

# Duboka i mračna strana interneta

---

Maurus, Ena

Undergraduate thesis / Završni rad

2021

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **Josip Juraj Strossmayer University of Osijek, Faculty of Humanities and Social Sciences / Sveučilište Josipa Jurja Strossmayera u Osijeku, Filozofski fakultet**

Permanent link / Trajna poveznica: <https://um.nsk.hr/um:nbn:hr:142:311720>

Rights / Prava: [In copyright](#) / [Zaštićeno autorskim pravom.](#)

Download date / Datum preuzimanja: **2024-09-21**



**FILOZOFSKI FAKULTET**  
SVEUČILIŠTE JOSIPA JURJA STROSSMAYERA U OSIJEKU

Repository / Repozitorij:

[FFOS-repository - Repository of the Faculty of Humanities and Social Sciences Osijek](#)



Sveučilište J.J. Strossmayera u Osijeku  
Filozofski fakultet Osijek  
Preddiplomski studij Informatologije

Ena Maurus

**Duboka i mračna strana interneta**

Završni rad

Mentor: doc.dr.sc. Milijana Mičunović

Osijek, 2021.

Sveučilište J.J. Strossmayera u Osijeku  
Filozofski fakultet Osijek  
Preddiplomski studij Informatologije

Ena Maurus

## **Duboka i mračna strana interneta**

Završni rad

Područje društvenih znanosti, informacijske i komunikacijske znanosti,  
informacijski sustavi i informatologija

Mentor: doc.dr.sc. Milijana Mičunović

Osijek, 2021.

## **Prilog: Izjava o akademskoj čestitosti i o suglasnosti za javno objavljivanje**

Obveza je studenta da donju Izjavu vlastoručno potpiše i umetne kao treću stranicu završnog odnosno diplomskog rada.

### **IZJAVA**

Izjavljujem s punom materijalnom i moralnom odgovornošću da sam ovaj rad samostalno napravio te da u njemu nema kopiranih ili prepisanih dijelova teksta tuđih radova, a da nisu označeni kao citati s napisanim izvorom odakle su preneseni.

Svojim vlastoručnim potpisom potvrđujem da sam suglasan da Filozofski fakultet Osijek trajno pohrani i javno objavi ovaj moj rad u internetskoj bazi završnih i diplomskih radova knjižnice Filozofskog fakulteta Osijek, knjižnice Sveučilišta Josipa Jurja Strossmayera u Osijeku i Nacionalne i sveučilišne knjižnice u Zagrebu.

U Osijeku, 6. rujna 2021.

Ena MAURUS, 0111121161

---

ime i prezime studenta, JMBAG

## Sažetak

Cilj ovog rada je prikazati glavne značajke, sadržaj i pristup dubokom i mračnom webu i dati primjere tih dvaju dijelova interneta. World Wide Web se sastoji od tri dijela, odnosno čini ga površinski web, duboki web i mračni web. Površinski web je vidljivi ili indeksirani web, dostupan je svim korisnicima putem standardnih preglednika i tražilica. Nevidljivim dijelom weba smatra se duboki i mračni web, neindeksirano područje kojemu se može pristupiti putem određenim preglednika, tražilica i softvera. Standardne tražilice ne mogu vidjeti niti dohvatiti sadržaj na dubokom webu jer te stranice ne postoje sve dok se dinamički ne stvore kao rezultat određenog pretraživanja. Duboki web pohranjuje svoj sadržaj u pretraživi dio baza podataka gdje samo dinamički daju rezultate kao odgovor na izravan zahtjev. Sadržaj na dubokom webu može se podijeliti na četiri kategorije - komercijalne i državne baze podataka, intranet, društvene medije te posebne zbirke koje čine pravne, akademske i istraživačke, znanstvene i tehnološke, medicinske, knjižnične baze podataka. Najpoznatija tražilica dubokog weba je DuckDuckGo. Mračni web je dio dubokog weba, a njegove stranice su skrivene kako bi se osigurala povjerljivost i anonimnost. Mračni web sinonim je za ilegalne aktivnosti, međutim koriste ga svi koji žele pretraživati anonimno i privatno, bez obzira je li svrha ilegalna ili legalna. Mračnom webu se može pristupiti putem decentraliziranih, anonimiziranih čvorova na brojnim mrežama poput Tor softvera (*The Onion Router*), I2P mreže (*Invisible Internet Project*) te Freenet platforme.

**Ključne riječi:** internet, World Wide Web, duboki web, mračni web

## Sadržaj

1. Uvod.....	1
2. Povijesni razvoj i struktura interneta i World Wide Weba.....	1
3. Duboki web.....	3
3.1. Definicija, opis i glavne karakteristike dubokog weba .....	3
3.2. Struktura i sadržaj dubokog weba .....	4
3.3. (Ne)indeksiranost sadržaja i pristup dubokom webu .....	5
3.3.1. Tražilice dubokog weba.....	6
3.3.1.1. DuckDuckGo .....	6
3.3.1.2. Qwant.....	6
3.3.1.3. Scirus.....	7
3.4. Primjeri stranica .....	8
3.4.1. OAIster .....	8
3.4.2. OpenDOAR .....	9
3.4.3. Kwangmyong.....	9
4. Mračni web .....	10
4.1. Definicija, opis i glavne karakteristike mračnog weba .....	10
4.2. Struktura i sadržaj mračnog weba .....	11
4.2.1. Mreže mračnog weba: softver Tor, mreža I2P, platforma Freenet.....	11
4.2.1.1. Tor (The Onion Router).....	11
4.2.1.2. I2P (Invisible Internet Project).....	12
4.2.1.3. Freenet.....	13
4.2.2. Sadržaj mračnog weba.....	14
4.2.3. Mračni web i kriptovalute.....	16
4.3. (Ne)indeksiranost sadržaja i pristup mračnom webu .....	16
4.3.1. Tražilice mračnog weba.....	17
4.3.1.1. Ahmia.....	17
4.3.1.2. Torch.....	17
4.3.1.3. Candle .....	17
4.4. Pozitivna strana mračnog weba.....	18
4.5. Primjeri stranica .....	19
4.5.1. Silk Road .....	19
4.5.2. DarkMarket.....	20

4.5.3. AlphaBay i Hansa .....	20
4.5.4. DeepDotWeb .....	21
5. Zaključak.....	21
6. Literatura.....	23

## 1. Uvod

Pojavom interneta prikupljanje, organiziranje, preuzimanje i dijeljenje informacija postalo je lakše. Korisnici su povezani i mogu komunicirati iz bilo kojeg dijela svijeta u bilo kojem vremenu. Internet je narastao iz male zatvorene mreže namijenjene samo vladi i znanstvenicima u veliku globalnu mrežu koju mogu koristiti svi. Međutim ono što je danas najveći problem na internetu je privatnost koju je teško sačuvati, ali tom problemu su ipak doskočili neki softveri, preglednici i tražilice koji omogućuju privatnost i anonimnost. To je, pak, dovelo do zlouporabe i ilegalnih aktivnosti koji se danas nalaze na mračnom webu.

U ovome radu će se prvo ukratko opisati povijesni razvoj i struktura interneta te upoznati s World Wide Webom koji se dijeli na tri razine - površinski web, duboki web i mračni web. Zatim slijedi drugo poglavlje o dubokom webu gdje se definira isti te prikazuju glavne karakteristike, struktura i sadržaj. Daje se pregled tražilica dubokog weba, kao i primjeri stranica baze podataka, institucijskog repozitorija i intraneta. Treće poglavlje daje pregled mračnog weba koji je dio dubokog weba. U ovom poglavlju se također prikazuju glavne značajke, ali se i opisuje način pristupa mračnom webu te njegova pozitivna strana. Na kraju slijedi zaključak i popis literature.

## 2. Povijesni razvoj i struktura interneta i World Wide Weba

Prema Hrvatskoj enciklopediji, internet je sustav međusobno povezanih računalnih mreža koji korisnicima omogućuje razmjenu podataka i informacija te komunikaciju.<sup>1</sup> Razvoj interneta započinje 1960-ih godina kada je u tijeku bio Hladni rat između SAD-a i SSSR-a. Američko Ministarstvo obrane 1969. godine razvija mrežu ARPANET (*Advanced Research Projects Agency Network*) radi umrežavanja istraživačkih institucija za razvoj vojne tehnologije.<sup>2</sup> ARPANET su lansirali Bolt Beranek i Newman, zvani BBN, čiji je zadatak bio dizajnirati četiri sučelja za obradu poruka, odnosno strojeva koji će omogućiti otvorenu komunikaciju između četiri različita računala koja rade na četiri različita operativna sustava stvarajući prvu računalnu mrežu na velike udaljenosti i povezivajući se između nekoliko američkih sveučilišta. Putem ARPANET-ovog protokola za mrežnu kontrolu korisnici su mogli pristupiti i koristiti računala na drugim mjestima i dijeliti datoteke između računala. To je bio istraživački projekt koji je

---

<sup>1</sup> Usp. Internet. // Hrvatska enciklopedija. Leksikografski zavod Miroslav Krleža. URL : <http://www.enciklopedija.hr/Natuknica.aspx?ID=27653> (2021-05-03)

<sup>2</sup> Usp. Isto.



ispitivao najpovoljniji način izgradnje mreže koja bi funkcionirala kao pouzdani komunikacijski medij. Glavna prepreka koju je trebalo savladati bila je razvoj skupa signala između različitih računala koji bi otvorili komunikacijske kanale, omogućavajući prijenos podataka s jedne točke na drugu, a ti signali su se zvali protokoli.<sup>3</sup> 1972. godine komercijalna verzija ARPANET-a pod imenom Telnet postala je prva javna usluga paketnih podataka. Telnet je bio jednostavan mehanizam koji je omogućavao osnovnu komunikaciju između dva računala-hosta (*hosts*). Telnet omogućuje korisnicima prijavu i upravljanje udaljenim računalima te se može koristiti za pretraživanje i pregledavanje udaljenih baza podataka, poput knjižničnog kataloga.<sup>4</sup>

Godinu dana kasnije ARPANET je povezan s međunarodnim hostovima. Protokol za prijenos datoteka (*File Transfer Protocol* - FTP) nastao je i funkcionirao pomoću arhitekture klijentskog poslužitelja, a omogućio je dijeljenje datoteka između računala. Telnet, FTP i TALK bili su prvi programi koji su postali dostupni na ARPANET-u i koji se i danas koriste u nekom obliku na internetu.<sup>5</sup> TALK je bio prvi program koji je korisnicima omogućio razgovor u stvarnom vremenu putem interneta, a koristio se tako što su korisnici tipkali poruke na podijeljeni zaslon i čitali odgovore napisane na dnu zaslona.<sup>6</sup> 1974. godine su Vint Cerf i Robert Kahn razvili niz protokola u koji su implementirali otvorenu arhitekturu, a ti novi protokoli bili su *Internet Protocol* (IP) i *Transmission Control Protocol* (TCP). IP uključuje pravila za usmjeravanje pojedinih paketa podataka, a TCP uključuje pravila koja računala na mreži koriste za uspostavljanje i prekidanje veza. Upravo su Vint Cerf i Robert Kahn prvi upotrijebili termin "internet".<sup>7</sup> Početkom 1980-ih dolazi do kontinuiranog rasta ARPANET-a i drugih mreža, a sredinom 1980-ih internet ulazi u svoju komercijalnu fazu. 1988. godine Jarkko Oikarinen napisao je komunikacijski program koji je proširio mogućnosti programa TALK i nazvao ga je *Internet Relay Chat* (IRC). Koristili su ga mnogi znanstvenici i akademici kako bi vodili rasprave o teorijama, eksperimentima i inovacijama.<sup>8</sup>

1989. godine istraživač iz CERN-a Tim Berners-Lee predložio je ideju međunarodnog sustava protokola, odnosno izgradnju distribuiranog hipermedijskog poslužitelja koji bi korisnicima omogućio pripremu elektroničkih dokumenata i njihovo dijeljenje, a to je nazvao World Wide Web (WWW). Prvi WWW klijent bio je preglednik u NeXTStep-u te je napisao

---

<sup>3</sup> Usp. Cohen-Almagor, Raphael. Internet History. // International Journal of Technoethics 2, 2(2011), str. 46-48. URL : [https://www.researchgate.net/publication/215660523\\_Internet\\_History](https://www.researchgate.net/publication/215660523_Internet_History) (2021-06-05)

<sup>4</sup> Usp. Isto., str. 49.

<sup>5</sup> Usp. Isto.

<sup>6</sup> Usp. Isto., str. 50.

<sup>7</sup> Usp. Isto.

<sup>8</sup> Usp. Isto., str. 52.

većinu softvera za komunikaciju, definirajući adresu web stranice, tj. URL-ove (*Uniform Resource Locator*), HTTP (*Hypertext Transfer Protocol*) i HTML (*HyperText Markup Language*).<sup>9</sup>

1990. godine projekt ARPANET je službeno gotov. Sredinom 90-ih godina dolazi do masovnog širenja interneta koji postaje žarište komunikacije, informacija i poslovanja, a istovremeno su korisnici mogli stvarati vlastite web stranice. Razvoj interneta zadobiva novi obrat jer je sve veći broj velikih i srednjih organizacija počeo pokretati TCP/IP protokole na svojim unutarnjim komunikacijskim mrežama zvanim intranet.<sup>10</sup> Nadalje, pronalaženje informacija na webu postalo je teže. Više nije bilo problem povezivanje nego pretraživanje i lociranje informacija. Tom problemu su doskočili Larry Page i Sergey Brin, studenti sa Stanforda, koji su započeli rad na tražilici BackRub koja omogućuje povratnu vezu. Kasnije su svoju tražilicu preimenovali u Google, a prvu verziju Google-a objavili su na web stranici Sveučilišta Stanford u kolovozu 1996. godine te je danas najpopularnija i najčešće korištena tražilica na internetu.<sup>11</sup>

Danas se WWW sastoji od tri dijela - površinskog weba, dubokog weba i mračnog weba. Površinski web je poznat i kao vidljivi ili indeksirani web, dostupan je javnosti putem standardnih preglednika i tražilica. Međutim na površinskom webu korisnik dobije samo 0.03% rezultata od cjelokupnog weba.<sup>12</sup> Duboki i mračni web se još naziva nevidljivi ili skriveni web te nije dostupan široj javnosti, a o njima će biti više riječi u nastavku rada.

### **3. Duboki web**

#### **3.1. Definicija, opis i glavne karakteristike dubokog weba**

1994. godine Jill Ellsworth prvi je puta upotrijebio termin nevidljivi web jer su informacije bile nevidljive za standardne tražilice, a 2001. godine Michael Bergman stvorio je termin duboki web koji je nevidljiv za standardne tražilice te se njegovom sadržaju može pristupiti samo putem alternativnih alata za pretraživanje.<sup>13</sup> Pojam dubokog weba može se definirati kao dio

---

<sup>9</sup> Usp. Isto., str. 53.

<sup>10</sup> Usp. Isto., str. 55.

<sup>11</sup> Usp. Isto.

<sup>12</sup> Usp. Kaur, Shubhdeep; Randhawa, Sukhchandan. Dark Web : A Web of Crimes. // Wireless Personal Communications, 112(2020), str. 2132. URL :

[https://www.researchgate.net/publication/338878596\\_Dark\\_Web\\_A\\_Web\\_of\\_Crimes](https://www.researchgate.net/publication/338878596_Dark_Web_A_Web_of_Crimes) (2021-06-03)

<sup>13</sup> Usp. Prasad M. R., Murali. Deep Web : Librarian's Perspective. // PEARL - A Journal of Library and Information Science 11, 4(2017), str. 419. URL :

[https://www.researchgate.net/publication/321851210\\_Deep\\_Web\\_Librarian%27s\\_Perspective](https://www.researchgate.net/publication/321851210_Deep_Web_Librarian%27s_Perspective) (2021-06-03)

interneta koji je enkriptiran te skriven od standardnih tražilica i preglednika. Sastoji se od neindeksiranih web mjesta, baza podataka te nepovezanog sadržaja, ali više o samom sadržaju dubokog weba slijedi u sljedećem poglavlju.<sup>14</sup> Duboki web također uključuje određeni dio površinskog weba kao što su Amazon, Netflix i IMDB jer su oni prilagođeni korisnicima i nema potrebe za indeksiranjem svakog URL-a. Većina ljudi koristi duboki web, a da to i ne zna. Primjerice, pojedine web stranice poput Facebooka i Instagrama također se smatraju dijelom dubokog weba jer se tim web mjestima može pristupiti pomoću web aplikacije. Duboki web sadrži sve podatke koji se ne mogu pronaći uz pomoć standardnih tražilica. Njegova stvarna veličina nije u potpunosti poznata, ali se pretpostavlja da je 400 do 500 puta veća od površinskog weba.<sup>15</sup> Jedini način na koji korisnik može pristupiti ovom dijelu interneta je upisivanjem usmjerenog upita u obrazac za pretraživanje, čime se dohvaća sadržaj unutar baza podataka koji nije povezan.<sup>16</sup>

### 3.2. Struktura i sadržaj dubokog weba

Podaci na dubokom webu se u potpunosti razlikuju u kvaliteti i količini od podataka na površinskom webu. Dostupni podaci na dubokom webu su uži i specifičniji od podataka na površinskom webu te su namijenjeni za akademsku i istraživačku zajednicu. Sadržaj na dubokom webu može se podijeliti na četiri kategorije - komercijalne i državne baze podataka, intranet, društvene medije te posebne zbirke koje čine pravne, akademske i istraživačke, znanstvene i tehnološke, medicinske i knjižnične baze podataka. Sadržaj baza podataka generira se dinamički i ne mogu ga otkriti standardne tražilice. Većina komercijalnih baza podataka temelji se na pretplati ili na naknadi po čitanju ili preuzimanju, a njihovom sadržaju mogu pristupiti samo pretplatnici. Takve baze su na primjer EBSCO, ProQuest i Science Direct. Ono što je karakteristično za duboki web je autorizacija prijave. Neke web stranice zahtijevaju autentifikaciju korisničkog imena, lozinke ili IP adrese za pristup svojim web mjestima. Može biti besplatno ili na temelju naknade, a primjer bi bio Moodle. Sljedeća karakteristika je pretraživanje u stvarnom vremenu. Standardne tražilice ne pretražuju podatke o trenutnim događajima. Stranice u dubokom webu su nepovezane, a standardne tražilice

---

<sup>14</sup> Usp. Čekerevac, Zoran; Dvorak, Zdenek; Čekerevac, Petar. Dali je "tamni internet" dubok i taman? // FBIM Transactions 4, 2(2016), str. 54.

<sup>15</sup> Usp. Yadav, Divya; Bhushan, Bharat; Saxena, Shivam. The Dark Web : A Dive Into the Darkest Side of the Internet. // SSRN Electronic Journal, (2020), str. 2. URL : [https://www.researchgate.net/publication/341420503\\_The\\_Dark\\_Web\\_A\\_Dive\\_Into\\_the\\_Darkest\\_Side\\_of\\_the\\_Internet](https://www.researchgate.net/publication/341420503_The_Dark_Web_A_Dive_Into_the_Darkest_Side_of_the_Internet) (2021-06-03)

<sup>16</sup> Usp. Pederson, Steve. Understanding the Deep Web in 10 minutes.

indeksiraju web stranice prateći poveznice s jedne web stranice na drugu, ako ne postoje veze do bilo koje web stranice, one ih možda neće pronaći. Neke web stranice blokirane su protokolima za izuzeće pri indeksiranju i nisu za otvoreni pristup kao što je intranet. U sadržaj dubokog weba pripadaju i društvene mreže poput Facebooka, Instagrama i LinkedIna. Što se tiče formata, sadržaj na dubokom webu je dostupan u različitim formatima kao što je tekst (*.doc, .pdf*), audiovizualna datoteka (*.jpeg, .mp3, .mp4*), slika (*.jpeg, .tiff*) i sl., te standardnim tražilicama treba vremena za indeksiranje ovih formata. S obzirom na to da su podaci u dubokom webu dinamični te izvori pohranjuju svoje podatke u baze podataka koje se mogu pretraživati, a koje odgovaraju samo na izravne upite, istovremeno je u bazama podataka dopušten samo jedan izravni upit i to je naporan način pretraživanja. Potrebne su specijalizirane vještine, alati i tehnike za pronalaženje podataka iz tih web izvora, pa u takvom slučaju informacijski stručnjak ima ključnu ulogu u pretraživanju i dijeljenju informacija dubokog weba.<sup>17</sup>

### **3.3. (Ne)indeksiranost sadržaja i pristup dubokom webu**

Pretraživanje na internetu može se usporediti s povlačenjem mreže preko površine oceana. Iako puno toga može biti uhvaćeno u mrežu, još uvijek postoji mnoštvo podataka koji su duboko skriveni. Razlog tome je što većina podataka na internetu je zakopana, a standardne tražilice ih ne mogu pronaći. Standardne tražilice indeksiraju tako što “puzaju” po površinskom webu, a stranica da bi bila otkrivena mora biti statična te povezana s drugim mrežnim stranicama. Standardne tražilice ne mogu vidjeti niti dohvatiti sadržaj na dubokom webu jer te stranice ne postoje sve dok se dinamički ne stvore kao rezultat određenog pretraživanja. Duboki web pohranjuje svoj sadržaj u pretraživi dio baza podataka gdje samo dinamički daju rezultate kao odgovor na izravan upit.<sup>18</sup> Upiti dubokog weba “umotavaju” se u web stranice u obliku zapisa podataka i generiraju se dinamički. Standardne tražilice temeljene na indeksiranju teško indeksiraju takve web stranice. Većina informacija na dubokom webu je dostupna bez preplate, ali su duboko zakopane na dinamički generiranim web mjestima, a standardne ih tražilice nikad ne mogu pronaći. Indeksiranje znači da se povezani podaci mogu pronaći putem poveznice s domene početne stranice. Iako duboki web ima veliku količinu podataka, za razliku od površinskog weba, svi ti podaci su centralizirani na jednom mjestu, što znači da za svako

---

<sup>17</sup> Usp. Prasad M. R., Murali. Nav. dj., str. 419-421.

<sup>18</sup> Usp. Bergman, Michael K. White Paper: The Deep Web: Surfacing Hidden Value. // Journal of Electronic Publishing 7, 1(2001), str. 1.

područje (npr. medicina, ekonomija i sl.) postoji jedan broj tražilica koji je kreiran za pretraživanje u dubokom webu.<sup>19</sup>

### 3.3.1. Tražilice dubokog weba

#### 3.3.1.1. DuckDuckGo

Jedna od najpoznatijih tražilica dubokog weba je DuckDuckGo tražilica osnovana 2008. godine. Osigurava anonimnost i privatnost, a korisnik može pretraživati privatno pomoću aplikacije ili proširenja (*extension*), dodati privatno web pretraživanje u svoj omiljeni preglednik ili pretraživati izravno preko mrežne stranice tražilice. Ne prikuplja niti dijeli nikakve osobne podatke korisnika te nema povijest pretraživanja. Korisnici često znaju pretraživati u *incognito* načinu pretraživanju koji uglavnom samo briše podatke s korisnikovog računala i ničim ne sprječava Google da sprema njegova pretraživanja, niti zaustavlja tvrtke, pružatelje internetskih usluga ili vladu da prate korisnika putem interneta. Suprotno tome, pretraživanje na DuckDuckGo potpuno je anonimno. Uz njihovu aplikaciju i proširenje pretraživanje je u potpunosti privatno, kao i pregled rezultata pretraživanja.<sup>20</sup>

#### 3.3.1.2. Qwant

Qwant je francuska tražilica razvijena 2011. godine., a objavljena 2013. godine. Mjesečno doseže do 189 milijuna pretraživanja te ju koristi 37 zemalja. Glavni cilj tražilice je privatnost, stoga ne prikuplja osobne podatke niti omogućuje ciljno oglašavanje. Algoritmi za klasifikaciju informacija jamče neutralne i iscrpne rezultate, bez filtriranja i bilo kojeg drugog kriterija osim relevantnosti. Mnoge poznate tvrtke i institucije poput Microsoft, Huawei, Samsung, Allianz, Prime Video i L'oreal koriste ovu tražilicu. 2016. godine je Europska banka počela koristiti pa se broj korisnika udvostručio u godinu dana. Qwant tražilica nudi tri proizvoda - pretraživanje, kartu i pretraživanje za djecu. Qwant pretraživanje omogućava zaštitu i privatnost, a sučelje je ugodno zahvaljujući tehnologiji indeksiranja. Ne sprema povijest pretraživanja i nema "kolačića" koji služi za reklame. Qwant karta pomaže u pronalaženju obližnjih restorana i smještaja bez praćenja, kao i personalizaciju istog. Kako bi pronašao sve adrese koristi se alatima OpenStreetMap, OpenAddresses i YellowPages. Beta verzija Qwant karte izašla je

---

<sup>19</sup> Mwila, Kingston Ali. The Deep Web. URL : [https://www.researchgate.net/publication/335336010\\_The\\_Deep\\_Web](https://www.researchgate.net/publication/335336010_The_Deep_Web) (2021-05-28)

<sup>20</sup> Usp. DuckDuckGo - Privacy, simplified. URL : <https://duckduckgo.com/> (2021-05-28)

2019. godine. Ono što ovu tražilicu čini drugačijom od ostalih je što nudi tzv. Qwant Junior tražilicu objavljenu 2015. godine koja je dizajnirana za djecu od 6 do 12 godina kako bi naučili pretraživati internet u sigurnom i zabavnom okruženju, bez oglasa. Na početnoj stranici djeca mogu birati između pretraživanja, informiranja, igranja, učenja i aktivnosti. Pretraživanje i informiranje nude najnovije vijesti, zatim mogu učiti sve školske predmete - od jezika preko povijesti, geografije, fizike, kemije pa sve do umjetnosti i sporta. Qwant Junior filtrira rezultate kako ne bi prikazivao nasilni ili pornografski sadržaj. Djeca također ne mogu pristupiti e-trgovinama i stranicama koje se nalaze na crnoj listi, a kako bi ta lista bila ažurna razvili su algoritme koji analiziraju metapodatke, fotografije, ključne riječi i sl. kojima identificiraju neprikladne web stranice. Tražilicu preporučuje *National Education Association* koji potiče škole da ju koriste.<sup>21</sup>

### 3.3.1.3. Scirus

Scirus je najopsežnija tražilica za znanstveno istraživanje. Omogućava korisniku da brzo i jednostavno pretražuje znanstvene informacije, uključujući recenzirane članke, autorske početne stranice te sveučilišne web stranice. Scirus pokreće tehnologija pretraživanja koju pruža *Fast Search and Transfer ASA* (FAST). Scirus se fokusira samo na web stranice koje sadrže znanstveni sadržaj te ih dubinski indeksira. Pretražuje svjetske mreže besplatnih izvora informacija i najveće svjetske baze podataka znanstvenih, medicinskih i tehničkih časopisa. Pronalazi unaprijed tiskane članke, recenzirane članke i patente. Ima intuitivno sučelje i nudi napredne značajke pretraživanja koje ga čine jednostavnim za upotrebu. Može čitati netekstualne datoteke omogućujući pristup PDF i PostScript datotekama koje su često nevidljive drugim tražilicama. Scirus ima partnere, a neki od njih su ScienceDirect, MEDLINE, Beilstein, BioMed Central i Američki ured za patente. Scirus poboljšava rangiranje i relevantnost rezultata primjenom inteligentnog prepisivanja upita koji su kreirani da automatski razumiju namjeru korisnika i omoguće inteligentnije pretraživanje prepisivanjem upita.<sup>22</sup>

---

<sup>21</sup> Usp. Qwant – the European search engine that respects your privacy. URL : <https://about.qwant.com/> (2021-06-25)

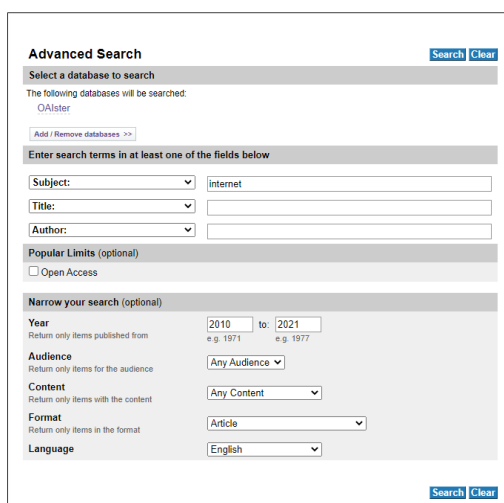
<sup>22</sup> Usp. How Scirus Works. URL : [http://spvp.zesoi.fer.hr/seminari/white\\_papers/WhitePaper\\_Scirus.pdf](http://spvp.zesoi.fer.hr/seminari/white_papers/WhitePaper_Scirus.pdf) (2021-05-29)

## 3.4. Primjeri stranica

### 3.4.1. OAIster

OAIster je katalog za pretraživanje preko milijun OAIster zapisa metapodataka u OAIster bazi podataka. Izrađen je korištenjem OAI-PMH (*Open Archives Initiative Protocol*) protokola za prikupljanje metapodataka. Danas OAIster ima više od 50 milijuna zapisa koji predstavljaju digitalne izvore više od 2000 suradnika. OAIster baza podataka je uključena u WorldCat, a prikupljanje metapodataka prolazi kroz *WorldCat Digital Collection Gateway*. Omogućava korisniku da sam napravi raspored harvestiranja te prilagodi mapu metapodataka u zbirke. Zapisi OAIster u potpunosti su dostupni putem WorldCat i uključeni su u rezultate pretraživanja zajedno sa zapisima iz tisuća knjižnica širom svijeta. Bazu podataka OAIster moguće je pretraživati na usluzi OCLC FirstSearch. OAIster sadrži multidisciplinarnе izvore kao što su digitalizirane knjige, članci u časopisima, novine i rukopisi, audio datoteke (.wav, .mp3), video datoteke (.mp4, QuickTime), fotografije (.jpg, .tif, .gif), statistički podaci, teze i istraživački radovi.<sup>23</sup>

OAIster baza podataka omogućuje jednostavno i napredno pretraživanje. Na slici 1. prikazano je napredno pretraživanje za temu internet. Prva polja odnose se na upisivanje ključnih riječi, naslova, autora, predmeta, ISBN-a, ISSN-a, jezika, nakladnika i sl. Sljedeća stvar koju korisnik može odabrati su rezultati u otvorenom pristupu. Zadnje, kako bi se suzilo pretraživanje, korisnik može upisati od kada do kada želi rezultate, te odabrati publiku (mladi ili stari), sadržaj (biografija, fikcija, teze i disertacije, glazbeni zapisi i dr.), format (knjiga, audio-knjiga, članak, karta, video i dr.) te na kraju jezik.



Slika 1. Napredno pretraživanje OAIster baze podataka

<sup>23</sup> Usp. OAIster : Catalog of open access resources. URL : <https://www.oclc.org/en/oaister.html> (2021-06-03)

### 3.4.2. OpenDOAR

Najpoznatiji registar/direktorij repozitorija je OpenDOAR (*Directory of Open Access Repositories*). OpenDOAR je direktorij repozitorija otvorenog pristupa koji osigurava kvalitetu. Pruža besplatan, otvoren pristup akademskim rezultatima i resursima. Svaki zapis repozitorija unutar OpenDOAR-a pažljivo je pregledan i obrađen od strane uredničkog tima što omogućava pouzdanu uslugu za zajednicu. Usluga je pokrenuta 2005. godine kao proizvod suradničkog projekta Sveučilišta Nottingham i Sveučilišta Lund, koji su financirali OSI, Jisc, SPARC Europe i CURL.<sup>24</sup>

Na OpenDOAR se pretražuje na način da se pod *Search* se upiše ime repozitorija te se pretražuje prema državi ili se može odabrati napredno pretraživanje. Napredno pretraživanje omogućuje da korisnik pretraži prema nazivu repozitorija, organizaciji, tipu repozitorija (institucijski, disciplinarni i dr.), nazivu softvera (*EPrints*, *Greenstone*, *Open Repository* i dr.), tipu sadržaja (članak, bibliografija, izvješće, knjiga i dr.), temi (zdravlje i medicina, filozofija i religija, matematika i statistika, pravo i politika i dr.) te na kraju se odabere država i regija. Kao primjer repozitorija na OpenDOAR-u odabran je institucijski repozitorij Sveučilišta u Leicesteru koji je multidisciplinarni i koji sadrži objekte učenja iz područja poput arheologije, povijesti, kriminalistike, genetike, prava, politike i psihologije.<sup>25</sup>

### 3.4.3. Kwangmyong

Prema Hrvatskoj enciklopediji, intranet je “privatna računalna mreža neke tvrtke, institucije i sličnoga, zasnovana na internetskim tehnologijama.”<sup>26</sup> Održava interne mrežne stranice, omogućuje sigurnu razmjenu podataka i dostupna je samo određenom broju korisnika.<sup>27</sup> Jednostavno rečeno, to je privatna mreža, a ono što je karakteristično za intranet je da korisnici moraju imati svoje podatke kako bi mogli pristupiti autorizaciji. Kao primjer intraneta može se uzeti Kwangmyong, intranet Sjeverne Koreje. Naime, Sjeverna Koreja ima najrestriktivniju politiku pristupa internetu. Od 1996. godine ima izgrađenu nacionalnu mrežu na koju se građani mogu povezati na WWW kada vlada Sjeverne Koreje to odluči. Nacionalna mreža ili intranet pod nazivom Kwangmyong, što znači sjajno svjetlo, izgrađena je u studenom 2002.<sup>28</sup>

<sup>24</sup> Usp. About OpenDOAR. URL : <https://v2.sherpa.ac.uk/opensoar/about.html> (2021-06-08)

<sup>25</sup> Usp. University of Leicester OER Repository. URL : <https://www2.le.ac.uk/projects/oer> (2021-06-08)

<sup>26</sup> Intranet. // Hrvatska enciklopedija. Leksikografski zavod Miroslav Krleža. URL : <https://www.enciklopedija.hr/natuknica.aspx?id=68095> (2021-06-07)

<sup>27</sup> Usp. Isto.

<sup>28</sup> Usp. Ko, Kyungmin; Lee, Heejin; Jangc, Seungkwon. The Internet dilemma and control policy: political and economic implications of the Internet in North Korea. // The Korean Journal of Defense Analysis 21, 3(2009), str. 284. URL :



Kwangmyong povezuje knjižnice, sveučilišta i vladine odjele te sadrži brojne domaće web stranice, mrežne sustave za učenje i elektroničku poštu. Web mjesta pripadaju nacionalnim vijestima, vladinim informatičkim centrima, sveučilištima te službenim organizacijama.<sup>29</sup> Većina ureda središnje vlade u Sjevernoj Koreji je povezana putem intraneta, a mreža se proširuje na regionalni i lokalni ured. No međunarodne veze su ograničene pa web stranice izvan Sjeverne Koreje nisu dostupne većini građana. Postoje dvije kategorije sjevernokorejskih web stranica, jedna je za političku propagandu, a druga za komercijalne svrhe te objema država upravlja i određuje kakav će biti sadržaj.<sup>30</sup>

## 4. Mračni web

### 4.1. Definicija, opis i glavne karakteristike mračnog weba

Mračni web je dio dubokog weba, a njegove stranice su skrivene kako bi se osigurala povjerljivost i anonimnost. Mračni web sinonim je za ilegalne aktivnosti, međutim koriste ga svi koji žele pretraživati anonimno i privatno, bez obzira je li svrha ilegalna ili legalna. Primjerice, koriste ga stanovnici zemalja gdje vlada jaka cenzura, transrodne osobe koje žele razgovarati o svojim problemima ili imigranti bez dokumenata koji posjeduju pravo na pristup informacijama i potrebna im je zaštita privatnosti kako bi to ostvarili. Razvoj mračnog weba proizašao je iz potrebe za privatnom i sigurnom komunikacijom između vojske i obavještajne službe.<sup>31</sup> Glavne komponente mračnog weba su preglednici koji omogućuju pristup mračnom webu, virtualne privatne mreže (VPN) za prijenos podataka, tehnika za šifriranje podataka i algoritam usmjeravanja. Za pristup mračnom webu vrlo je važno ostati anonimn te nije dovoljno koristiti određeni preglednik već je potrebno koristiti dobar VPN.<sup>32</sup>

Ponekad je teško reći tko su korisnici mračnog weba s obzirom na to da razina anonimnosti predstavlja izazov kod istraživanja. Tijekom 2013. i 2014. godine američko-japanska tvrtka za sigurnost *Trend Micro* istražila je i analizirala veliki broj stranica na

---

[https://www.researchgate.net/publication/233186994\\_The\\_Internet\\_dilemma\\_and\\_control\\_policy\\_political\\_and\\_economic\\_implications\\_of\\_the\\_Internet\\_in\\_North\\_Korea](https://www.researchgate.net/publication/233186994_The_Internet_dilemma_and_control_policy_political_and_economic_implications_of_the_Internet_in_North_Korea) (2021-06-07)

<sup>29</sup> Usp. North Korea's Ruling Elite Are Not Isolated. URL : <https://go.recordedfuture.com/hubfs/north-korea-internet-activity.pdf> (2021-06-07)

<sup>30</sup> Usp. Ko, Kyungmin; Lee, Heejin; Jangc, Seungkwon. Nav. dj., str. 285.

<sup>31</sup> Usp. Coffey, Mollie L. Library application of Deep Web and Dark Web technologies. // School of Information Student Research Journal 10, 1(2020), str. 2-3. URL : [https://www.researchgate.net/publication/344161017\\_Library\\_application\\_of\\_Deep\\_Web\\_and\\_Dark\\_Web\\_technologies](https://www.researchgate.net/publication/344161017_Library_application_of_Deep_Web_and_Dark_Web_technologies) (2021-06-03)

<sup>32</sup> Usp. Kaur, Shubhdeep; Randhawa, Sukhchandan. Nav. dj., str. 2134.

mračnom webu te dala mali uvid u korisnike istog. Prema analiziranim podacima, engleski jezik je bio glavni jezik za najmanje 2154 web mjesta od obrađenih 3454 domena, što čini oko 62% web mjesta mračnog weba. Nakon toga slijedi ruski i francuski jezik. Međutim promatrajući distribuciju jezika prema broju URL-ova, ruski jezik ipak dominira jer engleski ima više web mjesta, ali ruski ima više web stranica. Osim kroz jezik, korisnike mračnog weba se može promatrati kroz tržište dobavljača. Tako se kroz analizu uvidjelo kako korisnici najviše pretražuju i kupuju kanabis, MDMA i lijekove. Mnogi korisnici možda nisu svjesni da na mračnom webu postoji više od standardnih web mjesta. *Trend Micro* grupirao je URL-ove prema njihovoj URI shemi (HTTP, HTTPS, FTP itd.). Gotovo 22 000 prikupljenih domena bilo je povezano s HTTP ili HTTPS protokolom. Više od 100 domena koristi ili IRC ili IRCS protokol, odnosno chat poslužitelje koji se mogu koristiti kao okupljalište zlonamjernih aktera za sastanak i razmjenu robe ili kao komunikacijski kanal za botnet.<sup>33</sup>

## 4.2. Struktura i sadržaj mračnog weba

Karakteristično za mračni web je da koristi *peer-to-peer* mrežu, posebice preko Freenet platforme. *Peer-to-peer* mreža, skraćeno p2p, je vrsta računalne mreže koja se primarno koristi za distribuciju digitalnih medijskih datoteka. U *peer-to-peer* mreži svako računalo djeluje i kao poslužitelj i kao klijent, odnosno opskrbljuje i prima datoteke s propusnom širinom i obradom raspoređenim među svim članovima mreže. Takva decentralizirana mreža koristi resurse koji su učinkovitiji od tradicionalne mreže te je manje osjetljiva na kvarove sustava.<sup>34</sup>

U narednim potpoglavljima se prikazuje način pristupanja mračnom webu, a to su tri najčešća načina – putem Tora, I2P mreže te Freenet platforme. Nakon toga se opširnije opisuje sadržaj mračnog weba.

### 4.2.1. Mreže mračnog weba: softver Tor, mreža I2P, platforma Freenet

#### 4.2.1.1. Tor (The Onion Router)

Mračnom webu se može pristupiti putem decentraliziranih, anonimiziranih čvorova na brojnim mrežama poput Tor softvera (*The Onion Router*), I2P mreže (*Invisible Internet Project*) te Freenet platforme. Prvo će se opisati Tor softver. Ideja je započela sredinom devedesetih

---

<sup>33</sup> Usp. Ciancaglini, Vincenzo.[et al.]. *Below the Surface : Exploring the Deep Web*. Irving : Trend Micro, 2015.

<sup>34</sup> Usp. P2P computer network. // Encyclopedia Britannica. URL : <https://www.britannica.com/technology/P2P> (2021-06-03)

zahvaljujući Rogeru Dingledinu i Nicku Mathewsonu. Prepoznavši korist Tora za digitalna prava *Electronic Frontier Foundation* počeo je financirati Rogerov i Nickov rad na Toru 2004. godine, a 2006. godine osnovana je Tor Project, Inc., neprofitna organizacija koja održava razvoj Tor mreže. 2007. godine organizacija se bavi cenzurom i zaobilaženjem “zidova” kako bi korisnici mogli pristupiti otvorenom webu. Tor je počeo stjecati popularnost među aktivistima i korisnicima zainteresiranim za privatnost, no i dalje je bilo poteškoća pri korištenju, pa je počevši od 2005. započeo razvoj alata koji nisu samo proxy Tor mreže.<sup>35</sup>

Razvoj preglednika Tor započeo je 2008. godine.<sup>36</sup> Tor preglednici koriste nasumične ulazne točke u mreži *.onion* na temelju podataka koje pruža Tor poslužitelj te izlistava slučajne ulazne točke. Zahtjevi za podacima šifriraju se i prosljeđuju zajedno s konačnom adresom odredišta. Svaka sljedeća točka releja na putu dešifrira adresu, ponovno šifrira zahtjev i prosljeđuje dalje. Zna samo odakle su podaci posljednji put došli i kamo idu dalje. U svakoj se točki na putu podaci šifriraju između čvorova. Nijedan relej ne može odrediti cijeli put kojim prolaze podaci. Nakon što podaci dođu do izlazne točke usmjeravaju se na svoje konačno odredište. Uz to, daljnji zahtjevi za Tor mrežu dobivaju novi put svakih 10 minuta kako bi pružili daljnju privatnost u slučaju da netko vrši analizu prometa na pojedinačnom čvoru.<sup>37</sup>

Prednost Tor preglednika je što pruža anonimnost web mjestima i poslužiteljima, štiti privatnost korisnika skrivajući njihove IP adrese, podržava sve *.onion* stranice kojima ne može pristupiti nijedan drugi preglednik, aktivnosti korisnika se ne mogu pratiti te pruža sigurnost prosljeđivanjem podataka kroz različite relej poslužitelje. Nedostaci su što preglednik može usporiti dok se podaci prenose, ne pokušava zaštititi od nadzora prometa, ne može pružiti *end-to-end* šifriranje te je sigurnost na izlaznim čvorovima vrlo niska.<sup>38</sup>

#### 4.2.1.2. I2P (Invisible Internet Project)

*Invisible Internet Project* (I2P) je potpuno šifrirani sloj privatne mreže koji je razvijen u svrhu privatnosti i sigurnosti kako bi zaštitio identitet, mjesto i aktivnosti korisnika. Softver se isporučuje s usmjerivačem koji povezuje korisnika s mrežom i aplikacijama za dijeljenje i komunikaciju. I2P skriva poslužitelj od korisnika i korisnika od poslužitelja. Sav I2P promet interni je na I2P mreži te promet unutar I2P ne komunicira izravno s internetom. Koristi

---

<sup>35</sup> Usp. Tor Project | Anonymity Online. URL : <https://www.torproject.org/> (2021-06-03)

<sup>36</sup> Usp. Isto.

<sup>37</sup> Usp. Ehney, Ryan; Shorter, Jack D. Deep Web, Dark Web, Invisible Web and the Post Isis World. // Issues in Information Systems 17, 4(2016), str. 37. URL : [https://iacis.org/iis/2016/4\\_iis\\_2016\\_36-41.pdf](https://iacis.org/iis/2016/4_iis_2016_36-41.pdf) (2021-06-03)

<sup>38</sup> Usp. Kaur, Shubhdeep; Randhawa, Sukhchandan. Nav. dj., str. 2138.

šifrirane jednosmjerne tunele između korisnika, stoga nitko ne može vidjeti odakle dolazi promet ili koji je njegov sadržaj. Uz to, I2P ne omogućuje prepoznavanje i blokiranje od strane cenzora. I2P nudi softver za preuzimanje koji povezuje korisnika s mrežom, a pruža i aplikacijski sloj koji omogućava ljudima upotrebu i kreiranje aplikacija za svakodnevnu upotrebu. I2P nudi svoj jedinstveni DNS tako da korisnik može samostalno hostirati sadržaj na mreži te posjedovati vlastitu platformu koju može dodati u I2P direktorij ili pozvati samo svoje prijatelje. I2P mreža funkcionira na isti način kao i Internet. Kada se preuzme I2P softver, on uključuje sve što je potrebno kako bi se korisnik privatno povezo. I2P ima vlastitu bazu podataka koja omogućuje sigurnu distribuciju podataka o usmjeravanju i kontaktima.<sup>39</sup>

Prednosti I2P mreže su što se mreža temelji isključivo na porukama, pošiljatelj i primatelj ne otkrivaju svoje IP adrese trećoj strani zbog kriptografskih identifikatora, temelji se na usmjeravanju *.onion* stranica te je dijeljenje datoteka učinkovitije. Nedostaci su što najbolje radi samo na Linuxu, dok se na Windowsu i Macu lako prati, ima problema s pouzdanošću i implementacijom te bi za pristup sadržaju korisnik trebao biti prijavljen, a u slučaju drugih anonimnih preglednika, korisnik može izravno pristupiti sadržaju.<sup>40</sup>

#### 4.2.1.3. Freenet

Freenet je distribuirana *peer-to-peer* platforma razvijena za anonimno objavljivanje i distribuciju informacija bez cenzure. Cilj je osigurati distribuirani sustav za objavljivanje i pristup informacijama. Funkcionira tako što se dokumenti pohranjuju u mrežu s pridruženom adresom ili ključem koji se sastoji od binarnog niza. Ključem se odlučuje gdje će se u mreži pohraniti dokument i autentifikacija dokumenta kada se on prenese. Korisnik koji želi pristupiti dokumentu šalje upit za preuzimanje ili za usmjereno pretraživanje dubokim webom s povratnim praćenjem. Kada zahtjev pronađe čvor koji sadrži kopiju dokumenta, cijeli se dokument vraća putem pretraživanja. Freenet čvorovi ne jamče postojanost dokumenata, ali ih zadržavaju pomoću algoritma koji uklanja dokumente slučajnim odabirom kada se poslužitelj čvora preplavi.<sup>41</sup>

Prednosti Freeneta su što se umetnuti podaci prenose preko velikog broja hostova, svaki čvor pridonosi brzini preuzimanja, ne dopušta da se brzina korisnikovog preglednika uspori te omogućuje brzo preuzimanje velikih datoteka. Nedostaci su što ne dopušta korisniku da obavlja

---

<sup>39</sup> Usp. I2P Anonymous Network. URL : <https://geti2p.net/en/> (2021-06-04)

<sup>40</sup> Usp. Kaur, Shubhdeep; Randhawa, Sukhchandan. Nav. dj., str. 2139.

<sup>41</sup> Usp. Clarke, Ian. [et al.]. Private Communication Through a Network of Trusted Connections: The Dark Freenet. URL : <https://freenetproject.org/papers/freenet-0.7.5-paper.pdf> (2021-06-08)

velike računalne aktivnosti poput igranja igrica u stvarnom vremenu, loše postupaju sa zainteresiranim stranama, ne postoji fiksna veličina skladišnog prostora stoga ne garantira trajno spremanje datoteka te nema vlastiti sustav pretraživanja.<sup>42</sup>

#### 4.2.2. Sadržaj mračnog weba

Mračni web nudi određenu razinu anonimnosti zbog čega su ljudi skloniji baviti se ilegalnim aktivnostima. Najzastupljenije ilegalne aktivnosti su trgovina drogom, trgovina oružjem, krađa dokumenata, pornografija, pedofilija, naručivanje ubojstva i nasilja. Najbrojniji proizvodi na mračnom webu su farmaceutski lijekovi i rekreativne droge, a slijede ih ukradeni i krivotvoreni dokumenti poput osobnih iskaznica, kreditnih kartica, vjerodajnica i putovnica. Neke web stranice nude usluge hakiranja i tehnološkog kriminala, uključujući zlonamjerni softver i iznajmljivanje osoba za hakiranje.<sup>43</sup>

Jedna od najčešćih aktivnosti mračnog weba je zasigurno prodaja i kupnja ilegalnih droga. Dostupnost ilegalnih droga razlikuje se od stranice do stranice. Neke web stranice prodaju sve, od kanabisa koji je u nekim zemljama legaliziran do psihodelika, kokaina i drugih težih droga. Jedna od najpoznatijih web stranica za prodaju i kupnju droge je *Grams* koja omogućuje ljudima da lako pretražuju i indeksiraju stranice mračnog weba koje se bave ilegalnim drogama.<sup>44</sup>

Nadalje postoji trgovina oružja, odnosno platforme za ilegalno trgovanje oružja. Prema istraživanju tvrtke RAND, mračni web zaista povećava dostupnost oružja po sličnim cijenama kao što su one dostupne na ulicama crnih tržišta. Također je utvrđeno da je Europa najveći izvor oružja. Danska je dio ovog mračnog tržišta s najvećim udjelom prodavača oružja od 12.98%, a nakon nje slijedi Njemačka s udjelom od 5,31%.<sup>45</sup>

Slijedeća stvar koja se može pronaći na mračnom webu su ukradeni računi te ukradene osobne iskaznice i putovnice za prodaju. Što se tiče ukradenih računa, mogu se pronaći brojevi kreditnih kartica, bankovnih računa, ali i ponude poput ukradenih vjerodajnica za PayPal račun.<sup>46</sup> Na mračnom webu postoji prilično puno web stranica koje prodaju osobne iskaznice i putovnice po različitim cijenama, ovisno o zemlji i prodavaču. Njihovu je valjanost teško

---

<sup>42</sup> Usp. Kaur, Shubhdeep; Randhawa, Sukhchandan. Nav. dj., str. 2138.

<sup>43</sup> Usp. Kumar, Aditi; Rosenbach, Eric. The Truth About The Dark Web. // Finance and Development, (2019), str. 22-24. URL : <https://www.imf.org/external/pubs/ft/fandd/2019/09/pdf/the-truth-about-the-dark-web-kumar.pdf> (2021-06-03)

<sup>44</sup> Usp. Ciancaglini, Vincenzo..[et al.]. Nav. dj.

<sup>45</sup> Usp. Kaur, Shubhdeep; Randhawa, Sukhchandan. Nav. dj., str. 2143.

<sup>46</sup> Usp. Ciancaglini, Vincenzo..[et al.]. Nav. dj.

provjeriti bez stvarne kupnje robe, pogotovo u slučaju državljanstva.<sup>47</sup> Od dokumenata se još mogu pronaći vladini službeni dokumenti i podaci poznatih osoba.

Na mračnom webu se odvija i trgovina ljudima, a jedno od takvih mjesta je *Black Death*. Zbog mračnog weba se trgovina ljudima zakopala dublje u tajnost, ali i zbog čestog mijenjanja URL-ova. Većina ljudi koji su preživjeli trgovinu ljudima regrutirana je za trgovinu seksa i trgovinu radnom snagom. Jedna od žrtava bila je Chloe Ayling, britanski model koju su oteli 2017. godine u Milanu gdje je došla na lažno fotografiranje.<sup>48</sup>

Dječja pornografija je također vrlo česta na mračnom webu. Najpoznatije web mjesto koje sadrži dječju pornografiju je *Lolita City* koje je ugašeno. Sadržavalo je preko 100 GB fotografija i videozapisa dječje pornografije te je brojilo preko 1500 članova.<sup>49</sup> 2015. godine FBI je proveo istragu na mračnom webu gdje je pronašao web mjesto s dječjom pornografijom poznatom kao *Playpen* koje je imalo gotovo 215 000 članova. Iste godine sudac Okružnog suda u Virginiji odobrava nalog za pretres kako bi policija, koristeći se posebnim istražnim tehnikama, pokušala identificirati stvarne IP adrese računala koja se koriste za pristup Playpenu. FBI je uspio otkriti oko 1300 IP adresa te pronaći pojedince protiv kojih je podnesena kaznena prijava.<sup>50</sup>

Ono što je još zabrinjavajuće na mračnom webu je usluga ubojstva, a takvih je nekoliko web mjesta. Glavno obilježje usluge je vrlo tajna priroda njihovog poslovanja. Njihovi ugovori su privatni te ne mogu ponuditi dokaz o prošlom radu ili uspjesima, čak ni povratne informacije od prethodnih klijenata. Od korisnika traže da unaprijed dokažu da imaju dovoljno bitcoina za uslugu, ali će se naplatiti tek kada je usluga izvršena i pruženi su dokazi o tome. Cijene se razlikuju ovisno o načinu smrti ili ozljede te statusu osobe. Jedna od web stranica zove se *C'thulu* na kojoj se može vidjeti detaljan popis usluga. Također postoji i web stranica *Dead Pool* koja nudi "atentat na gomilu" te omogućuje korisnicima postavljanje potencijalnih ciljeva. Osobe koje vrše ubojstvo mogu anonimno predvidjeti kada će i kako umrijeti ciljana osoba. Ako osoba stvarno umre, otkrivaju se sva predviđanja i oni koji su pogodili mogu tražiti novac.<sup>51</sup>

---

<sup>47</sup> Usp. Isto.

<sup>48</sup> Usp. Kaur, Shubhdeep; Randhawa, Sukhchandan. Nav. dj., str. 2141.

<sup>49</sup> Usp. Isto., str. 2142.

<sup>50</sup> Usp. Finklea, Kristin. Dark Web, 2017. URL :

[https://digital.library.unt.edu/ark:/67531/metadc700882/m1/1/high\\_res\\_d/R44101\\_2015Jul07.pdf](https://digital.library.unt.edu/ark:/67531/metadc700882/m1/1/high_res_d/R44101_2015Jul07.pdf) (2021-06-07)

<sup>51</sup> Usp. Ciancaglini, Vincenzo.[et al.]. Nav. dj., str. 33.

### 4.2.3. Mračni web i kriptovalute

Novčane transakcije na mračnom webu vrše se putem kriptovaluta kao što su bitcoin, monero, ethereum, dash i litcoin. Dugo je vremena bitcoin glavnom kriptovalutom kojom se plaćaju usluge i proizvodi na mračnom webu. I danas je bitcoin valuta koja se često koristi u transakcijama na mračnom webu. To je decentralizirana digitalna valuta koja koristi anonimne *peer-to-peer* transakcije. Bitcoin služi za plaćanje, mijenjajući tradicionalnu valutu, ili za rudarenje. Kada se bitcoin koristi u transakciji, transakcija se evidentira u blockchainu. Podaci zabilježeni u blockchainu su bitcoin adrese pošiljatelja i primatelja te adresa identificira određenu transakciju. Adrese korisnika povezane su i pohranjene u tzv. novčaniku koji sadrži privatni ključ pojedinca, a to je tajni broj sličan lozinci koji omogućuje osobi potrošnju bitcoina iz odgovarajućeg novčanika. Adresa za transakciju i kriptografski potpis koriste se za provjeru transakcija. Novčanici mogu biti hostirani na web ili mobilnoj aplikaciji.<sup>52</sup> Povezivanje mračnog weba s kriptovalutama dovelo je do porasta kriminala, a time i do širenja negativne percepcije kriptovalute. Naime, 2009. godine još uvijek nepoznati stručnjak za kriptografiju koristeći se pseudonimom Satoshi Nakamoto razvio je prvu svjetsku mrežu za valute i plaćanja koja nije pod nadzorom nacionalne vlade i to je bio upravo bitcoin. 2011. godine bitcoin se pojavljuje kao valuta za prodavače i kupce droga na mračnom webu, a prva web stranica na kojoj se pojavljuje je *Silk Road*.<sup>53</sup> Izvješće vodeće analitičke tvrtke za kripto-plaćanja *Chainalysis* pokazalo je da su bitcoin transakcije na mračnom webu 2012. godine porasle otprilike s 250 milijuna na 872 milijuna američkih dolara u 2018. godini. Izvješće je također pokazalo da je udio bitcoin transakcija povezanih s ilegalnim poslovima pao za 6% od 2012. godine te čini manje od 1% svih aktivnosti bitcoina.<sup>54</sup>

### 4.3. (Ne)indeksiranost sadržaja i pristup mračnom webu

Stranice na mračnom webu su skrivene i ne može im se pristupiti bez posebnog softvera, preglednika i tražilice. Alati za pretraživanje tražilice nisu u mogućnosti indeksirati web stranice mračnog weba. Glavna karakteristika mračnog weba je da korisnici usluge ostaju anonimni, odnosno da niti davatelj web mjesta ne može identificirati posjetitelje, niti posjetitelj može identificirati pružatelja usluge, a takve usluge se nazivaju skrivenim uslugama.<sup>55</sup>

---

<sup>52</sup> Usp. Finklea, Kristin. Nav. dj.

<sup>53</sup> Usp. Kumar, Aditi; Rosenbach, Eric. Nav. dj., str. 23.

<sup>54</sup> Usp. Isto., str. 24.

<sup>55</sup> Usp. Koch, Robert. *Hidden in the Shadow: The Dark Web – A Growing Risk for Military Operations?*, 2019. URL : [https://www.researchgate.net/publication/333507885\\_Hidden\\_in\\_the\\_Shadow\\_The\\_Dark\\_Web\\_-\\_A\\_Growing\\_Risk\\_for\\_Military\\_Operations](https://www.researchgate.net/publication/333507885_Hidden_in_the_Shadow_The_Dark_Web_-_A_Growing_Risk_for_Military_Operations) (2021-06-07)



### 4.3.1. Tražilice mračnog weba

#### 4.3.1.1. Ahmia

Ahmia je tražilica mračnog weba koja pretražuje skrivene usluge na mreži Tor. Podijeljena je na tri dijela. Prvi dio je indeks koji se odnosi na podatke koje je Ahmia prikupila te za održavanje tih podataka koristi *Elasticsearch*. Drugi dio su alati za indeksiranje koji indeksiraju *.onion* stranice na Tor mreži, a jedan od alata je *Scrapy*. Treći dio je web mjesto koje je temeljna odrednica Ahmije te uključuje dizajn web stranice i čini tražilicu ispravnom. Ahmia prikuplja popis poznatih *.onion* stranica, informacije o njima i sprema ih u svoju bazu podataka. Prikupljeni podaci filtriraju se radi uklanjanja sadržaja kao što je zlostavljanje djece, odnosno ima svoju crnu listu. Nakon što se podaci filtriraju, dostupni su za pretraživanje na Ahmia. Ahmia koristi *robots.txt* standard, odnosno pomoću tog standarda može spriječiti indeksiranje web stranice tako da se stranica ne prikazuje u rezultatima pretraživanja. S druge strane, stranica se i dalje prikazuje na popisu svih poznatih skrivenih usluga koje su na mreži.<sup>56</sup>

#### 4.3.1.2. Torch

Torch ili TorSearch je tražilica za skriveni dio interneta te je ujedno i najstarija tražilica na Toru. Torch ima preko milijardu indeksiranih web stranica na mračnom webu. Ne cenzurira rezultate pretraživanja niti prati što korisnik pretražuje. Ne sprema prijave i objave tako da nema zapisa o korisnikovim pretraživanjima. Također ne koristi nijedan kôd za praćenje ili analitiku radi privatnosti. Torch koristi *.onion* stranice, stoga je potrebno instalirati Tor preglednik. Preglednik je dostupan na Windowsima, Macu, Linuxu i Androidu.<sup>57</sup>

#### 4.3.1.3. Candle

Candle je tražilica mračnog weba izgrađena na Bing Search API-ju. Vodi se trima načelima - transparentnost, stručnost i privatnost. Uključuje ocjene kvalitete za vijesti, političke i medicinske izvore informacija. Rezultati pretraživanja temelje se na Bingu i NewsAPI-ju za pokrivanje vijesti u stvarnom vremenu. Candle koristi dva pokazatelja evaluacije rezultata pretraživanja, a to su pouzdanost i neutralnost. Pouzdanost pokazuje jesu li uzorci nezavisnih izvora za provjeru činjenica i naša vlastita procjena otkrili bilo kakve probleme s

---

<sup>56</sup> Usp. Ahmia - Search Tor Hidden Services. URL : <https://ahmia.fi/> (2021-06-03)

<sup>57</sup> Usp. Torch Search - Search The Dark Net. URL : <https://torchsearch.wordpress.com/> (2021-06-03)



vjerodostojnošću izvora. Neutralnost pokazuje nagovora li vijest čitatelja na određeni stav ili na neki drugi način zauzima jasan stav koji djeluje na sadržaj. Primjerice, politička povezanost, zagovaranje i komercijalni programi su stavovi koji mogu utjecati na ocjenu neutralnosti. Beta verzija ove tražilice postupno uvodi detaljnije načine promatranja evaluacije koji dovodi do rezultata pouzdanosti i neutralnosti, a primjeri takvih čimbenika su namjera, asertivnost, zauzimanje stavova i sl. Tijekom beta verzije procjene kvalitete temelje se na meta analizi više izvora nezavisnih proizvođača kao što su Allsides, Snopes, Poynter, Politifact i dr., te na provjeri činjenica o pristranosti medija i popisu pouzdanih izvora Wikipedije. Candle tražilica je povezana s *Amazon Associates*. Za analitiku web stranica koristi alat *Fathom* koji identificira ponovljene posjete unutar 24 sata pomoću anonimnih jednosmjernih hashova koji se ne mogu identificirati s pojedinačnim korisnikom, a nakon 24 sata su anonimni identifikatori uništeni.<sup>58</sup>

#### **4.4. Pozitivna strana mračnog weba**

Zbog anonimnosti koju pružaju Tor i drugi softveri poput I2P i Freeneta, mračni web koristi se za legalne i ilegalne aktivnosti. U legalne svrhe koristi se radi anticenzure i političkog aktivizma. Primjerice, u disidentskim pokretima u Iranu i Egiptu, Tor se koristi za zaštitu i anonimizaciju komunikacije i lokacija. Tor također koriste osobe koje žele pristupiti chat sobama i drugim forumima za osjetljivu komunikaciju, kako za osobnu tako i za poslovnu svrhu. Kao anonimne osobe mogu slobodno razgovarati o viktimizaciji ili tjelesnim i mentalnim bolestima. Također se može koristiti za zaštitu djece na mreži jer se prikriva IP adresa. Nadalje, neke tvrtke koriste mračni web kako bi zaštitile svoje projekte i spriječile špijune u stjecanju konkurentske prednosti. Novinari koriste Tor za komunikaciju i dijeljenje dokumenata.<sup>59</sup> Uporaba mračnog weba može donijeti koristi, ali to ne vrijedi samo za građane i tvrtke kojima je bitna privatnost na internetu već i za određene državne sektore, odnosno koristi se za provođenje zakona, vojnih i obavještajnih aktivnosti. Mračni web se koristi za provođenje zakona kako bi mogli pratiti zlonamjerne aktivnosti.<sup>60</sup> Isto tako se koristi i u vojnim i obavještajnim službama za zaštitu vojnih zapovjednih i kontrolnih sustava na terenu od identifikacije i hakiranja protivnika. Vojska može koristiti mračni web za proučavanje okruženja u kojem djeluje, kao i za otkrivanje aktivnosti koje predstavljaju operativni rizik za

---

<sup>58</sup> Usp. Candle | The search engine for critical minds. URL : <https://candle.to/> (2021-06-03)

<sup>59</sup> Usp. Finklea, Kristin. Nav. dj.

<sup>60</sup> Usp. Isto.

vojne jedinice. Mračni web omogućava da američko Ministarstvo obrane nadgleda sve aktivnosti terorističkih grupa kako bi ih spriječilo u njihovom djelovanju.<sup>61</sup>

2019. godine zabilježeno je preko 65 000 jedinstvenih URL-ova na Tor mreži koji završavaju s .onion. Tvrтка za računalnu sigurnost *Hyperion Gray* provela je istraživanje 2018. u kojem je katalogizirala oko 10% .onion stranica te otkrila da se najviše radi o forumima, chat sobama, hostovima datoteka te trgovinama. Istraživačka tvrtka *Terbium Labs* je 2016. godine provela istraživanje u kojem je nasumično odabrala 400 .onion stranica te su došli do zaključka da je više od polovine tih stranica zapravo legalno. Osobama koje žive u represivnim režimima koji blokiraju veliki dio interneta mračni web je spas koji pruža pristup informacijama i zaštitu od progona. U slobodnom društvu mračni web može biti mjesto koje štiti od odmazde ili osuđivanja na radnom mjestu ili u zajednici. Također omogućuje anonimnost i privatnost onima koji brinu prati li ih vlada. Danas mnoge organizacije, uključujući novinske kuće, Facebook, pa čak i američku Središnju obavještajnu agenciju (CIA), održavaju skrivenu web stranicu na Toru upravo zbog privatnosti.<sup>62</sup>

## 4.5. Primjeri stranica

### 4.5.1. Silk Road

*Silk Road* je jedno od najzloglasnijih mjesta koja su se nalazila na mračnom webu, a bio je globalno tržište za ilegalne usluge i krijumčarenje, uglavnom za drogu. Pokrenuo ga je Ross William Ulbricht u veljači 2011. godine koji je na mračnom webu bio poznat kao *Dread Pirate Roberts*. Prodavači ilegalnih supstanci nalazili su se u više od 10 zemalja diljem svijeta, a krijumčareni proizvodi i usluge pruženi su za 100 000 kupaca. Procjenjuje se da je *Silk Road* ostvario 1.2 milijarde američkih dolara prodaje u razdoblju od siječnja 2011. do rujna 2013. godine kada su federalni agenti zaplijenili market. U listopadu iste godine FBI je uhitio Ulbrichta, a u svibnju 2015. godine je osuđen na doživotni zatvor zbog pokretanja i upravljanja ilegalnim tržištem. Ulbricht je dobio preko 13 milijuna američkih dolara od prodaje Silk Rooda. Iako se *Silk Road* primarno koristio za prodaju ilegalnih droga, nudio je i digitalnu robu poput zlonamjernog softvera i piratskih medija, krivotvorine, uključujući lažne putovnice i kartice

---

<sup>61</sup> Usp. Isto.

<sup>62</sup> Usp. Kumar, Aditi; Rosenbach, Eric. Nav. dj., str. 22.

socijalnog osiguranja te usluge poput hakiranja računala.<sup>63</sup> Mjesec dana nakon Ulbrichtova uhićenja njegovi administratori otvaraju *Silk Road 2.0* koji je bio ugašen nakon godinu dana.<sup>64</sup>

#### 4.5.2. DarkMarket

*DarkMarket* je bilo najveće ilegalno tržište na mračnom webu te je na početku 2021. godine isključen iz mreže u međunarodnoj operaciji u kojoj su sudjelovale Njemačka, Danska, Ujedinjeno Kraljevstvo, Ukrajina, Moldavija, SAD i Australija. Europol je podržao uklanjanje *DarkMarketa* specijalističkom operativnom analizom te je koordinirao suradnike uključenim zemljama. *DarkMarket* je imao oko 500 000 članova, više od 2400 prodavača, 320 000 transakcija, 4650 bitcoina te 12 800 monero kriptovalute. Iznos koji su zaradili bio je veći od 140 milijuna eura. Prodavači na *DarkMarketu* su trgovali svim vrstama droga, prodavali krivotvoreni novac i podatke o kreditnim karticama, SIM karticama i zlonamjerni softver. Središnji odjel kriminalističkog istraživanja u Oldenburgu u Njemačkoj uhitio je australskog državljanina koji je navodni operater *DarkMarketa* u blizini njemačko-danske granice. Istraga koju je vodila jedinica za cyber kriminal javnog tužiteljstva u Koblenzu omogućila je službenicima da pronađu i zatvore *DarkMarket*, isključe web poslužitelje i zaplijene kriminalnu infrastrukturu koja je brojala više od 20 web poslužitelja u Moldaviji i Ukrajini.<sup>65</sup>

#### 4.5.3. AlphaBay i Hansa

*AlphaBay* i *Hansa*, nasljednici *Silk Rода*, su tržišta stvorena kako bi se olakšalo širenje podzemne kriminalne ekonomije. *AlphaBay* je bilo kriminalno tržište na mračnom webu, koristeći skrivenu uslugu na Tor mreži za učinkovito prikrivanje identiteta korisnika i lokacija web poslužitelja. Prije uklanjanja *AlphaBay* je dosegao preko 200 000 korisnika i 40 000 dobavljača. Na *AlphaBayu* je bilo preko 250 000 popisa ilegalnih droga i otrovnih kemikalija, a preko 100 000 popisa ukradenih i lažnih identifikacijskih dokumenata i uređaja za pristup, krivotvorene robe, zlonamjernog softvera i ostalih alata za hakiranje računala, vatrenog oružja i prijevara. Procjenjuje se da je tržište doseglo zaradu od milijardu američkih dolara od njegovog stvaranja 2014. godine. Transakcije su se plaćale u bitcoinima i drugim kriptovalutama. *Hansa* je bila treće najveće tržište kriminala na mračnom webu, nakon

---

<sup>63</sup> Usp. Finklea, Kristin. Nav. dj.

<sup>64</sup> Usp. Kumar, Aditi; Rosenbach, Eric. Nav. dj., str. 25.

<sup>65</sup> Usp. DarkMarket: world's largest illegal dark web marketplace taken down. URL : <https://www.europol.europa.eu/newsroom/news/darkmarket-worlds-largest-illegal-dark-web-marketplace-taken-down> (2021-06-07)

DarkMarketa i AlphaBaya, trgujući velikom količinom nedozvoljenih droga i druge robe. 2016. godine Europol je započeo istragu kako bi identificirao adrese te je u drugoj polovici 2017. godine došao do 10 000 adresa kupaca, a *Hansa* je bila zatvorena. U međuvremenu se pod vodstvom američkog FBI i DEA vodila operacija naziva *Bayonet* kako bi identificirali pokretača i administratora Alphabaya te su došli do kanadskog državljanina koji živi na Tajlandu. 2017. godine je uhićen, *AlphaBay* je uklonjen, a zarada od njega od milijun dolara je zaplijenjena.<sup>66</sup>

#### 4.5.4. DeepDotWeb

*DeepDotWeb* je bilo tržište za ilegalnu kupovinu opasnih droga, oružja i zlonamjernog softvera, a djelovalo je od 2013. do 2019. godine. Prema sudskim dokumentima, Tal Prihar, 37-godišnji izraelski državljanin s prebivalištem u Brazilu, posjedovao je i upravljao *DeepDotWebom* zajedno sa suokrivljenim Michaelom Phanom iz Izraela. Za pružanje usluga su Prihar i Phan primali povratne uplate, približno 8155 bitcoina što je otprilike 8.4 milijuna američkih dolara. Kako bi prikrrio prirodu i izvor ilegalnog plaćanja, Prihar je prebacio uplate iz svog *DeepDotWeb* bitcoin novčanika na druge bitcoin i bankovne račune. *DeepDotWeb* su zaplijenile savezne vlasti u travnju 2019. godine.<sup>67</sup>

## 5. Zaključak

Pojava interneta omogućila je globalnu povezanost, kao i pristup, prikupljanje, dijeljenje, slanje i organizaciju informacija. Zbog količine i dostupnosti informacija, internet se danas podijelio na površinski, duboki i mračni web. Mnogi korisnici pretražuju na površinskom webu koji se naziva još vidljivi web, ali im je dostupan samo dio sadržaja, dok se većina podataka krije u nevidljivom ili skrivenom webu, odnosno dubokom i mračnom webu kojem standardne tražilice poput Google-a ne mogu pristupiti. Duboki web se sastoji od raznih baza podataka, društvenih medija i intraneta, a još dublji sadržaj nalazi se na mračnom webu koji je zbog svoje anonimnosti i privatnosti sinonim za ilegalne aktivnosti. Duboki web posebno je koristan

---

<sup>66</sup> Usp. Massive blow to criminal dark web activities after globally coordinated operation. URL : <https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation> (2021-06-06)

<sup>67</sup> Usp. DeepDotWeb Administrator Pleads Guilty to Money Laundering Conspiracy. URL : <https://www.justice.gov/opa/pr/deepdotweb-administrator-pleads-guilty-money-laundering-conspiracy> (2021-06-07)

znanstvenoj i poslovnoj zajednici budući da sadrži informacije potrebne stručnjacima različitih profila. Iako sadrži mnoštvo informacija kojima se može pristupiti tako putem odgovarajućih stranica, servisa i sl., duboki se web za razliku od mračnog weba ne smatra ilegalnim i tamnim prostorom interneta. Mračni web je dio dubokog weba na kojem se mogu pronaći kriminalne radnje poput nasilja, pornografije, pedofilije, krivotvorina i ukradenih dokumenata, naručivanje ubojstava i sl. Ipak, mračni web ne koristi se samo u negativne svrhe. Ima i svoju pozitivnu stranu, a to je anonimna komunikacija korisnika o fizičkim i mentalnim bolestima, nudi roditeljima mogućnost da djeca mogu koristiti skriveni web kako bi izbjegla oglašavanje, nasilni i pornografski sadržaj, koriste ga i novinari, politički aktivisti i zviždači kako bi slobodno i sigurno, tj. anonimno mogli dijeliti informacije. Na mračnom webu se ponajviše koriste kriptovalute koje omogućuju novčane transakcije, tj. plaćanje usluga i proizvoda. Bitcoin je u početku bio najpopularnija i najkorištenija kriptovaluta na mračnom webu koji je djelomično i pridonijeo njegovoj popularnosti, no u posljednje se vrijeme sve više koriste i druge kriptovalute poput litcoina i dasha koje su se pokazale stabilnijima pa tako i jednostavnijima za korištenje. Zaključno, duboki i mračni web koristi sve veći broj korisnika. Internet prostranstvo dubokog i mračnog weba nudi puno više informacija i sadržaja nego površinski web omogućujući korisnicima da dođu do tražene i potrebne informacije, odnosno da ju podijele s ostatkom zajednice. Također, tražilice vidljivog weba, kao što je Google, konstantno prikupljaju osobne podatke i povijest pretraživanja što se korisnicima ne sviđa pa zbog zaštite privatnosti i osiguravanja anonimnosti često pribjegavaju tražilicama i preglednicima skrivenog weba.

## 6. Literatura

1. About OpenDOAR. URL : <https://v2.sherpa.ac.uk/opensoar/about.html> (2021-06-08)
2. Ahmia - Search Tor Hidden Services. URL : <https://ahmia.fi/> (2021-06-03)
3. Bergman, Michael K. White Paper: The Deep Web: Surfacing Hidden Value. // Journal of Electronic Publishing 7, 1(2001), str. 1-25.
4. Candle | The search engine for critical minds. URL : <https://candle.to/> (2021-06-03)
5. Ciancaglini, Vincenzo.[et al.]. Below the Surface : Exploring the Deep Web. Irving : Trend Micro, 2015.
6. Clarke, Ian.[et al.]. Private Communication Through a Network of Trusted Connections: The Dark Freenet. URL : <https://freenetproject.org/papers/freenet-0.7.5-paper.pdf> (2021-06-08)
7. Coffey, Mollie L. Library application of Deep Web and Dark Web technologies. // School of Information Student Research Journal 10, 1(2020), str. 2. URL : [https://www.researchgate.net/publication/344161017\\_Library\\_application\\_of\\_Deep\\_Web\\_and\\_Dark\\_Web\\_technologies](https://www.researchgate.net/publication/344161017_Library_application_of_Deep_Web_and_Dark_Web_technologies) (2021-06-03)
8. Cohen-Almagor, Raphael. Internet History. // International Journal of Technoethics 2, 2(2011), str. 45-64. URL : [https://www.researchgate.net/publication/215660523\\_Internet\\_History](https://www.researchgate.net/publication/215660523_Internet_History) (2021-06-05)
9. Čekerevac, Zoran; Dvorak, Zdenek; Čekerevac, Petar. Dali je “tamni internet” dubok i taman? // FBIM Transactions 4, 2(2016), str. 53-65.
10. DarkMarket: world’s largest illegal dark web marketplace taken down. URL : <https://www.europol.europa.eu/newsroom/news/darkmarket-worlds-largest-illegal-dark-web-marketplace-taken-down> (2021-06-07)
11. DeepDotWeb Administrator Pleads Guilty to Money Laundering Conspiracy. URL : <https://www.justice.gov/opa/pr/deepdotweb-administrator-pleads-guilty-money-laundering-conspiracy> (2021-06-07)
12. DuckDuckGo - Privacy, simplified. URL : <https://duckduckgo.com/> (2021-05-28)
13. Ehney, Ryan; Shorter, Jack D. Deep Web, Dark Web, Invisible Web and the Post Isis World. // Issues in Information Systems 17, 4(2016), str. 36-41. URL : [https://iacis.org/iis/2016/4\\_iis\\_2016\\_36-41.pdf](https://iacis.org/iis/2016/4_iis_2016_36-41.pdf) (2021-06-03)
14. Finklea, Kristin. Dark Web, 2017. URL : [https://digital.library.unt.edu/ark:/67531/metadc700882/m1/1/high\\_res\\_d/R44101\\_2015Jul07.pdf](https://digital.library.unt.edu/ark:/67531/metadc700882/m1/1/high_res_d/R44101_2015Jul07.pdf) (2021-06-07)

15. How Scirus Works. URL :  
[http://spvp.zesoi.fer.hr/seminari/white\\_papers/WhitePaper\\_Scirus.pdf](http://spvp.zesoi.fer.hr/seminari/white_papers/WhitePaper_Scirus.pdf) (2021-05-29)
16. I2P Anonymous Network. URL : <https://geti2p.net/en/> (2021-06-04)
17. Identity Information SEARCH & API for Professionals | Pipl. URL :  
<https://pipl.com/> (2021-05-28)
18. Internet. // Hrvatska enciklopedija. Leksikografski zavod Miroslav Krleža. URL :  
<http://www.enciklopedija.hr/Natuknica.aspx?ID=27653> (2021-05-03)
19. Intranet. // Hrvatska enciklopedija. Leksikografski zavod Miroslav Krleža. URL :  
<https://www.enciklopedija.hr/natuknica.aspx?id=68095> (2021-06-07)
20. Kaur, Shubhdeep; Randhawa, Sukhchandani. Dark Web : A Web of Crimes. // Wireless Personal Communications, 112(2020), str. 2131–2158. URL :  
[https://www.researchgate.net/publication/338878596\\_Dark\\_Web\\_A\\_Web\\_of\\_Crimes](https://www.researchgate.net/publication/338878596_Dark_Web_A_Web_of_Crimes)  
(2021-06-03)
21. Ko, Kyungmin; Lee, Heejin; Jangc, Seungkwon. The Internet dilemma and control policy: political and economic implications of the Internet in North Korea. // The Korean Journal of Defense Analysis 21, 3(2009), str. 279-285. URL :  
[https://www.researchgate.net/publication/233186994\\_The\\_Internet\\_dilemma\\_and\\_control\\_policy\\_political\\_and\\_economic\\_implications\\_of\\_the\\_Internet\\_in\\_North\\_Korea](https://www.researchgate.net/publication/233186994_The_Internet_dilemma_and_control_policy_political_and_economic_implications_of_the_Internet_in_North_Korea)  
(2021-06-07)
22. Koch, Robert. Hidden in the Shadow: The Dark Web – A Growing Risk for Military Operations?, 2019. URL :  
[https://www.researchgate.net/publication/333507885\\_Hidden\\_in\\_the\\_Shadow\\_The\\_Dark\\_Web\\_-\\_A\\_Growing\\_Risk\\_for\\_Military\\_Operations](https://www.researchgate.net/publication/333507885_Hidden_in_the_Shadow_The_Dark_Web_-_A_Growing_Risk_for_Military_Operations) (2021-06-07)
23. Kumar, Aditi; Rosenbach, Eric. The Truth About The Dark Web. // Finance and Development, (2019), str. 22-25. URL :  
<https://www.imf.org/external/pubs/ft/fandd/2019/09/pdf/the-truth-about-the-dark-web-kumar.pdf> (2021-06-03)
24. Massive blow to criminal dark web activities after globally coordinated operation. URL : <https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation> (2021-06-06)
25. Mwila, Kingston Ali. The Deep Web. URL :  
[https://www.researchgate.net/publication/335336010\\_The\\_Deep\\_Web](https://www.researchgate.net/publication/335336010_The_Deep_Web) (2021-05-28)
26. North Korea's Ruling Elite Are Not Isolated. URL :  
<https://go.recordedfuture.com/hubfs/north-korea-internet-activity.pdf> (2021-06-07)

27. OAIster : Catalog of open access resources. URL :  
<https://www.oclc.org/en/oaister.html> (2021-06-03)
28. P2P computer network. // Encyclopedia Britannica. URL :  
<https://www.britannica.com/technology/P2P> (2021-06-03)
29. Pederson, Steve. Understanding the Deep Web in 10 minutes.
30. Prasad M. R., Murali. Deep Web : Librarian's Perspective. // PEARL - A Journal of Library and Information Science 11, 4(2017), str. 418-423. URL :  
[https://www.researchgate.net/publication/321851210\\_Deep\\_Web\\_Librarian%27s\\_Perspective](https://www.researchgate.net/publication/321851210_Deep_Web_Librarian%27s_Perspective) (2021-06-03)
31. Tor Project | Anonymity Online. URL : <https://www.torproject.org/> (2021-06-03)
32. Torch Search - Search The Dark Net. URL : <https://torchsearch.wordpress.com/>  
(2021-06-03)
33. University of Leicester OER Repository. URL : <https://www2.le.ac.uk/projects/oer>  
(2021-06-08)
34. Yadav, Divya; Bhushan, Bharat; Saxena, Shivam. The Dark Web : A Dive Into the Darkest Side of the Internet. // SSRN Electronic Journal, (2020), str. 1-7. URL :  
[https://www.researchgate.net/publication/341420503\\_The\\_Dark\\_Web\\_A\\_Dive\\_Into\\_the\\_Darkest\\_Side\\_of\\_the\\_Internet](https://www.researchgate.net/publication/341420503_The_Dark_Web_A_Dive_Into_the_Darkest_Side_of_the_Internet) (2021-06-03)