Tampereen yliopisto

Jimi Niemi

TOR-VERKON HYÖDYNTÄMINEN YKSITYISYYDEN SUOJAAMISESSA

Informaatioteknologian ja viestinnän tiedekunta
Kandidaattitutkielma
Syyskuu 2023

TIIVISTELMÄ

Jimi Niemi: Tor-verkon hyödyntäminen yksityisyyden suojaamisessa
Kandidaattitutkielma
Tampereen yliopisto
Tietojenkäsittelytieteiden tutkinto-ohjelma
Syyskuu 2023

Dataa liikkuu enemmän verkossa kuin koskaan aiemmin ja ihmisten on yhä vaikeampaa pitää kiinni omasta yksityisyydestään verkossa. Tämän takia kysyntä käyttäjän yksityisyyttä suojaaville palveluille on kasvanut. Tor-verkko on yksi keino käyttäjälle suojata omaa yksityisyyttään verkossa. Tor-verkko on maailman suurin anonyymi verkko, jota ylläpitää TorProject ja vapaaehtoiset ympäri maailmaa. Tor on myös ilmainen ja sen lähdekoodi on avointa. Verkossa käyttäjistä kerätään dataa, mutta Tor-verkon avulla tätä dataa on paljon vaikeampi yhdistää itse käyttäjään. Tämä on yksi tavoista, joilla Tor kasvattaa käyttäjän anonymiteettiä ja suojaa käyttäjän yksityisyyttä.

Tämän tutkimuksen tarkoituksena oli olla informatiivinen katsaus Tor-verkkoon ja siihen, miten Tor-verkkoa voidaan hyödyntää yksityisyyden suojaamisessa käyttäjän näkökulmasta. Aineisto koostui pääosin tieteellisistä ja vertaisarvioiduista teksteistä viimeisen kymmenen vuoden ajalta. Työssä kerrotaan ensin Tor-verkon toiminnasta, sekä yksityisyyden perusasioista. Tämän jälkeen keskitytään Tor-verkon käyttöön ja käyttäjiin, jota seuraa osio Tor-verkon hyödyistä, uhkista sekä haavoittuvuuksista. Lopussa vielä pohdintaa ja yhteenveto saaduista tuloksista.

Tutkimuksen tulosten perusteella voidaan todeta, että Tor-verkosta on selkeää hyötyä käyttäjän yksityisyydelle. Lähteissä tuli usein esille, että Tor-verkollakin on haavoittuvuutensa mutta näitä haavoittuvuuksia vastaan hyökkäämiseen tarvittiin mahdollisuus tarkkailla ainakin osaa verkkoliikenteestä. Tor-verkon käyttäjämäärä on nousussa ja kun Tor-verkon suosio nousee niin myös sen antama suoja kasvaa, koska tällöin Tor-verkossa olevien solmujen määrä kasvaa. Solmujen määrän kasvaessa hyökkäyksille altistuneiden solmujen määrä verrattuna ehjiin solmuihin on pienempi. Tämän takia Tor-verkon antama suoja yksityisyydelle tulee vain kasvamaan tulevaisuudessa. Tor-verkko on hyödyllinen työkalu varsinkin maissa, joissa hallinto tai jokin muu taho pyrkii kontrolloimaan ihmisten internetin käyttöä.

Avainsanat: yksityisyys, Tor-verkko, anonymiteetti

SISÄLLYSLUETTELO

1 Johdanto

Nykypäivän maailma pyörii enemmän ja enemmän internetin ympärillä ja ihmisten huoli omasta yksityisyydestä internetissä on samalla kasvanut. Tämä on aiheuttanut kysynnän yksityisyyttä parantaville teknologioille kuten Tor-verkolle (Avdoshin & Lazarenko, 2016). Internetissä liikkuu enemmän dataa kuin koskaan aiemmin ja datan määrän kasvaessa myös oman yksityisyyden suojaamisesta on tullut entistä tärkeämpää, mutta samalla myös vaikeampaa yleistyvien tietomurtojen sekä lisääntyvän datan keräämisen vuoksi.

Yksi tavoista, joilla käyttäjä voi suojata omaa yksityisyyttään internetissä on Tor-verkko. Tor-verkon avulla käyttäjä voi vähentää datan määrää, jota hänestä kerätään verkossa. Tor:in kehitys alkoi USA:n laivaston tutkimuslaitoksessa vuonna 1995 (Harboth & Pape, 2020). Tor tulee sanoista The Onion Router ja projektia ylläpitää nykyään The Tor Project. Tor on onnistunut vakiinnuttamaan asemansa palveluna, joka mahdollistaa valtion valvonnan ja yritysten datan keräämisen kiertämisen (Brandl ym., 2019).

Tässä tutkielmassa tehdään kirjallisuuskatsaus siihen mitä hyötyä Tor-verkosta on käyttäjälle yksityisyyden näkökulmasta, mutta myös mitä haavoittuvuuksia ja riskejä Tor-verkon käyttöön liittyy. Keskityn tutkielmassa peruskäyttäjiin.

Tutkielman tavoitteena on olla informatiivinen katsaus siihen mitä hyötyä Tor-verkon käytöstä on yksittäiselle käyttäjälle. Työ pyrkii tähän kertomalla mitä uhkia käyttäjän yksityisyydelle on verkossa ja osoittamalla, miten käyttäjä voi hyödyntää Tor-verkkoa näiden uhkien minimoimiseen. Tutkielmassa on myös osio Tor:in uhkista ja haavoittuvuuksista, jonka avulla pyritään osoittamaan, että Tor ei kuitenkaan ole täysin aukoton ratkaisu ongelmaan.

Tutkimus koostuu tutkimusmenetelmästä luvussa 2, jonka jälkeen käydään läpi keskeiset asiat Tor:ista ja yksityisyydestä luvussa 3. Luvussa 4 käydään tarkemmin läpi Tor-verkon käyttöä, mikä vaikuttaa siihen alkaako henkilö käyttämään Tor-verkkoa sekä missä päin maailmaa Tor-verkkoa käytetään ja miksi. Luvussa 5 punnitaan Tor-verkon hyötyjä ja riskejä. Luvussa 6 pyrin kokoamaan mitä hyötyä Tor-verkosta on yksityisyyden näkökulmasta käyttäjälle. Luvussa 7 pyrin tiivistämään tutkielman tärkeimmät asiat ja löydetyt tulokset.

2 Tutkimusmenetelmä

Kirjallisuuden etsimisessä käyttämäni tietokannat olivat ACM, IEEE ja SpringerLink. Käytin myös aluksi Andoria, mutta totesin melko nopeasti, että löydän muista tietokannoista haluamani lähteet helpommin. Suurimman osan kirjallisuudesta löysin kuitenkin ACM:n avulla. Suodatin tuloksia 2010 vuodesta eteenpäin, mutta käytin myös yhtä lähdettä vuodelta 2004. Kyseinen lähde oli lähteenä useassa muussa tutkimuksessa ja oli hyödyllinen Tor:in historian ja perustoiminnan selittämiseen. Yhtenä lähteenä käytin myös Tor Projectin omaa ”Tor Metrics”-sivustoa. Sivustolta löysin hyviä tilastoja Tor-verkon käyttäjämäärän kehitykseen, sekä käyttäjiin eri osissa maapalloa ja siihen mitkä asiat ovat johtaneet käyttäjämäärän nopeisiin muutoksiin tietyissä maissa.

Tor on julkaistu 2002, joten suurin osa kirjallisuudesta aiheeseen liittyen sijoittuu noin viimeisen 20 vuoden ajalle. Hakusanoina käytin pääasiallisesti sanoja Tor, Onion, privacy ja anonymity. Hakulausekkeeni olivat yleensä muotoa ”Tor OR onion AND privacy OR anonymity”, jolla pyrin saamaan tuloksia sellaisista tutkimuksista, joissa puhuttiin yksityisyydestä juuri Tor:in tapauksessa. Välillä käytin myös hakusanoja kuten vulnerability tai attack, kun halusin löytää tietoa esimerkiksi juuri Tor:in haavoittuvuuksista ja millaiset hyökkäykset toimivat Tor-verkossa.

Valitsin tuloksista ensin otsikon perusteella ne, jotka voisivat parhaiten sopia aiheeseeni ja tämän jälkeen karsin niitä tiivistelmän avulla. Viimeisen karsimisen tein lukemalla siitä, mikä tutkimuksen tarkoituksena on ollut, miten on tutkittu ja mitä tuloksia on saatu. Jos oli useampi lähde, jotka liittyivät samaan asiaan, pyrin lukemaan kyseiset lähteet tarkemmin ja näin päättämään kumpi lähteistä on parempi juuri omaan tutkielmaani. Lähteideni kielenä oli englanti, koska käytin hakusanoina englanninkielisiä sanoja. Päätin hakea lähteitä englanniksi, koska ajattelin että suurin osa tutkimuksista on todennäköisesti englanniksi.

3 Tor ja yksityisyys

Tässä luvussa esitellään Tor:in toimintaa, sekä yksityisyyden liittyvät keskeiset asiat. Käydään läpi Tor:in perustoimintaa ja miksi yksityisyys on tärkeää, sekä mitä uhkia nykymaailmassa on yksityisyyden näkökulmasta

3.1 Tor

Tor-verkko on suurin anonyymi verkko koko maailmassa ja sillä on miljoonia päivittäisiä käyttäjiä (Ahmad & Licciardi, 2020). Tor mahdollistaa ilmaiseksi anonyymin kommunikoinnin pienellä viiveellä, toimii normaalissa internetissä ja tarjoaa kohtuullisen tasapainon anonymiteetin, käytettävyyden ja tehokkuuden välillä. Tor-verkon käytön ilmaisuus sekä toiminen usealla eri alustalla tekevät siitä helposti saavutettavan. (Winkler & Zeadally, 2015.) Tor:in päätavoitteena on vaikeuttaa datan yhdistämistä käyttäjään, mutta samalla sen tavoitteena on myös olla helposti käytettävä, joustava ja yksinkertainen (Dingledine ym., 2004).

Päätavoitteeseen se pyrkii muun muassa sipulireitityksen avulla. Sipulireitityksessä käyttäjän data kulkee solmujen (engl. Node) läpi. Tor-verkossa käyttäjä toimii käyttäjäsolmuna (engl. Client node), joka käyttää Tor-verkkoa anonyymiin kommunikaatioon. Käyttäjän data kulkee kolmen satunnaisesti valitun solmun läpi, jotka valitaan hakemistopalvelimen (engl. Directory server) antamasta listasta. Käyttäjän data kulkee ensin sisääntulosolmulle (engl. Entry node), joka lähettää sen eteenpäin välisolmuille (engl. Middle node). Sisääntulosolmun tulee olla vakaa ja sillä tulee olla iso kaistanleveys. Reititysketjun päässä on ulosmenosolmu (engl. Exit node), joka lähettää datan itse kohdepalvelimelle. Koska data tulee palvelimelle ulosmenosolmulta, ei palvelin saa käyttäjän IP-osoitetta ja käyttäjä pysyy näin anonyyminä. (Koizumi & Yoshiura, 2020.) Data kulkee reititysketjun sisällä salattuna ja kiinteän kokoisina paketteina. Reititysketjussa kulkevien pakettien salausta puretaan jokaisella solmulla kerros kerrokselta. Jokainen solmu Tor-verkossa toimii sipulireitittimenä ja solmujen välillä on TLS-yhteys. Jokaisella solmulla on tunnistusavain, jota käytetään TLS-varmenteiden allekirjoittamiseen ja salauksen purkamiseen. (Dingledine ym., 2004.) Tor-verkossa olevat solmut tietävät edeltävän ja seuraavan solmun, mutta eivät tiedä missä kohti reititysketjua ne sijaitsevat. Solmuja ylläpitää tuhannet vapaaehtoiset ja solmut voivat olla osana monta reititysketjua yhtä aikaa, sekä olla myös eri rooleissa eri ketjuissa. (Koizumi & Yoshiura, 2020).

Yksi syy miksi Tor-verkko on vakiinnuttanut asemansa palveluna, joka mahdollistaa valtion valvonnan ja yritysten datan keräämisen kiertämisen on sipulipalvelut (engl. Onion service). Sipulipalvelut ovat Tor-verkon verkkopalveluita, joita voi käyttää sekä ylläpitää anonyymisti ja joilla on useita eri käyttökohteita. Esimerkiksi The New York Times ja The Guardian ovat käyttäneet sipulipalveluita kommunikoidessa pilliin puhaltajien (engl. Whistleblower) kanssa, kun taas toiset kiertävät sen avulla sensuuria. Sipulipalvelut tunnetaan myös piilopalveluina (engl. Hidden service). (Steinebach ym., 2019.) Piilopalvelut pyörivät piilopalvelimilla (engl. Hidden server), jotka generoivat julkisia ja yksityisiä avaimia, joiden avulla käyttäjä voi yhdistää palvelimiin. Piilopalveluilla on sipuliosoitteet (engl. Onion address). Sipuliosoite koostuu 16 merkin mittaisesta merkkijonosta, jossa voi olla sekä numeroita että kirjaimia ja niiden pääte on .onion. Käyttäjät yhdistävät piilopalveluihin sipuliosotteiden avulla ja ne toimivat ainoastaan Tor-verkossa. (Koizumi & Yoshiura, 2020.)

Tor-verkon monikerroksinen salaus ja IP:n suojaaminen lähetetyn datan määränpäässä tekevät siitä vahvemman suojan käyttäjälle kuin Proxy tai VPN. Vaikka Tor-verkko antaa vahvan suojan käyttäjälleen ei se kuitenkaan pysty suojaamaan käyttäjiä, jotka antavat henkilökohtaisia tietojaan esimerkiksi tietojenkalaasteluhuijauksille (engl. Phishing scheme) (Hoang & Pishva, 2014.)

3.2 Yksityisyys

Yksityisyys verkossa määritellään yleensä sillä, kuinka tunnistettavissa käyttäjän henkilöllisyys on muille käyttäjille (Winkler & Zeadally, 2015). Ihmiset pitävät yksityisyyttä oikeutena ja ihmisten käyttäytyminen muuttuu, kun heitä tarkkaillaan tai vakoillaan, joka osoittaa kuinka tärkeä asia yksityisyys on (Rutherfoord & Rutherfoord, 2010).

Useat ihmiset ovat huolissaan yksityisyydestään, koska yksityisyyttä internetissä pidetään olennaisena osana sananvapautta. Tämän takia kysyntä yksityisyyttä parantavia teknologioita kohtaan on kasvanut. (Avdoshin & Lazarenko, 2016.) Uudet tietosuoja-asetukset kuten GDPR ja palvelut kuten DuckDuckGo parantavat yksilön tietosuojaa ja kontrollia omasta datasta. Samalla kun tietosuojaa parantavien palveluiden määrä on kasvanut myös palveluiden kuten Tor:in ja DuckDuckGo:n käyttäjien määrä on kasvanut. (Steinebach ym., 2019.) GDPR:n avulla pyritään antamaan yksilölle enemmän mahdollisuuksia kontrolloida itsestä kerättyä dataa, joka voidaan yhdistää kyseiseen henkilöön. Yritykset, jotka rikkovat GDPR:ää joutuvat maksamaan 4 % vuoden

liikevaihdosta tai 20 miljoonaa euroa. (Cha ym., 2019.) Internetissä yksityisyys ei ole kovinkaan suojattua, koska siellä liikkuva data sisältää lähettäjän ja vastaanottajan tietoja. Tämä mahdollistaa sen, että internet-palveluntarjoaja pystyy tunnistamaan keitä lähettäjä ja vastaanottaja ovat. (Koizumi & Yoshiura, 2020.)

Tietosuojaan liittyvä tutkimus on noussut merkittävämmäksi kasvavan henkilötietojen keräämisen, sekä kasvavien tietomurtojen takia (Harboth & Pape, 2020). Yksi mahdollinen uhka yksityisyydelle tietojen keräämisen ja tietomurtojen takia on älykkäät sähköjärjestelmät. Älykkäät sähköjärjestelmät keräävät dataa siitä paljonko energiaa talous käyttää tiettyinä aikoina. Tämän avulla voidaan päätellä esimerkiksi, milloin ihmiset ovat yleensä paikalla, jota rikolliset voivat käyttää hyödykseen, jos tämä dataa vuotaa tietomurron yhteydessä. (Cha ym., 2019.)

Myös urheilu- ja älykellot ovat yleistyneet viime vuosina. Nämä kellot keräävät sijainti- ja terveystietoja, kuten dataa nukkumisesta ja sykkeestä. Tilanteessa, jossa tämä dataa vuotaa voi jokin kolmas osapuoli käyttää vuotanutta dataa päätelläkseen missä henkilö liikkuu ja milloin hän nukkuu. Tämänkaltaisten uhkien takia oman yksityisyyden suojaaminen on entistäkin tärkeämpää. (Cha ym., 2019.)

Yksityisyyttä verkossa vastustetaan pääasiassa sen takia, että ihmisiä on silloin vaikeampi saada vastuuseen teoistaan. Yksityisyys vaikeuttaa jäljitettävyyttä, joka mahdollistaa rikollisen toiminnan ja vaikeuttaa rikollisten kiinnisaantia. Toisaalta yksityisyys tuo myös suojaa esimerkiksi pilliin puhaltajille. Teknologiat kuten Tor ja VPN, jotka mahdollistavat anonymiteetin verkossa perustuvat käyttäjän IP-Osoitteen piilottamiseen. (Winkler & Zeadally, 2015.)

4 Tor-verkon käyttö

Tässä luvussa kerrotaan tarkemmin, miten Tor-verkkoa käytetään. Käsitellään asioita kuten Tor-selain, millaista Tor-verkon käyttö on, sekä mitkä asiat vaikuttavat siihen käyttääkö käyttäjä Tor-verkkoa. Lopussa myös Tor-verkon käyttäjämäärän kasvusta, sekä siitä missä maissa Tor-verkkoa käytetään ja miksi.

4.1 Miten Tor-verkkoa käytetään

Jotta käyttäjä voi yhdistää Tor-verkkoon tulee käyttäjällä olla ladattuna Tor-klientti (engl. Tor-client), joista tunnetuin on TorBrowser. TorBrowser on muokattu versio Mozilla Firefoxista, jossa on Tor-ohjelmistot sisäänrakennettuna. TorBrowserin avulla käyttäjä pystyy rakentamaan reititysketjun Tor-verkossa kuten luvussa 3.1 kerrottiin. (Avdoshin & Lazarenko, 2016.)

Tor:in käyttökokemusta voi myös parantaa käyttämällä ohjelmia kuten Vidalia. Vidalia on työkalu, jonka avulla Tor-käyttäjä voi vaihtaa pakettiensa reittiä ja näin parantaa omaa yksityisyyttään. Tämä erottaa Tor:in VPN:stä, jossa käyttäjä ei pysty vaihtamaan omaa IP-osoitettaan yhtä usein. Tor on myös ilmainen, kun taas VPN-ohjelmat ovat yleensä maksullisia täysversioina. Ilmaisuus onkin yksi syy Tor-verkon suosioon. Vaikka Tor onkin ilmainen ei se heikennä sen korkeaa tietoturvaa, koska ilmaisuus tuo lisää käyttäjiä ja mitä enemmän käyttäjiä Tor-verkossa on sitä enemmän on myös reititysvaihtoehtoja, joka kasvattaa käyttäjän suojaa. (Hoang & Phisva, 2014.)

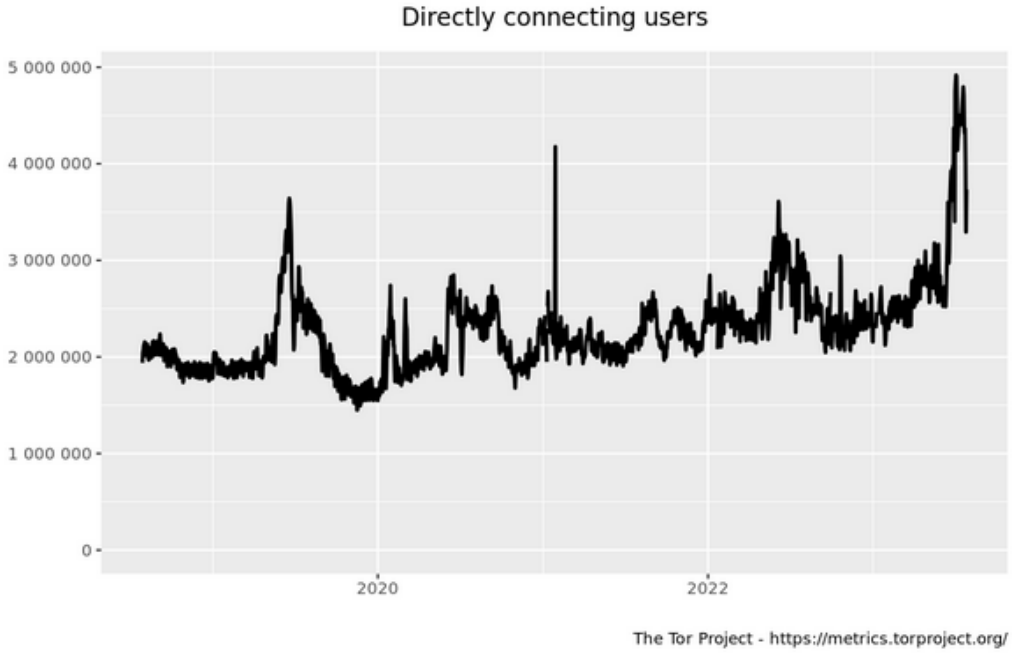
Harboth ja Pape tutkivat 2020 tutkimuksessaan ” How Privacy Concerns, Trust and Risk Beliefs, and Privacy Literacy Influence Users’ Intentions to Use Privacy-Enhancing Technologies—The Case of Tor” mitkä asiat vaikuttavat siihen alkaako käyttäjä käyttämään tietosuojaa parantavia palveluita. Tutkimuksessa tietosuojaa parantava palvelu oli Tor. Tutkimuksessa huomattiin, että käyttäjän luottamuksella palvelua kohtaan on suuri merkitys siihen alkaako käyttäjä hyödyntämään sitä. Tämän takia yhtiöiden kuten The Tor Project kannattaa panostaa siihen kuinka luotettavana heitä pidetään. Tutkimuksessa huomattiin myös, että tietosuojahuolilla, sekä sillä kuinka paljon käyttäjä tietää tietosuojaan liittyvistä asioista on positiivinen vaikutus siihen alkavatko he käyttämään tietosuojaa parantavia palveluita kuten Tor:ia. (Harboth & Pape, 2020.)

Yksi Tor:in käyttämisen heikkouksista on sen korkea viive. Tutkimusten mukaan normaali käyttäjä jaksaa käyttää palvelua vielä 3 sekunnin viiveellä. Tästä korkeampi viive karkottaa käyttäjiä. Tor:in viive on noin 17 sekuntia, joka tutkimusten mukaan karkottaisi 88 % käyttäjistä. Vaikka Tor:illa on korkea viive verrattuna normaaliin, niin

muihin samankaltaisiin teknologioihin verrattaessa sen viive on itseasiassa matala. Esimerkiksi vastaavalla palvelulla, I2P:llä viive oli noin 103 sekuntia eli lähes 6-kertainen verrattuna Tor:iin. Korkea viive saattaa kuitenkin karkottaa uusia käyttäjiä, jotka haluavat käyttää Tor:ia vain normaaliin netin selaamiseen. (Winkler & Zeadally, 2015.)

Jotkin ihmiset käyttävät Tor-verkkoa hyödykseen hyökätessään palveluita kohtaan esimerkiksi spämmäämällä foorumeita, jonka vuoksi jotkin palvelujentarjoajat kohtelevat anonyymeistä palveluista yhdistäviä ihmisiä huonommin kuin muita käyttäjiä. Tor-verkosta yhdistävä käyttäjä voi joutua tekemään monta CAPTCHA:a tai ei edes kykene yhdistämään sivulle, koska Tor-verkosta yhdistävät käyttäjät on blokattu sivulta. (Ahmad & Licciardi, 2020.)

4.2 Tor-verkon käyttäjät



Kuva 1. Suoraan yhdistävät käyttäjät 5 vuoden ajalta (Metrics, 2023)

Kuvassa 1 nähdään luvussa 3 mainittu Tor-verkon käyttäjien määrän kasvu. Kuvaajassa on otettu huomioon ainoastaan suoraan yhdistävät käyttäjät, eikä siinä ole siltojen (engl. Bridge) kautta yhdistäviä käyttäjiä. Tor-verkossa sillat tarkoittavat palvelimia, jotka eivät ole julkisia. Siltojen avulla myös käyttäjät, joiden pääsy Tor-verkkoon on estetty voivat käyttää Tor-verkkoa. (Metrics, 2023.)

Country	Mean daily users
Iran	19973 (24.20 %)
Russia	19518 (23.65 %)
United States	9152 (11.09 %)
Germany	2573 (3.12 %)
China	2270 (2.75 %)
India	1714 (2.08 %)
United Kingdom	1659 (2.01 %)
Turkey	1442 (1.75 %)
France	1363 (1.65 %)
Belarus	1285 (1.56 %)

This table shows the top-10 countries by estimated number of clients connecting via bridges.

Kuva 2. Siltojen kautta yhdistävät käyttäjät viimeisen 5 vuoden ajalta (Metrics, 2023)

Kuvassa 2 näkyy kuinka lähes puolet siltojen kautta yhdistävistä käyttäjistä ovat joko Iranista tai Venäjältä. Venäjällä useat internet-palveluntarjoajat ovat pyrkineet estämään käyttäjien pääsyn Tor-verkkoon 2021 joulukuusta lähtien. Tämän takia siltojen avulla yhdistävien käyttäjien määrä on kasvanut. Tor-verkon käyttäjien määrä Iranissa kasvoi merkittävästi vuoden 2022 syyskuussa. (Metrics, 2023.) Iranin hallitus blokkasi useat sosiaaliset mediat ja esti ihmisten pääsyn internettiin osissa maata syyskuussa alkaneiden kapinoiden vuoksi. Ihmiset pyrkivät kiertämään sensuuria Tor-verkon avulla. Valtion omistamien palveluntarjoajien kautta useat autoritaariset hallinnot pystyvät sensuroimaan internetissä käytävää keskustelua tai sulkemaan internetin kokonaan. Iranin hallitus kontrolloi internetin käyttöä ja uutisia varsinkin poliittisesti arkoina aikoina. (Momen, 2023.)

5 Hyödyt ja riskit

Tässä luvussa kerrotaan Tor-verkon käyttämisen hyödyistä, sekä riskeistä. Käsitellään mitä hyötyjä Tor-verkosta on käyttäjän yksityisyydelle ja mitä vaaroja Tor-verkon käyttämiseen liittyy.

5.1 Tor-verkon hyödyt

Tor-verkon käytöllä on käyttäjälle useita hyötyjä, kuten jo tutkielmassa mainitut käyttäjän anonyymiys, sensuurin kiertäminen, sekä käyttäjästä kerätyn tiedon vähentäminen. Anonyymiys lisää käyttäjän yksityisyyttä ja koska data liikkuu salattuna ja suojattuna Tor-verkossa suojaa Tor käyttäjäänsä myös tietomurroilta. Kuten luvussa 3.2 mainittiin internetissä liikkuva data sisältää vastaanottajan ja lähettäjän tietoja, jolloin internet-palveluntarjoaja pystyy tunnistamaan heidät. Tor-verkko tarjoaa tähän ratkaisun, koska data liikkuu reititysketjun läpi ja ketjussa ainoastaan ulosmenosolmu kommunikoi internetin kanssa.

Kuten luvussa 4.2 käytiin läpi Tor-verkon hyöty korostuu maissa, joissa jokin taho kuten hallinto pyrkii sensuroimaan kansalaisten Internetin käyttöä. Tor-verkkoon voi yhdistää myös siltojen kautta esimerkiksi tilanteessa, jossa edellä mainittu taho blokkaisi ihmisten pääsyn Tor-verkon julkisiin palvelimiin.

Luvussa 3.1 ja 3.2 puhuttiin myös siitä, kuinka Tor-verkon tuoman suojan ansiosta pilliin puhaltajat uskaltavat kertoa tiedoistaan lehdille, kuten The New York Timesille tai The Guardianille. Näin eri tahojen tekemät väärinkäytökset saadaan tuotua julkisuuteen.

5.2 Uhat ja haavoittuvuudet

Vaikka Tor:in alkuperäinen tavoite oli olla tapa kiertää sensuuria vaikeuttamalla datan yhdistämistä yksittäiseen käyttäjään, on tämä tuonut palveluun myös rikollista toimintaa. Piilopalveluita käytetään rikolliseen toimintaan, joista tunnetuin esimerkki on todennäköisesti kauppapaikka ”Silk Road”, jossa myytiin mm. huumeita ja väärennettyjä passeja. Vaikka rikollisia, jotka myyvät näitä tuotteita saadaan kiinni, on itse sipulipalvelun omistajan kiinnisaaminen paljon vaikeampaa Tor:in antaman suojan takia. (Koizumi & Yoshiura, 2020.)

Käyttäjä voi hyödyntää Tor-verkkoa parantaakseen omaa yksityisyyttään, mutta myös Tor-verkossa voidaan tehdä erilaisia hyökkäyksiä, joiden avulla pyritään purkamaan käyttäjän anonymiteetti (engl. Deanonymization). Hyökkäykset voidaan jakaa passiivisiin ja aktiivisiin hyökkäyksiin. Passiivisissa hyökkäyksissä hyökkääjä tarkkailee

verkkoliikennettä, kun taas aktiivisessa hyökkäyksessä hyökkääjä muokkaa verkkoliikennettä. (Lazarenko & Avdoshin, 2016.) Avdoshin ja Lazarenko tutkivat vuonna 2016 tutkimuksessaan ”Anonymity of Tor: Myth and Reality” onko käyttäjän anonymiteetin purkaminen Tor-verkossa mahdollista pienilläkin resursseilla. Tutkimuksen tuloksena todettiin, että jos hyökkääjällä on tarpeeksi osaamista voi hän onnistua purkamaan käyttäjän anonymiteetin verkkosivun sormenjälkeä hyödyntäen. (Avdoshin & Lazarenko, 2016.) Tor pyrkii suojaamaan käyttäjää hyökkääjältä, joka pystyy seuraamaan tai kontrolloimaan osaa verkkoliikenteestä, mutta se ei pysty suojaamaan globaalilta viholliselta, joka pystyy seuraamaan kaikkia verkkoyhteyksiä (Harboth & Pape, 2020).

Vaikka tutkijat ovat huomanneet, että yksi Tor-verkon haavoittuvuuksista on tarkkailla sen ulosmenosolmua ei tämä ole suuri ongelma sen dynaamisen IP:n käytön vuoksi (Hoang & Phisva, 2014).

6 Keskustelu

Tutkielmassa käyttämissäni lähteissä korostui se, kuinka ihmisten yksityisyys ei ole kovinkaan hyvä verkossa ja siksi käyttäjien tulisi alkaa hyödyntämään enemmän yksityisyyttä parantavia palveluita kuten Tor-verkkoa. Lähteissä puhuttiin myös paljon siitä, kuinka paljon dataa nykypäivänä kerätään ja kuinka useat eri laitteet ovat nykyään yhteydessä verkkoon.

Toisaalta useissa lähteissä puhuttiin myös siitä, että näiden palveluiden käyttö on lisääntynyt viime vuosina. Kuten esimerkiksi DuckDuckGo:n, sekä Tor:in (Brandl ym., 2019). Tor:in käyttäjien lisääntyminen samalla kasvattaa sen tuomaa suojaa, koska palvelulle tulee uusia reititysvaihtoehtoja.

Tor-verkolla on omat uhkansa, mutta ne eivät ole kovinkaan vakavia. Vakavuus on matala, koska esimerkiksi vääränlaiselle sivulle päätyminen on usein vaikeaa ja se tuskin tapahtuu vahingossa. Hyökkäykset itse verkon sisällä tarvitsevat usein mahdollisuuden tarkkailla jotain osaa verkkoliikenteestä. Toisaalta anonymiteetti voidaan purkaa myös verkkosivun sormenjälkeä hyödyntämällä (Avdoshin & Lazarenko, 2016). Jos taas hyökkääjä voi tarkkailla koko verkkoliikennettä, ei Tor tällöin voi suojata käyttäjän anonymiteettiä. Tilanne, jossa hyökkääjä pääsee tarkkailemaan koko verkkoliikennettä, on kuitenkin epätodennäköinen, joten tämäkään riski ei ole kovin merkittävä.

Tor-verkon hyödyt ovat suuremmat kuin uhat, koska Tor-verkon avulla käyttäjä voi suojata omaa yksityisyyttään helposti verkkoa selatessaan. Tor-verkon käyttöönotto on yksinkertaista ja Tor-verkon käytössä tarvitsee ainoastaan hieman kärsivällisyyttä viiveen takia. Vaikka Tor:ista puhutaan pienen viiveen anonyyminä verkkona, on viive kuitenkin usein suurempi kuin normaalia verkkoa käyttäessä. Toisaalta verrattaessa muihin vastaaviin palveluihin on Tor:in viive huomattavasti pienempi. Yksi Tor-verkon suurimmista hyödyistä on myös yksi sen tavoitteista eli sensuurin kiertäminen. Maissa kuten Iranissa ja Venäjällä, joissa internet-palveluntarjoajat sekä hallinto pyrkivät sensuroimaan ja kontrolloimaan ihmisten internetin käyttöä, on Tor-verkko hyvä työkalu näiden esteiden kiertämiseen.

Tor-verkon avulla voidaan suojata omaa yksityisyyttään, koska Tor-verkko salaa käyttäjän IP-osoitteen, salaa kaiken datan, jota se lähettää ja lähettää datan samankokoisina paketteina, jolloin niitä on vaikeampi erottaa muista Tor-verkon käyttäjistä. Viime kädessä vastuu omasta anonymiteetistään on kuitenkin itse käyttäjällä ja mikään määrä palvelun antamaa suojaa ei voi suojata käyttäjää omilta teoiltaan.

7 Yhteenveto

Tässä tutkielmassa selvitettiin miten Tor-verkkoa voidaan hyödyntää yksityisyyden suojaamisessa. Tor-verkossa liikkuva data on aina suojattua ja kulkee solmujen läpi, jolloin data, jota käyttäjästä jää ei ole yhdistettävissä itse käyttäjään. Tämä parantaa yksityisyyttä, koska se tarjoaa käyttäjälle anonymiteetin. Vaikka anonymiteetti on purettavissa, tarjoaa Tor-verkko kuitenkin suojaa käyttäjälleen ja samalla myös hyvää suorituskykyä sekä käytettävyyttä.

Yksityisyys on nykymaailmassa ja varsinkin verkossa vaikea saavuttaa, vaikka ihmiset arvostavatkin omaa yksityisyyttään ja ovat alkaneet huolehtia siitä enemmän kuin aiemmin. Tämän näkee esimerkiksi palveluiden kuten DuckDuckGo ja Tor käyttäjien määrän nousussa. Uudet tietosuoja-asetukset kuten GDRP antavat ihmisille enemmän työkaluja siihen, miten heidän tietojansa käsitellään, kuitenkin samalla esimerkiksi älykellot ja kodin älykkäät sähkölaitteet ovat yleistyneet ja dataa kerätään enemmän kuin koskaan ennen.

Tor-verkko on ilmainen ja toimii usealla eri alustalla, joten kuka tahansa voi alkaa käyttämään sitä. Käytön aloittaminen on myös helppoa, koska TorBrowser eli selain, jolla Tor-verkkoa voi käyttää on muokattu versio Mozilla Firefoxista, joka on yksi käytetyimmistä verkkoselaimista ja näin myös useille tuttu. Vaikka Tor-verkkoa käyttämällä nettisivujen yhdistämiseen tulee lisää viivettä, on Tor kuitenkin huomattavasti nopeampi kuin vastaavat palvelut kuten I2P. Tor-verkon käyttäjämäärä kasvaa jatkuvasti, jolloin sen antama suoja myös kasvaa. Tämän takia Tor-verkosta tulee olemaan vain enemmän hyötyä tulevaisuudessa.

Tor-verkko tuo huomattavaa hyötyä yksityisyyden näkökulmasta käyttäjälleen. Tor-verkon avulla käyttäjä antaa vähemmän itseensä yhdistettävää dataa käyttämälleen palvelulle ja kasvattaa näin anonymiteetin suojaa. Tor-verkossa on kuitenkin omat uhkansa, joista suurin osa liittyy rikolliseen toimintaan. Näille sivuille kuitenkin käyttäjä tuskin eksyy vahingossa, joten riski ei ole kovinkaan merkittävä ja kokonaisuudessaan Tor-verkon käytöstä on enemmän hyötyä kuin haittaa.

Lähdeluettelo

Ahmad, W. & Liccardi, I. (2020). Addressing Anonymous Abuses: Measuring the Effects of Technical Mechanisms on Reported User Behaviors. In Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (CHI '20). Association for Computing Machinery, New York, NY, USA, 1–14. *https://doi-org.libproxy.tuni.fi/10.1145/3313831.3376690*

Avdoshin, S. & Lazarenko, A. (2016): Anonymity of Tor: Myth and Reality. CEE-SECR ’16: Proceedings of the 12th Central and Eastern European Software Engineering Conference in Russia *https://doi-org.libproxy.tuni.fi/10.1145/3022211.3022221*

Brandl, K., Karakuz, A., Schäfer, M., Steinebach, M. & Yannikos,Y. (2019). Detection and Analysis of Tor Onion Services. In Proceedings of the 14th International Conference on Availability, Reliability and Security (ARES '19). Association for Computing Machinery, New York, NY, USA, Article 66, 1–10. *https://doi-org.libproxy.tuni.fi/10.1145/3339252.3341486*

Cha, S. -C., Hsu, T. -Y., Xiang, Y. & Yeh, K. -H. (2019) "Privacy Enhancing Technologies in the Internet of Things: Perspectives and Challenges," in IEEE Internet of Things Journal, vol. 6, no. 2, pp. 2159-2187, April 2019, doi: 10.1109/JIOT.2018.2878658.

Dingledine, R., Mathewson, N. & Syverson, P. (2004): Tor: The Second-Generation Onion Router. SSYM'04: Proceedings of the 13th conference on USENIX Security Symposium, Volume 13 *https://www.usenix.org/legacy/publications/library/proceedings/sec04/tech/full_papers/dingledine/dingledine.pdf*

Harboth, D. & Pape, S. (2020): How Privacy Concerns, Trust and Risk Beliefs, and Privacy Literacy Influence Users’ Intentions to Use Privacy-Enhancing Technologies—The Case of Tor. ACM SIGMIS Database: the DATABASE for Advances in Information Systems, Volume 51, Issue 1, s 51-69 *https://doi-org.libproxy.tuni.fi/10.1145/3380799.3380805*

Koizumi, K. & Yoshiura, N. (2020). A Method of Collecting the IP Addresses of Hidden Server in Tor Networks. In Proceedings of the 2020 9th International Conference

on Software and Computer Applications (ICSCA 2020). Association for Computing Machinery, New York, NY, USA, 242–246. *https://doi-org.libproxy.tuni.fi/10.1145/3384544.3384589*

Metrics, (2023), Tor Metrics, https://metrics.torproject.org/ (Haettu 29.7.2023)

Momen, N. (2023), Freedom of Expression in the Digital Age: Internet Censorship. In: Romaniuk, S.N., Marton, P.N. (eds) The Palgrave Encyclopedia of Global Security Studies. Palgrave Macmillan, Cham. *https://doi-org.libproxy.tuni.fi/10.1007/978-3-319-74319-6_31*

Phong Hoang, N. & Pishva, D. (2014) "Anonymous communication and its importance in social networking," 16th International Conference on Advanced Communication Technology, Pyeongchang, Korea (South), 2014, pp. 34-39, doi: 10.1109/ICACT.2014.6778917.

Rutherfoord, J. & Rutherfoord, R. (2010). Privacy and ethical concerns in internet security. In Proceedings of the 2010 ACM conference on Information technology education (SIGITE '10). Association for Computing Machinery, New York, NY, USA, 131–134. *https://doi-org.libproxy.tuni.fi/10.1145/1867651.1867686*

Winkler, S. & Zeadally, S. (2015). An analysis of tools for online anonymity. International Journal of Pervasive Computing and Communications, 11(4), 436-453. *https://doi.org/10.1108/IJPCC-08-2015-0030*