kriminal je postao domen organizovanih grupa: tradicionalnih organizovanih kriminalnih grupa ili novih kriminalnih grupa koje se formiraju za delovanje u sajber prostoru, a zasnovane su na mrežnoj strukturi i labavim unutrašnjim vezama. Uloga i organizacija kriminalnih društvenih foruma na Internetu i stvaranje onlajn kriminalnih tržišta, očiti su dokaz nastanka novog oblika kriminala – organizovanog visokotehnološkog kriminala. Tradicionalne organizovane kriminalne grupe nisu u potpunosti iskoristile prednosti koje pruža Internet, jer nemaju odgovarajući alat za njegovu kriminalnu eksploataciju, ali ni tradicionalno ostvarivanu kontrolu nad fizički određenom teritorijom. Ove grupe uspešno koriste Internet kao pomoćno sredstvo i alat za izvršavanje tradicionalnih oblika kriminala. Umrežavanje kriminalaca koje je omogućio Internet jedan je od najvećih preobražaja kriminala, jer onlajn kriminalne društvene mreže, prvenstveno namenjene podršci kriminalnih aktivnosti, predstavljaju osnov za egzistenciju i razvoj onlajn kriminalnih tržišta, kao najorganizovanijeg delovanja kriminalaca u sajber prostoru. Ovaj rad predstavlja pokušaj da se, analizom odabrane literature iz ovog područja, identifikuju neki od organizacionih oblika delovanja kriminalaca u sferi visoko tehnološkog kriminala, prezentuju njihove osnovne odlike i mogući budući razvoj. Radom su obuhvaćeni i zaključci istraživanja prema relevantnim studijama o strukturi i funkcionisanja kriminalnih grupa, kao i drugi bitni elementi organizovanja kriminalaca u sajber prostoru.

Ključne reči: *organizovani visokotehnološki kriminal, organizovane kriminalne grupe, kriminalne mreže, onlajn kriminalni forumi, uslužni kriminalni servisi, onlajn kriminalna tržišta*

## Uvod

Globalizacioni procesi i razvoj Interneta predstavljaju osnov za razvoj organizovanog visoko tehnološkog kriminala (VTK) na transnacionalnom nivou. Komercijalizacija Interneta i razvoj novih modula kao što su WWW sistem za komunikaciju, internet telefonska tehnika – VoIP i računarstvo u oblacima (*Cloud computing*) doprinele su širenju i većoj uspešnosti izvršenja kriminalnih aktivnosti na mreži, a pojavile su se i nove

pretnje u vidu informacionog oružja, novih vrsta katastrofa zbog grešaka ili zloupotreba globalnih informaciono – komunikacionih tehnologija (IKT) i novih kriminalnih dela (VTK), bilo da se ona izvršavaju pojedinačno ili organizovano.

Postoji široka saglasnost u akademskoj zajednici i diskusijama eksperata za bezbednost da su sajber prostor (*cyber space*) i njegov integralni deo – Internet, ponudili mnogo novih mogućnosti za sve kriminalce, uključujući i organizovani kriminal. Pri razmatranju spajanja i ukrštanja VTK i organizovanog kriminala, mogu se pojaviti dva različita rezultata: organizovani VTK svoje delovanje ispoljava u sajber prostoru, prvenstveno na Internetu, i usmerava ga na računarske sisteme, mreže i podatke; i, za izvršenje dela tradicionalnog kriminala koriste se nove mogućnosti, gde konvencionalne organizovane kriminalne grupe (OKG) koriste Internet kao primarnu pomoć, iako ta pomoć nije neophodna za izvršenje kriminalne aktivnosti [1].

Internet je omogućio saradnju kriminalaca na globalnom nivou i stvaranje transnacionalnog organizovanog kriminala u sajber prostoru [2, 3]. Kriminalci koriste novu tehnologiju da komuniciraju, da se bolje organizuju, da prošire domen i usavrše tehniku i način delovanja (*modus operandi*) ili da izbegnu procesuiranje od strane nadležnih organa [4: 8]. Savremeni globalizacioni procesi stvaraju nove mogućnosti povezivanja kriminalaca, a računarske mreže postaju mesto, meta, cilj i sredstvo izvršenja kriminalnih aktivnosti [5, 6, 7]. Razvoj IKT i Interneta uticao je na povezanost kriminalaca i njihovo efikasnije delovanje širom sveta, na početku kao delovanje pojedinaca, a kasnije i kao delovanje kriminalnih grupa koje su koristile Internet da bi olakšale izvršenje dela u stvarnom svetu [8, 9, 10]. Prvi vidovi saradnje između hakera uočeni su još 1989. godine kada su napade na IKT sisteme institucija izvodili pojedinci koji su, preko ekstenzivne onlajn mreže, diskutovali o stvarima od zajedničkog interesa [11, 12]. Sprovedena istraživanja početkom XXI veka ukazuju da se, u to vreme, VTK poistovećivao sa delovanjem hakera i da nije bilo organizacija nivoa gangova (bandi), ali da postoje slučajevi delovanja organizovanog VTK na nižem nivou organizovanja [13: 24-25].

Najnovije statistike institucija koje prate organizovani VTK ukazuju na stotine miliona žrtava kojima su pričinjene štete i da je ovaj kriminal postao jedna od primarnih pretnji sa kojom se suočavaju nacije, korporacije i obični ljudi [14, 15, 16]. Ovo izaziva pitanje kako se VTK razvio u takav veliki problem uprkos decenijskim istraživanjima o kompjuterskoj bezbednosti. Problem sa trenutnom praksom bezbednosti na Internetu jeste i to što se ista previše razmatra kao tehnološki izazov, umesto da se prihvati kao širi socijalno – tehnološki fenomen, jer su ljudi centralni problem, kako sa stanovišta žrtava, tako i sa stanovišta kriminalaca [17]. Izazov koji je razvoj i sve veća primena IKT, ali i njihova zloupotreba, postavio pred istraživače društvenih i tehničkih nauka, zahteva holistički pristup. Potrebno je razumevanje funkcionisanja tehničkih sistema IKT, kako bi se smanjili efekti njihove zloupotrebe, ali je potrebno i razumevanje ponašanja i bihevioralnih razlika ljudi koje dovode do ovakvog ponašanja [18: 2]. Fokusiranjem samo na tehnologiju, efekti bezbednosti postaju ograničeni brzinom tehnološkog napretka koji donosi i nove ranjivosti računara i mreža, a koje kriminalci koriste. Ono što ostaje postojano tokom vremena, i u stvarnom i u virtuelnom svetu kriminala, su ljudi koji čine krivična dela, njihova motivacija i stavovi, njihovo ponašanje i okruženje u kome im je omogućen napredak [19]. Motivacija izvršilaca krivičnih dela VTK, uglavnom je lična finansijska dobit, ali postoje i druge motivacije kao što su zadovoljenje intelektualne radoznalosti ili izazova, opšta zlonamer-

nost, osveta, zadobijanje poštovanja i moći unutar onlajn zajednice ili jednostavno – dosada [20: 6]. Iako se njihovi zločini mogu počiniti u virtuelnom svetu, njihov profit i njihove žrtve su u stvarnom svetu [21].

Gotovo svi autori koji su istraživali VTK kao oblik organizovanog kriminala, konstantuju nepostojanje opšteprihvaćene definicije novog kriminalnog delovanja i njen nedostatak nastoje da otklone opisujući ovaj tip kriminala i navodeći njegove ključne karakteristike [3, 22, 23, 24, 25, 26, 27]. Pored karakteristika samog kriminala, u radovima se istražuju i svojstva i organizacija kriminalnih grupa koje vrše ovaj tip kriminala i daju se njihove klasifikacije [11, 23, 28, 29, 30]. Usled povezanosti i usklađenog dejstva članova kriminalnih organizacija, različite forme njihovog organizovanja često se nazivaju i kriminalnim mrežama [1, 13, 25, 31, 32, 33, 34].

Sve veći broj eksperata smatra da je VTK postao domen organizovanih grupa, da je vreme hakera pojedinaca prošlo, a da je malo poznatih činjenica o strukturama i trajanju takvih organizacija, kako je u njima osigurano poverenje ili kakav je odnos sa drugim vidovima kriminala [29: 4]. Sinergija između organizovanog kriminala i Interneta, povećala je nesigurnost digitalnog sveta [35, 36, 37]. Sajber prostor i Internet su omogućili OKG da koriste i prevare vezane za identitet ne bi li na taj način sakrili sopstveni identitet, zaštitili svoju imovinu od konfiskacije ili kao olakšicu za činjenje različitih prevara i drugih kriminalnih aktivnosti [38: 5].

Neke tradicionalne OKG svoje delovanje prenose iz stvarnog sveta u virtuelni svet ili se za izvršenje VTK stvaraju nove organizovane kriminalne grupe. Organizovani VTK i kriminalne mreže uključene u ovaj oblika kriminala, sve više privlače pažnju istraživača iz različitih disciplina, pa je tako sve više radova iz različitih naučnih oblasti koji se bave ovim fenomenom [30, 39, 40, 41, 42, 43].

Ovaj rad ima za cilj da na osnovu sagledane relevantne literature iznese viđenja strukture, funkcionisanja i drugih bitnih karakteristika kriminalnih grupa koje se bave organizovanim VTK, bez obzira na način njihovog organizovanja, ali i bez pretenzija da se iz toga izvode generalni zaključci.

## Kriminalne organizacije visokotehnološkog kriminala

Kao i sama pojava organizovanog VTK, ni organizacije koje se njime bave nisu u dovoljnoj meri poznate, jer su informacije o pojedincima, grupama i njihovim mrežama – ograničene [25, 44]. Pri izučavanju ovih grupa, istraživači se oslanjaju na slučajeve procesuiranih kriminalaca i ograničeni su prigodnim uzorkom [10, 45, 46]. Pojedini podaci prikupljaju se i analizom aktivnosti na indeksiranim (legalnim) i neindeksiranim (nelegalnim) forumima Interneta, tako da je u izučavanju kriminala oformljena i posebna oblast koja se bavi analizom društvenih mreža (SNA – social network analysis), čijom primenom se izbegavaju tradicionalne klasifikacije i empirijski se određuju strukture kriminalnih grupa [17, 47, 48, 49, 50, 51]. Nema sigurnih pokazatelja kako su ove grupe organizovane: da li kao tradicionalne OKG ili kao grupe koje isključivo vrše kriminalne aktivnosti u digitalnom svetu [13, 52, 53]. Većina ovih grupa može se poistovetiti sa ekonomijama (kriminalne ekonomije) kojima je krajnji cilj prisvajanje novca korišćenjem Interneta [45, 54, 55]. Delovanje OKG može biti usmereno na mete u virtuelnom svetu, mogu samo ko-

ristiti virtuelne alatke za delovanje protiv meta u stvarnom svetu ili mogu kombinovati mete u stvarnom i virtuelnom svetu [7, 52].

Čista hijerarhijska struktura u organizaciji kriminala, opovrgnuta je i kod klasičnih italijansko-američkih porodičnih kriminalnih zajednica (mafija), jer se novijim istraživanjima pokazalo da je struktura mnogo komplikovanija od proste piramidalne strukture [29, 30]. Za razliku od neslaganja istraživača po mnogim pitanjima u vezi sa organizovanim kriminalom, visok stepen koncenzusa u literaturi postignut je oko nekih karakteristika OKG, prvenstveno da su one prilagodljive i fleksibilne po prirodi i da su sposobne da koriste sve raspoložive prilike da zarade novac [56: 14]. U akademskim, stručnim i političkim krugovima postoji saglasnost da „tradicionalne" kriminalne grupe sve više napuštaju klasične metode izvršenja krivičnih dela i svoje delovanje preusmeravaju na krivična dela u sajber prostoru [6, 25, 29].

Izvršioci određenih krivičnih dela VTK, iako predstavljaju grupu od tri ili više lica, ne mogu se po svim elementima uklopiti u koncepciju „organizovane kriminalne grupe" prema *Konvenciji UN protiv transnacionalnog organizovanog kriminala*[1] [57], posebno po određenju koje se odnosi na „postojanje u izvesnom vremenskom periodu": neki izvršioci mogu biti samo trenutno uključeni u deo kriminalne aktivnosti OKG, dok drugi mogu biti angažovani u različitom trajanju i različitim vremenskim periodima. Ako se kao vreme organizovanog delovanja smatra i period internet komunikacije među počiniocima, izvršena kriminalna dela mogu se smatrati organizovanim kriminalom [58].

Kako su aktivnosti OKG VTK povezane sa komunikacijama članova grupa i zahtevaju komunikacionu platformu, jedno od prvih istraživanja u oblasti povezivanja izvršilaca krivičnih dela VTK, u vreme kada aktivne mreže, Internet i WWW modul nisu bili razvijeni, pokazalo je da su hakeri koji su delovali pojedinačno, koristili računarske mreže i oglasni sistem novinarske kuće BBC kako bi uspostavljali vezu sa drugim hakerima i razmenjivali iskustva [11: 49-53]. Kasnija istraživanja koja su bila usmerena na analizu strukture i funkcionisanja kriminalnih grupa, pokazala su da ilegalni društveni forumi na Internetu imaju izuzetno važnu ulogu u organizovanju kriminalnih aktivnosti VTK [40, 46, 59, 60, 61, 62].

## *Klasifikacija kriminalnih grupa visokotehnološkog kriminala*

Organizacione strukture OKG u sajber prostoru su veoma raznolike [25, 63, 64, 65], a njihova klasifikacija se može izvršiti na različite načine: prema lokaciji mete (u virtuelnom ili stvarnom svetu), prema jačini veza i odnosima između članova grupe [66], prema specifičnim aktivnostima kriminalne grupe [13] ili prema drugim kriterijumima [17, 29, 67].

Iz klasifikacije OKG koju je dao ruski akademik Aleksandar Ivanovič Gurov [68] i koja je široko prihvaćena u ruskoj literaturi, izdvajaju se tri nivoa organizovanja: I nivo

[1] "*Grupa za organizovani kriminal* označava organizovanu grupu od tri ili više lica, koja postoji u izvesnom vremenskom periodu i koja deluje sporazumno u cilju činjenja jednog ili više teških zločina ili krivičnih dela utvrđenih u skladu sa ovom konvencijom, radi zadobijanja, posredno ili neposredno, finanskijske ili duge materijalne koristi" (član 2. Konvencije).

– stabilne i upravljive zajednice sa funkcionalnom hijerarhijskom strukturom koje nemaju koruptivne veze (prvi i primitivni stepen organizovanog kriminala); II nivo – organizacije koje se grupišu i stvaraju savršeniju i po društvo opasniju strukturu, to su organizacije I tipa sa korupcijskim vezama sa državnim organima i organima vlasti; III nivo – kriminalne organizacije sa mrežnom strukturom, sa dva ili više nivoa upravljanja i sa prenešenim ovlašćenjima na niže nivoe upravljanja. Organizovani VTK može se pripisati organizacijama III nivoa, koje se kvalitativno razlikuju od organizacija prva dva tipa, pre svega u ustaljenosti lidera, boljoj organizaciji kriminalne sredine, podelama funkcija unutar organizacije, kvalitetom rukovođenja kriminalnim radom i direktnim učešćem u izvršenju određenih kriminalnih aktivnosti. U strukturi ovih grupa mogu se razlikovati osnovni elementi: (a) organizaciono i menadžersko jezgro, koje čine lideri kriminalnih grupa, a bavi se opštim upravljanjem i razvojem velikih operacija; (b) organizaciona i pomoćna grupa, koju čine lideri kriminalnih grupa sa bliskim okruženjem, a grupe imaju određene zadatke i užu specijalizaciju; i (c) neposredni izvršioci u svakoj kriminalnoj grupi [69, 70].

*Struktura kriminalne grupe* je ključni faktor u razmatranju njenog funkcionisanja. Jedna od prvih klasifikacija kriminalnih grupa za aktivnosti VTK prema njihovoj strukturi, predstavlja rezultat pilot istraživanja VTK u više zemalja koje je radila UNODC[2], a obuhvata pet ključnih tipova [71: 34]:

– *Standardna hijerarhija*: hijerarhijska grupa sa jakim unutrašnjim sistemom discipline i rukovođenja: jedan lider, grupa poznata po imenu, jak društveni ili etnički identitet, nasilje kao značajan faktor aktivnosti, često jak uticaj ili kontrola određene teritorije.

– *Regionalna hijerarhija*: hijerarhijski strukturirane grupe sa snažnim internim linijama rukovođenja, kontrole i discipline: pojedinačna struktura lojalnosti, linija komandi iz centra, autonomije na regionalnom nivou i više regionalno usmerenih aktivnosti, često jak društveni ili etnički identitet, nasilje je suštinskog značaja za aktivnosti.

– *Grupisana hijerarhija*: grupa kriminalnih grupa koje su uspostavile sistem koordinacije i kontrole od slabijeg ka jačem, retko se pojavljuju i sastoje se od više kriminalnih grupa: postoji upravna struktura za potčinjene kriminalne grupe, ciljevi centralne organizacije su najbitniji i jači od ciljeva nižih kriminalnih grupa, grupe imaju određeni stepen autonomije, struktura često formirana prema društvenom i istorijskom kontekstu.

– *Jezgrovita grupa*: relativno čvrsto organizovana, ali nestrukturirana grupa: ima organizaciono jezgro u kome je ograničen broj pojedinaca, oko koga se formira mreža pridruženih manjih grupa ili pojedinačnih članova: nizak nivo unutrašnje discipline, retko poznata po imenu, retko ima socijalni ili etnički identitet.

– *Kriminalna mreža*: labava i fluidna mreža pojedinaca, često sastavljena od osoba sa specifičnim znanjima i veštinama potrebnim za pojedine kriminalne projekte: isticanje značaja veština pojedinaca, lične lojalnosti pojedinaca sa vezama koje su važnije od etničke ili socijalne komponente, mrežni priključci čine savez oko nosilaca, vršenje reforme mreže ako istu napuste osnovni članovi mreže.

[2] UNODC – United Nations Office on Drugs and Crime (Kancelarija UN za pitanja droge i kriminala).

Klasifikacija koja je slična datoj, a zasnovana je takođe na empirijskim istraživanjima, jeste i klasifikacija koja je često navođena [66] i koja pokazuje različitost formi organizovanja u zavisnosti od toga da li su aktivnosti grupe usmerene na ciljeve u sajber prostoru, da li one samo koriste onlajn alate koji im omogućavaju kriminalne aktivnosti u stvarnom svetu ili u svom delovanju kombinuju onlajn i oflajn mete. Procenjeno je da polovina kriminalnih grupa VTK ima šest i više ljudi, a da je četvrtina od ukupnog broja grupa postojala manje od šest meseci. Studijom je predložena tipologija kriminalnih grupa VTK („najbolja pretpostavka“) od šest vrsta osnovnih struktura, koje se često ukrštaju na različite načine, slika 1. Tipologija uključuje tri glavna tipa organizacione strukture grupa, od kojih je svaki tip grupe, u zavisnosti od snage veza između članova, podeljen na dve podgrupe [66]:

I) Grupe I tipa funkcionišu u suštini na mreži i mogu se dalje podeliti na grupe sa strukturom rojeva (swarms) i čvorišta (hubs). Grupe deluju uglavnom u sajber prostoru, a poverenje među članovima se procenjuje na osnovu reputacije u nelegalnim aktivnostima na mreži:

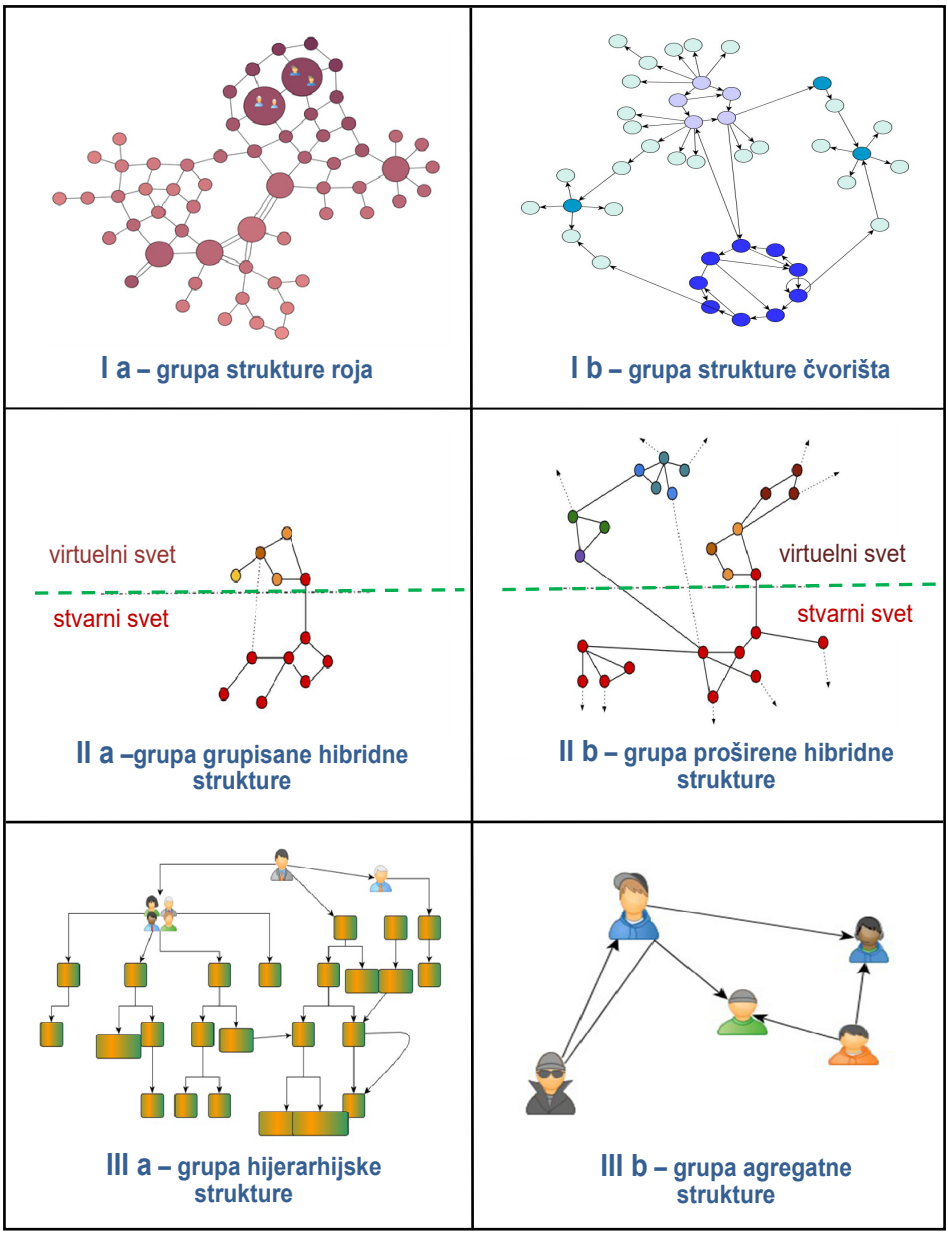
Ia) Grupe tipa Ia – *grupe sa strukturom roja* imaju karakteristike mreža i opisuju se kao „neorganizovane organizacije“ sa zajedničkom namenom i bez liderstva. Grupe poseduju minimalan lanac komandovanja. Čini se da su grupe sa strukturom rojeva najaktivnije u sajber aktivnostima koje su ideološke prirode, poput zločina mržnje na mreži i političkih otpora. Grupe kao rojevi su velike, kolektivne, nedovoljno organizovane, najčešće sastavljene od kratkotrajnih manjih podgrupa pojedinaca.

Ib) Grupe tipa Ib – *grupe sa strukturom čvorišta* su aktivne na mreži i imaju jasno definisanu funkciju komandovanja. Grupe su sastavljene od članova u čvoru strukture (žarište) oko koga se okupljaju periferni saradnici. Njihove onlajn aktivnosti su raznovrsne, uključujući pirateriju, fišing napade, botnet mreže i onlajn seksualno nasilje. Grupe oformljene na čvorišnoj strukturi, često se uključuju u distribuiranje skrivenog softvera. Ovakvu strukturu, verovatno, poseduju nelegalna tržišta podataka o kreditnim karticama i tržišta narkotika. Osnovna obeležja su centralna komandna struktura, koja može biti hijerarhijski ustrojena, i jake veze među pojedincima.

II) Grupe II tipa su hibridi (hybrids) koje aktivnosti kombinuju u sajber prostoru i stvarnom svetu. Podgrupe koje egzistiraju, imaju strukturu grupisanih hibrida (clustered hybrids) i strukturu proširenih hibrida (extended hibrids):

IIa) Grupe tipa IIa – *grupe grupisane hibridne strukture* aktivnosti artikulišu oko male grupe pojedinaca i fokusiraju se na specifične aktivnosti i metode. One su donekle slične grupama sa strukturom čvorišta, ali se njihove aktivnosti nalaze između kriminala na mreži i van nje. Tipične grupe ovog tipa su one koje se bave prevarama sa kreditnim karticama, kada koriste podatke za onlajn kupovine ili prodaju podatke putem karding mreža.

IIb) Grupe tipa IIb – *grupe proširene hibridne strukture* funkcionišu na sličan način kao grupisane hibridne grupe, ali su mnogo manje centralizovane. One obično uključuju mnogo saradnika i podgrupa i sprovode različite kriminalne aktivnosti uz zadržavanje određenog nivoa koordinacije potrebnog za uspeh.




Slika 1 – *Tipovi grupa organizovanog visoko tehnološkog kriminala prema organizacionoj strukturi (prilagođeno prema: [66, 72]).*

III) Grupe III tipa obavljaju aktivnosti uglavnom van mreže, ali onlajn tehnologiju koriste za pomoć u oflajn aktivnostima. MekGvajer smatra da ovaj tip grupa treba uzeti u razmatranje jer sve više doprinose digitalnom organizovanom kriminalu. Podkategorije ove grupe, u odnosu na stepen povezanosti i organizacije, su grupe sa hijerarhijskom strukturom (hierarchies) i agregatnom strukturom (aggregates):

IIIa) Grupe tipa IIIa – *grupe hijerarhijske strukture* se najbolje opisuju kao tradicionalne kriminalne grupe (npr. kriminalne porodice) koje obavljaju neke onlajn aktivnosti, kao na primer: tradicionalna umešanost nekih mafijaških grupa u prostituciju sada se produžava i na pornografske veb stranice, uključivanje u onlajn kockanje, iznude i ucene pretnjama o blokadama računarskih sistema ili pristupanje privatnim zapisima pomoću napada malverima ili hakovanjem.

IIIb) Grupe tipa IIIb – *grupe agregatne strukture* imaju labavu organizaciju, privremene su i često bez jasne svrhe. Članovi ovakvih grupa koriste digitalne tehnologije na *ad hoc* način, što ipak može da nanese štetu. Primeri uključuju korišćenje mobilnih telefona da bi se koordinirala aktivnost bandi ili poremećaji u javnosti.

Ove klasifikacije daju osnov da se organizovanost VTK razmatra sa aspekta delovanja tradicionalnih kriminalnih grupa, koje mogućnosti Interneta još uvek ne koriste u dovoljnoj meri, i, sa aspekta drugih organizacionih formi koje deluju u sajber prostoru. Prema tvrđenjima pojedinih savremenih istraživača, među kojima je i Roderik Brodharst (Roderic Broadhurst), konvencijalna koncepcija organizovanog kriminala je zastarela, kao i klasični organizacioni „modeli mafije“ kao etnički zasnovane, monolitne i hijerarhijski strukturirane organizacije kojom rukovodi jedan čovek [29: 2]. Devedesetih godina XX veka istraživači organizovanog kriminala su počeli da tvrde da aktivnosti čvrsto struktuiranih trajnih OKG postepeno preuzimaju labave koalicije manjih kriminalnih grupa koje deluju u kraćem vremenskom periodu, a ideju vertikalno integrisanih organizacija je preuzela metafora mreže [36: 64]. Eksteritorijalnost sajber prostora, principi slobodnog globalnog tržišta i uvođenje elektronskog poslovanja, doprineli su ustrojstvu OKG za aktivnosti organizovanog VTK [38: 9].

## *Tradicionalne organizovane kriminalne grupe u sajber prostoru*

Organizovane kriminalne grupe spoznale su vrednost informacija i IKT i njihovu ulogu u olakšavanju izvršenja krivičnih dela [38: 9]. Na početku XXI veka, pre nego što je postalo očigledno da raste moć društvenih mreža, pojavila su se istraživanja o strukturi organizovanog VTK [73, 13]. Postoje određeni pokazatelji koji ukazuju da su Internet, u toj fazi razvoja, i postojeći forumi za zabavu, olakšavali aktivnosti organizovanog VTK i da organizaciona struktura OKG nije obavezno hijerarhijski ustrojena, nego može da ima i izmenjenu i slobodniju (fluidnu) formu [73]. I pored postojanja slučajeva organizovanog VTK, generalno nije bilo indicija da će ovaj oblik kriminala poprimiti obeležja organizovanog kriminala, već da će delovati na granicama virtuelnog prostora [13].

Logika sugeriše da bi Internet, sa mogućnostima za ostvarivanje velikih kriminalnih profita sa malim rizicima, trebalo da privuče i tradicionalne OKG, jer su one uvek pokazivale značajne sposobnosti prilagođavanja novim tehnološkim mogućnostima [74: 11-12]. Neke od ovih grupa se postepeno okreću od tradicionalnih kriminalnih aktivnosti prema

profitabilnijim i manje rizičnim operacijama u sajber prostoru [75], ali kako mnoge vrste VTK zahtevaju visok stepen organizacije i specijalizacije, nema dovoljno dokaza da li u aktivnostima VTK učestvuju OKG i kakav oblik ili strukturu one mogu da imaju.

Uprkos sugestijama o postojanju organizovanog kriminala na Internetu, osporavanja učešća tradicionalnih OKG u aktivnostima VTK, baziraju se na: *prvo*, ove grupe ne poseduju odgovarajući alat za rad na Internetu, osim pojedinih sredstava prinude kao što su DDoS napadi i iznuđivanja; *drugo*, sa konceptom tradicionalnog organizovanog kriminala povezano je posedovanje teritorije i kontrola te teritorije, što Internet ne omogućava, osim ako se pod tim ne podrazumeva kontrola nad serverima ili botnetom; *treće*, postoji problem u formiranju čvrstih grupa na mreži sa sopstvenim integritetom i otpornošću na veće pritiske konkurencije i organa zakona, ali je moguće da će neke od ovih organizacija obezbediti organizovano i stabilno prisustvo u sajber prostoru, ali samo kao lažnu onlajn manifestaciju, a inače će praktično delovati u stvarnom svetu [63: 58-59].

U kojoj meri će OKG koristiti Internet kao sredstvo i kakvi su primenjeni modeli, zavisi od osposobljenosti grupa i vrste osnovnih kriminalnih aktivnosti, prema čemu se tradicionalne OKG mogu smatrati poslovnim OKG ili OKG u stilu mafije [1: 157].

– *Poslovne OKG* (business-like groups) imaju mnogo zajedničkih karakteristika sa legalnim komercijalnim poslovanjem, jer se bave nelegalnom transnacionalnom trgovinom. Grupe deluju kao oportunistički ekonomski agenti i nije im važno čime trguju ako tom trgovinom ostvaruju profit. Ove grupe mogu da budu veoma heterogene: od dugotrajno uspostavljenih kriminalnih mreža do labavih kriminalnih organizacija kojima upravljaju mladi lideri. Koristeći prednosti Interneta ove grupe mogu da posluju na transnacionalnom nivou, tako da je fizička lokacija aktera manje važna nego ranije. Pružaju im se mogućnosti delovanja u državama sa prazninama u zakonodavstvu i bezbednosti, a lako se mogu povezati sa udaljenim kriminalnim vršnjacima [76].

– *OKG u stilu mafije* (mafia-style groups) bave se širokim spektrom kriminalnih aktivnosti povezanih sa podzemnim ekonomijama, od trgovine ljudima do iznuđivanja, ali i aktivnostima legalne ekonomije i javnog sektora, zbog infiltracije u lokalnu socijalnu sredinu. Za ove OKG je značajno da njihove aktivnosti u velikoj meri zavise od povezanosti i fizičkog prisustva na teritoriji. Postoje dokazi da ove grupe koriste Internet u trgovini ljudima, kockanju i pranju novca, ali nema pokazatelja korišćenja za druge kriminalne aktivnosti [1: 157-158].

Neka istraživanja, sprovedena anketiranjem žrtava, pokazuju da oko 25% ispitanika smatra da su krivična dela VTK izvršile OKG [20]. Slična zapažanja iznose i Internet provajderi koji smatraju da je sve više ciljanih a ne nasumičnih napada, što ukazuje na organizovane napade. Postalo je vrlo verovatno da su tradicionalne OKG shvatile vrednost IKT i počele da ih koriste za olakšavanje ili poboljšanje načina vršenja kriminalnih aktivnosti u stvarnom svetu ili na granici između stvarnog i virtuelnog sveta: IKT se koriste radi lakše trgovine drogom, trgovinu korporativnim tajnama i ličnim podacima, vršenje iznuda, prevara i prevara na mreži, pranja novca uz upotrebu sistema za plaćanje putem Interneta, kao i za distribuiranje nelegalnog sadržaja putem mreže [28: 39]. Tradicionalne OKG, kao što su italijanska mafija, japanske jakuze, kineske triade i kolumbijski karteli narkotika, preusmerile su svoje resurse iz uobičajenih kriminalnih aktivnosti na kriminal u sajber prostoru kako bi, uz veću anonimnost i ograničenu policijsku kontrolu, lakše došli do profita [77: 33]. Neke od ovih grupa direktno su povezane i sa piraterijom računarskog softvera i falsifikovanjem kreditnih kartica [28: 39-40]. Ove OKG se sve više uključuju u

VTK, tako da je opovrgnut ranije naglašavan stav da ove grupe ne mogu same da deluju na Internetu jer im nedostaju obučeni IT stručnjaci koje moraju da angažuju kao pomagače za kriminalne aktivnosti u fizičkom, a ne u virtuelnom svetu [3: 270].

Međutim, neki autori navode da nema dovoljno dokaza da tradicionalne OKG pokreću aktivnosti na Internetu, osim da su pojedine razvile onlajn pomoćne alate za neke od svojih klasičnih kriminalnih aktivnosti, kao što je kockanje [63, 78]. Korišćenje ransomvera, fišinga i drugih oblika VTK ne pokazuje znake klasičnog organizovanog kriminala i delovanje mafije, već sličnost sa virtuelnim komercijalnim modelom, što navodi na to da je organizacija kriminala izvan tradicionalnih OKG [25: 85]. Logično je da se smatra da mogućnosti koje pruža Internet treba da budu atraktivne i za tradicionalne OKG; međutim, empirijske razlike između fizičkog sveta i sajber prostora, verovatno su tako značajan faktor da sprečavaju efektivan prenos određenih postojećih kriminalnih aktivnosti iz stvarnog u virtuelni svet, jer nema naznaka da su se OKG do sada prilagodile korišćenju raspoloživih mogućnosti Interneta [1].

Na osnovu velikog uzorka poznatih slučajeva VTK, Majkl MekGvajer (Michael McGuire) je utvrdio da oko 80% izvršenih dela VTK može da bude rezultat nekog oblika organizovanog delovanja. To ne znači da ove grupe imaju oblik tradicionalnih OKG sa hijerarhijskom strukturom ili da ove grupe vrše isključivo VTK. Tradicionalne OKG proširuju svoje aktivnosti na digitalno okruženje, uz nove oblike organizovanja, prvenstveno kao labavije strukture kakve su kriminalne mreže [66]. Sa nedostatkom pouzdanih podataka o OKG VTK, i pored prisutnih sugestija o organizovanom kriminalnom ponašanju u sajber prostoru, treba ostaviti mogućnost formiranja ovakvih grupa, a uzimajući u obzir specifičnosti sajber prostora, od ovih grupa ne bi trebalo očekivati da budu onlajn replika tradicionalnih OKG [63: 59].

## *Organizovane kriminalne grupe za delovanje u sajber prostoru*

Mnogi kriminalci VTK nisu organizovani na tradicionalan način, već deluju kao labave onlajn mreže i deo su globalnog podzemnog onlajn tržišta, gde se, pored ostalog, može trgovati i tehničkim alatima ili uslugama potrebnim za sajber napade [79: 165]. Ovi pojedinci se udružuju u labave organizacione forme, ne veže ih hijerarhijska struktura i vlast i moć pojedinaca, rade zajedno kao slobodni članovi grupe, a vreme trajanja organizovane grupe je kraće nego kod tradicionalnih OKG. Ove karakteristike nisu svojstvene organizaciji nelegalnih onlajn tržišta kod kojih je prisutan određeni stepen hijerarhijskog rukovođenja radi održavanja stabilnosti tržišta i poverenja klijenata [63: 53]. Drugi autori ne isključuju postojanje hijerarhije u kriminalnim grupama, jer se time ostvaruju veći efekti kriminalnog rada [80, 81].

Kriminolozi i praktičari sve više usvajaju mrežne perspektive za istraživanje kriminalnih pojava, tako da se, od devedesetih godina XX veka, sve veći broj definicija organizovanog kriminala bazira na mrežnoj strukturi OKG. Istovremeno se formalna analiza mreža sve više koristi za proučavanje interakcija među kriminalcima [65: 2]. Mrežna organizacija je idealan način organizovanja kriminalaca zbog brojnih pogodnih karakteristika [36], a pored ostalog, omogućava brzo usvajanje novih tehnoloških promena, čime se usavršavaju kriminalne aktivnosti, i veoma brzo reagovanje na promene zakona i ponašanja organa za sprovođenje zakona [23: 107].

Široko rasprostranjena i nekritička pretpostavka da su Internet i društvo „bačeni na kolena“ od strane organizovanih kriminalnih grupa tipa mafije, nije podržana istraživanjem organizacije onlajn kriminalnih grupa za koje se smatra da se bave organizovanim kriminalom. Takve organizacije su identifikovane kao neorganizovani ili distribuirani modeli organizacije, a ne kao grupe sa hijerarhijskom komandnom i kontrolnom strukturom [25: 71]. Osporavanje organizovanog VTK, osim onlajn kriminalnih tržišta, bazira se na nekoliko odlika kriminalnih grupa: *prvo*, onlajn kriminalne grupe su male, labavo strukturirane i bez jasnog programa; *drugo*, čvrsto strukturirane kriminalne grupe koje imaju elemente da postanu OKG, mogu biti uključene u prevare, hakovanje, DDoS napade i druge aktivnosti, ali ovi kriminalci se bave jednostavnim prevarama i nisu sposobni da organizuju upravljanje i ozbiljan rad u grupi [63: 54-55].

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. Kriminalni imaju važnu ulogu za funkcionisanje kriminalnih mreža kao mesta gde se sreću digitalni prestupnici, pronalaze specijalizovani saradnici i/ili vrše kupovine malvera potrebnog za izvođenje napada. Oni predstavljaju najvidljiviji i najdokumentovaniji oblik organizovanog VTK po modelu kojim se želi „preslikana mafija“ i uglavnom funkcionišu kao veb stranice [63: 54].

Osnovna razlika između tradicionalnih OKG i kriminalnih grupa VTK ogleda se u informacionoj prirodi, mrežnoj organizacionoj strukturi i globalnom dometu VTK. Kriminalne grupe koriste nove umrežene tehnologije koje su relativno jeftine, tako da su početni troškovi relativno mali, a kako deluju u sajber prostoru i ne treba im „zaštitnik“ za poslovanje, izbegavaju da im se nametne uticaj tradicionalnih OKG. U suštini, kriminalci VTK se suprotstavljaju svakom tradicionalnom modelu organizovanog kriminala, izbegavaju kontrolu od strane tradicionalnog organizovanog kriminala na isti način na koji izbegavaju i kontrolu organa zakona [25: 72-73].

Kriminalne grupe, iako su specijalizovane za niz različitih aktivnosti, pokazuju mnoge slične organizacione karakteristike, tako da su prilično kratkotrajne i amorfne u smislu organizacije i fleksibilne u skladu sa trenutnim zahtevima i mogućnostima. Izgleda da grupe imaju odliku samoodrživosti, jer su reaktivne u odgovorima na delovanje okruženja, a po strukturi su skoro slične strukturama malih gazdinstava. Često ih vodi pojedinac ili vrlo mala grupa ljudi [25, 34, 66].

Kako je za uspešnu realizaciju dela VTK potreban širok spektar znanja i veština, kriminalci su uspostavili međusobnu saradnju trgujući robama i uslugama potrebnim za ostvarivanje kriminalnih aktivnosti, a pojavila su se i regrutovanja potrebnih talentovanih kadrova sa univerziteta [17]. Kriminalci koji se bave VTK, na osnovu znanja i sposobnosti kojima raspolažu radi preduzimanja sajber napada, mogu se klasifikovati u tri kategorije [82]:

(a) mala i elitna grupa pojedinaca koji poseduju velika znanja, sposobni su da se upuste u sofisticirane napade, da identifikuju nove ranjivosti računarskih sistema i razviju nove alate i tehnike za preduzimanje sajber napada;

(b) grupa polukvalifikovanih hakera, brojnija od prve, koji su sposobni da koriste visoko stručne alate i tehnike, ali nemaju znanja, veštine i inovacioni potencijal za kreiranje sopstvenih alata; i

(c) grupa nekvalifikovanih hakera, najveća prema ovoj klasifikaciji, sastavljena je od hakera koji poseduju malo znanja i alata za izvršenje ozbiljnijih napada VTK.

Struktura kriminalnih mreža je fluidna i sastavljena je od jezgra mreže (čvorišta), stalnih profesionalnih saradnika, regrutovanih saradnika i lica za prenos novca [81]. Sastav grupe je relativno mali i odražava MekGvajerovu analizu organizacije onlajn kriminala [66: 58], naročito centričnih tipova grupa sa mrežnom strukturom: tipovi rojeva ili čvorišta. Pojedini članovi grupe mogu biti istovremeno i članovi drugih kriminalnih grupa, pa čak i tradicionalnih OKG [25: 85]. Sastav mreža je fiksan samo u jezgru grupe u kome su osnovni (ključni) članovi grupe, dok ostali članovi čine promenljivi deo mreže i redovno se menjaju, a osnovnu strukturu grupe čine [25, 63, 81]:

– *Jezgro grupe* može da čini pojedinac ili manja grupa ljudi, a osnovna funkcija jezgra je da pokreće i rukovodi kriminalnim aktivnostima. U okviru jezgra može postojati hijerarhija, ali ona nije izražena kod većine grupa. Istaknuti članovi jezgra iniciraju i koordiniraju napade, upravljaju i kontrolišu ostale članove mreže i podgrupe ključnih članova mreže i izvršavaju sekundarne kriminalne aktivnosti. Ostali članovi jezgra sa saradnicima rade na izvršenju i eksploataciji napada, zaključno sa prenosom novca u jezgro mreže.

– *Izvršioci napada* su lica izvan jezgra grupe koja se regrutuju ili su angažovani profesionalci, sa aktivnostima kao što su snabdevanje imejl adresama, izrada malvera, razvoj fišing sajtova, snabdevanje lažnom dokumentacijom, prenos novca, zamena valuta, pomoć u pranju novca.

– *Pomagači* čine deo osoblja koji može biti angažovan iz kompanija koje su mete napada (banke i druge finansijske institucije) i iz kompanija preko kojih se obezbeđuje druga potrebna podrška (telefonske kompanije, Internet provajderi).

– *Prenosači novca* izvršavaju prenos novca preko sopstvenih računa ili kurirskom službom, a za to se angažuju osobe koje uživaju poverenje članova jezgra.

Kriminalne mreže mogu se ocenjivati prema više kriterijuma, kao na primer, prema: (a) primenjenoj tehnologiji i stručnosti članova, njihovoj užoj ili široj specijalizaciji; (b) načinima, učestalosti i karakteristikama interakcija sa žrtvama; i, (c) internacionalnom karakteru mreže koji uključuje razmatranje da li je član grupe iz inostranstva i da li radi u inostranstvu, kao i da li je žrtva iz inostranstva. Na osnovu primenjene tehnologije i osposobljenosti, kriminalne mreže se ne mogu lako i oštro podeliti na dve granične kategorije koje imaju potpuno različite karakteristike: slabo tehnološki i kadrovski osposobljene grupe (mreže sa nerazvijenom tehnologijom) i specijalizovane grupe (visoko tehnološke mreže), jer postoji mnogo varijanata između graničnih mreža.

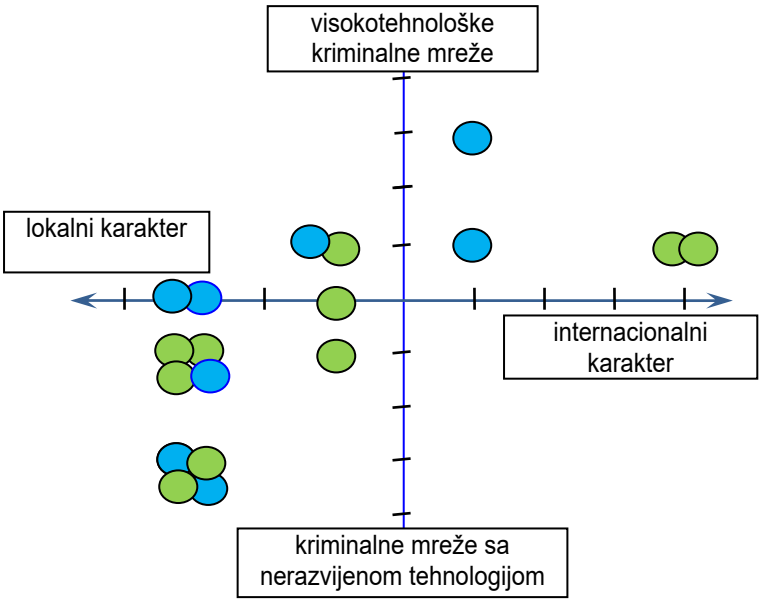
Međuzavisnost svojstava grupa[3] prikazana je na slici 2: *x-osa* predstavlja stepen do koga mreža ima međunarodne komponente, a na *y-osi* je prikazan stepen tehnološke razvijenosti. Posebno, plavom bojom su prikazane kriminalne mreže sa specijalističkim kadrom koji je usko specijalizovan za jedan tip napada, dok su zelenom bojom prikazane kriminalne mreže koje u svom sastavu imaju opšte obrazovan kadar. Sa slike 2 je vidljivo da postoji jasna razlika između mreža sa visokom tehnologijom i mreža koje poseduju nerazvijenu tehnologiju: mreže koje koriste nerazvijenu tehnologiju nemaju žrtve u dru-

[3] Istraživanje kriminalnih mreža [81] obuhvatilo je organizacije koje vrše različite oflajn i onlajn kriminalne radnje, sa osnovnim usmerenjem na fišing delovanje i onlan bankarstvo. Analizirano je 18 kriminalnih mreža na osnovu dokumentacije policijskih istraga koje su obuhvatile kriminalne mreže i bankovne poslovne računarske mreže u Holandiji za period 2004-2014. godine. Ove kriminalne grupe bave se i aktivnostima povezanim sa prevarama, napadima na finansijske transakcije u kojima se IKT ne koriste, trgovinom ukradenom robom, čak i drogom, trgovinom ljudima, prevarama sa kreditnim karticama i drugim kriminalnim aktivnostima.

gim državama i članovi jezgra i glavni pomagači su iz iste države i deluju u okviru nje; visoko tehnološke mreže imaju više međunarodnih komponenti, tako da četiri mreže imaju internacionalni karakter po pitanju ključnih članova i/ili pomagača, a žrtve su iz različitih zemalja, dok dve mreže nemaju internacionalni karakter i aktivnosti sprovode na državnom nivou. Razlike među mrežama ispoljavaju se tako da [81]:

a) mreže sa nerazvijenom tehnologijom svoje aktivnosti usmeravaju na lokalne žrtve (unutar države) i pri tome su prinuđene da ostvaruje određene interakcije sa žrtvama, čime povećavaju mogućnost da im budu otkrivane namere;

b) visoko tehnološke mreže su sposobne da izvrše napad bez značajne interakcije sa žrtvom (uglavnom je nema), imaju više mogućnosti i koriste ih za napade izvan državnih granica i sastoje se od manjeg broja osnovnih članova i iznajmljenih saradnika.




Slika 2 – *Međuzavisnost karakteristika delovanja kriminalnih grupa (prilagođeno prema: [81])*

Sofisticirana struktura mreža i pristup glavnim operacijama koje se dodeljuju samo proverenim članovima OKG, sprečavaju otkrivanje kriminalnih mreža, koje mogu uključivati od desetak do nekoliko hiljada članova. Bez obzira na broj članova i filijala, mreže pokreće mali broj iskusnih onlajn kriminalaca koji deluju kao preduzetnici. Neke elitne kriminalne mreže deluju kao zatvorene organizacije i ne učestvuju na onlajn forumima, jer poseduju dovoljno sredstava za stvaranje i održavanje lanca vrednosti za ceo ciklus izvršenja dela VTK [75]. Mnogi od najpoznatijih kriminalaca VTK odustaju od komunikacija na javnim forumima i prelaze duboko u podzemlje, na zaštićene ili privatne kanale, gde se formira jezgro organizacije od stalnih članova koji postaju karijerni kriminalci [21].

# Kriminalni forumi i tržišta na Internetu

Pored brzog širenja Interneta, globalizacionih procesa i digitalizacije ekonomskih aktivnosti, jedan od ključnih faktora koji doprinosi naglom širenju VTK u svetskim okvirima je funkcionisanje onlajn podzemnog tržišta, gde kriminalci sa lakoćom pribavljaju potreban alat za vršenje dela VTK, kao i usluge obrazovanog i visokostručnog kadra, što omogućava veću efikasnost i fleksibilnost rada [17, 38]. Pribavljanje efikasnih tehničkih rešenja putem Interneta, posebno zbog činjenice da su u porastu broj i kvalitet usluga koje se nude na uslužnim servisima (*as-a-service*), a cene usluga se smanjuju, omogućava OKG da se fokusiraju na druge aspekte delovanja [83: 3]. To je dovelo do nastanka pojmova kao što su *ekonomija onlajn kriminala* (*economy of online crime*) [31], *globalna industrija VTK* (*global cybercrime industry*) [47], *ekonomija VTK* (*cyber crime economy*) [84] ili *ekonomija digitalnog podzemlja* (*digital underground economy*) [17].

Verovanja da pretraga na Guglu (*Google*) može, za određeni predmet, identifikovati većinu informacija koje su dostupne na Internetu – nisu osnovane: postoji celi onlajn svet, ogroman i izvan Gugla ili bilo kog drugog opšte poznatog pretraživača. Procenjeni broj neindeksiranih veb stranica na Internetu, na mreži koja je poznata kao *duboka mreža* (*Deep Web*)[4], mogao bi da bude 400 do 500 puta veći od broja indeksiranih veb stranica smeštenih na *površinskoj mreži Interneta* (*Surface Web*). Masa podataka koji se čuvaju na samo 60 podzemnih *Deep Web* lokacija je oko 40 puta veća od mase podataka koji se čuvaju na svim legalnim površinskim lokacijama; „duboka mreža Interneta ujedno je i njegova tamna strana koja cveta“ [85: 5]. Deo duboke mreže Interneta koriste i ljudi koji poštuju zakone (novinari, politički disidenti), kao i legalne organizacije, prvenstveno za svoje arhivske materijale, ali jedan njegov deo, poznat kao *tamna mreža* (*Darknet*)[5], postao je kanal za ilegalne kriminalne aktivnosti.

Onlajn forumi i podzemna tržišta u različitim oblicima postoje već više decenija: inicijalni *Internet Relay Chat* (IRC), stvoren 1988. godine, na početku je funkcionisao kao mreža od 35 do 40 posebno aktivnih servera i obezbeđivao je razmenu informacija o raspoloživim robama i uslugama i njihovim cenama (ukradene kreditne kartice, brojevi bankovnih računa, pranje novca, gotovinske usluge, botnet) [59, 86]. Kanali IRC postoje i danas, ali u osavremenjenom dizajnu i sa novim funkcijama koje obezbeđuju aktivnosti kriminalaca. Tokom vremena, sa širenjem obima informacija i usluga, mnoga od ovih tržišta su počela da koriste javno dostupne forume, na kojima se obično nude ukradeni podaci sa kreditnih kartica i drugi bankovni kredincijali, kao i sve vrste malvera [40, 87]. Korišćenje legalnih foruma od strane kriminalnih aktera, kasnije je odjednom smanjeno i kriminalci su se preorijentisali na distributivne mreže koje nisu indeksirane kod legalnih pretraživača, tako da je *Deep Web* naglo proširen i sada sadrži najviše svežih informacija na Internetu. Tome je doprineo i razvoj IKT, *cloud* računarstvo i masovna upotreba mobilnih uređaja, napredak u razvoju sigurnosnih sistema koji obezbeđuju anonimnost i upotreba kriptovaluta [85: 7].

[4] *Deep Web* ili *Deep Net* (duboka mreža) ili *Hidden Web* (sakrivena mreža) je termin za pretragu sadržaja na Internetu koji nije indeksiran od strane standarnih pretraživača. Duboka mreža je suprotnost površinskoj mreži (*Surface Web*).

[5] *Darknet* (tamna mreža) je mreža Interneta kojoj se može pristupiti samo određenim softverom, konfiguracijama ili autorizacijom, često koristeći nestandardne komunikacijske protokole i portove.

U oblasti podzemnog tržišta ili drugih vidova profitabilnog udruživanja kriminalaca na Internetu, do sredine 2000-tih godina je dolazilo do brojnih onlajn neprijatnosti po žrtve, pojedince i organizacije, koje su izazvali hakeri (brisanje veb stranica, pisanje i distribucija zlonamernog softvera, prevare kreditnim karticama i slično). Nakon toga je hakerska zajednica postepeno ojačavala i pojavila su se podzemna tržišta. Za ovaj period je karakteristično naglo širenje računarskih virusa i crva: na početku radi dokazivanje znanja programera, da bi kasnije njihova distribucija počela da nanosi velike štete računarima i sistemima, tako da je oko polovine kriminala imalo digitalnu ili elektronsku pozadinu [45: 45]. Nakon 2004. godine javlja se ekonomija VTK kao ozbiljna ekonomska delatnost koja ne predstavlja „mali biznis", već se kriminalci udružuju u kriminalne mreže – onlajn podzemna tržišta (crna tržišta – *black markets*) [31: 3-4]. Aktivnije se koriste malveri za pronalaženje ranjivosti računarskih sistema i daljinski protokoli za pristup, plasiraju se kompleti softvera za eksploataciju tuđih računarskih sistema (*exploit kits*), a na tržištu dominiraju bolje organizovane i strukturirane grupe sa više unutrašnje discipline. Ove grupe biraju specifične ciljeve za napad, obično profitabilne kompanije ili finansijske institucije [45: 46].

U analizama zajedničkih odlika i razlika između podzemnih tržišta i podzemnih foruma, mnogi autori ova dva pojma poistovećuju [45, 49, 61]. Prema sagledanoj literaturi, čini se da bi forumi imali nešto šire funkcije, bar po pitanju prenosa znanja i drugih poslovnih i privatnih kontakata i ćaskanja. Takođe, pojmovno je dosta teško razdvojiti delovanje organizovanih grupa VTK i funkcionisanje podzemnih onlajn nelegalnih tržišta, s obzirom na veliku podudarnost poslova koji se obavljaju, ali usled podele poslova i prema tome ko su neposredni izvršioci krivičnih dela, može se ustanoviti da ove kategorije imaju velika preklapanja, ali i razlike. Postoje mišljenja da je samo organizacija kriminalnih onlajn tržišta ona organizacija čije aktivnosti bi se mogle smatrati organizovanim VTK, dok su sve druge organizovane kriminalne aktivnosti izvan koncepcije organizovanog kriminala [63].

## *Nelegalne društvene mreže na Internetu – forumi*

Široko umrežavanje koje je kriminalcima omogućilo da koriste nove mogućnosti, ne bi bilo moguće bez posredstva Interneta [17, 25, 31, 88]. Da bi se olakšala ova potreba za umrežavanjem, formirane su mnoge podzemne društvene mreže na Internetu [79, 86, 89]. Društveni forumi se od strane kriminalaca koriste na različite načine: za oglašavanja roba i usluga, za razmenu znanja, pružanje pomoći početnicima ili za stvaranje novih kontakata, a većina foruma ima trgovinske odeljke, uključujući i aukcije ukradene robe [46, 61, 80].

Kriminalni forumi ili onlajn mesta za sastanke kriminalaca, najmanje predstavljaju mesta za sastanke i uglavnom se koriste kao polazne tačke za VTK. Većina mreža je potekla iz fizičkih kontakata, jer su članovi odrasli zajedno, počeli da rade zajedno, pohađali isti univerzitet ili bili zajedno u zatvoru. Druge mreže nastaju iz onlajn kontakata, ali je nepoznato kada i gde su ti kontakti otpočeli. Forumi su ključna mesta na kojima se pronalaze saizvršioci sa potrebnim kvalifikacijama, znanjima i veštinama. Prisustvo strukture upravljanja od vrha prema dnu hijerarhijske lestvice, sa deljenjem uloga i obaveza, ukazuje na to da postoje timovi ili čak formalne organizacije koje upravljaju forumima ili kanalima [62].

## *Funkcije nelegalnih foruma*

Forumi imaju višestruku ulogu u funkcionisanju organizovanog VTK, ali se mogu izdvojiti tri osnovne uloge – funkcije: socijalna funkcija, funkcija učenja i tržišna funkcija [46: 2-4].

*Socijalna funkcija*: forumi su mesta gde se kriminalci mogu sastajati i formirati nove saveze, što olakšava razvoj i rast kriminalnih mreža. Formiranje partnerstava prevazilazi usluge kupovine zlonamernog softvera ili usluga prenosa novca: na forumima se spajaju kriminalci različitih profila i znanja, tako da kriminalne organizacije (kriminalne mreže) za pojedine vrste poslova koriste specijalizovane profesionalce koje pronalaze i angažuju na forumima [46: 3-4].

*Funkcija učenja*: forumi se koriste za razmene informacija među kriminalcima, što se smatra delom subkulture, posebno među hakerima, pri čemu se razmenjuju i specifična znanja. Mali broj kriminalaca ima tehnička znanja za primenu alata koje su drugi kreirali, ali znanje polako prelazi iz grupe stručnjaka u niže slojeve kriminalaca. Pretpostavlja se da puno znanja i stručnosti u subkulturi VTK dolazi iz malog procenta kriminalaca koji imaju veoma visok stepen tehničke stručnosti [62: 27]. Većina foruma omogućava slanje poruka drugim članovima, kao i deljenje informacija i učenje od drugih članova („univerziteti podzemnog sveta") [90].

*Tržišna funkcija* se ostvaruje kroz funkcionisanje podzemnih tržišta koja uglavnom koriste dva specifična i dominantna tipa kanala [61]: (a) Internet Relay Chat (IRC), kao poznati, popularni i legalni kanali za ćaskanje, vremenom su nadograđeni novim funkcijama potrebnim za kriminalnu delatnost kreiranjem sopstvenih pravila protokola, zaštitom od spamera i nepozvanih prodavaca i aktivnim nadzorom administratora; b) veb forumi, kao specifičan oblik onlajn društvenih mreža, za razliku od otvorenih soba za ćaskanje na IRC, uglavnom su zatvorenog tipa ili ograničenog pristupa. U odnosu na aktivnosti koje su ranije ostvarivane na kanalima IRC, podzemni forumi (*underground forums*) su omogućili veću stabilnost tržišta i mogućnost njegove regulacije [49: 210].

Pojedine lokacije na Internetu (*Deep Web, Dark Net, Secret Web, Invisible Internet*), pored ponude piratskih sadržaja, predstavljaju i tržišta droge, falsifikovanog novca, ukradenih bankarskih kartica i računa, ukradene raznovrsne robe, ukradenih identiteta, ličnih dokumenata, oružja, municije, eksploziva, video zapisa seksualnog zlostavljanja dece, trgovine ljudima i ljudskim organima i drugom „robom" [77: 223]. Podzemna mreža se upotrebljava i u legalne svrhe kao što to čine novinari, uzbunjivači, politički disidenti i zagovornici ljudskih prava [85: 7]. Vrlo labavo postavljene organizacije koje su uključene u tranzitni kriminal deluju veoma efikasno. Za mešovite organizacije, gde su zastupljene i tradicionalne OKG, zahtevaju se i veće organizacione sposobnosti za uspešno funkcionisanje organizacije. Mnoge od ovih organizacija, iako su ranije koristile i otvorene veb stranice, počele su sa korišćenjem skrivenih veb stranica (*Deep Web*), koje su nedostupne velikom delu internet populacije [74: 12-13]. Virtuelni forumi mogu godinama da rade na jedinstvenim lokacijama i zajedno sa legitimnim sajtovima [59].

Neki od ovih foruma su specijalizovani i počeli su da koriste i zatvorenu varijantu, tako da je pristup novih članova moguć samo uz odobrenje ili preporuku postojećih članova ili se roba i usluge nude samo na privatnim forumima koji mogu biti i usko specijalizovani [91]. Cilj postojanja ovih foruma je i proširenje baze znanja učesnika i proširenje skupa potencijalnih partnera u trgovini. Postupak pristupa pojedinaca mreži ima svoje vremensko trajanje i proceduru: kandidati čekaju u grupi za pristup, vrše se provere kan-

didata, a po pozitivnom ishodu provera, pristupa se „novoj“ grupi odakle je omogućeno i dalje napredovanje, što donosi članovima i veća ovlašćenja, a time se i forumi sve više proširuju [60: 74][6].

## *Uslužni servisi*

Servisi na mreži se mogu smatrati „crnim“ ili „sivim“, zavisno od toga ko su korisnici usluga i kakve su im namere [45], tako da se kao „sivi“ servisi mogu klasifikovati servisi na kojima je teško odrediti aktivnosti ili stvarne kupce. Model kriminalnog servisa kriminal-kao-usluga (*Crime-as-a-Service – CaaS*) predstavlja novu opasnost od kriminala uopšte, a posebno od VTK, jer omogućava lak pristup alatima i uslugama čitavog spektra VTK, od ulaznog nivoa do vrhunskih profesionalaca, uključujući i druge aktere kao što su haktivisti, pa čak i teroristi [92: 29]. Na forumima postoji mnogo vrsta usluga (servisa) koje potencijalni kriminalci mogu koristiti, kao što su [83: 4-5]:

– *Usluge istraživanja* za razliku od drugih servisa, ne moraju poticati iz ilegalnih izvora, već mogu postojati i u okviru sivog tržišta. Predstavljaju istraživanje i identifikaciju ranije nepoznatih ranjivosti u ciljanim računarskim sistemima. Istraživanja ranjivosti, uključno i istraživanja ranjivosti nultog dana[7] (*zero-day vulnerabilities*), vrše zlonamerni i plaćeni pojedinci ili organizacije, ali se istim poslom bave i legalne komercijalne kompanije koje prodaju rezultate istraživanja organizacijama koje su vlasnici računarskih Sistema [31]. Na tržištu se pojavljuju i pojedinci (brokeri) koji preprodaju takvu intelektualnu svojinu kupcima - kriminalcima. Zbog različitih aktera uključenih u istraživanja i plasman rezultata, ovakvo tržište se smatra „sivim“ tržištem.

– *Usluge kriminalnog softvera* podrazumevaju prilagođavanje postojećeg softvera stvarnim potrebama, izradu novog softvera, ili jednostavno – prodaju ili pozajmicu postojećeg softvera[8]. Usluge uključuju razvijanje koda za iskorišćavanje specifičnih ranjivosti računarskih sistema i izradu raznih tipova softvera (za prikrivanje malvera, za dostupnost računarskim sistemima radi finansijskih prevara, za hakovanje računarskih sistema i drugo). Pojavljivanje profesionalnog tržišta malvera znači da malver više nisu izradili tinejdžeri kako bi zadivili vršnjake, već specijalizovane profitne firme koje se bave istraživanjima, razvojem i testiranjem zlonamernog softvera [31: 3]. Pojavili su se i specijalizovani servisi ransomvera (*Ransomware-as-a-Service – RaaS*), što je uticalo na povećanje aktivnosti povezanih sa njima; ovim su uključeni programeri malvera koji kreiraju komplete alata i prilagođavaju ih potrebama napadača, razvijajući nove varijante ransomvera [15: 63].

– *Usluge infrastrukture* podrazumevaju iznajmljivanje (ili eventualnu prodaju) elemenata infrastrukture radi izvršenja krivičnog dela (iznajmljivanje mreže računara radi DDoS napada, slanje spam poruka, distribucija malvera). Postoji veliki broj dostupnih infrastrukturnih

[6] Istraživanje [60] predstavlja analizu policijske i tužilačke arhive baza podataka (SQL dumps) za 6 podzemnih foruma (BlackHatWorld, Carders, HackSector, HackE1ite, Freehack i L33tCrew). Arhiva svakog foruma je sadržala podatke o registrovanim korisnicima, promenama statusa članova, međusobne privatne i poslovne komunikacije i druge informacije.

[7] Ranjivost nultog dana je sigurnosni propust računarske aplikacije koji je otkriven i poznat napadačima pre nego što je isti uočen od strane proizvođača i javnosti i za koji proizvođač nije objavio „zakrpe“ kojima otklanja problem.

[8] Cene zlonamernog softvera u 2016: osnovni bankarski komplet trojanaca – 100$; trojanci za krađu lozinki – 25$ do 100$; trojanci za Android bankarstvo – 200$; malveri za zaštitu od otkrivanja (*Malware crypter service*) – 20$ do 40$; ransomveri – 10$ do 1800$ (15: 52).

servisa kojima se omogućava izvršenje dela VTK. Ovakve usluge pružaju i legalni provajderi, kada svoje veb stranice ustupaju kriminalcima, ignorišući zakonska i etička ograničenja.

– *Usluge hakovanja* potencijalnih žrtava vrše se radi pribavljanja informacija potrebnih za krađu identiteta, pribavljanje bankarskih kredincijala, detalja sa veb stranica i slično. Ove informacije se mogu prikupljati za poznate naručioce ili se već prikupljeni podaci mogu prodavati na tržištu. Usluga hakovanja je dostupna kriminalcima koji imaju potrebna finansijska sredstva, čime skraćuju vreme potrebno za pripremu i izvršenje napada.

## *Nelegalna kriminalna tržišta na Internetu*

Tržište se obično definiše kao „socijalno-materijalna infrastruktura koja se nalazi u prostoru u kome su moguće tržišne transakcije" [93: 384]. Ovakvo određenje odgovara i empirijskom fenomenu podzemnih onlajn kriminalnih tržišta, uz razliku što se ova tržišta nalaze u sajber prostoru [49: 210].

Postojeća podzemna tržišta nude sve potrebne alate i usluge kako bi se u celini realizovala aktivnost hakera kao pojedinaca ili OKG, čime se omogućava snabdevanje velikog broja kriminalaca, koji svoje aktivnosti ne usmeravaju samo na pojedince kao žrtve, već i na preduzeća i državne institucije [55: 60-61]. Tržište sadrži mnogo zainteresovanih strana: od legalnih organizacija koje prodaju otkrivene ranjivosti računarskih sistema drugim legalnim organizacijama sa ciljem povećanja njihove bezbednosti, do pojedinaca i organizacija koje stvaraju, preprodaju, kupuju i prodaju usluge radi izvršenja kriminala. Mali broj istraživanja koja su rađena radi sagledavanja strukture i funkcionisanja podzemnih kriminalnih tržišta, pokazala su da se lični podaci i informacije koje su dobijene različitim metodima, prodaju na forumima i na kanalima Internet Relay Chat, pojedincima i drugim kriminalnim organizacijama [39, 40, 49, 60, 80, 87, 94, 95]. Informacije i usluge kojima se trguje na ilegalnim tržištima su [49]:

– softverski proizvodi za sticanje neovlašćenog pristupa računarima i mrežama,
– znanja o ranjivosti bezbednosnog sistema, npr. ranjivost nultog dana [96],
– lozinke i identiteti ličnosti, resursi za spam poruke i prevare,
– zamena kriptovaluta i druge finansijske usluge [31],
– podaci i uputstva o korišćenju ukradenih kreditnih kartica,
– falsifikovani lični i drugi dokumenti.

Neka tržišta svoje delovanje zasnivaju na širokom asortimanu roba i usluga kojima se obezbeđuje potpuni ciklus funkcionisanja tržišta, od inicijalnih kriminalnih aktivnosti do njihovog unovčavanja. Pojedini prodavci se oglašavaju na više tržišta, dok se drugi pridržavaju poslovanja na nekoliko ili na samo jednom tržištu [45: 4].

Hakerska tržišta su evoluirala tokom vremena i sada se pojavljuju u mnogim oblicima. Do 2000. godine ova tržišta su se fokusirala na robu i usluge, zatim su svoje aktivnosti proširila na blokiranje akreditiva za e-bankarske naloge i društvene medije, da bi se u najnovije vreme njihova aktivnost preusmerila na jednu vrstu robe i rad specijalizovanih servisa. Procene su da su 2000. godine oko 80% učesnika na tržištu bili pojedinci ili članovi manjih kriminalnih grupa, a da je 2014. godine taj broj opao na 20% i da su primat na tržištima, u svim resorima, preuzele kriminalne organizacije [45: 4]. Obzirom na različitost roba i usluga koje se nude na podzemnom virtuelnom tržištu, osnovne vrste tržišta su opredeljene prema dostupnosti i lokaciji tržišta (isključujući IRC kanale) [49: 210]:

a) *Regularne stranice za internetsku trgovinu*: trgovina se obavlja preko legitimnih veb stranica i na njima se nude robe ili usluge povezane sa VTK. Ove internet lokacije ne pripadaju poznatim svetskim operativnim korporacijama, već manjim provajderima regionalnog značaja koji primenjuju i manji stepen kontrole sadržaja veb stranica.

b) *Regularne forumske stranice*: forumi koji su prvobitno imali drugu namenu i čiji su vlasnici odustali od njihovog korišćenja, zauzimaju se i preuzimaju od strane nekoliko prodavaca, a zatim se šire pristupanjem drugih aktera.

c) *Direktne tržišne stranice*: neki trgovci ličnim podacima postavljaju svoja prodajna mesta na dubokoj mreži Interneta, samostalno i uz sve karakteristike onlajn prodavnica sa primenjenom automatizacijom transakcija i uobičajenim načinom plaćanja i isporuka robe.

d) *Otvoreni forumi za ilegalnu trgovinu:* ovo je najčešći oblik tržišta i obično se sastoji od brojnih podforuma za trgovanje različitom robom, a samo trgovanje na forumu se naplaćuje. Za povezivanje sa Internetom iznajmljuju se provajderi u zemljama gde su kontrole i zakonska regulativa najpovoljniji za ovakvu vrstu foruma. Rukovođenje forumom je prepušteno administratoru koji ima ovlašćenja da nadgleda rad foruma, prati poštovanje pravila i obezbeđuje sigurnost transakcija. Pristup tržištu nije jednostavan i zahteva registraciju.

e) *Zatvoreni forumi za ilegalnu trgovinu*: organizovani su na isti način kao i otvoreni forumi, a osnovni cilj zatvorene forme im je sprečavanje pristupa nepouzdanih prodavaca (ripera). Broj članova foruma je obično ograničen, a učesnici na forumu se pozivaju ili im se daje posebna dozvola za privremeni pristup.

Jedna od delatnosti na crnim i sivim onlajn podzemnim tržištima je i prisvajanje ličnih podataka građana preuzetih od legalnih organizacija i državnih institucija i trgovanje njima[9]. Kao drugi vidovi napada pojavljuju se: napadi na kompromitovane i napuštene veb stranice na kojima su „ostale“ baze podataka i drugi materijali; napadi malverima ubačenim u onlajn reklame, kojima se po otvaranju reklame od strane žrtve, zarazi računar i nad njim preuzme daljinska kontrola, instalira dodatni komplet malvera za eksploataciju i kradu podaci; i, napadi na veb lokacije koje su već preopterećene DDoS napadima botneta, čime je olakšan pristup traženim podacima [45: ix].

## *Organizacija nelegalnih kriminalnih tržišta na Internetu*

Pojedini istraživači koriste pojam tržište kako bi opisali strukturu IRC kanala i foruma, jer oni služe kao lokacija i infrastruktura za učesnike koji se bave transakcijama [59, 62, 79]. Drugi istraživači, koji se bave istraživanjem organizacione strukture, definišu tržište sa aspekta odnosa između aktera, tako da tržište predstavlja određenu relacionu strukturu između aktera, koja je uglavnom neusaglašena sa različitim aktivnostima i obavezama učesnika [93, 97]. Ograničena istraživanja strukture društvenih mreža i odnosa između aktera, vršena su prvenstveno koristeći strukturu malih foruma [60] ili arhivske podatke poznatih tržišta ukradenih podataka, koja su rasformirana zbog akcija policijskih organa [34].

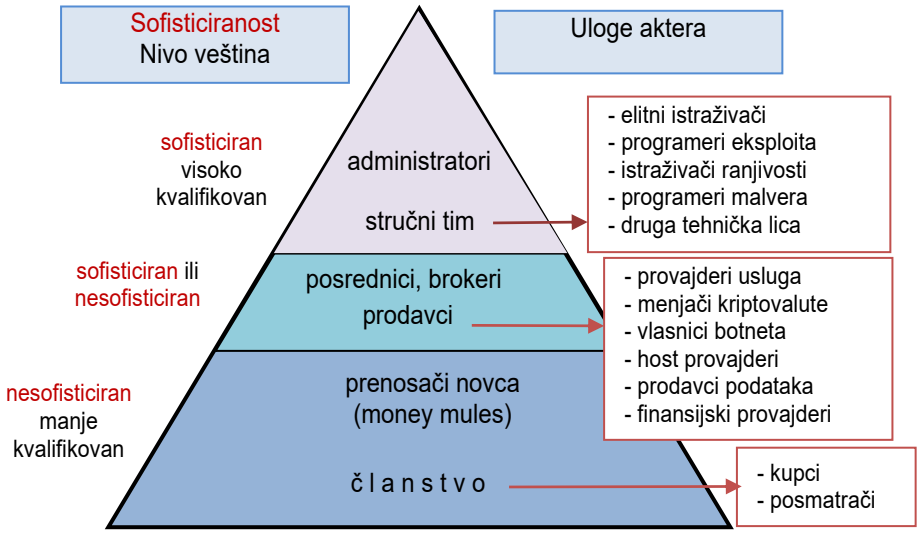
Pri poređenju realnog svetskog tržišta ilegalnih proizvoda i onlajn podzemnog tržišta, dve su ključne razlike: rizik od hapšenja ima minimalni uticaj na kupce i prodavce na digi-

[9] Krajem 2013. godine ukradeni su podaci iz baze podataka maloprodajnog giganta Target (*Target Corporation, US, Minneapolis*) koji raspolaže podacima za 40 miliona kreditnih kartica i 70 miliona korisničkih naloga, koji su se kasnije pojavili na podzemnom tržištu (45: ix).

talnom tržištu, i, malo je dokaza o upotrebi ili opasnosti od fizičkog nasilja među učesnicima transakcija [80: 1]). U skladu sa funkcionisanjem tradicionalnih ekonomija, podzemna tržišta obuhvataju prodavce (snabdevanje), kupce (potražnja) i posrednike. Kupci su pojedinci, kriminalne organizacije i komercijalna preduzeća, a posrednici mogu delovati kao treća strana i mogu olakšati transakcije, procenjivati i vrednovati kupce i prodavce, štititi njihov identitet i stvarati određena ograničenja u transakcijama.

U okviru tržišta, kao i kod OKG VTK, često postoje hijerarhijski određene i specijalizovane uloge: na vrhu su administrator sa timom stručnih lica koja imaju sofisticirano znanje o određenom području (tehnički eksperti, programeri, istraživači ranjivosti, kriptoanalitičari), slede posrednici, brokeri, a zatim i ostali članovi, uključno i prenosači novaca (*money mules*). Hijerarhijski sistem upravljanja forumima, i pored nedostataka koji se manifestuju u lakšem otkrivanju od strane organa gonjenja, rukovodioci foruma zadržavaju kao osnovni sistem rukovođenja, jer time obezbeđuju veću efikasnost rada i ostvaruju veću kontrolu nad forumom. Hijerarhijska organizaciona struktura olakšava koordinaciju rada pojedinih komponenata i poboljšava odnose između pojedinaca na nižim nivoima organizacije. Prednosti ove strukture poremećene su činjenicom da su one manje otporne na poremećaje koji nastaju iz okruženja. Uklanjanje ključnih čvorova unutar hijerarhijskih struktura izaziva uklanjanje i veza sa drugim čvorovima unutar organizacije ili izvan nje, tako da može bitno uticati i na dalje funkcionisanje cele mreže [33]. Napredovanje u hijerarhiji tržišta zavisi od kvaliteta rada i sprovedenih provera, ali i od ličnih odnosa. Nema pouzdanih podataka koliko ljudi je uključeno u tržište [45, 54].

U opštoj populaciji i u elitnoj klasi profesionalaca, većina kriminalaca VTK u grupama je specijalizovana prema opštem modelu VTK, slika 3. To čini i preduslov za dobru reputaciju u svojoj oblasti, uspostavljanje stabilnih odnosa sa klijentima i redovnim kupcima i ostvarivanje većih profita [29: 7].




Slika 3 – *Različiti nivoi, proporcionalni udeo, sofisticiranost i uloge aktera podzemnog tržišta (prema: [45: 5-8])*

Osnovne specijalnosti tipičnog organizovanog VTK, prema Stivenu Čabinskom,[10] su [21]:

– Programeri – stvaraju zlonamerne programe i druge alate potrebne za izvršenje krivičnog dela.

– Distributeri ili prodavci – trguju i prodaju ukradene podatke i robu drugih specijalista i predstavljaju garante za isporučenu robu.

– Tehničari – održavaju kriminalnu infrastrukturu i prateće tehničke sisteme, kao što su serveri, priključci provajdera, korisničke šifre i druga oprema.

– Hakeri – pretražuju i eksploatišu ranjivosti u aplikacijama, sistemima i mrežama, kako bi pristupili zaštićenim računarskim sistemima.

– Specijalisti za prevare – razvijaju i primenjuju šeme socijalnog inženjeringa, uključujući i fišing, spam i druge neovlašćene pristupe računarskim sistemima.

– Host provajderi – obezbeđuju "sigurne" objekte za korišćene servere i njihovo umrežavanje, formiraju mrežu botneta, a mogu i iznajmljivati svoju opremu kao uslugu drugim kriminalnim grupama.

– Računovođe – kontrolišu račune i obezbeđuju isplate drugih članova grupe i obično upravljaju kuririma za prenos novca i specijalnim prenosačima novca.

– Prenosači novca (*money mules*) – prenose nezakonito stečen novac (npr: ukraden) za račun kriminalne grupe na sigurne lokacije i to čine lično, putem kurirske službe ili elektronski, često ne znajući da se kreću u kriminalnom okruženju[11].

– Blagajnici – pomažu u prenosu i pranju ilegalnih prihoda kroz digitalnu valutu i vrše usluge razmene za različite nacionalne valute ili putem menjačnica.

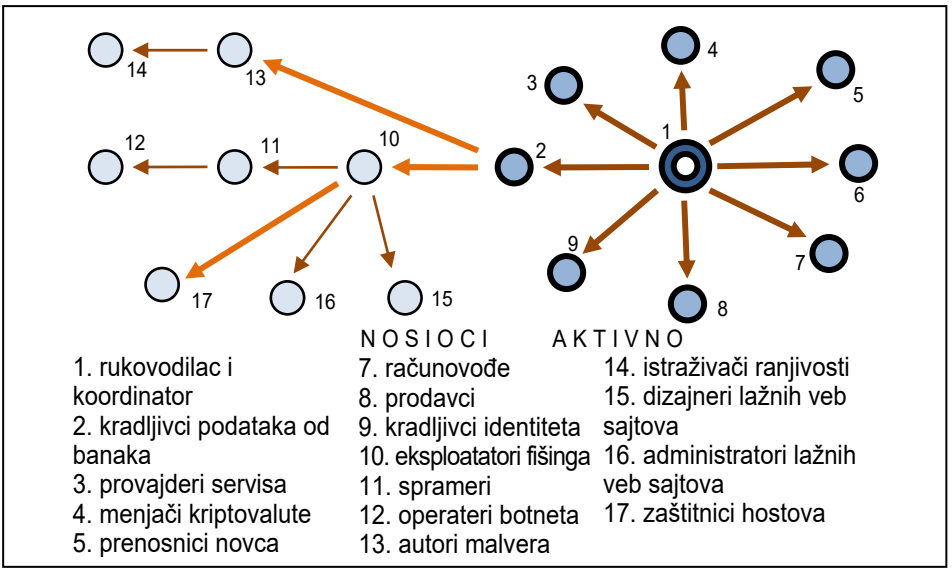
– Rukovodioci organizacija (lideri) – obično nemaju specijalizovana, već opšta znanja i veštine, određuju ciljeve, regrutuju i primaju nove članove, vode računa o članovima, izdaju zadatke i kontrolišu izvršenja i odlučuju o distribuciji i korišćenju prihoda.

Na slici 3 prikazane su proporcije različitih nivoa učesnika na podzemnom tržištu, nivoi sofisticiranosti i nivoi veština i dati su primeri aktera sa specifičnim zanimanjima i ulogama u organizaciji tržišta (prema: [45: 5-8]).

Osnaživanje pojedinaca kao preduzetnika u kriminalnim organizacijama koje deluju na onlajn nelegalnim tržištima, jedna je od najdubljih preobražaja organizovanog VTK. Na tržištima se stvara jezgro koje rukovodi njihovim radom, a potrebni specijalisti raznih znanja i veština čvrsto se povezuju sa njim. Funkcionisanje jednog jezgra onlajn nelegalnog tržišta sa hijerarhijskim vezama, prikazano je na slici 4, iz koje je vidljiva podela funkcija među članovima i potrebne specijalističke veštine. Ovakva specijalizacija je izuzetno korisna za sajber kriminalce: umesto angažovanja stotina ljudi koji se bave svim aspektima VTK, podzemlje sajber prostora se sastoji od stručnjaka za predmetne poslove, koji svoje vreme i energiju fokusiraju na poboljšanje svojih tehnika, roba i usluga i na taj način se specijalizuju [21]. Idealna podela posla i uska specijalizacija nisu nužno povezane sa formalnom i fiksnom organizacijom. Neke funkcije mogu biti i izdvojene izvan organizacije, na širem nivou, kada se u mreže uključuju lica sa kojima se komunicira na mreži ili u onlajn pričaonicama [29: 7].

[10] Stiven R. Čabinski (Steven R. Chabinsky) 2010. godine bio je zamenik direktora FBI i rukovodilac odseka za borbu protiv VTK.

[11] Prema objavi Evropola od 01.03.2016, u vremenu od 22-26.02.2016. godine, Evropol, pravosudni i drugi organi više država EU, ali i nečlanica (Moldavija i druge), udružilo je snage u akciji protiv "novčanih mula", a rezultat operacije bilo je identifiovanje skoro 700 lica za prenos novca, uhapšeno je 81 lice, otkriveni su i sprečeni značajni finansijski gubici i otkriveno je preko 900 žrtava nedozvoljenih transakcija [98].




Slika 4 – *Ekonomija (tržište) digitalnog podzemlja (prema: [17])*

Pojedini forumi za diskusiju funkcionišu kao virtuelna podzemna tržišta koja oglašavaju, na primer, ukradene brojeve kreditnih kartica [40]. Među nekim kriminalcima VTK (npr. kineski kriminalci) popularne usluge su razmene trenutnih saznanja u vidu poruka ili ćaskanja, kao i privatni kontakti na forumima koji se odvijaju u vezi sa tržištem ukradenih kreditnih kartica i njihovim transakcijama [99].

## *Funkcionisanje nelegalnih kriminalnih tržišta na Internetu*

Beskrajna priroda onlajn komunikacija otežava korišćenje tradicionalnih verbalnih i neverbalnih znakova prema kojima mogu da se prepoznaju potencijalno opasni akteri na tržištu, kako od strane policijskih organa, tako i od kradljivaca na tržištu [80: 2]. Nelegalna onlajn tržišta su dobri primeri tržišta koja nisu regulisana od strane država i gde nema pravne zaštite imovine, a glavna prepreka za ilegalno onlajn poslovanje je nepoverenje zbog rizika od prevara aktera, uglavnom prodavaca [49: 209]. Rast digitalnih operacija i usluga na legalnom tržištu je ključni mehanizam za OKG VTK, kako za činjenje tradicionalnih krivičnih dela, tako i za razvoj novih vrsta ilegalnih aktivnosti. Koristeći poslovne modele koji su dokazali svoju efikasnost u stvarnom poslovnom svetu, OKG upravljanje podzemnom ekonomijom sprovode kao svoju dugotrajnu kriminalnu aktivnost [75]. Tržište hakera – pojedinaca pretvorilo se u visoko organizovane i finansijski dobro vođene diskretne kriminalne mreže i sofisticirane grupe. Uprkos naporima organa za sprovođenje zakona radi prekida i zatvaranja različitih delova tržišta, od finansijskih do popularnih, podzemna ekonomija je pokazala visok stepen otpornosti i sposobnosti oporavka, čak i nakon izvršenih hapšenja glavnih aktera, kada druga lica iz mreže brzo preuzimaju liderstvo, čime se sprečava delovanje kon-

kurentskih foruma na preuzimanju poslova [45: ix]. Pokušaji da se proceni veličina onlajn tržišta u oblasti VTK, čini se kao nemoguć zadatak[12] [62].

Većina kriminalnih foruma se koristi kao podzemna tržišta na kojima se nude sve vrste ukradene robe i nude ili traže nelegalne usluge. Većina izvršenih prodaja odnosi se na neku vrstu ukradenih podataka (preko 80%), a većina prodavaca je ponudila zbirne kolekcije podataka koji se odnose na podatke o bankovnim računima ili kreditnim karticama [62: 2].

Prema vrsti roba i usluga koje se nude na tržištima, mogu se razlikovati tri osnovne kategorije podzemnih tržišta [46: 2-3][13]:

– tržišta ukradenim podacima (podaci sa kreditnih kartica, bankovni računi, računi za plaćanje na mreži (PayPal) i lična dokumenta);

– tržišta alatima za VTK (kompleti fišing softvera, malveri, softver za hakovanje, botnet softver);

– servisi VTK (omogućavaju siguran transfer novca, razmenu kriptovalute za novac, prenos novca u toku kriminalnih aktivnosti – „mule“ za prenos novca, trgovanje ukradenim kreditnim karticama).

Tržišta su ili specijalizovana samo za pojedine vrste usluga ili se na jednom tržištu mogu naći sve vrste kriminalnih alata i usluga. Kontakti kupaca i prodavaca ostvaruju se različitim kanalima, kao što su privatne poruke na forumima ili pričaonice izvan foruma. Podzemno tržište je izgrađeno i funkcioniše na digitalnoj valuti (kriptovaluta), koja se može pretvarati u stvarnu valutu preko izmenjivača valuta – menjačnica [55: 62], a plaćanja usluga se vrše kriptovalutama koje se u tom trenutku koriste (PayPal, e-Gold, Liberty Reserve, WebMoney, Yandex, Western Union) [40: 42].

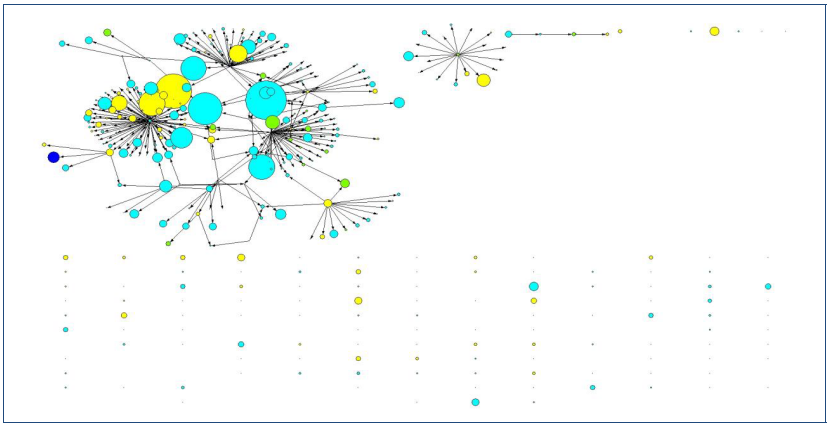
Praksa aktera na podzemnom slična je praksi na stvarnom tržištu, ali ima svoje specifičnosti: virtuelni koncept nezakonitih tržišta menja ponašanje prodavaca i kupaca, oni ne poznaju lične karakteristike svojih poslovnih partnera i nema opasnosti od fizičkog nasilja u slučajevima nezadovoljnih aktera [49, 59]. Prodavci imaju manji rizik u transakcijama, s obzirom da se na ovim tržištima plaćanje vrši unapred. Kupci, s druge strane, u strahu da će biti prevareni, imaju razrađene određene strategije zaštite od rizika. Ove strategije se zasnivaju na korišćenju resursa provajdera (kao koordinatora aktivnosti tržišta) sa ciljem da se smanji rizik od gubitaka koji mogu da nastanu zbog nepouzdanih ili nepoštenih prodavaca (riperi). Zato neka tržišta omogućavaju pritužbe na prodavce, radi njihovog sankcionisanja

[12] Ministarstvo unutrašnjih poslova Srbije (MUP), a povodom hapšenja jednog državljanina Srbije zbog reklamiranja prodaje, prodaje i davanja na upotrebu sredstava za pravljenje lažnih platnih kartica, saopštilo je 08.02.2018. godine da je uhapšeni član kriminalnog foruma „Infraud“. Ovaj kriminalni forum se bavio pribavljanjem i prodajom ukradenih podataka, uključujući podatke o kompromitovanim platnim karticama, ličnim podacima građana, bankarskim i finansijskim podacima građana, banaka i kompanija, malicioznih softvera, kao i ukradenih identiteta. Ukradeni podaci su uglavnom prodavani na *Dark Web*-u. Procenjuje se da je „Infraud“ bio jedan od najvećih kriminalnih foruma za prodaju ukradenih podataka zabeleženih do sada, na kome je, kako se sumnja, prodato oko četiri miliona podataka o ukradenim platnim karticama, pre nego što je on oboren u ovoj velikoj međunarodnoj akciji. Forum je u međunarodnoj policijskoj akciji ugašen, a sumnja se da je forum bio jedan od najvećih nelegalnih foruma po broju članova (blizu 11 hiljada članova). Ministarstvo pravde SAD pretpostavlja da je ovaj kriminalni forum odgovoran za gubitke više od 530 miliona dolara [100].

[13] Rezultati istraživanja, koje je vršeno na osnovu detaljnih opisa 40 aktivnih kriminalnih mreža u Holandiji (18), Nemačkoj (3), Velikoj Britaniji (9) i SAD (10), a rekonstrukcije su izvršene na osnovu analize policijskih dosijea i/ili intervjua sa policijskim službenicima i javnim tužiocima, pokazali su postojanje tri osnovne kategorije podzemnih tržišta [46].

[80: 16).[14] Zbog visokog nivoa prevara unutar ilegalnih onlajn tržišta, postoje pretpostavke da bi mogla postojati dva nivoa poslovanja: otvoreni nivo koji je namenjen za neiskusne korisnike i zatvoreni nivo koji je namenjen iskusnim kriminalcima [95].

Na osnovu kvantitativne analize kriminalnih društvenih foruma koja je primenjena za istraživanje mrežne organizacione strukture, većina foruma koji su istovremeno i onlajn kriminalna tržišta, zasniva se na formalnim organizacijama, menadžerskom upravljanju i na dugoročnom delovanju [62]. U strukturi mreže najzastupljeniji su prodavci, ali su kupci i neutralni korisnici veoma često uključeni u aktivnostima deljenja informacija, posebno o reputaciji prodavaca. Na slici 5 prikazana je jedna organizaciona mrežna struktura koju karakteriše funkcionisanje na globalnom nivou (kao mera funkcionisanja mreže u celini i svih interakcija na mreži) i funkcionisanje na lokalnom nivou (kao mera koja proučava identifikovanje i način funkcionisanja određenih čvorova mreže prema okruženju). Za organizaciju onlajn tržišta prikazanu na slici 5, grafički prikaz veličina čvorova predstavlja količinu informacija od tih čvorova prema drugim učesnicima ili njihovu centričnost. Postojanje više čvorova koji su povezani sa centralnim čvorom u mreži pokazuje da postoje komunikacije kojima se učesnici ili korisnici mreže povezuju samo sa pojedinim čvorovima, opredeljujući se prema njihovim nosiocima (kao što su izabrani prodavci), njihovoj reputaciji ili nivou posedovanog znanja. Izvan osnovne strukture tržišta, na slici 5, prikazani su kupci i posmatrači, prema učešću i vrstama delatnosti kojima su povezani sa tržištem [62: 8-12].



Slika 5 – *Organizaciona struktura jednog tržišno opredeljenog onlajn foruma [62: 113-114]*

Da bi smanjili nesigurnost transakcija, administratori tržišta uređuju svoje forume tako da institucionalno štite zasnovano poverenje među akterima tržišta, za šta poseduju tehničke mogućnosti. Oni obezbeđuju minimalni nivo stabilnosti i umanjuju obim i razmeru eksce-

[14] Istraživanjem koje je sproveo Tomas Holt (Thomas Holt) sa saradnicima, obuhvaćeno je 13 internet foruma (10 foruma na kojima se kao primarni jezik koristio ruski i tri foruma na kojima se kao primarni jezik koristio engleski) koji su se bavili prodajom ukradenih podataka o ličnostima radi njihove dalje upotrebe u krađi identiteta i prevarama. Većina "proizvoda" koji su prodati na ovim tržištima su ukradni podaci (84,3%), većina prodavaca je ponudila podatke koji se odnose na bankovne račune ili kredite (44,7%), kao i različite podatke sa kreditnih kartica (34,9%) [62, 80].

snih prevara [49: 209]. Prisustvo i praksa administratora i moderatora na forumima, koji deluju kao rukovodioci i posrednici, pozitivno utiče na odnos kupaca i prodavaca. Oni nude sredstva, tehnike i metode promovisanja međusobnog poverenja i pomoći u transakcijama, sve sa ciljem zadržavanja kupaca na svom tržištu i sticanja dobiti [80: 16-17]. Kada administratori i moderatori foruma sprovode pravila foruma i nadgledaju ponašanje korisnika, oni podižu stepen poverenja u svetu u kome ovakvo poverenje u velikoj meri nedostaje [63: 55]. Radi pravilnog usmeravanja korisnika, administratori foruma mogu zabraniti pojedine aktivnosti ili uticati na status prodavaca i njihov udeo na tržištu, što formira određene mehanizme regulacije transakcija na forumu i štiti kupce od beskrupuloznih prodavaca [95: 42]. Forumski administratori imaju pravila koja važe za taj forum, sa njima se upoznaju svi novi akteri na tržištu, a za kršenje pravila slede sankcije. Za rad na tržištu, prodavcima se prodaje tržišni pristup ili licenca za prodaju određene vrste robe [49: 211].

Iako prodavci pojedinci javno objavljuju oglase na forumima, anonimne i privatne razmene koje se obavljaju, nose znatne elemente rizika: kupci moraju prvo da izvrše plaćanje, a tek potom da sačekaju isporuku tražene robe. Virtuelna struktura tržišta omogućava prodavcima i kupcima da konstruišu složenije metode snimanja, validacije i prodaje na načine koji nisu mogući u stvarnim ilegalnim tržištima i globalnom kriminalu. Stepen rizika usled slabe informisanosti kupaca je veoma mali, jer oni imaju mogućnost da se na forumu detaljno informišu o svim prodavcima, što im proširuje saznanja o svim akterima na tržištu [59]. Prodavci često garantuju životni vek svojih proizvoda ili vrednost, a neki i prate šta kupac radi sa proizvodom – hakerska verzija "digitalnog upravljanja pravima". Stalno učešće u poslu na tržištu rezultira reputacijom aktera – prodavaca, koja je vidljiva iz ocena ranijih kupaca, ali ova reputacija, zbog mogućnosti promene identiteta, može se zlonamerno modifikovati ili ukrasti [45: ix].

## *Mehanizmi regulacije i samoregulacije onlajn kriminalnih tržišta*

Onlajn nelegalna tržišta ne podležu državnoj regulativi i sredstvima za sprovođenje i poštovanje ugovora i ugovornih obaveza, tako da su primorana da stvore i koriste alternativne mehanizme za izgradnju poverenja među učesnicima na tržištu [49]. Regulacija tržišta nastala je iz potrebe da se, u osnovi neorganizovano tržište na neki način uredi, da se uvedu određena pravila i osigura njegovo stabilno funkcionisanje. U cilju prevazilaženja glavnih izazova onlajn anonimnosti i korišćenja njenih prednosti, kriminalci su razvili niz mehanizama koji unapređuju poverenje i obezbeđuje stabilnost funkcionisanja tržišta, što uključuje mehanizme koji se odnose na: (a) uspostavljanje sajber-kriminalnih identiteta; (b) procenjivanje atributa roba i usluga koje su objekat transakcija; i (c) vanpravno upravljanje [42: 72]. Osnovni elementi regulacije (samoregulacije) onlajn ilegalnih tržišta su [49, 61]:

– *Održavanje reda na tržištu* postignuto je aktivnom ulogom administratora (operatera) koji olakšavaju usklađivanje potražnje i ponude, generišu pravila i prate usaglašenost tržišta, a za svoje poslove naplaćuju proviziju od prodavaca. Provajderi vrše dodelu licenci za korišćenje tržišta, formiraju pravila ponašanja na tržištu i prate njihovo poštovanje, ukidaju korisničke naloge nepoštenim prodavcima, vrše usluge deponovanja roba i plaćenih nadoknada do završetka transakcije i slično.

– *Mreže* omogućavaju spajanje kupaca i prodavaca koji se na ilegalnom onlajn tržištu suočavaju sa dva rizika: rizik od otkrivanja od strane organa zakona i odsustvo imovinskog prava, koje bi ih štitilo u slučajevima nesporazuma prilikom transakcija i od nepoštenih prodavaca. Funkcionisanje mreže pod zaštitnim sistemom koji obezbeđuju administratori sa svojim stručnim timom, daje određenu sigurnost učesnicima tržišta, ali su prevare ostale kao znatna prepreka onlajn poslovanju.

– *Nasilje ili pretnja nasiljem* u fizičkoj formi, zbog nesprovođenja sporazuma, onemogućeno je zbog anonimnosti aktera. Moguće nasilje može da se ispolji u digitalnom obliku, kao što je oštećenje veb stranica i DDoS napadi, što može da uzrokuje znatne štete.

– *Ugled* koji pojedinac stiče na forumu i pozitivna reputacija obezbeđuje povoljniji položaj i potvrđen status prodavca, za razliku od istrajnih prevaranata koji trpe sankcije. Stečeni ugled na digitalnom tržištu može biti predmet prevara zbog narušavanja identiteta lica sa reputacijom ili njegovog prisvajanja. Ako akteri ne ispunjavaju svoje obaveze, posledica je smanjenje učešća ili isključenje sa foruma, što u stvarnom svetu odgovara postupku sprovođenja društvene kontrole i javnosti rada [24].

– *Društvene norme* usklađuju ponašanje aktera i proizlaze iz opšteg poverenja, mada nema potvrđenih nalaza u istraživanjima koje su to norme, osim poštovanja sporazuma i zabrane prevara [49: 209].

Nedostatak unutrašnje regulatornog mehanizma tržišta, stvara znatne poteškoće kupcima kada proizvodi (ili usluge) nisu isporučeni nakon uplate ili su isporučeni ali nemaju dogovorene karakteristike ili kvalitet. Korišćenje garancija koje pruža organizacija onlajn kriminalnog tržišta, predstavlja vredan mehanizam za smanjenje rizika kupaca od prevara, od strane beskrupuloznih prodavaca [40, 49, 95].

## *Budući razvoj onlajn kriminalnih tržišta*

Propusti banaka, prodajnih lanaca, državnih institucija i drugih organizacija, nenamerno gubljenje ili krađa podataka, omogućili su da na podzemnom onlajn tržištu postoji veliki broj ličnih podataka koji se prodaju (u 2016. godini je ukradena 1,1 milijarda ličnih podataka, što je dvostruko više nego 2015. godine, a njihova eksploatacija izaziva desetine miliona dolara gubitaka od prevara [15]). U budućnosti će se verovatno povećavati broj ljudi na nelegalnim onlajn tržištima, posebno visokokvalifikovanog kadra sa traženim znanjima i veštinama. Onlajn kriminalna tržišta su danas dostupnija nego pre desetak godina, čemu su doprineli širenja veb lokacija gde se može trgovati robom, povećanje specijalnih vodiča za kupovinu koji se objavljuju na Google i YouTube i povećanje opšte sofisticiranosti koja će zahtevati kvalifikovane pojedince za obavljanje najsloženijih kriminalnih aktivnosti [45: 5-8].

Na osnovu indikatora koji pokazuju smene na kriminalnim tržištima, gde se sve više pojavljuju aktivnosti manjih grupa i pojedinačnih kriminalnih preduzetnika, ovaj trend će se posebno odraziti na onlajn kriminalna tržišta [92: 7]. Kriminalci su oduvek bili vični da koriste moderne tehnologije, ali stopa tehnoloških inovacija i sposobnost organizovanih kriminalaca da koriste ove tehnologije, u stalnom je porastu. Razvoj onlajn trgovine će biti značajan u narednom periodu, tako da će aktivnosti na ovim tržištima unositi sve veće poremećaje u uspostavljen tradicionalan model distribucije oflajn kriminalnih tržišta [92: 10].

Razvoj podzemnih ekonomija, kao specifičnog oblika kriminalnog organizovanja, biće okarakterisan sledećim bitnim elementima [45: x-xi]:

– povećaće se broj aktivnosti na podzemnim tržištima i način proveravanja njegovih aktera, stvoriće se mogućnosti za veću anonimnost korisnika, a više pažnje biće usmereno na šifrovanje i zaštitu komunikacija i transakcija na mreži;

– opremljenost tržišta i sposobnosti napadača, verovatno će prevazilaziti sposobnosti zaštite i odbrane potencijalnih žrtava;

– hiperkonekcija na Internetu će stvoriti više tačaka koje će se koristiti za napade i eksploataciju kriminalnih dobitaka, pa će kriminal sve više poprimati umreženu komponentu, a međunarodna podzemna komunikacija između kriminalaca omogućiće brzu podelu postojećeg kriminalnog znanja;

– nastaviće se rast eksploatacije društvenih mreža i mobilnih uređaja;

– usled veće specijalizacije i povećanja znanja i veština pojedinaca, povećaće se broj ponuda usluga hakera, posrednika, brokera i izvršilaca drugih specijalizovanih usluga.

Stručnjaci nisu saglasni oko toga koji subjekti će najviše uticati na rast podzemnog tržišta, da li su to male ili velike organizacije ili pojedinci, koji će proizvodi biti aktuelni na tržištu (zamenljive robe kao što su informacije o kreditnim karticama ili nefunkcionalna roba kao što je intelektualna svojina), koje vrste napada će biti dominantne (uporni – stalni i dugotrajni ciljani napadi ili oportunistički napadi sa korišćenjem povoljnih prilika po principu „udari i zgrabi“) [45: x-xi].

## *Zaključak*

Ovim radom je učinjen pokušaj da se, na osnovu dostupne i izabrane literature, sistematizuju saznanja o dostignutom nivou organizovanosti VTK, strukturama kriminalnih grupa i drugih organizacionih formi, kao i o metodima i načinima njihovog delovanja.

Organizovanost VTK je još uvek nedovoljno istražena, ali postoji visok stepen saglasnosti eksperata da se VTK u većini slučajeva izvršava na organizovan način (prema nekim tvrđenjima u čak 80% slučajeva). Zbog velikog nedostatka empirijskih pokazatelja o delovanju OKG VTK, postoje određene rezerve i suzdržanost među istraživačima o tome na koji način je izvršeno organizovanje radi delovanja u sajber prostoru. Postalo je vrlo verovatno da su tradicionalne OKG spoznale mogućnosti koje pruža Internet, da su neke OKG pojedina svoja delovanja usmerile na sajber prostor i da su razvile alate koji im olakšavaju aktivnosti. Još nema pouzdanih pokazatelja koliko su ovakve grupe uključene u „čisti“ VTK, jer korišćenje malvera, ransomvera i drugih oblika napada VTK ne ukazuje da ove aktivnosti izvode tradicionalne OKG. Tipičan koncept organizovanog kriminala koji se zasniva na monolitnim, hijerarhijski i etnički baziranim grupama, koje teže ostvarivanju profita osloncem na podmićivanje i nasilje, većina istraživača smatra zastarelim, kako u virtuelnom, tako i u stvarnom svetu. Preovladava stav da ove organizacije još nisu sposobne da ispolje jače delovanje u sajber prostoru, jer ne poseduju odgovarajući alat za rad na Internetu, ne mogu da ostvare povezanost sa teritorijom kao u stvarnom svetu i postoji problem u funkcionisanju čvrstih organizacija na mreži zbog njihove neprilagodljivosti. Moguće je da će se ove grupe pojaviti na Internetu u vidu lažne manifestacije, a da će praktično delovati u stvarnom svetu.

Nelegalni društveni forumi su osnov za delovanje i utočište aktera nelegalnih onlajn tržišta i kriminalnih grupa. Digitalna tehnologija je uslovila mrežne oblike organizacije i druge tipove kolektivnih akcija, a kriminalne grupe i tržišta, u većini slučajeva, čine integralnu celinu. Ove grupe su identifikovane kao neorganizovani ili distribuirani modeli organizacije, a ne kao grupe koje se zasnivaju na hijerarhijskoj strukturi. Osnovna razlika između ovakve organizacije i tradicionalnih OKG ogleda se u njihovoj informacionoj prirodi, mrežnoj organizaciji i globalnom dometu Interneta. Bez obzira na specijalizaciju i aktivnosti kojima se bave, većina grupa pokazuje slične organizacione karakteristike: prilično su kratkotrajne, amorfne su u smislu organizacije i fleksibilne prema zahtevima i mogućnostima. One verovatno poseduju odlike samoodržanja i reaktivnog ponašanja na delovanje okruženja. Neke kriminalne grupe mogu biti brojnije, sa uspostavljenom labavom hijerarhijskom organizacijom, kada su strukturirane u nekoliko nivoa: jezgro sa osnovnim članovima, izvršioci kriminalnih aktivnosti, pomagači i lica za prenos i manipulaciju novcem. Bez obzira na broj članova, kriminalne mreže pokreće mali broj iskusnih profesionalaca koji deluju kao preduzetnici.

Prisutna su i osporavanja jedne grupe istraživača o postojanju i mogućem razvitku samostalnih OKG (osim onih na onlajn kriminalnim tržištima), koja su bazirana na odlikama kriminalnih grupa: onlajn kriminalne grupe su male, labavo strukturirane i bez jasnog programa. Čvrsto strukturirane kriminalne grupe koje imaju bitne elemente da postanu OKG, mogu biti uključene u prevare, hakovanje, DDoS napade i druge aktivnosti, ali ovi kriminalci se bave jednostavnim prevarama i nisu sposobni da organizuju upravljanje i ozbiljan rad u grupi.

Analizirana istraživanja kriminalnih grupa VTK i podzemnih onlajn tržišta, sugerišu da je jedan od najvećih preobražaja kriminala, upravo onlajn kriminalno umrežavanje omogućeno Internetom. Kriminalne društvene mreže predstavljaju osnov za pojavu globalne onlajn podzemne ekonomije koja je najvidljiviji i najdokumentovaniji oblik organizovanog VTK. Istraživanjima je utvrđeno da onlajn forumi i podzemna tržišta, koja uglavnom funkcionišu na dubokoj mreži Interneta (*Deep Web*), omogućavaju da se kriminalni proces završi u celini, od inicijalnih kriminalnih aktivnosti do inkasiranja novca u kriminalnoj organizaciji. Ovo se obezbeđuje kroz osnovne funkcije foruma kao što su socijalna funkcija, funkcija učenja i razmena iskustava i tržišna funkcija. Ilegalna onlajn tržišta su dobri primeri tržišta koja nisu regulisana od strane država i gde nema pravne zaštite imovine. Iz potrebe da se u osnovi neorganizovano tržište uredi, uvedu određena pravila ponašanja i obezbedi njegovo stabilno funkcionisanje, stvoreni su mehanizmi regulacije i samoregulacije. U osnovi mehanizama su održavanje reda na tržištu, kontrola transakcija i poštovanje prihvaćenih pravila, a posebno sprečavanje nepoštenog rada pojedinih prodavaca. Istraživanjima je pokazano da na velikim tržištima postoji hijerarhija i određene specijalizovane uloge i da hijerarhijski sistem upravljanja forumima i tržištima, i pored mana zbog lakšeg otkrivanja, obezbeđuje veću efikasnost rada i bolju kontrolu.

Zbog sve veće pristupačnosti IKT širokom spektru ljudi i zbog povećanog broja napada koji će biti posledica velike automatizacije koju omogućavaju alati i Internet, u budućnosti se može očekivati dalji razvoj organizovanog VTK, usavršavanje rada ilegalnih onlajn tržišta, veća rasprostranjenost DDoS napada korišćenjem *cloud* infrastrukture, bolja zaštita i povećana bezbednost servera kriminalaca i povećanje broja elektronskih napada na kritičnu infrastrukturu i uređaje povezane sa Internetom.

## *Literatura*

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

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

[3] McCusker, R. (2006). Transnational organised cyber crime: distinguishing threat from reality. *Crime, law and social change*, *46*(4-5), 257-273. Pristupljeno 10.05.2018. na http://tees.openrepository.com/tees/bitstream/10149/115450/2/115450.pdf?origin=publication

[4] Savona, E. U., & Mignone, M. (2004). The fox and the hunters: How IC technologies change the crime race. *European Journal on Criminal Policy and Research*, *10*(1), 3-26.

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

[6] 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.

[7] 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/.

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

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

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

[11] Meyer, G. R. (1989). *The social organization of the computer underground*. Northern, USA: Northern Illinois University De Kalb.

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

[13] 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.

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

[15] Symantec. (2017). *Internet Security Thteat Report*. Pristupljeno 28.04.2018. na https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf.

[16] 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.

[17] Yip, M., Shadbolt, N., Tiropanis, T., & Webber, C. (2012a). 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_de2012submission. pdf

[18] Holt, T. J. (Ed.). (2017). *Cybercrime Through an Interdisciplinary Lens*. In T. J. Holt (Ed.), Cybercrime Through an Interdisciplinary Lens. New Jork: Routledge, 1-14.

[19] Von Lampe, K. (2005). *Making the second step before the first: Assessing organized crime*. Crime, Law and Social Change. 42(4), 227–259.

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

[21] Chabinsky, S. R. (2010). TheCyber Threat: Who's Doing What to Whom?. Federal Bureau Invegastion. Pristupljeno 10.04.2018. na https://www.fbi.gov/news/speeches/ speeches.

[22] Brenner, S. W. (2001). Is There Such a Thing as' Virtual Crime'?. *California Criminal Law Review, 4*(1), 1-72.

[23] 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.

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

[25] 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.

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

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

[28] 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.

[29] 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.

[30] 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.

[31] Moore, T., Clayton, R., & Anderson, R. (2009). The economics of online crime. *The Journal of Economic Perspectives*, *23*(3), 3-20.

[32] 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.

[33] Bakker, R. M., Raab, J., & Milward, H. B. (2012). A preliminary theory of dark network resilience. *Journal of policy analysis and management*, *31*(1), 33-62.

[34] Yip, M., Webber, C., & Shadbolt, N. (2013). Trust among cybercriminals? Carding forums, uncertainty and implications for policing. *Policing and Society*, *23*(4), 516-539.

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

[36] Williams, P. (2001b). Transnational criminal networks. In J. Arquilla, & D. Ronfeldt (Eds.), *Networks and netwars: the future of terror, crime, and militancy.* Rand Corporation, 61-98.

[37] Bell, R. E. (2002). The prosecution of computer crime. *Journal of Financial Crime, 9*(4), 308–325.

[38] Broadhurst, R., & Choo, K. K. R. (2009). Cybercrime and on-line safety in cyberspace.

[39] Peretti, K. K. (2008). Data breaches: what the underground world of carding reveals. *Santa Clara Computer & High Tech. LJ*, *25*, 375.

[40] Holt, T. J., & Lampke, E. (2010). Exploring stolen data markets online: products and market forces. *Criminal Justice Studies, 23*/1, 33-50.

[41] Soudijn, M. R., & Zegers, B. C. T. (2012). Cybercrime and virtual offender convergence settings. *Trends in organized crime*, *15*(2-3), 111-129.

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

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

[44] Von Lampe, K. (2009b). Human capital and social capital in criminal networks: introduction to the special issue on the 7th Blankensee Colloquium. *Trends in Organized Crime*, *12*(2), 93-100.

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

[46] Leukfeldt, R., Kleemans, E., & Stol, W. (2017c). The Use of Online Crime Markets by Cybercriminal Networks: A View From Within. *American Behavioral Scientist 00(0),* 1-6.

[47] Kshetri, N. (2010). *The global cybercrime industry: economic, institutional and strategic perspectives*. Springer Science & Business Media.

[48] Carrington, P. J. (2011). Crime and social network analysis. In J. Skott & J. Carrington (Eds.), *The SAGE handbook of social network analysis*. London: SAGE Publications Ltd, 236-255.

[49] 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.

[50] Kriegler, A. (2014). Using social network analysis to profile organised crime. Pristupljeno 03.03.2018. na https://issafrica. s3. amazonaws. com/site/uploads/PolBrief57.pdf.

[51] Neto, J. (2017). Social Network Analysis and Organised Crime Investigation: Adequacy to Networks, Organised Cybercrime, Portuguese Framework. In *Cybercrime, Organized Crime, and Societal Responses* Springer International Publishing. 179-199.

[52] Broadhurst, R., Grabosky, P., Alazab, M., Bouhours, B., Chon, S., & Da, C. (2013). Crime in cyberspace: offenders and the role of organized crime groups.

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

[54] Yip, M., Shadbolt, N., & Webber, C. (2012b). Structural analysis of online criminal social networks. In *Intelligence and Security Informatics (ISI), 2012 IEEE International Conference on* (pp. 60-65). IEEE.

[55] Sood, A. K., Bansal, R., & Enbody, R. J. (2013). Cybercrime: Dissecting the state of under-ground enterprise. *IEEE internet computing*, *17*(1), 60-68.

[56] Mitchel P. R. (2010). *GlobalOrganized Crime.* USA, Santa Barbara: ABC-CLIO, LLC.

[57] Народна Скупштина РС (НСРС). (2001). Закон о потврђивању конвенције Уједињених нација против транснационалногорганизованог криминала и допунских протокола. *Сл. лист СРЈ - МУ, бр. 6/2001*

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

[59] Franklin, J., Perrig, A., Paxson, V., & Savage, S. (2007). An inquiry into the nature and causes of the wealth ofinternet miscreants. In *ACM conference on Computer and communications security,* 375-388.

[60] 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.

[61] Fallmann, H., Wondracek, G., & Platzer, C. (2010). Covertly probing underground economy marketplaces. In *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*. Berlin: Springer, Heidelberg, 101-110.

[62] Holt, T. J., & Smirnova, O. (2014). *Examining the structure, organization, and processes of the international market for stolen data*. Pristupljeno 25.02.2018. na https://www. ncjrs. gov/pdffiles1/nij/grants/245375. pdf.

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

[64] 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.

[65] Campana, P. (2016). Explaining criminal networks: Strategies and potential pitfalls. *Methodological Innovations*, *9*, 1-10.

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

[67] Wall, D. (2005/15). The Internet as a conduit for criminal activity. In A. Pattavina, (Ed), *Information Technology and the Criminal Justice System*, Thousand Oaks, CA: Sage, 77-98.

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

[69] Леонов, А. П., и Черкасова, Т. В. (2004). О криминологических признаках организованной киберпреступности. Crime-research. ru А. Сухаренко (17.04.2004), 185-187. Pristupljeno 03.03.2018. na https://scholar.google.com

[70] Шинкаренко, А. П. (2011). Организованная киберпреступность. Pristupljeno 02.04.2018. na https://scholar.google.com.

[71] United Nations Office on Drugs and Crime (UNODC). (2002). Results of a pilot survey of forty selected organized criminal groups in sixteen countries. New York: United Nations.

[72] Bosco, F. (2013). Cyber crime is geting organised. Hague: World forum. Pristupljeno 10.05.2018. na https://www.scribd.com/document/225998776/Francesca-Bosco.

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

[74] 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.

[75] Tropina, T. (2010). Cybercrime and Organized Crime. *Freedom from Fear Magazine*, *7*(3). Pristupljeno 12.04.2018. na http://f3magazine.unicri.it/?p=310.

[76] Shelley, L. (2003), Organized crime, terrorism and cybercrime. In A. Bryden & P. Fluri, (Eds.), *Security sector reform: institutions, society and good governance.* Baden-Baden: Nomos Verlagsgesellschaft.

[77] Goodman, M. (2015). *Future crimes: Everything is connected, everyone is vulnerable and what we can do about it*. Anchor. Pristupljeno 25.05.2018. na http://executivebookreview.com/wp-content/uploads/2017/04/Future-Crimes.pdf.

[78] 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.

[79] Holt, T. J. (2013). Examining the forces shaping cybercrime markets online. *Social Science Computer Review*, 31: 165-177.

[80] 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.

[81] Leukfeldt, E. R., Kleemans, E. R., & Stol, W. P. (2017a). A typology of cybercriminal networks: from low tech locals to high tech specialists. *Crime, Law and Social Change, 67*(1), 21-37.

[82] Holt, T. J., & Kilger, M. (2012) . Examining Willingness to Attack Critical Infrastructure Online and Offline. *Crime & Delinquency, 58* (5): 798–822.

[83] 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.

[84] Hopkins, M., & Dehghantanha, A. (2015). Exploit kits: the production line of the cybercrime economy?. In *Information Security and Cyber Forensics (InfoSec), 2015 Second International Conference on* (pp. 23-27). IEEE.

[85] 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.

[86] Thomas, R., & Martin, J. (2006). The underground economy: priceless. *USENIX; login*, *31*(6), 7-16.

[87] Chu, B., Holt, T. J., & Ahn, G. J. (2010). Examining the creation, distribution, and function ofmalware on-line. US: National Institute of Justice/NCJRS.

[88] 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.

[89] Glenny, M. (2011). *Darkmarket: Cyberthieves, cybercops and you*. Random House.

[90] Hutchings, A., & Holt, T. J. (2014). A crime script analysis of the online stolen data market. *British Journal of Criminology*, *55*(3), 596-614.

[91] Stone-Gross, B., Holz, T., Stringhini, G., & Vigna, G. (2011). The Underground Economy of Spam: A Botmaster's Perspective of Coordinating Large-Scale Spam Campaigns. *In Proceedings of LEET,* 11.

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

[93] Aspers, P. (2007). Theory, reality, and performativity in markets. *American Journal of Economics and Sociology*, *66*(2), 379-398.

[94] Holz, T., Engelberth, M., & Freiling, F. (2009). Learning more about the underground economy: A case-study of keyloggers and dropzones. *Computer Security–ESORICS 2009*, 1-18.

[95] Herley, C., & Florêncio, D. (2010). Nobody sells gold for the price of silver: Dishonesty, uncertainty and the underground economy. *Economics of information security and privacy*, 33-53.

[96] Pohl, H. (2009). Zero-day und less-than-zero-day vulnerabilities und exploits. In *Forschungsspitzen und Spitzenforschung* (pp. 113-123). Physica-Verlag HD.

[97] Powell, W. W. (1990). Neither market nor hierarchy: Network forms of organization. *Research in Organizational Behavior, 12,* 295-336.

[98] Eurojust. (2016). *Europe-wide action targets money mule schemes.* Eurojust – Europol (01.03.2016). Pristupljeno 10.05.2018. na http://www.eurojust.europa.eu/press/ pressreleases/ pages/2016/2016-03-01.aspx.

[99] Yip, M. (2011). An investigation into Chinese cybercrime and the applicability of social network analysis.

[100] Министарство унутрашњих послова РС (МУП). (2018). Саопштења (08.02.2018). Београд: МУП. Pristupljeno 09. 05. 2018. na http://www. mup. gov. rs/wps/portal/sr/.