FBIM Transactions
DOI 10.12709/fbim.04.04.02.05

DA LI JE „TAMNI INTERNET" DUBOK I TAMAN?

IS THE "DARK WEB" DEEP AND DARK?

Zoran Čekerevac
Faculty of Business and Industrial Management of the "Union – Nikola Tesla" University in Belgrade, Belgrade, Serbia

Zdenek Dvorak
Faculty of Security Engineering, University in Žilina, Žilina, Slovakia

Petar Čekerevac
Hilltop Strategic Servis, Belgrade, Serbia

JEL Category: **H12, L86**

Apstrakt

Od svog nastanka Internet se zbog principa na kojima je kreiran razvijao u različitim smerovima. U tom njegovom razvoju iskristalisala su se dva dela, jedan vidljiv i dostupan običnim korisnicima i alatima, koji treba da omoguće da njegova upotreba bude jednostavna i udobna, a drugi, teže pristupačan i dostupan samo onima koji se malo više potrude, za mnoge nevidljiv. Iako nevidljiv, on nije ekskluzivan, jer svako može da mu se priključi, ako hoće. U ovom radu se težilo da se napravi jedan presek stanja u korišćenju Interneta na početku 2016. godine i da se proanaliziraju prednosti i mane oba dela Interneta. Posmatrani su samo veb sadržaji Interneta, a u potpunosti su isključeni iz analize sadržaji koji se nalaze na privatnim intranetima iza fajervola, iako se tu radi o velikim količinama podataka. Na početku rada je razmatrana terminologija koja se koristi u literaturi i u međusobnim komunikacijama korisnika Interneta. Nadalje su razmatrani vidljivi i nevidljivi Internet, a akcenat je stavljen na nevidljivi Internet, jer je u javnosti manje poznat. Posebno su razmotreni razlozi zbog kojih je nevidljivi Internet postao atraktivan, kao i načini kreiranja i postupci njegovog korišćenja. Razmotreni su i rizici kojima je izložen nevidljivi Internet, ali i rizici kojima mogu da budu izloženi njegovi korisnici. U okviru zaključaka su razmotrene dilema „transparentnost ili privatnost", da li je tamni Internet stvarno taman, kao i perspektive razvoja Interneta.

Ključne reči: *Vidljivi Internet, nevidljivi Internet, tamni Internet, duboki Internet, izgubljeni Internet, Tor, I2S, Internet arheologija*

Adresa autora zaduženog za korespodenciju:
Zoran Čekerevac
zoran@cekerevac.eu

Abstract

Since its foundation the Internet has, due to the principles on which it was created, evolved in different directions. During its development, two main parts were crystallized, one visible and accessible to ordinary users and tools which should ensure that its use is simple and comfortable, and the other, less affordable and accessible only to those who make a little more effort, for many invisible. Although invisible, it is not exclusive, because everyone can join it, if they want to. This paper intended to make an overview of the state of use of the Internet at the beginning of 2016 and to analyze advantages and disadvantages of both parts of the Internet. Here are considered only the contents of the Internet, and the contents on private intranet facilities that are located behind firewalls are completely excluded from the analysis, although they contain a large amount of data. At the beginning of the paper, there is considered the terminology used in the literature and in mutual communications of Internet users. Further, there an analysis of visible and invisible parts of the Internet, and an emphasis is placed on the invisible Internet, because it is a less public, and most of people are not familiar with it. The reasons why the invisible Internet has become attractive are discussed in more detail, as well as the way it is created and procedures for its use. Here are also considered the risks to which the invisible Internet is exposed, as well as risks to which its users may be exposed. In the framework of the conclusions, the dillema of "transparency or privacy" is discussed, along with the topic of whether the dark web is really dark, as well as perspectives of development of the Internet.

Keywords: *surface web, invisible web, dark web, deep web, lost Internet, Tor, I2S, Internet archaeology*

1 UVODNA RAZMATRANJA

Od svog nastanka Internet je težio da ostvari dve, obično suprotne, želje: transparentnost i privatnost. Jedna grupa korisnika insistira na transparentnosti, a druga na privatnosti. Paradoksalno je da obe grupe ponekad žažele da iskoriste nešto od onog što zastupa „protivnička" strana. Najglasniji zastupnici transparentnosti Interneta, i borbe protiv terorizma i kriminala svake vrste, imaju potrebu da zaštite svoje podatke od uvida javnosti. Poznati su slučajevi uzbunjivača koji su dobili zamašne zatvorske kazne ili se kriju po ambasadama i stranim zemljama. S druge strane i najglasniji zastupnici privatnosti imaju potrebu ponekad da pogledaju „u tuđe dvorište", a to je lakše uraditi kad je sve transparentno. Takva situacija je pobudila diskusije o Internetu kao celini i o pojedinim njegovim delovima. Tema je dugo tinjala, ali je krajem 2015. dobila zamah.

Prvo što se može uočiti u ovoj oblasti je da je u današnjim rečnicima teško naći jednoznačno objašnjenje za izraze i pojmove kao što su: „tamni Internet", „tamni veb", „duboki veb" i „duboki Internet". Još veća konfuzija vlada u literaturi na engleskom jeziku gde se pojavljuju: „dark Internet", „dark address", „dark address space", „sparse darknets", „darknet", „dark web", „deep web" i slični izrazi. Na srpskom i srodnim jezicima najčešće su u upotrebi izrazi „duboki Internet" i „tamni internet", a na engleskom „deep web", „dark web" i „darknet" (ili „dark net", zavisno od autora)[1]. Ono što je zajedničko za sve navedene izraze je da se njihovo značenje vezuje za deo Interneta koji nije indeksiran na uobičajeni način i koji nije dostupan uobičajenim pretraživačima.

„Duboki Internet" („Deep Web" ili „deep web" ili „deep Web") se kao pojam pojavio 2001. godine u radu (Bergman, 2001), a definisan je kao „deo Interneta koji je enkripcijom skriven od konvencionalnih pretraživača; skup neindeksiranih sajtova: privatnih baza podataka kao i drugih nelinkovanih sadržaja na dubokom Internetu." (deep-web, 2015) Duboki Internet neki od autora poistovećuju sa svim onim sadržajima Interneta koji nisu dostupni na konvencionalni način, iz bilo kog razloga. (Davis, 2011) Darknet se prvi put pojavljuje kao pojam 2002. godine, a

[1] Neki koji vole da se preciznije izražavaju prave razliku između "dark net"-a i "dark veb"-a, pa pod „dark net", podrazumevaju mrežu kojoj se može pristupiti samo sa specifičnim softverom, konfiguracijom, ili autorizacijom. Pod „dark web", podrazumevaju deo World Wide Web-a koji postoji samo u tamnoj mreži. (Egan, 2015)

odnosi se na „bilo koju mrežu ili softver koji ilegalno distribuira autorskim pravima zaštićene digitalne fajlove, kao što je npr. muzika, sa zaštitom od otkrivanja" (darknet, 2015) Tamni Internet („Dark web") kao pojam počeo je da koristi paralelno sa „dubokim Internetom" a odnosi se na: „deo Interneta koji je namerno sakriven od pretraživača, koristi maskirane IP adrese, i dostupan je samo posebnim veb pretraživačima: deo dubokog Interneta. (dark-web, 2015) Neki od autora tamni Internet povezuju sa razmenom fajlova (uključujući i P2P razmenu), kao i sa IRC čet relejima od kojih većina nema ni mogućnost indeksiranja. (Davis, 2011) Nedavno su se pojavila i tumačenja da je „Dark Web" pojam koji se odnosi na kolekciju veb sajtova koji su javni, vidljivi, ali kriju IP adresu servera na kojima su hostovani. (Egan, 2015).

Iako se iz navedenih definicija može zaključiti da je tamni Internet samo deo dubokog Interneta, mnogi ova dva pojma izjednačavaju po značenju. Cilj ovog rada je da analizira upotrebu Interneta i da ukaže na prednosti i nedostatke pojedinih načina upotrebe njegovog vidljivog dela („surface web") i nevidljivog dela („invisible Internet"). Pri tome će se pod vidljivim internetom podrazumevati: „Sadržaji Vorld Vide Veba (www) koji su dostupni javnosti i koji se indeksiraju od strane robota (paukova)." (PC, 2015)

U okviru ove analize biće posmatrani samo veb sadržaji Interneta, a u potpunosti će biti zanemareni sadržaji koji se nalaze na privatnim intranetima iza fajervola, iako se tu radi o velikim količinama podataka. Takođe, neće biti razmatran ni tzv. „izgubljeni Internet" („lost net"). O njemu je detaljnije razmatrano u (Labovitz, Ahuja, & Bailey, 2001), a ovde će se samo spomenuti da prema istraživanjima Hany SalahEldeen i Michael Nelson-a (Internet Archaeologists Reconstruct Lost Web Pages, 2013) za godinu dana se na Internetu izgubi 11% podataka, a za dve godine 27%. Razlozi leže uglavnom u gašenju pojedinih sajtova i nestanku linkova prema pojedinim sadržajima Interneta. Kada se ima u vidu da se Internet sadržaji čuvaju na mnogo različitih servera, i da jednom objavljeno (praktično) nikad ne nestaje u potpunosti, onda se lako može zaključiti da bi se zbog toga mogla uspešno razvijati jedna nova oblast Interneta, Internet arheologija.

Da bi se izbeglo šarenilo i nepreciznosti u terminologiji, u nastavku će biti uglavnom korišćeni izrazi: vidljivi i nevidljivi Internet.

2 VIDLJIVI I NEVIDLJIVI INTERNET

I vidljivi i nevidljivi Internet se nalaze na jednom mestu, na računarima koji imaju pristup Internetu. Zajedničko im je što oboje (delom) koriste iste, standarde i protokole, a razlika je u tome što je vidljivi Internet baziran na DNS sistemu i ICANN[1] bazi, a nevidljivi nije.

2.1 Vidljivi Internet

Vidljivi Internet se u literaturi naziva i „površinski Internet" i „skenirani veb" i „javni veb", a linkovi ka stranicama na površini veba prikazuju se među rezultatima pretraživača. Opisni tekst na stranicama kao i meta podaci skriveni unutar veb stranice identifikuju sadržaj stranice. Površinski, vidljivi, Internet je suprotnost dubokom Internetu.

Da bi neki Internet sadržaj pripao vidljivom delu Interneta on mora da bude dostupan javnim Internet pretraživačima (npr. Google, Yahoo, …) i robotima koji ga indeksiraju, tj. evidentiraju i njega i sve linkove koji vode ka njemu i od njega. Od vidljivog Interneta se očekuje da ima statičke sajtove postavljene na serverima i da im je vidljiv html kod. U slučaju potrebe za promenom sadržaja sajta, menja se html kod koji se potom podiže na server kao zamena ili dodatak prethodnoj verziji. Sve je transparentno. Na taj način vidljivi Internet postaje javna biblioteka sa mnoštvom sadržaja, koja je dostupna neprekidno. Pored vidljivog html koda, bitan element vidljivog Interneta je DNS (engl. Domain name system) čiji je glavni zadatak da imena računara povezuje sa njihovim IP adresama. Međutim, DNS baza omogućava i pristup nekim drugim podacima. Najčešći tipovi evidencija koji se čuvaju u DNS bazi podataka se odnose na:

- administratora DNS zone, odn. početni DNS server, tj. početak nadležnosti (SOA[2]);

[1] Internet Corporation for Assigned Names and Numbers; Detaljnije u (ICANN)

[2] Detaljnije o SOA u (What is a SOA Record?, 2015)

- IP adrese (A[1] i AAAA[2]),
- servere elektronske pošte (MX[3]),
- server imena (NS[4]),
- ukazivače za obrnuto DNS pretraživanje (PTR[5]),
- aliase naziva domena (CNAME[6]).

Iako DNS baza nije namenjena da bude baza opšte namene, ona može da skladišti zapise i za druge vrste podataka, kao što su npr. DNSSEC[7] evidencije za automatizovano pretraživanje, ili zapise o odgovornim licima (RP) za pojedinačne korisničke upite. Kao baza opšte namene, DNS se takođe u realnom vremenu koristi u borbi protiv neželjene e-pošte (spam) pomoću BlackHole liste sačuvane u DNS-u.

Sa načinima korišćenja vidljivog Interneta, njegovim mogućnostima, prednostima i nedostacima upoznat je skoro svako ko je ikad počeo da ga koristi. Međutim, na osnovu brojnih istraživanja utvrđeno je da je taj deo Interneta mnogo manji od onog dela koji nije dostupan uobičajenim pretraživačima. Procene se kreću u vrlo širokom dijapazonu, ali zbog nemogućnosti provere tih podataka i svakodnevnih promena i enormnog povećanja broja i količine sadržaja, ovde neće biti pominjane konkretne vrednosti.

2.2 Nevidljivi Internet

Pod nevidljivim Internetom se podrazumevaju svi sadržaji koji ne pripadaju vidljivom Interetu. Međutim, ako se ide u detalje, i vidljivi deo Interneta je bar jednom bio nevidljiv. Mereno od trenutka postavljanja pojedinog sadržaja na Internet, postoji vreme koje je potrebno da on postane vidljiv. Međutim, takve situacije nisu predmet ovog rada.

Kao što je navedeno u uvodnom delu, u vezi sa nevidljivim Internetom u literaturi se najčešće sreću pojmovi: „duboki Internet" i „tamni Internet". Najčešće se radi o prevodu naziva na engleskom jeziku: „deep web" i „dark web" (ili „darknet"). Interesantno je da se na srpskom i srodnim jezicima češće koristi izraz „duboki-", a na engleskom „dark-". Ovi nazivi su postali i inspiracija za mnoge spektakularne naslove novinskih članaka, kao: „Šest najužasnijih stvari koje skriva tamna strana interneta" (24sata, 2015), „Tamna strana interneta: Stisni 'enter' za ubojstvo i kriminal" (Blotnej, 2015), „Tamna strana interneta osvaja tržište" (Srna, 2013)… „Otkriće: Tamna strana Interneta, mesto gde možete kupiti drogu, seks i nepristojne slike" (Peachey, 2013)… Budući da je poznato da se u oblasti nevidljivog Interneta odvijaju najrazličitije aktivnosti, i legalne i nelegalne, i da se ovaj rad više bavi tehnologijom, za sada ćemo celu ovu zonu nazivati nevidljivi Internet.

Nisu uvek sadržaji koji se pojavljuju na nevidljivom internetu ilegalni i zlonamerni. Većina, ako ne i velika većina, mogu da budu sadržaji koji iz nekog razloga, npr. zastarelosti, nisu interesantni da stoje neprekidno na veb sajtu, već se mogu staviti u neku arhivu kojoj se može pristupiti nekim unutrašnjim pretraživačima. Tako se ti fajlovi čuvaju na nekim serverima koji su dostupni korisnicima sa pravom pristupa toj bazi, ali nisu dostupni robotima.

Ovde treba pomenuti još jednu karakteristiku nevidljivog interneta. Njegovi sajtovi su obično dinamički i koriste aplikacije koje iščitavaju svoje baze podataka i na osnovu iščitanog sadržaja kreiraju html kod veb stranice. Na taj način sajtovi ostaju nevidljivi za robote pretraživača. (Goodman, 2015)

2.2.1 Zbog čega je nevidljivi Internet uopšte interesantan?

Svedoci smo svakodnevnih kiber napada. Čak i najbeznačajniji sajtovi, sa minimalnom posetom i uticajem, svakodnevno postaju žrtve hakerskih i drugih napada. Oni značajniji, sa većim uticajem i većom posetom su stalna meta napada. Čak su i obični korisnici, sa promenljivom, dinamičkom, IP adresom, potencijalne žrtve napada. Ti napadi nisu istog intenziteta, ali ni svi korisnici nemaju iste kapacitete u pogledu svoje zaštite. Nevidljivi Internet drži (korisne) sadržaje daleko od očiju velike većine korisnika Interneta. Korišćenjem

[1] Detaljnije o A zapisu u (Nerd, 2015)
[2] Detaljnije o AAAA zapisu u (What is an AAAA record or IPv6?)
[3] Detaljnije o MX zapisu u (Cunningham, 2011)
[4] Detaljnije o NS u (Nicholson, 2014)
[5] Detaljnije o PTT u (Microsoft)
[6] Detaljnije o CNAME u (What is a CNAME record?, 2015)
[7] Detaljnije o DNSSEC u (Dnssec.net, 2015)

nevidljivog Interneta, korisnik sa pravom očekuje da će biti teže pronađen i da će njegovi sadržaji, samim tim što su manje dostupni, biti i bolje zaštićeni.

Takođe, svakodnevno se čuju priče o prisluškivanju komunikacija (Greenwald & MacAskill, 2013), (Čekerevac, Anđelić, & Radović, 2011), (Kessler, 2013), (Čekerevac, 2013), (Čekerevac & Radonjić, 2013), (Čekerevac, Dvorak, & Čekerevac, 2014), nebezbednosti elektronske pošte (Osterman Research, 2013), (Čekerevac, Dvorak, & Čekerevac, 2014), (Čekerevac, Čekerevac, & Vasiljević, 2014), kao i o bezbednosti socijalnih mreža (Bishop, 2013), (Wüest, 2010), pa čak i o prisluškivanju prostorija u kojima korisnik radi koristeći neki softverski paket, kao što je to objašnjeno u (Falkvinge, 2015).

Mnogi korisnici su svesni toga da sve što se jednom pojavi na Internetu ostaje na Internetu večno, u ovom ili u onom obliku, i nemoguće ga je potpuno ukloniti. Zbog toga se svaki objavljeni post, mišljenje, fotografija i sl. u nekom trenutku od strane vlade, političkih protivnika ili bilo kog drugog lica mogu upotrebiti kao oružje protiv onog koji ih je objavio. To čak i prosečnog korisnika navodi na ideju da bar za neke od aktivnosti beži u zonu nevidljivog Intereta. Da li će stvarno i pobeći u tamni Internet zavisi od više faktora, a neki od njih su: nivo poznavanja korišćenja Interneta i softvera, i strah od nepoznatog.

Pored navedenih razloga, koji se moraju smatrati legalnim i legitimnim, moguć je još jedan razlog prelaska u tamnu zonu Interneta, postavljanje ili deljenje ili kupovina ilegalnih sadržaja (Yale, 2014). Pecanje u zoni nevidljivog Interneta daje male šanse za uspeh, pa su i ovakvi korisnici teško uhvatljivi.

Ipak, niko sa garancijom ne može tvrditi da će podaci na nevidljivom Internetu biti garantovano zaštićeni od hakovanja i krađa. O tome nam govori i naslov: „Anonimus hakeri instalirali Viagra oglas na propagandni sajt islamske države" (Titcomb, 2015)

Ne postoji lista svih raspoloživih usluga nevidljivog Interneta, mada se na pojedinim stranicama vidljivog interneta mogu naći pojedinačni katalozi usluga. Mnogo toga u vezi sa upotrebom nevidljivog Interneta zavisi od samih korisnika. Skriveni servisi ne koriste izlazne nodove pa je enkripcijom obezbeđena puna zaštita od prisluškivanja, end-to-end.

2.2.2 Kako se kreira nevidljivi Internet?

Iako izgleda tajnovito i teško, kreiranje nevidljivog Interneta je u suštini jednostavno. U najjednostavnijem obliku, dovoljno je kreirati neki sadržaj i postaviti ga u odgovarajući folder na veb sajtu. Pri tome ne sme da bude ni izlaznih ni ulaznih linkova ka tom sadržaju. Pošto roboti idu vidljivim linkovima, neće zapaziti postojanje tih sadržaja i neće ih indeksirati. Normalno, moguće je određene sadržaje staviti u baze podataka veb sajta, a lozinkama i enkripcijom ograničiti pristup tim sadržajima. Na taj način, ti sadržaji ostaju nevidljivi za robote.

Drugi način bi bio da se među fajlove regularnog veb sajta postavi veb stranica sa šifrovanim pristupom. Roboti ne mogu da indeksiraju šifrovane sajtove ili stranice, pa sajt (ili stranica) ostaju neindeksirani, nevidljivi.

Treći, često dovoljan, a efikasan način je da se Robot.txt datoteka konfiguriše tako da blokira sve robote koji posećuju veb sajt, npr:

User-Agent: *
Disallow: /

Ukoliko se želi da neki deo sadržaja, neki URL, bude vidljiv svim robotima, može se dodati:

Allow: /…URL…/

A, ako se želi vidljivost samo za određenog pauka-robota, npr. Googlebot, može se dodati: User-Agent:

Googlebot
Allow: /…URL… /

Ili msnbot

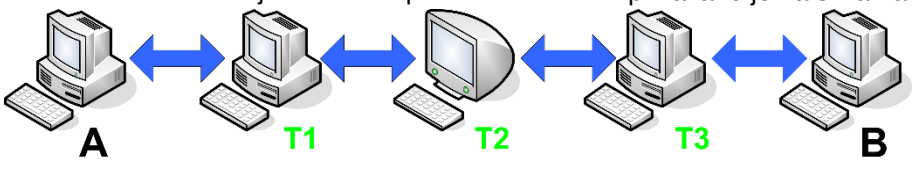
User-Agent: msnbot
Allow: /…URL… /

Kao pomoć programerima mogu da posluže razni Robots.txt fajl generatori, npr. (SEOBook, n.d.).

2.2.3 Kako se koristi nevidljivi Internet?

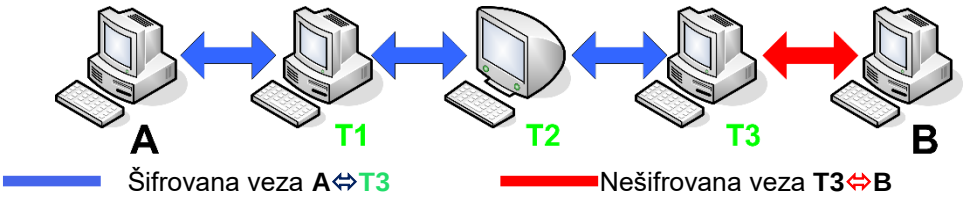
Za pristup nevidljivom Internetu mogu se koristiti razni načini. Od svih načina najverovatnije je da je Tor (skraćenica od The Onion Router) mreža najjednostavnija za upotrebu. Njena je namena da posluži kao gejtvej ka nevidljivom Internetu. Tor preusmerava signale preko 6.000 servera da sakrije adresu Internet klijenta, čime praktično onemogućava forezničarima da uđu u trag

korišćenoj IP adresi. On koristi tajne stranice sa *.onion* sufiksima koji su dostupni samo Tor brauzeru. (Goodman, 2015) Kako to funkcioniše, prikazano je na slikama 1 i 2.



Tor logo

Slika 1 Način rada TOR rutiranja *Autori na osnovu (Yale, 2014)*



Slika 2 Način rada TOR rutiranja *Autori na osnovu (Yale, 2014)*

Sa T1, T2 i T3 obeleženi su serveri, izabrani po slučajnom izboru, preko kojih se informacija prenosi od računara A do računara B. Na svom putu od računara A preko servera grupe T informacija ide u šifrovanom obliku sve do računara B. (Slika 1) Na ovaj način se može pristupiti sajtovima koji su dostupni samo preko TOR-a.

Međutim, moguće je i da se šifrovana veza održava od računara A i preko svih servera grupe T, a da od poslednjeg u nizu računara grupe T do računara B veza nije šifrovana. (Slika 2) Na taj način korisnik računara A može da dođe anonimno do javnog sadržaja hostovanog na računaru B. Detaljnije o TOR-u, njegovom nastanku i principima rada opisano je u (Syverson, 2005), (Tor) i u mnogim drugim dokumentima iz ove oblasti.

Hostovanje veb stranica na Tor mreži je takođe jednostavno. Tu ne vladaju zakoni i (u principu) vlada apsolutna sloboda, ali je baš zbog toga treba koristiti razumno i odgovorno, da se ne bi izrodila u svoju suprotnost i kriminal. Da bi se postavila veb stranica, treba prethodno instalisati Tor, u Tor „control panel" izabrati „novi identitet" i Tor će korisniku dodeliti novu IP adresu i kompletno novi identitet čak i za korišćenje vidljivog interneta. Sa instalisanim Tor-om korisnik može da pristupa *.onion* domenima. On može u „settings"-u i da konfiguriše skrivene servise izborom porta, ukazivača na lokalni host i radnog fajla za ovu svrhu. Tor će automatski generisati heš string koji se može dati drugim korisnicima da pristupe serveru na kom se nalazi veb stranica - iako oni neće imati način da otkriju vlasnika sajta. (Davis, 2011)

I dok se Tor prvenstveno fokusirao na razmenu fajlova, drugi oblik tamnog Interneta je I2P[1] mreža, ili, možda, bolje rečeno, mrežni sloj, fokusira se na anonimnu komunikaciju između aplikacija. Za implementaciju ovog sloja koristi se softver I2P ruter. Pri tome računar koji radi na I2P postaje I2P čvor. Pošto je I2P anonimni mrežni sloj, on je dizajniran tako da obezbeđuje i anonimnu komunikaciju.

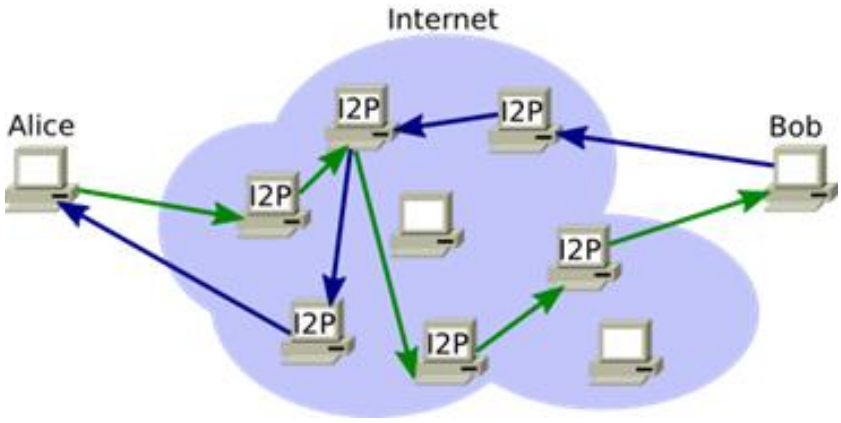
I2P je sličan Tor-u, ali je nešto fleksibilniji i podržava razne vrste protokola i aplikacija. Upotreba uključuje anonimno surfovanje Internetom, razgovor, blogovanje i transfer fajlova, kao i e-mejl uslugu. Pri umrežavanju, korisnicima su na raspolaganju:

- *I2Ptunnel*, alat za povezivanje sa I2P mrežom i obezbeđivanje I2P usluga. Destinacija jednog I2PTunnela može se definisati pomoću imena hosta, Base32, ili kompletnog 516-bajtnog ključa odredišta. Uspostavljeni I2PTunnel će biti dostupan na klijentskom računaru kao localhost:port. Ako korisnik želi da pruži uslugu na I2P mreži, on treba samo

[1] Invisible Internet Project (I2P)

da kreira I2PTunnel do odgovarajućeg porta (ip_adress:port). Odgovarajući 516-bajtni ključ odredišta će biti generisan za tu uslugu i postaće dostupan celoj I2P mreži. Veb interfejs za upravljanje I2PTunnel-om je dostupan na localhost:7657/i2ptunnel/. (I2P, n.d.) I2PTunnel aplikacija omogućava da i TCP/IP aplikacije komuniciraju preko I2P postavljanjem "tunela" kojima se može pristupiti povezivanjem na unapred određene portove na lokalnim hostovima;

- SAM[1] protokol koji omogućava da klijent aplikacija pisana u bilo kom programskom jeziku može da komunicira preko I2P, pomoću soket baziranog interfejsa sa I2P ruterom (SAM V3, 2015);
- BOB[2] manje kompleksna aplikacija za ruter protocol, slična "SAM"-u (BOB, 2015);
- Orchid – I2P plugin (Orchid, 2014).



Slika 3. Rutiranje paketa u I2P *Izvor: (Mergen, 2015)*

Prema mišljenju eksperata koji su poredili Tor i I2P, I2P je otporniji na napade putem analize protoka saobraćaja podataka iz dva razloga (Mergen, 2015):

- ne postoji razlika između releja i izlaznih čvorova: u I2P se podrazumeva da je svaki klijent istovremeno i izlazni čvor, čime se dopunski skriva saobraćaj klijenta i povećava broj izlaznih tačaka;
- veze u Tor-u su dvosmerne, dok su veze u I2P jednosmerne: za dvosmernu komunikaciju u I2P, se kreiraju dve potpuno različite rute (slika 3), što otežava analizu saobraćaja.

Kada se uporedi komfor rada na Tor-u i I2P-u može se videti da je upotreba Tor-a znatno jednostavnija, jer zahteva samo preuzimanje i instalaciju brauzera. Instalacija i konfiguracija I2P je znatno kompleksnija, mada izvodljiva za većinu korisnika računara. Ako konfigurisanje aplikacije nije limitirajući faktor, I2P može da bude bolje rešenje, jer pruža šire mogućnosti i obezbeđuje (veću) anonimnost.

3 RIZICI NEVIDLJIVOG INTERNETA

Nevidljivi Internet neki porede sa „Divljim Zapadom", jer tu u načelu svako radi šta hoće, i može se reći da je jedino pravilo da nema pravila. Zbog toga se često pojam duboki (tamni) Internet povezuje sa kriminalnim aktivnostima. Nesumnjivo je da na takvu sliku znatno utiču i mediji svojim spektakularnim i sugestivnim naslovima. Međutim, kao i u običnom životu, kriminalne aktivnosti izvodi znatno manji deo populacije, a, pored toga, svako je odgovoran za svoja dela. Ovde se nećemo baviti analizom primene Interneta u kriminalne svrhe, već ćemo pod rizicima smatrati samo ono što može da utiče na srž i suštinu ideje nevidljivog Interneta, a to su mogućnosti i načini za gubljenje anonimnosti.

Bez obzira na to što su skriveni, sadržaji nevidljivog interneta su u suštini obične, standardne, veb aplikacije, sa slabostima koje ih čine podložnim hakerskim napadima. Ako ovi napadi uspeju da preko sajta "prodru" do servera, onda je moguće dopreti i do njegogvog vlasnika. Ako se zanemari činjenica da su vlasnici sadržaja na nevidljivom Internetu ljudi i da ponekad imaju

[1] Simple Anonymous Messaging

[2] Basic Open Bridge

želju da se pohvale svojim (ne)delom[1] najprimenjivanija taktika za otkrivanje i onesposobljavanje TOR sajtova je korišćenje DDoS[2] napada na grupu IP adresa i praćenje, u kom trenutku koji sajtovi postaju neoperativni. Daljim sužavanjem grupe IP adresa može se izdvojiti konkretna adresa servera. Normalno, ovo važi ako se prezentacija ne premešta sa servera na server. U protivnom je malo efikasna.

Nevidljivost nevidljivog Interneta može da bude kompromitovana i od strane samog korisnika koji će svojom nepažnjom ili neznanjem da pristupi servisima, npr. društvenim mrežama, na kojima je prijavljen pod svojim imenom, prezimenom i adresom. Tada je cela upotrebe alata nevidljivog Interneta obesmišljena.

Takođe, u određenim slučajevima anonimnost može da bude ugrožena i pri pristupu sajtovima vidljivog Interneta iz zone nevidljivog Interneta. Obično su ti čvorovi pod nadzorom hakera i/ili raznih vladinih agencija (bez obzira na to u kojoj se državi server nalazi) koji prisluškivanjem imaju mogućnost da preuzmu kopije podataka o korisnicima i šiframa koje oni koristi. Ovde od neke pomoći može da bude korišćenje šifrovane HTTPS veze, mada ni to nije sigurna garancija (v. (Čekerevac, Dvorak, & Čekerevac, 2014))

Jedna od mogućnosti napada je da se neko pojavi kao vlasnik ogromnog broja kompjutera u Tor mreži. Pošto Tor zavisi od mreže volontera koji primaju i prenose poruke (ponekad suočeni sa velikim rizikom), ako neko raspolaže izuzetno velikom grupom računara on dobija mogućnost da se veliki deo saobraćaja odvija preko njegovih računara, a onda praćenjem toka saobraćaja može da razbije anonimnost mreže. Ta pojava je nazvana Sibil napad. Tako je u februaru 2014 zapaženo priključivanje enormnog broja računara sa iste IP adrese. Održavanje Tor-a nije na vreme obratilo pažnju na ovu pojavu, a novembra 2015. je obelodanjeno da su napad izveli istraživači Karnegi Melon Univerziteta iz Pitsburga. Rezultat je da su locirani mnogi ilegalni vebsajtovi i da je pohapšena velika grupa kriminalaca, ali u akciji nisu prikupljeni samo podaci o kriminalcima, već i o raznim aktivistima, borcima za ljudska prava, „šaptačima" i drugim korisnicima koji nisu kriminalci, već samo žele da privatno pretražuju Internet (Hill, 2015). Drugi rezultat je da je glavni arhitekta Tor-a uveo novu filozofiju: „Prvo blokiraj, a pitanja postavljaj kasnije" (Hill, 2015). Interesantno je da su metodologiju napada u vrlo sličnom obliku još 2011. godine opisali istraživači ESIEA[3] i objavili je u (Kumar, 2011). Ukratko, inventarisanjem mreže, istraživači su u Tor mreži pronašli 6000 računara od kojih su mnogi imali javno dostupne IP adrese. Drugim inventarisanjem su otkrili i skrivene bridževe, njih 181. Na taj način su dobili sliku o kompletnoj Tor arhitekturi. U laboratorijskim uslovima su izveli eksperiment u kome su specifičnim napadom, koji je uključivao kreiranje virusa koji su mogli da obezbede sistemske privilegije i identifikuju ranjive računare, i masovnim DDoS napadom na čiste računare, usmerili saobraćaj ka inficiranim računarima. Ostalo je bilo relativno lako.

Postoje izvesni rizici i pri korišćenju Tor-ovih skrivenih usluga. Npr. usluge koje su dostupne preko Tor-ovih skrivenih usluga i javnog Interneta su podložne korelacionim napadima i samim tim nisu potpuno skrivene. Drugi rizici se mogu javiti u obliku lošeg konfigurisanja usluge, vođenja statistika, intersekcijskih napada, ili, opet, korisnikovih grešaka. (Tor) Pored navedenih rizika Tor mrežu je izložena raznim vrstama prisluškivanja[4], napadima analizom saobraćaja[5], napadima „trula jabuka"[6], blokiranju izlaznih nodova[7] i drugim rizicima.

Na kraju, ali izuzetno velika opasnost po slobodu Interneta leži u nastojanjima vlada i korporacija da ga stave pod kontrolu. Libertarijanci O'Brien i Clark zastupaju stav da se nevidljivi Internet, ma kako on bio definisan, mora apsolutno braniti, jer je bitan za obezbeđenje ljudskih prava, a kriminalne aktivnosti se odvijaju i na vidljivom Internetu, potpuno javno. Tehnički je moguće kroz mrežu pustiti viruse koji će uništiti npr. sve sadržaje sa dečjom pornografijom, ali tada bi

[1] Vlasnik Silk Road-a je uhvaćen zbog toga što je sopstvenom sajtu pristupao iz Internet kafea, ali ne preko Tor mreže, već direktno. (WEBnSTUDY, 2015)
[2] Detaljnije o DDoS napadima u (Beal, n.d.)
[3] École d'ingénieurs du numérique, l'ESIEA
[4] Detaljnije u (Akhoondi, Yu, & Madhyastha, 2012)
[5] Detaljnije u (Danezis, 2005)
[6] Detaljnije u (Le Blond, et al., 2011)
[7] Detaljnije u (Mikhailian, n.d.)

svako ko ima ključ tog softvera za filtriranje postao meta. Da kriminala ima i na javnom Internetu i da samo treba znati gde ga potražiti govori i portparol Centralne policijske jedinice za E-kriminal Metropoliten policije (PCeU), ali ističe da se pri svakom korišćenju Interneta negde nešto beleži i samo je pitanje identifikacije onog ko drži te informacije, a da li će istraga naići na opstrukciju, odgovor je: „Ne." (Beckett, 2009)

Poseban paradoks je da se 80% budžeta za održavanje Tor-a obezbeđuje iz ulaganja vlade SAD. (Hill, 2015)

4 ZAKLJUČAK

Na osnovu izloženog može se zaključiti da će dilema „Privatnost ili transparentnost?" odn. „Slobodan ili kontrolisani Internet?" ostati i dalje nerešena. I zastupnici stavova obe strane će u nekim situacijama biti u pravu, a u drugim će pobijati sopstvene stavove. Razlog leži u tome da ni u životu ništa nije uvek crno ili uvek belo. Činjenica je da današnji Internet ima dve zone koje, iz navedenih razloga, teže, ali i odbijaju da se isprepleću. Da li će i, ukoliko hoće, koliko će se povezati, pokazaće vreme.

Vidljivi deo Interneta pruža relativnu udobnost rada i laku dostupnost, kao i računarstvo u oblaku, ali korisnika izlaže različitim rizicima od kojih je jedan i gubitak privatnosti. Sa malo truda lako se mogu pronaći osnovni podaci o skoro svakoj osobi na planeti, a uz više truda i mnogi detalji iz privatnog života. Ako se izuzme nedavni uspešni napad na deo Tor-a, nevidljivi deo Interneta pruža više zaštite privatnosti, zaštitu disidenata od odmazde, skriveno čuvanje i razmenu fajlova, lakšu prodaju i kupovinu robe koja podleže raznim ograničenjima i još mnogo toga. Opet, nisu retki slučajevi kada istražitelji zakucaju na vrata korisnika Tor-a, posebno u slučajevima kada su njihovi računari i izlazni nodovi iz Tor mreže. Po zakonu ništa nije zabranjeno, ali sticaj okolnosti može da dovede do toga da se aktivnost korisnika Tor-a može podvesti i u grupu zabranjenih aktivnosti. Sumnju mogu da izazovu svi korisnici Tor-a, ali i u vidljivom delu Interneta postoji mogućnost slanja šifrovanih poruka. Šta raditi sa njima?

Sigurno je da će se oba dela Interneta i u budućnosti ubrzano širiti, kao i softveri i njihove mogućnosti. Pored već poznatih Tor, I2P, Freenet, GNUnet (i drugih postojećih), razvijaće se i nove peer-to-peer i friend-to-friend mreže nevidljivog Interneta, bilo kao specijalizovane za određene zadatke, bilo kao mreže opšteg tipa.

Na kraju, posle svih pomenutih analiza, ne može se reći da je nevidljivi Internet dubok i taman. U njemu mogu da surfuju i vrhunski eksperti i neplivači, ili, bolje rečeno, prosečni plivači. Da li je nedostupan? Nije, svako mu se može priključiti. Da li pruža apsolutnu zaštitu privatnosti? Ne, samo primorava vlasti i hakere da se mnogo više potrude nego u slučaju vidljivog Interneta, sve do granice isplativosti.

CITIRANI RADOVI

24sata. (2015, Avgust 18). Šest najužasnijih stvari koje skriva tamna strana interneta. *24 sata*. Retrieved from http://www.24sata.hr/tech/sest-najuzasnijih-stvari-koje-skriva-tamna-strana-interneta-422927/foto

Akhoondi, M., Yu, C., & Madhyastha, H. V. (2012, May). LASTor: A Low-Latency AS-Aware Tor client. *Proceedings of IEEE Symposium on Security and Privacy (Oakland'12).* San Francisco, CA. Retrieved from http://lastor.cs.ucr.edu/oakland12.pdf

Beal, V. (n.d.). *DDoS attack - Distributed Denial of Service.* Retrieved December 04, 2015, from webopedia: http://www.webopedia.com/TERM/D/DDoS_attack.html

Beckett, A. (2009, November 26). *The dark side of the internet .* Retrieved from theguardian: http://www.theguardian.com/technology/2009/nov/26/dark-side-internet-freenet

Bergman, M. K. (2001). White Paper: The Deep Web: Surfacing Hidden Value. *JEP the journal of electronic publishing, 7*(1). doi:http://dx.doi.org/10.3998/3336451.0007.104

Bishop, E. (2013, November 18). *5 threats to your security when using social media.* Retrieved from SocialTimes: http://www.adweek.com/socialtimes/5-social-media-threats/493325

Blotnej, B. (2015, maj 17). *Tamna strana interneta: Stisni 'enter' za ubojstvo i kriminal.* Retrieved from 24 sata: http://www.24sata.hr/news/tamna-strana-interneta-stisni-enter-za-ubojstvo-i-kriminal-419601

BOB. (2015, November). *BOB - basic open bridge.* Retrieved from I2P: https://geti2p.net/en/docs/api/bob

Cunningham, P. (2011, August 6). *Email Fundamentals: What is an MX record, and how do they work?* Retrieved from exchangeserverpro.com: http://exchangeserverpro.com/mx-record/

Čekerevac, Z. (2013). Small an medium sized enterprises data seccurity in cloud computing. *ITEP 2013* (str. 280-283). Chernivtsi: Bukovinski Universitet.

Čekerevac, Z., & Radonjić, S. (2013). Some SMEs data safety and security issues in the in-house and in the cloud computing. *18. medzinarodna vedecka konferencia Riešenie krizovych situacii v špecifickom prostredi* (str. 99-106). Žilina: Fakulta špecialneho inžinierstva.

Čekerevac, Z., Anđelić, S., & Radović, D. (2011). Data protection in small and medium sized enterprises. *2011. PROCEEDINGS of International Conference "Smal and Medium Enterprises - Possibilities and Perspectives 2011"* (str. 445-456). Novi Pazar, Serbia: International University. Preuzeto sa http://news.uninp.edu.rs/media/filer_public/1e/fe/1efe18dc-cb15-4335-ad94-61c197a16e98/smepp2011.pdf

Čekerevac, Z., Čekerevac, P., & Vasiljević, J. (2014, Jan 15). Internet sigurnost MSP sa aspekta sigurnosti elektronske pošte. *FBIM Transactions, 2*(1), 45-56. doi:10.12709/fbim.02.02.01.05

Čekerevac, Z., Dvorak, Z., & Čekerevac, P. (2014). Internet safety of SMEs and e-mail protection in the light of recent revelations about espionage of internet communication system. *Zbirnyk naukovykh prats' Bukovyns'koho universytetu. Ekonomichni nauky, 10*.

Čekerevac, Z., Dvorak, Z., & Čekerevac, P. (2014, 07 15). Internet sigurnost u svetlu otkrića Edvarda Snoudena. (Z. Čekerevac, Ur.) *FBIM Transactions, 2*(2), 68-78. doi:10.12709/fbim.02.02.02.07

Danezis, G. (2005, January). *Introducing Traffic Analysis - Attacks, Defences and Public Policy Issues...* Retrieved from http://www0.cs.ucl.ac.uk/staff/G.Danezis/papers/TAIntro.pdf

darknet. (2015, November 2). Retrieved from Dictionary.com's 21st Century Lexicon: http://dictionary.reference.com/browse/darknet

dark-web. (2015, November 28). Retrieved from Dictionary.com Unabridged: http://dictionary.reference.com/browse/dark-web

Davis, R. (2011, Jun 25). *What is Dark Internet, How to Access Onion Domains and Configure Hosting for the Dark Web.* Retrieved from The ramblings of a weirdo: http://www.rogerdavies.com/2011/06/dark-internet/#torroutingdiagram

deep-web. (2015, November 28). (Dictionary.com) Retrieved November 28, 2015, from Dictionary.com Unabridged: http://dictionary.reference.com/browse/deep-web

Dnssec.net. (2015, Jun 16). *DNSSEC: DNS Security Extensions Securing the Domain Name System.* Retrieved from Dnssec.net: http://www.dnssec.net/

Egan, M. (2015, Nov 23). *What is the Dark Web? How to access the Dark Web. What's the difference between the Dark Web and the Deep Web?* Retrieved from PC Advisor: http://www.pcadvisor.co.uk/how-to/internet/what-is-dark-web-how-access-dark-web-deep-joc-3593569/

Falkvinge, R. (2015, June 18). *Google Chrome listening in to your room shows the importance of privacy defense in depth.* Retrieved from Privacy Online News: https://www.privateinternetaccess.com/blog/2015/06/google-chrome-listening-in-to-your-room-shows-the-importance-of-privacy-defense-in-depth/

Goodman, M. (2015, April 1). *Most of the web is invisible to Google. Kere's what it contains*. Preuzeto sa Popular Science: http://www.popsci.com/dark-web-revealed

Greenwald, G., & MacAskill, E. (2013, 06 07). NSA Prism program taps in to user data of Apple, Google and others. *The Guardian*. Preuzeto 08 04, 2013 sa http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

Hill, K. (2015, November 30). *The attack that broke the Dark Web—and how Tor plans to fix it.* Retrieved from Fusion: http://fusion.net/story/238742/tor-carnegie-mellon-attack/

I2P. (n.d.). *I2PTunnel.* Retrieved December 3, 2015, from I2P: https://geti2p.net/en/docs/api/i2ptunnel

ICANN. (n.d.). *ICANN.* Retrieved December 3, 2015, from Internet Corporation for Assigned Names and Numbers: http://archive.icann.org/tr/english.html

Internet Archaeologists Reconstruct Lost Web Pages. (2013, September 18). Retrieved from MIT Technology Review: http://www.technologyreview.com/view/519391/internet-archaeologists-reconstruct-lost-web-pages/

Kessler, M. (2013, July 23). *Deutsche User: Zwei Drittel halten ihre Daten im Netz für unsicher.* Retrieved from teltarif.de: http://www.teltarif.de/bitkom-internet-nutzer-daten-unsicher-befragung-prism/news/51871.html

Kumar, M. (2011, October 24). *Tor anonymizing network Compromised by French researchers.* Retrieved from The hacker news: http://thehackernews.com/2011/10/tor-anonymizing-network-compromised-by.html

Labovitz, C., Ahuja, A., & Bailey, M. (2001). *Shining light on dark address space.* Ann Arbor, Michigan, USA: Arbor Netwoks. Retrieved from http://mdbailey.ece.illinois.edu/publications/dark_address_space.pdf

Le Blond, S., Manils, P., Chaabane, A., Ali Kaafar, M., Castelluccia, C., Legout, A., & Dabbous, W. (2011, March). *One bad apple spoils the bunch: Exploiting P2P applications to trace and profile Tor users.* Retrieved from usenix: https://www.usenix.org/legacy/events/leet11/tech/full_papers/LeBlond.pdf

Mergen, L. (2015). *On anonymous networking in Haskell: announcing Tor and I2P for Haskell.* Retrieved December 3, 2015, from Luctor et Emergen: http://www.leonmergen.com/haskell/privacy/2015/05/30/on-anonymous-networking-in-haskell-announcing-tor-and-i2p-for-haskell.html

Microsoft. (n.d.). *Understanding Reverse Lookup.* Retrieved November 30, 2015, from https://technet.microsoft.com/en-us/library/cc730980.aspx

Mikhailian, A. (n.d.). *How to block Tor exit nodes from accessing your website.* Retrieved from mova.org: http://mikhailian.mova.org/node/194

Nerd, P. (2015, February 26). *DNS Crash Course: A, AAAA and PTR Records.* Preuzeto sa The Classic Yuppie: https://classicyuppie.com/dns-crash-course-a-aaaa-ptr-records/

Nicholson, J. (2014, February 28). *What is a name server? .* Retrieved from inmotion hosting: http://www.inmotionhosting.com/support/domain-names/dns-nameserver-changes/what-is-a-name-server

Orchid. (2014, March). Retrieved from Plugins.i2p.xyz/ plugins/ Orchid : http://plugins.i2p.xyz/plugins/orchid/

Osterman Research, I. (2013, July). *Why Should You Encrypt Email and What Happens if You Don't?* Retrieved from Osterman Research: http://www.ostermanresearch.com/whitepapers/orwp_0194.pdf

PC. (2015, November 28). *Definition of: surface Web*. Retrieved from PC Magazine Encyclopedia: http://www.pcmag.com/encyclopedia/term/52273/surface-web

Peachey, P. (2013, October 9). *Exposed: The dark side of the internet, where you can buy drugs, sex and indecent images.* Retrieved from Independent: http://www.independent.co.uk/news/uk/crime/exposed-the-dark-side-of-the-internet-where-you-can-buy-drugs-sex-and-indecent-images-8723048.html

SAM V3. (2015, November). Preuzeto sa I2P: https://geti2p.net/en/docs/api/samv3

SEOBook. (n.d.). *Robots.txt File Generator*. Retrieved November 30, 2015, from SEOBook: http://tools.seobook.com/robots-txt/generator/

Srna. (2013, oktobar 08). *Tamna strana interneta osvaja tržište.* Retrieved from Nezavisne novine: http://www.nezavisne.com/nauka-tehnologija/internet/Tamna-strana-interneta-osvaja-trziste/212804

Syverson, P. (2005). *Onion routing.* Retrieved December 3, 2015, from Onion-router: http://www.onion-router.net/

Titcomb, J. (2015, November 26). *Anonymous hackers install Viagra advert on Islamic State propaganda website*. Retrieved from The Telegraph: http://www.telegraph.co.uk/technology/internet/12019053/Anonymous-hackers-install-Viagra-advert-on-Islamic-State-propaganda-website.html

Tor. (n.d.). Retrieved December 3, 2015, from Torproject: https://www.torproject.org/about/overview.html.en

WEBnSTUDY. (2015, avgust 20). *Tamni Internet.* Preuzeto sa WEBnSTUDY: http://www.webnstudy.com/tema.php?id=tamni-internet

What is a CNAME record? (2015). Retrieved November 30, 2015, from DNSimple.

What is a SOA Record? (2015). Retrieved November 30, 2015, from DNSimple: https://support.dnsimple.com/articles/soa-record/

What is an AAAA record or IPv6? (n.d.). Retrieved November 30, 2015, from No-IP: http://www.noip.com/support/knowledgebase/what-is-an-ipv6-or-aaaa-record/

Wüest, C. (2010). *The Risks of Social Networking.* Retrieved from symantec: https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_risks_of_social_networking.pdf

Yale, B. (2014, October 21). *How the Internet Works: The Deep Web.* Retrieved from informIT: http://www.informit.com/blogs/blog.aspx?uk=How-the-Internet-Works-The-Deep-Web

Datum prve prijave: 10.12.2015.
Datum prijema korigovanog članka: 02.02.2016.
Datum prihvatanja članka: 23.03.2016.

Kako citirati ovaj rad? / How to cite this article?

*Style – **APA** Sixth Edition:*

Čekerevac, Z., Dvorak, Z., & čekerevac, P. (2016, July 15). Da li je „Tamni Internet" dubok i taman? (Z. Čekerevac, Ed.) *FBIM Transactions, 4*(2), 53-65. doi:10.12709/fbim.04.04.02.05

*Style – **Chicago** Sixteenth Edition:*

Čekerevac, Zoran, Zdenek Dvorak, and Petar čekerevac. 2016. "Da li je „Tamni Internet" dubok i taman?" Edited by Zoran Čekerevac. *FBIM Transactions* (MESTE) 4 (2): 53-65. doi:10.12709/fbim.04.04.02.05.

*Style – **GOST** Name Sort:*

Čekerevac Zoran, Dvorak Zdenek and čekerevac Petar Da li je „Tamni Internet" dubok i taman? [Journal] // FBIM Transactions / ed. Čekerevac Zoran. - Belgrade : MESTE, July 15, 2016. - 2 : Vol. 4. - pp. 53-65.

*Style – **Harvard** Anglia:*

Čekerevac, Z., Dvorak, Z. & čekerevac, P., 2016. Da li je „Tamni Internet" dubok i taman?. *FBIM Transactions,* 15 July, 4(2), pp. 53-65.

Style – **ISO 690** Numerical Reference:

Da li je „Tamni Internet" dubok i taman? **Čekerevac, Zoran, Dvorak, Zdenek and čekerevac, Petar.** [ed.] Zoran Čekerevac. 2, Belgrade : MESTE, July 15, 2016, FBIM Transactions, Vol. 4, pp. 53-65.