*Kriminalističke teme*
*Zbornik radova*
Godina XIX, Broj 5, 2019.
ISSN 1512-5505



# KRIMINALNI POTENCIJAL FENOMENA DARKNET-a
# THE DARKNET PHENOMENON CRIMINAL POTENTIAL

**Pregledni naučni rad**

**Sergej Uljanov**[85]
**Milan Milošević**[86]

**Sažetak**

**Inspiracija za rad:** Mogućnosti savremene globalne komunikacije inspirisale su autore da usmere pažnju na pogodnosti delova svetske informatičke mreže za kriminalno delovanje.
**Ciljevi rada:** Sledstveno tome, cilj ovog rada posvećen je istraživanju kriminalnog potencijala skrivene zone World Wide Web-a.
**Metodologija/dizajn:** Poštujući metodološki model utvrdjivanja fenomenoloških determinanti od opšteg preko posebnog ka pojedinačnom, autori nastoje da odrede pojmovni volumen najzagonetnijeg dela skrivenog Web-a čineći distinkciju pojmova Worl Wide Web, Web i Deep Web kroz sagledavanje njihovog odnosa. Finalno, u pojedinačnom segmentu, autori prikazuju fenomen Darknet-a i specifičnost njegove relacije sa Deep Web-om.
**Ograničenja rada/istraživanja:** Autori su svesni ograničenja ovakvog istraživanja, koje mogu predstavljati neosnovane predstave o globalnoj komunikaciji kao nasušnom vidu socijalizovanog ispoljavanja ljudskih prava i sloboda.
**Rezultati:** Kriminalni potencijal Darknet-a autori utvrđuju posredstvom uticaja intenziteta međunarodne prisutnosti pojava kriminalnih čvorišta, kriminalnih tržišta i dejstva faktora polikriminaliteta.
**Generalni zaključak:** Ukazivanje na postojanje Darknet-a, te njegov kriminalni potencijal, kako smatraju autori, čini neophodnu osnovu za dalja istraživanja skrivenih načina globalne komunikacije i njihovo kriminalizovanje.
**Opravdanost istraživanja/rada:** Upravo zato, autori nedvosmisleno ovim radom pokušavaju da jasno prikažu kriminalnu opasnost skrivenih zona mogućnosti globalne komunikacije i njen razorni uticaj na vrednosti savremene društvene zajednice.

**Ključne riječi**

Darknet, Deep Web, World Wide Web, kriminalno čvorište, kriminalno tržište, polikriminalitet

[85] Zaposlen u Ministarstvu unutrašnjih poslova Republike Srbije i docent Fakulteta za poslovne studije i pravo Univerziteta "Union – Nikola Tesla", Beograd, sputnik970@gmail.com
[86] Fakultet za poslovne studije i pravo Univerztiteta „UNION - Nikola Tesla", Beograd, Republika Srbija, milanmilos@gmail.com

**Summary**

**Reason for writing and research problem (s):** Nowadays global communication possibilities have inspired the authors to pay attention to having parts of world informatics network suitable enough to be exposed criminally.
**Aims of the paper (scientific and/or social):** Subsequently, the article's goal sticks to research of the criminal potential of a zone hidden within the World Wide Web.
**Methodology/Design:** Following the methodological model of establishing the phenomenological determinants from general through special to unique, the authors try to define terminological range of the most inscrutable bit within the hidden Web by doing distinction among the terms of the World Wide Web, the surface Web and the Deep Web with scoping their relation. Finally, at unique stage, the authors show the Darknet phenomenon and particularity of its relation to the Deep Web.
**Research/Paper limitation:** The authors are fully aware of the exploration limits that could be supportive to the arbitrary clues on global communication as necessary mode of human rights and freedoms being exposed socialized like.
**Results/Findings:** The criminal potential of the Darknet is to be established by the authors through influences of criminal hubs, criminal markets and poly-criminality being presented intensively as much as internationally.
**General Conclusion:** Pointing to the Darknet existence and its criminal potential, as the authors deem, creates essential ground to further researching of clandestine ways to communicate globally and their criminalization.
**Research/Paper Validity:** Thus, the authors intend undoubtedly to show in the article clearly the criminal danger of hidden zones of possibility to communicate globally and its devastating influence to the values of modern society.

**Keywords**

the Darknet, the Deep Web, the World Wide Web, criminal hub, criminal market, poly-criminality.

## UVOD

Danas, gotovo, da je uvreženo mišljenje da se pretragom na Googl-u može doći do traženog podatka prema kriterijumu zadatog pojma. Ipak, postoji čitavo on-line more informacija, koje je van domašaja Googl-a i ostalih javno dostupnih pretraživača Interneta. Zbog nepoznavanja okruženja i uslova koji kriminalno određuju taj nepoznati sajber prostor za traganje za podacima i razmenu informacija, akcije organa krivičnog gonjenja bivaju suštinski ograničene bez značajnije podrške donosilaca političkih odluka koji bi kreirali i javno promovisali koncept podizanja svesti na širem planu.

Razmere ovog nevidljivog dela Interneta su bezgranične. Broj web sajtova koji nisu indeksirani, kao što je slučaj u opšte poznatom i dostupnom površinskom delu World Wide Web-a, ispunjava Deep Web za koji se procenjuje da je 400 do 500 puta obimniji od svog vidljivog opozita. U vidljivom Web-u web sajtovi su registrovani i dostupni javnim pretraživačkim servisima, dok u tamnoj zoni Interneta odnosno dubokom Web-u to nije slučaj. Diskretnost ispod površinskog Web-a, svakako, pogoduje onim savesnim i dobronamernim korisnicima Interneta čije aktivnosti nisu kriminalne a anonimost čini imperativ u

njihovom delovanju, kao što je slučaj sa istraživačkim novinarstvom, političkim oponentima i uzbunjivačima. Međutim, postoji i tamni deo nevidljivog Web-a, čiiji informatički prostor neutvrđenog volumena sadrži podatke koji se dovode u vezu sa ilegalnim aktivnostima. Ova skrivena zona, poznata kao Dark Web ili Darknet, služi kao komunikacioni kanal imeđu organizovanih kriminalnih grupa, terorističkih ćelija, kao i onih korisnika Interneta koji tragaju za nedozvoljenim proizvodima. U njoj su virtuelna kriminalna tržišta, koja nude *inter alia* krijumčarenu robu, opojne droge, falsifikovane dokumente, ukradeno vatreno oružje, podatke o kreditnim karticama, te sadržaje u vezi sa iskorišćavanjem dece i maloletnih osoba u pornografske svrhe.

Obzirom na stalno uvećavanje nevidljivog Web-a i njegovog skrivenog pratioca Darkneta, eksponencijalno raste i rizik od podizanja efikasnosti ilegalnih aktivnosti zbog nemogućnosti kontrole njihove pripreme i organizovanja. Odgovor na ovakve izazove mora biti multidisciplinaran i zasnovan na platformi strategije nacionalne bezbednosti, jer sajber pretnje podjednako ugrožavaju ljudska prava i slobode, zaštitu života i zdravlja čoveka, kao i međunarodne tokove globalne ekonomije.

Uprkos ostvarenom napretku u geografskom determinisanju sveta i dalje postoje predeli naše planete koji nisu u potpunosti dokumentovani. Slično tome, novi virtuelni svet nepoznatih granica određen kao sajber prostor i pored naših napora da ga spoznamo u proteklih par decenija, ostaje zatvoren i nevidljiv za veliku većinu korisnika Interneta. Nažalost, masovno nepoznavanje informatičkog okruženja u kome živimo i dalje odnosi prevagu nad pojedinačnom upućenošću u mogućnosti i strukturu World Wide Web-a. Korišćenje pretraživača poput Googl-a i Bing-a, je samo plovidba uz obalu sajber mora čije granice nismo sposobni da sagledamo. Čitav jedan novi svet, sa svojim relacijama, okolnostima, uslovima i okruženjem, još uvek čeka da bude istražen, a činjenica njegove virtuelnosti nimalo ne umanjuje ovu potrebu.

## STRUKTURA SVETSKOG WEB-a

Kako razumeti fenomen World Wide Web-a? Da li zamišljeni prostor može biti struktuiran? Da li in esentio virtuelnost može imati neku materijalnu komponentu? Za početak valja odrediti gradivnu jedinicu World Wide Web-a. Mišljenja smo da je to informacija jer se u ovom virtuelnom sajber prostoru konstantno razmenjuju podaci za kojima tragaju zainteresovani korisnici Interneta. Adrese na kojima se do potrebnih podataka može doći dostupne su na površinskom Web-u odnosno u vidljivoj zoni World Wide Web-a. Ovo dalje znači da svetsko informatičko more, pored svoje površine, mora imati i svoj dubinski deo nevidljiv i nedostupan za redovno pretraživačko postupanje.

Kao i u fizičkom svetu, odnos prostranstva površine i volumena dubine mora nije ravnomeran, pogotovo ukoliko dubina nije određena već daleko premašuje granice mogućnosti našeg saznanja obzirom na virtuelnost svoje prirode. Analogno tome, strukturu World Wide Web-a možemo zamisliti kao more podataka, čiju površinu predstavlja vidljivi Web, dok skriveni duboki Web oslikava njegovu nepoznatu dubinu neshvatljivih razmera. Tako

bi dve osnovne komponente svetskog Web-a bile razgraničene faktorom vidljivosti i dostupnosti na površinski i Deep Web.

Tehnički nije moguće izmeriti obim dubokog Web-a, ali ako pođemo od činjenice da Google svojim pretraživačkim kapacitetom pokriva do 16% površinskog Web-a, a da samo na 60 najvećih sajtova u Deep Web-u ima 40 puta više pohranjenih podataka nego u celom vidljivom delu World Wide Web-a, tada možemo makar grubo predstaviti sliku strukture svetskog Web-a i međusobni odnos njenih ključnih delova (Sui, Caverlee i Rudesill, 2015).

Kao što u tmini morskih dubina postoje rasedi u podmorju, tako i duboki Web ima svoju tajnovitu tamnu oblast tzv. Dark Web ili Darknet, koji okuplja sve destinacije za pretragu koje se ne mogu dostići putem Interneta na redovan način. Tamna strana Deep Web-a ima brz rast, koji je direktno uslovljen anonimnim šerovanjem fajlova preko mreže sa adresama koje nisu indeksirane i koje nisu vidljive za standardne pretraživače površinskog Web-a. Kao faktor uvećavanja volumena dubokog Web-a, Darknet postaje njegova ključna komponenta zbog čega ga posmatramo kao još jedan od kompleksnih slojeva višedimenzionalne strukture World Wide Web-a.

Za razliku od informatičkog saobraćaja u vidljivom Web-u, ali i od nekih delova Deep Web-a, sajtovi Darkneta mogu se posetiti isključivo anonimno. Imajući u vidu da duboki Web raspolaže najvećim brojem „živih" informacija na Internetu, struktura njegovih sajtova više je determinisana vertikalno nego horizontalno pružajući mogućnost dubinskih pretraga koje nisu izvodljive na površinskom Web-u. Uslovi dubokog i tamnog Web-a nameću zbog težeg pristupa podacima njihovu veću zaštićenost, zbog čega su eksploatisani kako od strane timova uposlenih na poverljivim resornim projektima, tako i od pojedinaca i grupa koji se dovode u vezu sa najširim spektrom kriminalnih aktivnosti predstavljajući svojevrsan izazov za hakerske napade usmerene na obe navedene kategorije korisnika.

## DUBOKI I TAMNI WEB

Ekspanziji Deep Weba i Darkneta doprinose brojne informatičke tehnologije. Tako, volumen dubokog Web-a uvećavaju ubicomp, cloud i mobilno računarstvo, ali i sistemi umreženih senzora, dok rast tamnog Web-a podstiču razvoj u obezbeđivanju anonimnog i bezbednog pristupa hosting servisima, Dark Wallet platforma za omogućavanje anonimnih transakcija virtuelne valute Bitcoin i unapređivanje crimeware-a kao zloćudnih softvera za automatsko izvođenje on-line sajber napada radi istovremenog slanja zaraženih poruka na veliki broj elektronskih adresa, krađe podataka i iznude. Razne vrste virtuelnog novca, kao što su Bitcoin, Darkcoin ili Peercoin u upotrebi su pri izvršenju anonimnih transakcija u svrhu poslova koji se odvijaju na kriminalnim tržištima Darkneta. Hakeri skriveni iza ponuda za posao i višejezičkih centara za upućivanje poziva, takođe, ubrzavaju širenju dimenzije tamnog Web-a. Pored navedenog, Darknetove mogućnosti legitimno koriste novinari, uzbunjivači i zaštitnici ljudskih prava, kojima je anonimnost neophodna radi sopstvene zaštite i garanta uspeha u radu (Sui, Caverlee i Rudesill, 2015).

Za istraživanje Deep Web-a i Darkneta potrebni su posebni informatički alati i tehnike. Neki od njih su slični onima za pretraživanje površinskog Web-a. U korelaciji sa namerama i željama korisnika, različite dubine svetskog Web-a iziskuju upotrebu određenih informatičkih tehnika. U najvećem broju slučajeva, generalno se primenjuju dva posebna ali međusobno povezana protokola pristupanja dubokom i tamnom Web-u. Najpre, moguće je doći do ovih naročitih protokola upotrebom regularnih pretraživača, kao što su Internet Explorer, Firefox ili Chrome Safari. Ali, postoje specifični protokoli kojima se može pristupiti samo preko pretraživača TOR. Valja napomenuti da postoje grupe korisnika koje razvijaju protokole pristupa kreiranjem posebnih pretraživača linkova odnosno primenom softvera za komunikaciju putem aplikacija ili drugih različitih komponenti komunikacijskih softvera. Ovi alternativni modusi za ulazak u nevidljivi Web prilagođeni su potrebama okruženja različitih zona Deep Web-a. Ipak, pravi izazov predstavlja činjenica da svi do sada kreirani protokoli mogu samo da ostvare ulaz u mali deo dubokog Web-a (Sui, Caverlee i Rudesill, 2015). Zbog toga je i dalje neophodno posećivati tačno određene on-line direktorijume odnosno skrivene grupe web sajtova koji su diskretno popisani prema traženoj destinaciji korisnika, kao što je npr. https://sites.google.com/site/howto-accessthedeepnet/working-links-to-the-deep-web. Obzriom da ovi web sajtovi nisu indeksirani, oni ne mogu biti pronađeni putem regularnih pretraživača. Međutim, njihove web adrese mogu biti locirane na alternativne načine, tako da im se posle otkrivanja može pristupiti upotrebom standardnog pretraživača iako se nalaze u dubokom Web-u.

Neke od javnih baza podataka nalaze se u nevidljivom Web-u jer se najveći deo njihovog sadržaja ne može pretražen redovnim protokolima. Veliki broj korisnika Interneta dolazi u situaciju da ostvari interakciju sa delovima Weep Web-a upotrebom standarnih načina pretrage, a da nikada to ne sazna. Tako je npr. biblioteka američkog Kongresa sadržana u on-line bazi podataka na adresi www.loc.gov i može joj se pristupiti na standardan način iz površinskog Web-a, a da se pri tom ova baza podataka nalazi u Deep Web-u. Postoji veliki broj sajtova na kojima su ekonomski podaci, a koji su deo dubokog Web-a, kao što su: FreeLunch.com, Census.gov, Copyright.gov, PubMed, Web of Science, WWW Virtual Library, Directory of Open Acces Journals, FindLaw, te Wolfram Alpha (Sui, Caverlee i Rudesill, 2015).

Postoje, takođe, brojne baze podataka kojima se ne može pristupiti besplatno, kao npr. Westlaw i LexisNexis, te baze podataka sa obaveznim registrovanjem korisnika, što je slučaj sa velikim brojem on-line univerzitetskih biblioteka, koje su u oba navedena slučaja nalaze u Deep Web-u. U zoni nevidljivog Web-a nalazi se i veliki broj ličnih podataka koji su obezbeđeni lozinkama, poput PayPal računa. Pristup u ove delove dubokog Web-a je tehički limitiran i pravno zaštićen.

Sa opštom upotrebom Web 2.0, unapređene verzije Web-a, i mobilnih telefona sa višestrukom namenom, ogroman broj informacija pohranjen je na različite društvene mreže. Ovim podacima ne može se pristupiti upotrebom standardnih pretraživača. Neophodna je prethodna autorizacija korisnika kroz registrovanje ili ostvarivanje tzv. „prijateljstva“ sa drugim određenim grupama korisnika. Neki drugi servisi, kao što su Twitter i Facebook,

omogućuju javno dostupnu aplikaciju, kako bi korisnici mogli da pribave podatke preko takvih društvenih mreža u širem obimu. Ali mnoge od ovakvih društvenih mreža, poput YikYak i Wechat, zahtevaju pristupnu identifikaciju korisnika i ograničavaju dostupnost svojim masivnim bazama podataka iz razloga održavanja bezbednosti i poštovanja privatnosti.

U zonama Deep Web-a ostvaruje se i instant razmenjivanje poruka, kao još jedan od izvora podataka. Od prethodne forme on-line soba za razgovore, instant razmena poruka prerasta u komunikaciju između dva korisnika koja se ne arhivira, te tako privatnost razmenjenih podataka ostaje nenarušena. Ovaj prinic je u širokoj upotebri u on-line razgovorima i pružanju tehničke podrške.

U današnje vreme, neke mobilne aplikacije dozvoljavaju korisnicima da sačuvaju pregled razmene poruka na lokalnom nivou, tako da u slučaju potrebe mogu da pristupe ovom pregledu. Ipak, instant razmenjivanje poruka sve više postoje bazirano multimedijski, što otežava arhiviranje pregleda primljenih i poslatih poruka. Pristup ovom delu dubokog Web-a u kome se mogu pohraniti podaci iz razmenjenih poruka, moguć je ukoliko se u trenutku obavljanja konverzacije izvrši snimanje desktopa odnosno video zapisivanje.

Kao deo Deep Web-a, u poslednje vreme, Darknet sve češće služi za dogovaranje poslova, vođenje razgovora, distribuciju pojedinačnih podataka i fajlova, te transfere virtuelnog sredstva plaćanja. Potpuna anonimnost skrivenih kutaka Darkenta obezbeđuje privatnost on-line aktivnosti korisnika i za očekivati je progresivan rast njihovog prisustva u ovom tamnom delu Web-a. Da bi ovakav protokol pristupa web stranama u zoni Darkneta mogao biti realizovan, neophodna je upotreba specijalizovanog nestandardnog pretraživača, kao što je TOR, koji obezbeđuje anoniman pristup web adresama u Darknetu uz istovremeno maksimalno otežavanje eventualnog praćenja nečijih on-line aktivnosti u okviru protokola TOR-a. Za razliku od uslova u kojima se odvija komunikacija među korisnicima na površinskom Web-u, Darknet destinacije u okviru TOR-ove pretraživačke mreže često nisu stabilne jer bivaju nedostupne satima ili danima, a ponekad mogu i da nestanu uz neizvesnost ponovnog pojavljivanja. Često se sporo otvaraju, obzirom da TOR pravi konekciju kroz nasumično selektovane servere kako bi garantovao anonimnost prisustva korisnika.TOR pretraživač predviđen je za operativne sisteme mobilnih uređaja Android i iOs, što ih čini nebezbednim i manje preporučljivim za upotrebu prevashodnog broja prosečnih korisnika. Ovo se svakako odnosi i na TOR-ove dodatke za druge vrste pretraživača, što samo pojačava izazove i neizvesnost kretanja korisnika kroz duboke i tamne vode nevidljive sfere World Wide Web-a (Sui, Caverlee i Rudesill, 2015).

## KRIMINALNI ATRIBUTI DARKNET-a

Poslednjih godina, Darknet je postao jedna od tema o kojoj se vrlo često raspravljalo u krugovima sajber bezbednosti. S jedne strane, skrivene komunikacione mreže na Internetu su znak dostignute slobode građana, dok s druge strane, ove mogućnosti nisu ništa drugo do platforme za ispoljavanje i ispunjavanje želja korisnika rukovođenih kriminalnim

intencijama. Uopšte uzev, mediji profilišu Darknet kao okruženje za nesmetano odvijanje kriminalnih aktivnosti, koje zato ima predominantne kriminogene predispozicije (Mirea, Wang i Jung, 2019). Brojne medijske agencije ističu da se tamni Web i njegov prateći pretraživački servis TOR prevashodno upotrebljavaju za vršenje ilegalnih radnji (Chandran, 2015; Farell, 2017; McGoogan, 2016; Moloney, 2016; Samson, 2017; Wiesmann, 2015). Kao primer navodimo dva novinska naslova koja upućuju na navedeno mišljenje o kriminogenosti Darkneta, a to su „Darknet može da predstavlja rizik od urušavanja sektora Interneta" (Samson, 2017) i „TOR pretraživač Dark Web-a se gotovo sasvim koristi u kriminalne svrhe, prema istraživanjima" (McGoogan, 2016). Ova negativna percepcija Darkneta naširoko se plasira od strane državnih organa, ali i korisnika koji su vođeni strahom od nepoznatog informatičkog okruženja tamnog Web-a (Murray, 2014). Tako je npr. jedan od rukovodilaca bezbednosno obaveštajne agencije britanske Vlade i oružanih snaga (Government Communications Headquarters-GCHQ) uporedio Darknet sa Divljim Zapadom, tvrdeći da je neophodno uspostaviti kontrolu nad ovom skrivenom zonom dubokog Web-a (Omand, 2016).

U akademskim krugovima, prva kriminološka istraživanja ukazala su na vezu Darkneta sa kriminalnim aktivnostima označavajući tamni Web kao „piratsko skrovište" za učinioce krivičnih dela, navodeći kao primer anonimni promet nedozvoljenom robom, poput narkotika, koji se plaća virtuelnim novcem kao što je Bitcoin (Buxton i Bingham, 2015). Prema nekim autorima, ilegalna trgovina opojnom drogom, zaista, je jedna od izuzetno čestih nedozvoljenih aktivnosti na Darknetu (Dolliver, 2015; Owen i Savage, 2015). Početkom 2016. godine, ukupan prihod od opijata na Darknetovom kriminalnom tržištu opojnih droga bio je procenjen na iznos od 12.000.000 do 21.100.000 američkih dolara (Kruithof i sar., 2016). Ovo skriveno kriminalno tržište za ilegalni promet opojnom drogom predstavlja ozbiljnu brigu za organe za primenu zakona širom sveta (Horton-Eddison i Di Cristofaro, 2017). Druge ilegalne transakcije na ovakvim tržištima odnose se na nedozvoljenu trgovinu oružjem, kreditnim karticama i drugim ličnim podacima, te egzotičnim životinjskim vrstama (Chertoff i Simon, 2015; Holm, 2017). Ovo nam daje za pravo da tvrdimo da je polikriminalitet jedan od ključnih kriminalnih atributa Darkneta, kao i da okolnosti tamnog Web-a koje garantuju anonimnost korisnika afirmativno deluju na formiranje virtuelnih kriminalnih čvorišta kao pratećeg efekta usmerene razmene informacija u svrhu pripremanja, organizovanja, koordiniranja i činjenja kriminalnih aktivnosti na međunarodnom nivou.

Širenje „crnih" tržišta na Darknetu pomognuto je razvojem informatičkih tehnologija, koje obezbeđuju komunikacione mreže bazirane na anonimnosti, privatnosti i upotrebi virtuelnog novca (Mirea, Wang i Jung, 2019). Prema nekim mišljenjima, anonimna priroda prisustva korisnika u zoni Darkneta pojačava rizik od krađe identiteta (Holms, 2017). U tom pravcu postoje i shvatanja da obim rizika i pretnji, koji vrebaju iz okruženja Darkneta, još uvek nije dovoljno istražen (Byrne i Kimball, 2017). Najveći broj istraživanja Darkneta, do sada, bio je usmeren na kriminalne aktivnosti i njihove tehničke aspekte (Qaing i sar., 2014; Wright, 2008; Zheng i sar. 2013). Samo nekoliko projekata bilo je posvećeno pokušajima formiranja slike o sociološkoj i psihološkoj strani Darkneta (Everett, 2015; Lacson i Jones, 2016; Van Hout i Bingham, 2013).

Darknet je, po svemu sudeći, ispunjen nekontrolisanim zloćudnim informatičkim sadržajima i služi kao zaklon za mnoge uznemirujuće aktivnosti ispod vidljivog površinskog dela World Wide Web-a. Analizom vodećih ponuđača u nevidljivom Web-u, uočen je intenzivan ilegalni promet lakom opojnom drogom, zabranjenim sintetičkim drogama, te prepisanim lekovima kao što su Ritalin i Xanax. Za pristup sajtovima u Darknetu najviše se koriste protokoli van standardnih paramatera HTTP/HTTPS, kao što su IRC, IRCS, Gopher, XMPP i FTP. Hiljade sumnjivih sajtova može se dostići putem navedenih neregularnih protokola radi ostvarivanja pristupa sadržajima koji se nalaze u vezi sa zaraženim reklamnim materijalima, načinima za ulazak na blokirane web destinacije i iskorišćavanjem dece u pornografske svrhe. Agresivne grupe malware-a, kao što su VAWTRAK i CryptoLocker, koriste TOR kao komponentu svoje konfiguracije i tako se plasiraju u sisteme korisnika koji se kreću kroz okruženje Darkneta.

Ukidanje kriminalnih tržišta na Darknetu nije trajno rešenje koje će doprineti smanjenju intenziteta i obima ilegalne trgovine opojnom drogom jer će ona biti nastavljena kroz online radnje i forume koji su tematski usmereni. U tamnom Web-u rasprostanjena je upotreba virtuelne valute Bitcoin, ali i njenog „perača“ kao što je EasyCoin u svrhu još većeg skrivanja kretanja virtuelnih novčanih tokova. To je siguran pokazatelj da su u Darknetu, time i u Deep Web-u, prisutni nosioci kriminalnih aktivnosti, koji trguju ukradenim računima, putnim ispravama i identitetima posredstvom lažnih poslovnih foruma, kojom prilikom ističu kompletan opis ponuđene robe uz njenu cenu. Pored toga, prisutne su i ponude za usluge plaćenih likvidacija maskirane poslovnim uslugama na kriminalnim tržištima Dark Web-a (Ciancaglini i sar., 2015).

Kriminalna tržišta nedvosmislen su primer kriminalizovanosti Darknet okruženja, u kome se krije identitet učesnika transakcije zabranjenim proizvodima, obavljaju poslovi putem upotrebe virtuelnog novca i na svaki način izbegava regularnost u postupanju. Tržište opojnom drogom kao što je Silk Road bilo je primer informatičkog prostora u kome su se na Darknetu vršile nelegalne transakcije, koje su podrazumevale promet krijumčarenom robom. Čak i ako je reč o legalnim proizvodima u uslugama, na Darknetu se njihova nabavka i prodaja vrše uz izbegavanje plaćanja taksi i izbegavanje kontrole nad njihovim uvozom i izvozom (Sui, Caverlee i Rudesill, 2015). Dark Web služi ne samo kao deo dubokog Web-a kome se izvode ilegalne transakcije roba i usluga, te trendovskih hakerskih alata, već je i bojno polje u kome se vode sajber bitke i obračunavaju pojedinačno i grupno nosioci sajber špijunaže (Goodman, 2015).

Pogodnosti za realizovanje kriminalnih aktivnosti očigledan su preduslov za postojanje kriminalnih predispozicija nekog dela World Wide Web-a. S tim u vezi, prema nekim tvrdnjama Darknet je primer informatičkog okruženja čiji uslovi su više nego afirmativni za odvijanje široke skale raznolikih nezakonitih postupanja. Dark Web služi kao paravan, neutvrđenih razmera, za plasiranje i ilegalnu trgovinu opojnom drogom, oružjem, retkim životinjskim vrstama, te ukradenom robom i podacima, čime se ostvaruje kriminalni profit. Uz navedeno, prisutni su i kockarski sajtovi, mogućnost iznajmljivanja lopova i ubica, te čitava skladišta sa sadržajima koji se odnose na iskorišćavanje dece u pornografske

svrhe (Chertoff i Simon, 2015). Ipak, još uvek nema saznanja o širini rasprostanjenosti ovakvih sajtova na Darknetu. Tek 1,5% korisnika TOR-a posećuje ove kategorije destinacija u Dark Web-u (Greenberg, 2015). I dalje je nepoznat udeo adresa koje su u vezi sa kriminalnim tržištima u tamnom Web-u, a još manje je jasno koliko je pristupa sajtovima sa ilegalnim sadržajima ostvareno putem TOR-a (Finklea, 2017).

Istraživači sa britanskog Univerziteta Portsmouth ispitivali su saobraćaj pretraživača TOR usmeren ka serivisima skrivenim u Darknetu, kojom prilikom su angažovali 40 kompjuterskih radnih jedinica za ostvarivanje pristupa putem TOR-a. Na taj način došli su do kontakta sa čak 45.000 on-line skrivenih servisa, kojima su mogli pristupiti u bilo kom trenutku (Greenberg, 2014). Istraživači su utvrdili da je oko 2% sajtova u TOR-ovoj pretraživačkoj mreži bilo identifikovano u vezi sa pedofilskim sadržajima, ali da je 83% poseta skrivenim sajtovima bilo usmereno na sajtove sa ovakvim sadržajima, što bi značilo da je u periodu u kome je vršeno istraživanje potražnja za nevedenim sajtovima bila višestruko veća od ponude. Ovakva nesrazmera može se objasniti, u nekom stepenu, prisustvom policije u Darknetu, ali i hakera koji iz brojnih razloga posećuju ovu vrstu sajtova, od namere da ih unište do krađe i preprodaje njihovih sadržaja (Greenberg, 2014).

Još jedno istraživanje sa londonskog Univerziteta King's College bilo je posvećeno otkrivanju skrivenig usluga u TOR-ovoj pretraživačkoj mreži. Upotrebom dva popularna pretraživača u Dark Web-u po imenu Ahmia i Onion City, istraživači su uspeli da identifikuju 5.205 „živih" web sajtova (Moor i Rid, 2016). Od ovog broja utvrđen je sadržaj njih 2.723 i oni su klasifikovani prema prirodi svojih sadržaja. Dalje je utvrđeno da 1.547 ovakvih sajtova ima nedozvoljen sadržaj. Ovo je bio uzorak na web sajtovima na kojima se u okviru TOR-a nude skrivene usluge. Preko ovog uzroka, istraživači su kontaktirali čak 300.000 web sajtova sa 205.000 jedinstvenih adresa u okviru TOR-ove mreže skrivenih servisa. Na dnevnom nivou, oko 30.000 ovakvih servisa bilo je povezano sa TOR-om, pri čemu je utvrđeno da saobraćaj koji se ostvaruje prema ovim servisima čini samo 3,4% ukupne aktivnosti koja se odvija u TOR-ovoj pretraživačkoj mreži. U narednoj fazi istraživanja broj utvrđenih dnevnih aktivnosti skrivenih servisa porastao je na 50.000 do 60.000 (https://metrics.torproject.org/, 2017).

Darknet je, svojom skrivenom pozicijom u okviru dubokog Web-a i kriminalnim atributima koje poseduje, uključen u veliki broj kriminalnih aktivnosti. On služi kao forum sa sobama za razgovor i komunikacionim servisima u svrhu planiranja i koordinacije u vršenju nelagalnih radnji. Tako su se na Darknetu, primera radi, razmenjivala mišljenja o izbegavanju poreza i načinima kako da se to izvede (Krebs, 2015). Okruženje tamnog Web-a obezbeđuje i platformu za krijumčarenje nedozvoljenim proizvodima, kao i robom koja potiče iz izvršenih krivičnih dela. Iz okrilja Darkneta vrše se neovlašćeni upadi u sisteme, pa se tako frekventno plasiraju malware-i radi lociranja kreditnih i debitnih kartica da bi se tako dobijeni podaci zloupotrebljavali, prodavali i kupovali na kriminalnim tržištima tamnog Web-a (Finklea, 2017). Upravo tako se RAM scrapers, kao jedna vrsta malware-a, može nabaviti i posredno pokrenuti za štetno delovanje okviru prodajnih sistema (Zetter, 2014).

Ukradeni podaci prodaju se na Darknetu i tako se ostvaruje zarada od ilegalnih aktivnosti (Finklea, 2017). Nakon jednog većeg upada u prodajne sisteme, na „crnim" tržištima Dark Web-a došlo je do poplave ponuđenih podataka sa ukradenih kreditnih i debitnih kartica, čiji broj je premašivao jedan milion, dok su se one prodavale za 20 do 100 američkih dolara po komadu (Krebs, 2013). Ove ponude otuđenih podataka sa platnih kartica, iz tzv. radnji sa karticama, samo su jedan od primera specifičnosti funkcionisanja kriminalnih tržišta na Darknetu (Wueest, 2015).

Ne samo što podaci mogu biti ukradeni i prodati u tamnom Web-u, već se to čini izuzetno brzo. Ponuđač BitGlass izveo je istraživanje načinivši tzv. trezor sa ukradenim podacima, koji je bio lažan, u kome se nalazilo 1.500 imena, brojeva socijalnog osiguranja, brojeva kreditnih kartica i drugih ličnih podataka, naravno izmišljenih za navedenu potrebu istraživanja. Potom je „trezor" plasiran na DropBox i drugih sedam poznatih „crnih" tržišta na Darknetu. U periodu od dvanaest dana, ovim podacima je pristupljeno oko 1.100 puta u 22 države (Jackson Higgins, 2015).

## PERSPEKTIVE TAMNOG WEB-a

Podizanje javne svesti o postojanju Darkneta može dovesti do njegove povećane upotrebe radi ostarivanja nelegalnih ciljeva. Ipak, ne smatramo da u budućnosti korisnici imaju dovoljno razloga da ostvaruju svoje regularne pretrage pod velom anonimnosti u okruženju tamnog Web-a. U međuvremenu, više je verovatno da će tehnološki razvoj u polju informatike dovesti do još većeg umanjenja vidljivosti tamnih delova Deep Web-a. U ovom trenutku, vodi se trka između pobornika neograničenih građanskih sloboda i organa za primenu zakona, u kojoj je primetno traganje za novim modusima podizanja nivoa anonimnosti i skrivanja tragova kretanja u okruženju Dark Web-a. Međutim, nesumnjivo je da trgovina nedozvoljenim proizvodima predstavlja jednu od najčešćih aktivnosti u dubokom Web-u, te da će anonimnost korisnika skrivenih servisa, kriminalnih tržišta i transakcija virtuelnim novcem, još više dobiti na značaju u izgradnji poverenja između prodavaca i kupaca bez postojanja posredničke uloge banke.

U dolazećim vremenima, možemo očekivati potpuno decentralizovana tržišta koja funcionišu prema blockchain tehnologiji, koja isključuje posredničku ulogu bilo koje firme ili banke u obavljanju transakcije između prodavca i kupca. Na ovaj način već funkcionišu tokovi virtuelnih valuta koji nisu određeni domicilno jer takva valuta, kao npr. Bitcoin, nije nacionalno određena kao sredstvo plaćanja. Ova tehnologija bazira na principima primene teorije igara u ekonomiji i finansijama i otklanja teret koji predstavljaju posrednički subjekti u kreiranju i održavanju novčanih tokova. U ovako idealnoj postavci jedini problem može predstavljati činjenica da virtuelni novac neizostavno čini sredstvo plaćanja u dubokom i tamnom Web-u zbog čega će njegovi tokovi biti sve manje vidljivi i mogući za praćenje. Opasnost dolazi i od naprednih malware-a, koji će na svaki način pokušati da ugroze i eksploatišu blokchain tehnologiju koristeći odsustvo kontrole posredničkog subjekta u finansijskim kretanjima (Ciancaglini i sar., 2015).

U kriminalnoj sferi, naručioci likvidacije visoko profilisane mete činiće to uz jake garancije da se njihovom postupanju ne može uću u trag. Ne može se očekivati da će trgovci opojnom drogom želeti da svoja kriminalna tržiša postavljaju na on-line lokacije, na kojima ona mogu lako biti uočena od strane policije odnosno na adresama čiji „blizanci" već postoje na površinskom Web-u. Anonimnost će biti primaran uslov i prilikom prodaje ukradenih pasoša i kreditnih kartica, te ličnih podataka u vezi sa adresama i kontakt detaljima (Ciancaglini i sar., 2015).

Ali, pored diskretnosti u vršenju kriminalnih aktivnosti, postoje i drugi brojni razlozi zbog kojih korisnici žele da budu anonimni prilikom posete sajtova uz tendenciju da se njihovo kretanje na Internetu ne može pratiti, te da se lokacije takvih sajtova ne mogu utvrditi. Korisnici kojima je neophodno da zaštite svoju komunikaciju u odnosu na mere kontrole državnih organa, uvek će insistirati na skrivenosti koju pružaju okolnosti Darkneta. Uzbunjivači neće pristati da svoje insajderske informacije dele sa novinarima i da pri tom ostavljaju bilo kakav trag o tome. Politički neistomišljenici u restriktivnim režimima zahtevaće anonimnost prilikom obaveštavanja svetske javnosti o kršenju ljudskih prava i ograničavanju sloboda u svojim matičnim državama.

Na osnovu navedenog možemo zaključiti da ni svaki korisnik Darketovog okruženja ne mora biti samo zbog toga podrazumevan kao potencijalni nosilac ileganih aktivnosti. Anonimnost Darkneta ne mora u svakom slučaju biti preduslov sajber napada ili formiranja kriminalnog tržišta. Prema nekim mišljenjima, Darknet doprinosi razvoju konstruktivnih socijalnih i političkih vrednosti jer uslovljava poštovanje prava privatnosti i naprednog korišćenja virtuelnih valuta u legalne svrhe (Mirea, Wang i Jung, 2019). Ove činjenice ne umanjuju, kako smatramo, moguću kriminalizovanost Darkneta, ali svakako čine temelj za razvoj perspektive tamnog Web-a, kako u smislu davanja prostora za punu slobodu delovanja ljudske kreativnosti, tako i za jačanje razornog dejstva njenog kriminalnog antipoda.

## ZAKLJUČAK

Da li ćemo ikada dosegnuti krajnje granice World Wide Web-a i potpuno razumeti kapacitete Deep Web-a i Darkneta? U ovom trenutku, sasvim su izvesna tehnička i pravna ograničenja koja nas u ovome sputavaju. Neophodno je ovo pitanje razmatrati kao jednu od obaveznih tema za javne debate u kojima učestvuju, kako eksperti iz prakse tako i akademski istraživači, kako bi se makar približili spoznaji o multistrukturalnoj dimenzionalnosti i uticajima nevidljivog Web-a, te konstantnom porastu njegove nepristupačne dubinske komponente. U svakom slučaju, postavljanje balansa između imperativa zaštite sloboda i prava građana i brige za nacionalnu bezbednost obeležiće eru informatičke tehnologije, u kojoj će nesagledivi broj podataka skrivenih u dubokom Web-u predstavljati stalni izazov kreatorima politike u savremenom društvu.

Mišljenja smo da bi sledeći koraci mogli da budu neka vrsta putokaza u pokušajima našeg nesigurnog hoda kroz neprozirno prostranstvo dubokog i tamnog Web-a. Ab initio,

državni resor mora biti odgovoran za sajber bezbednost jer njime rukovode donosioci političkih odluka. U tom smislu, poželjno je odrediti nacionalnog koordinatora za pitanje sajber bezbednosti, određenog inokosno ili timski, koji će usmeravati aktivnosti na održavanju sajber bezbednosti. Zbog efikasnosti, nacionalno telo nadležno za sajber pretnje mora biti centralizovano i sa jedinstvenom bazom podataka. Naravno, temelj za delovanje protiv kriminalnih aktivnosti u sajber prostoru mora biti u posebnom normativnom sistemu, koji će biti posvećen zaštiti kritičke infastrukture i podataka koji se na nju odnose, te činiti osnov za uspostavljanje i delovanje agencija i organa za realizovanje sajber bezbednosti (Kovacs, 2018). Okvir strategije nacionalne sajber bezbednosti trebalo bi da bude određen harmonizovanjem postojećih propisa sa najboljom praksom na međunarodnom planu u oblasti procene rizika i pružanja usluga. Na taktičkom i operativnom nivou važno je izgraditi kapacitete za efikasno reagovanje u slučajevima sajber napada, pri čemu bi nosioci ovih aktivnosti bili za to posebno određeni resorni subjekti. Neophodnost podizanja svesti o sajber bezbednosti mora biti praćena sistemom obuka i planskom edukacijom, kao neizostvanim delovima koncepta nacionalnog obrazovnog sistema. Pored predominantno određene uloge državnih resursa u ostvarivanju sajber bezbednosti, nužno je zasnovati partnerstvo sa privatnim sektorom koje je funkcionalno i pouzdano, te fokusirano na različite oblasti koje mogu biti izložene sajber pretnjama (Kovacs, 2018). Naposletku, ali ne i manje značajno, jeste pitanje međunarodne saradnje, koje se nedvosmisleno i posledično nameće zbog činjenice nemogućnosti sprečavanja sajber pretnji u okvirima državnih granica, a time i olakšanog vršenja široke lepeze kriminalnih aktivnosti na svetskom planu.

Uvereni smo da bi efektivna međunarodna saradnja, u kojoj učestvuju funkcionalne nacionalne strategije sajber bezbednosti koncipirane na najboljim iskustvima inostranih resornih i vanresornih partnera, mogla da odredi dobar početak usmernih napora ka smanjivanju rizika od sajber opasnosti koja dolazi iz skrovitih delova nevidljivog Web-a.

## LITERATURA


- Buxton, J., & Bingham, T. (2015). The rise and challenge of dark net drug markets. *Global Drug Policy Observatory*, January 2017, Policy Brief No. 7, 1-24.
- Byrne, J.M., & Kimball, K.A. (2017). Inside the darknet: techno-crime and criminal opportunity. *Criminal Justice Technology in the 21st Century*, 3rd ed., 206–232.
- Chandran, N. (2015). From drugs to killers: exploring the deep web. *CNBC*. Dostupno na: http://www.cnbc.com/2015/06/23/from-drugs-to-killers-exploring-the-deep-web.html, preuzeto 04. 05. 2019.
- Chertoff, M., & Simon, T. (2015). The impact of the dark web on internet governance and cyber security. *Global Commission on Internet Governance*, February 2015, Paper Series No. 6, 1-8.
- Ciancaglini, V., et al. (2015). Below the surface: exploring the deep web. *Trend Micro*, June 2015, 1-48.
- Dolliver, D.S. (2015). Evaluating drug trafficking on the tor network: silk road 2, the sequel. *International Journal of Drug Policy*, 26 (11), 1113–1123.
- Everett, C. (2015). Should the dark net be taken out? *Network Security*, 2015 (3), 10–13.
- Farrell, P. (2017). Inside the darknet: where australians buy and sell illegal goods. *The Guardian*. Dostupno na: https://www.thegu ardia n.com/techn ology/2017/jul/04/inside-the-darknet-where-australians-buy-and-sell-illegal-goods, preuzeto 16.05.2019.
- Finklea, K. (2017). Dark web. *Congressional Research Service*, March 10, 1-16.
- Goodman, M. (2016). *Future crimes: Inside the digital underground and the battle for our connected world*. New York: Anchor Books.
- Greenberg, A. (2014). Over 80 percent of dark-web visits relate to pedophilia, study finds. *Security*. Dostupno na: https://www.wired.com/2014/12/80-percent-dark-web-visits-relate-pedophilia-study-finds/, preuzeto 16.05.2019.
- Greenberg, A. (2015). No, department of justice, 80 percent of tor traffic is not child porn. *Security*. Dostupno na: https://www.wired.com/2015/01/department-justice-80-percent-tor-traffic-child-porn/, preuzeto 18.05.2019.
- Holm, E. (2017). The Darknet: A new passageway to identity theft. *International Journal of Information Security and Cybercrime*, 6 (1), 41–50.
- Horton-Eddison, M., & Di Cristofaro, M. (2017). Hard interventions and innovation in crypto-drug markets: the escrow example. *Global Drug Policy Observatory*, August 2017, Policy Brief No. 11., 1-11.
- https://metrics.torproject.org/, preuzeto 28.05.2019.
- Jackson Higgins, K. (2015). What happens when personal information hits the dark web. *Information Week*. Dostupno na: https://www.darkreading.com/attacks-breaches/what-happens-when-personal-information-hits-the-dark-web/d/d-id/1319801?, preuzeto 09.05.2019.
- Kovacs, L. (2018). National cyber securiry as the corner stone of national security. *Land Forces Academy Review*, Vol. XXIII, No. 2 (90), 113-120.

- Krebs, B. (2013). Cards stolen in target breach flood underground markets. *Krebs on Security*. Dostupno na: https://krebsonsecurity.com/2013/12/cards-stolen-in-target-breach-flood-underground-markets/, preuzeto 12.05.2019.
- Krebs, B. (2015). Tax fraud advice, straight from the scammers. *Krebs on Security*. Dostupno na: https://krebsonsecurity.com/2015/03/tax-fraud-advice-straight-from-the-scammers/, preuzeto 23.05.2019.
- Kruithof, K., Aldridge, J., Décary-Hétu, D., Sim, M., Dujso, E., i Hoorens, S. (2016). *Internet-Facilitated Drugs Trade—An Analysis of the Size, Scope and the Role of the Netherlands*. Santa Monica, CA: Rand Europe.
- Lacson, W., & Jones, B. (2016). The 21st Century darknet market: lessons from the fall of silk road. *International Journal of Cyber Criminology*, 10 (1), 40–61.
- McGoogan, C. (2016). Dark web browser tor is overwhelmingly used for crime, says study. *The Telegraph*. Dostupno na: http://www.telegraph.co.uk/technology/2016/02/02/dark-web-browser-tor-is-overwhelmingly-used-for-crime-says-study/, preuzeto 28.05.2019.
- Mirea, M., Wang, V., & Jung J. (2019). The not so dark side of the darknet: a qualitative study. *Security Journal*, June 2019, Vol. 32, Issue 2, 102-118.
- Moloney, P. (2016). Dark net drug marketplace begin to emulate organised street crime. *The Sidney Morning Herald*. Dostupno na: http://www.smh.com.au/technology/technology-news/dark-net-drug-marketplaces-begin-to-emulate-organised-street-crime-20160111-gm3k1i.html, preuzeto 22.05.2019.
- Moore, D., & Rid, T. (2016). Cryptopolitik and the darknet. *Survival*, February 2016, Vol. 58, No. 1, 7-38.
- Murray, A. (2014). The dark web is not just for paedophiles, drug dealers and terrorists. *The Independent*. Dostupno na: http://www.independent.co.uk/voices/comment/the-dark-web-is-not-just-for-paedophiles-drug-dealers-and-terrorists-9920667.html, preuzeto 22.06.2019.
- Omand, D. (2016). The dark net: policing the internet's underworld. *World Policy*, Winter 2015/2016. Dostupno na: http://www.worldpolicy.org/journal/winter2015/dark-net, preuzeto 27.05.2019.
- Owen, G., & N. Savage. (2015). The tor dark net, *Global Commission on Internet Governance*, September 2015, Paper Series No. 20, 1-9.
- Paganini, P. (2015). How far do stolen data get in the deep web after a breach? *Security Affairs*. Dostupno na: https://securityaffairs.co/wordpress/35902/cyber-crime/propagation-data-deep-web.html, preuzeto 07.06.2019.
- Qiang, B., Zhang, R., Wang, Y., He, Q., Li, W., & Wang, S. (2014). Research on deep web query interface clustering based on hadoop. *Journal of Software*, 9 (12), 3057–3062.
- Samson, A. (2017). Dark net may pose 'disruptive risk' to internet sector—goldman. *Financial Times*. Dostupno na: https://www.ft.com/content/d045b27e-0842-3686-800e-080d8 ca883ae, preuzeto 01.06.2019.

- Sui, D., Caverlee, J., & Rudesill, D. (2015). The deep web and the dark net: a look inside the internet's massive black box. *Science and Technology Innovation Program*, STIP 03, August 2015, 1-17.
- Van Hout, M.C., & Bingham, T. (2013). 'Silk road', the virtual drug marketplace: a single case study of user experiences. *International Journal of Drug Policy*, 24 (5), 385–391.
- Weissman, C.G. (2015). The creepiest and most bizarre stories told by people who explored the internet's hidden websites. *Business Insider UK*. Dostupno na: http://uk.businessinsider.com/creepy-and-weird-deep-web-stories-from-reddit-2015-6?r=USand IR=T, preuzeto 24.06.2019.
- Wright, A. (2008). Searching the deep web. *Communications of the ACM*, 51 (10), 14–15.
- Wueest, C. (2015). Underground black market: thriving trade in stolen data, malware, and attack services. *Symantec*. Dostupno na: https://www.symantec.com/connect/blogs/underground-black-market-thriving-trade-stolen-data-malware-and-attack-services, preuzeto 10.05.2019.
- Zetter, K. (2014). How ram scrapers work: the sneaky tools behind the latest credit card hacks. *Security*. Dostupno na: https://www.wired.com/2014/09/ram-scrapers-how-they-work/, preuzeto 11.05.2019.
- Zheng, Q., Wu, Z., Cheng, X., Jiang, L., & Liu, J. (2013). Learning to crawl deep web. *Information Systems*, 38 (6), 801–819.