HAAGA-HELIA
ammattikorkeakoulu

The Onion Router – Tor-ohjelmistojen soveltuvuus yksityiselle tietokoneen käyttäjälle

Lauri Soivi

Opinnäytetyö
Tietojenkäsittelyn koulutusohjelma
2014

HAAGA-HELIA
ammattikorkeakoulu

Tiivistelmä

19.11.2014

Tietojenkäsittelyn koulutusohjelma

Tekijä Lauri Soivi	**Aloitusvuosi** 2011
Opinnäytetyön nimi The Onion Router – Tor-ohjelmistojen soveltuvuus yksityiselle tietokoneen käyttäjälle	**Sivu- ja liitesivumäärä** 76 + 31
Ohjaaja Petri Hirvonen	

Tämän opinnäytetyön tarkoituksena oli selvittää Tor-ohjelmistojen soveltuvuutta yksityisille tietokoneen käyttäjille. Soveltuvuutta pohdittiin sellaisten tutkimuskysymyksien pohjalta, joilla selvitettiin Tor-ohjelmistojen yleistymistä, tarpeellisuutta ja turvallista käyttämistä.

Teoriaosuudessa tarkastellaan Internet-sensuuria ja -seurantaa, joita on mahdollista välttää Tor-ohjelmistoilla. Teoriaosuudessa kerrotaan esimerkkeinä Kiinan ja Turkin Internet-sensuurista, joiden Internet-sensuuri on ollut viime aikoina paljon esillä julkisuudessa. Internet-seurantaan liittyvässä teoriaosuudessa käsitellään Yhdysvaltojen, Googlen ja Facebookin toteuttamaa tietojen keräämistä, koska näiden kolme organisaation tietojen kerääminen on ollut viime aikoina laajalti julkisuudessa. Työssä käsitellään myös suomalaisiin kohdistuvaa Internet-sensuuria ja -seurantaa, koska tutkimus on suurimmaksi osaksi suunnattu suomalaisille tietokoneen käyttäjille. Teoriaosuuden lopussa tarkastellaan Tor-ohjelmistoja, niiden toimintaa, riskejä ja käyttämistä.

Työn tutkimusosuus toteutettiin kahdessa eri osassa. Tutkimuksen ensimmäisessä osan lähestymistapa oli kvalitatiivinen, jossa aineisto koostui asiantuntijoille suunnatusta kyselystä. Tutkimuksen toisessa osassa käytettiin kvantitatiivista tutkimusmenetelmää, jossa kerättiin empiiristä aineistoa yksityishenkilöiltä testin muodossa. Tämän kaksiosaisen lähestymistavan tarkoituksena oli saada asiantuntijoiden vastauksien avulla teoreettinen näkökulma ja käyttöönoton testauksesta käytännönläheinen näkökulma.

Tutkimuksessa saatiin selville, että Tor-ohjelmistojen käyttö saattaa tulevaisuudessa kasvaa maltillisesti, jos ohjelmistoille nähdään tarvetta, mutta asiantuntijat ja testihenkilöt pitivät Tor-ohjelmistojen hyötyjä suomalaisille suhteellisen pienenä. Yksityiset tietokoneen käyttäjät kykenevät käyttämään halutessaan Tor-ohjelmistoja turvallisesti. Tor-ohjelmistot soveltuvat yksityisille tietokoneen käyttäjille silloin, kun he kokevat Tor-ohjelmistot tarpeellisiksi ja ovat valmiita ottamaan selville ennen Tor-ohjelmistojen käyttöönottoa, miten niitä käytetään oikein, jotta Tor-ohjelmistojen käyttö tapahtuu mahdollisimman turvallisesti. Käyttäjien oli tärkeää ymmärtää, mihin Tor-ohjelmistot pystyvät ja mihin eivät, ja että täydellistä tietoturvallisuutta on mahdotonta saavuttaa**.**

Asiasanat
Tor, anonyymiverkot, Internet, anonymiteetti, sensuuri, seuranta

HAAGA-HELIA
University of Applied Sciences

Abstract

19.11.2014

Degree programme in Information Technology

Author Lauri Soivi	**Year of entry** 2011
The title of thesis The Onion Router – The Suitability of Tor Software for Private Computer Users	**Number of report pages and attachment pages** 76 + 31
Advisor Pekka Hirvonen	

The purpose of this thesis was to find out the suitability of Tor software for private computer users. Suitability issues were discussed on the basis of research questions which focused on clarifying the future spread, need and secure use of Tor software.

The theoretical part of the thesis covers Internet censorship and surveillance which can be avoided by using Tor software. The Internet censorship of China and Turkey, which have recently received a lot of publicity, are discussed. The Internet surveillance executed by the United States, Google and Facebook are dealt with because the Internet surveillance of these three organizations has recently been covered in the media. The ways in which Internet-censorship and surveillance affect Finnish citizens are also considered because this thesis mainly concerns Finnish computer users. Also, the theoretical section examines Tor software, as well as its functions, risks and usage.

The study consists of two different parts. One part is of qualitative nature, as the material was gathered by carrying out a survey aimed at experts. The other part of the study was carried out by using the quantitative research method, as empirical research material was gathered from private computer users in the form of a test. The purpose of this two-sided approach was to get a theoretical point of view from the experts and a practical point of view through the test.

It was revealed in the study that the number of Tor users may grow moderately in the future if the Internet users experience a need to use Tor. Both the experts and the testees responded that the benefits of using Tor software were very small in Finland. Private computer users were shown to be able to use Tor software securely if they were willing to. Tor software is seen to be suitable for private computer users when they experience to have a need to use Tor and if they are ready to find out how to use Tor software safely before they actually start using them, in order to use Tor software securely. Furthermore, it was important to acknowledge the capabilities and incapabilities of Tor software and to understand that it is impossible to achieve perfect information security.

Key words
Tor, anonymity network, Internet, anonymity, censorship, surveillance

Sisällys

Keskeiset käsitteet

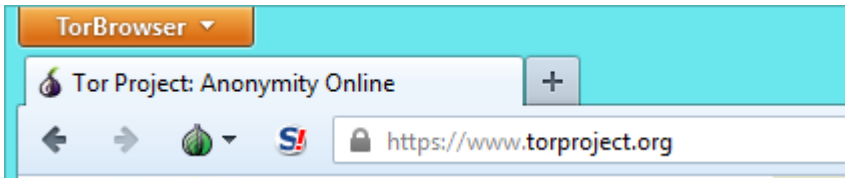
Avoimen lähdekoodin ohjelmisto ja vapaa ohjelmisto tarkoittavat ohjelmistoja, joiden lähdekoodia on mahdollista tutkia ja joita voidaan muokata tarvittaessa omiin tarpeisiin. Kyseisiä ohjelmistoja saa myös vapaasti levittää. (GNU 2014; Opensource.com 2014.) Esimerkiksi myöhemmin käsiteltävä Tor on vapaa ohjelmisto, ja NoScript-lisäosa on avointa lähdekoodia.

DNS (Domain Name System) on nimipalvelujärjestelmä, joka toimii Internetissä kuin puhelinluettelo. Puhelinluettelo yhdistää nimen ja puhelinnumeron, kun DNS yhdistää verkkotunnuksen (domain) IP-osoitteeseen. Internetiin on luotu nimipalvelujärjestelmiä, jottei IP-osoitteita tarvitsi muistaa ulkoa. (Mitchell 2014a.) Internet-käyttäjän halutessa päästä esimerkiksi www.torproject.org -sivustolle käyttäjän tietokone hakee nimipalvelujärjestelmältä Internet-sivustolle oikean IP-osoitteen, joka on 38.229.72.14 ja johon käyttäjä yhdistetään.

Eväste (cookie) on tiedosto, joka tallennetaan Internet-käyttäjän laitteelle. Niitä käytetään erilaisissa Internet-palveluissa, esimerkiksi verkkokaupoissa, jotta tiedot säilyvät Internet-palvelun sivustoilla liikkuessa. Laitteen Internet-selain tallentaa käyttäjän tietokoneelle tiedot esimerkiksi verkkokaupan ostoskorin sisällöstä, jotta ostoskorissa olevat tuotteet säilyvät siellä koko prosessin ajan. Evästeeseen voi myös tallentaa muun muassa käyttäjän IP-osoitteen, käytetyt Internet-sivut ja mistä Internet-osoitteesta käyttäjä on tullut kyseiselle Internet-sivulle. (Loshin 2013, 4; Viestintävirasto 2014.)

HTTP ja HTTPS. HTTP (Hypertext Transfer Protocol) on protokolla, jota Internet-selaimet käyttävät kommunikoidessaan palvelimien kanssa. HTTP-protokolla on salaamatonta liikennettä, toisin kuin HTTPS-protokolla (Hypertext Transfer Protocol Secure), joka salaa Internet-yhteyden Internet-selaimen ja Internet-sivuston välillä. (Loshin 2013, 17; Mitchell 2014b.) HTTPS-protokolla käyttää salaukseen TLS-protokollaa. Salatun HTTPS-yhteyden voi tunnistaa Internet-selaimessa olevasta lukosta, joka tulee yleensä osoiterivin viereen. (Järvinen 2014a, 252–254; Loshin 2013, 17.)

Seuraavassa kuviossa näkyy lukon kuva, joka kertoo salatusta HTTPS-yhteydestä (Kuvio 1).



Kuvio 1. Osoiterivillä oleva lukon kuva kertoo salatusta HTTPS-yhteydestä

Kansalaisoikeuksia puolustava järjestö EFF (Electronic Frontier Foundation) ja Tor-projekti on kehittänyt Internet-selaimille HTTPS Everywhere -lisäosan. Sen tarkoituksena on lisätä Internetin käytön turvallisuutta ottamalla HTTPS-protokolla käyttöön sellaisilla Internet-sivustoilla, joilla on tuki salatulle Internet-yhteydelle, mutta joilla salattu Internet-yhteys ei ole esimerkiksi oletuksena käytössä. (EFF 2014.) HTTPS Everywhere -lisäosa on käytössä joissakin Tor-projektin ohjelmistoissa, kuten Tor Browserissa ja Tails-käyttöjärjestelmässä, joita käsitellään myöhemmissä kappaleissa.

IP-osoite jaetaan jokaiselle laitteelle, joka on kytkettynä Internetiin, jotta se voidaan tunnistaa Internetissä. IP-osoite on yksilöity numerosarja, jonka Internet-palveluntarjoaja jakaa laitteille. IP-osoite on kuin kotiosoite, jonka perusteella laitteet löytävät toisensa Internetissä. (Loshin 2013, 4.)

NoScript. Osa Internet-sivustoista saattaa sisältää ohjelmia, jotka voivat olla haitallisia käyttäjälle tai tietokoneille. Nämä voivat olla esimerkiksi Javascriptillä, Javalla tai Flashilla tehtyjä ohjelmistoja, jotka käynnistyvät, kun palvelun käyttäjä tulee sivustolle. NoScript on Internet-selaimen lisäosa, jolla estetään Internet-sivustoilla ajettavat ohjelmat, ellei käyttäjä itse anna ohjelmalle lupaa toimia. (NoScript 2014.) NoScript-lisäosa on avointa lähdekoodia ja se tulee osassa Tor-projektin ohjelmistoissa mukana, kuten Tor Browserissa ja Tails-käyttöjärjestelmässä.

TLS ja SSL. TLS-protokolla (Transport Layer Security) on salaustekniikka, jolla salataan Internet-yhteys esimerkiksi Internet-selaimesta Internet-sivustolle. TLS-protokolla tunnettiin aikaisemmin nimellä SSL-protokolla (Secure Sockets Layer), johon on nimen

vaihdoksen jälkeen lisätty laajennuksia ja parannuksia. TLS-protokolla toimii yksinkertaisuudessaan niin, että Internet-yhteyden molemmat osapuolet varmentavat toisensa ja tämän jälkeen sopivat salauksessa käytettävästä salaustekniikasta. Tämän jälkeen molemmat osapuolet salaavat lähettämänsä tiedon Internet-yhteydessä, jolloin vain kyseiset osapuolet voivat avata salatussa Internet-yhteydessä lähetettävää dataa. (Järvinen 2014a, 188, 252–254.)

Välityspalvelin (proxy) varastoi välimuistiinsa Internet-sivustoja, jolloin samaa tietoa ei tarvitse hakea moneen kertaan uudestaan. Välityspalvelimet toimivat Internet-yhteydessä käyttäjän tietokoneen ja palvelimen välissä. Välityspalvelimia voidaan käyttää myös palomuureina, jotka suojaavat käyttäjän tietokonetta, tai ne voivat suodattaa tiettyjä Internet-sivustoja. Välityspalvelimilla on myös mahdollista kiertää palomuurien luomia Internet-sensuureita, joita käsitellään myöhemmissä kappaleissa (Loshin 2013, 5–6; Rouse 2014.)

1 Johdanto

Kiinan Internet-sensuuri, Turkin viimeaikaiset Internet-sivustojen estot sekä Snowdenin tietovuotopaljastukset koskien Yhdysvaltojen tiedusteluorganisaatioiden tekemää Internet-seurantaa ovat saaneet laajaa huomioita ympäri maailmaa. Viime vuosien ajan eri organisaatioiden tekemä Internet-sensuuri ja -seuranta on saanut Internetin käyttäjiä siirtymään yhä enemmän anonyymien verkkojen pariin. Anonyymien verkkojen avulla Internetin käyttäjillä on mahdollisuus välttää eri organisaatioiden harjoittamaa Internet-sensuuria ja -seurantaa. Näistä anonyymeistä verkoista mahdollisesti suosituimmaksi on noussut Tor (The Onion Router) (Ziccardi 2013, 175).

Tämän opinnäytetyön aiheena on Tor-ohjelmistojen soveltuvuus yksityisille tietokoneen käyttäjille. Valitsin opinnäytetyöni aiheeksi Tor-ohjelmistot, koska tietojeni mukaan tietokoneille ei ole vastaavanlaista anonyymiä verkkoa, joka mahdollistaisi normaalin Internetin käytön veloituksetta. Aihe on ajankohtainen, koska osa organisaatioista on luonut maailman laajuiseen Internetiin estoja ja seuraamista, jotka koskevat tavallisia Internetin käyttäjiä. Tällä hetkellä Internet-sensuuria tapahtuu koko maailmassa aina Kiinasta Suomeen saakka, tiedon keräämistä puolestaan Yhdysvaltojen NSA:sta aina Internet-palveluita tarjoavaan Googleen. Internetin käyttäjiin kohdistuvien estojen ja seuraamisen välttämiseksi osa Internetin käyttäjistä on hakeutunut Tor-ohjelmistojen pariin. Vaikka Tor-ohjelmistot mahdollistavat estojen kiertämisen ja anonyymin Internetin käytön, saattaa se aiheuttaa Tor-ohjelmistojen käyttäjille myös tietoturvauhkia, koska Tor-ohjelmistojen käytössä voi piillä riskejä, joita käyttäjä ei tiedosta.

Tor on vapaa ohjelmisto, joka on tarkoitettu sellaisille Internet-käyttäjille, jotka haluavat kiertää Internet-sensuureita ja käyttää Internetiä anonyymisti. Torin käyttämä verkko koostuu välityspalvelimista, joita kutsutaan solmuiksi. Torin käyttäjän Internet-yhteys ohjataan Tor-verkossa kolmen satunnaisesti valitun solmun kautta Internet-sivustolle, jolloin Internet-yhteyden alkuperää ja lopullista päämäärää on haastavaa selvittää samanaikaisesti. Torin käyttämiseen tietokoneella on kehitetty ohjelmistot Tor Browser -selain ja Tails-käyttöjärjestelmä. Tor Browser on selain, joka asennetaan tietokoneen käyttöjärjestelmään, kuten Microsoft Windowsiin, Apple OS X:n tai Linuxiin. Tails on itsessään Linux-pohjainen käyttöjärjestelmä, jota voidaan ajaa suoraan DVD-

levyltä, USB-muistitikulta tai SD-kortilta. Näihin veloituksettomiin Tor-ohjelmistoihin on asennettu mukaan Tor, joka ohjaa Internet-yhteyden Tor-verkon läpi.

Tämän opinnäytetyön tarkoituksena on saada selville sellaisia mahdollisia tekijöitä, joiden vuoksi Tor-ohjelmistot eivät soveltuisi tavallisille tietokoneen käyttäjille. Työn hyödyt kohdistuvat suurimmaksi osaksi tavallisiin tietokoneen käyttäjiin, jotta Tor-ohjelmistoista ja niiden toiminnasta saadaan kohtuullisen hyvä tietous ja jotta mahdolliset riskit pystytään välttämään. Opinnäytetyöni pohjalta tavalliset tietokoneen käyttäjät voivat itse arvioida omia tarpeitaan Tor-ohjelmistoille ja mahdollisesti välttää joitain riskitekijöitä, koska työssäni annan hyvän teoriataustan Internet-sensuurista ja -seuraamisesta sekä Tor-ohjelmistojen toiminnasta ja mahdollisista riskeistä. Työn tehtävänä on selvittää seuraavia asioita: Tor-ohjelmistojen tarve tulevaisuudessa, Tor-ohjelmistojen tarpeellisuus suomalaisille ja suomalaisten tietokoneen käyttäjien kyky käyttää Tor-ohjelmistoja turvallisesti. Tulevaisuuden tarpeella pystytään arvioimaan sitä, kuinka kriittisesti Tor-ohjelmistoja voidaan tulevaisuudessa tarvita maailmalla, mikä voi heijastua tulevana tarpeena myös Suomessa. Lisäksi mahdollinen käyttäjämäärän kasvu saattaa korostaa tutkimuksessa esille nousseiden asioiden tärkeyttä. Työssä arvioidaan myös Tor-ohjelmistojen tarpeellisuutta suomalaisille, mistä saattavat monet suomalaiset tietokoneen käyttäjät hyötyä pohtiessaan, tarvitsevatko Tor-ohjelmistoja vai eivät. Tor-ohjelmistojen käyttöönotolla saadaan selvitys siitä, onko Tor-ohjelmistojen käytössä joitain asioita, joita Tor-ohjelmistojen kehittäjät voisivat parantaa, jotta Tor-ohjelmistojen käyttäminen tapahtuisi turvallisemmin. Työllä saadaan myös tavallisille tietokoneen käyttäjille tietous siitä, miten Tor-ohjelmistoja pitäisi käyttää, jotta niiden käytöstä ei aiheutuisi mitään haittoja.

Tämän kaltaista työtä ei tietojeni mukaan ole vielä toteutettu, mutta työssäni esille tulevia eri osa-alueita on kuitenkin tutkittu. Internetin sensuroimiseen on perehtynyt muun muassa Ziccardi (2013) ja Human Right Watch (2006). Valtioiden ja yrityksen seuraamisesta on tutkinut muun muassa Järvinen (2014a) ja Loshin (2013), joista jälkimmäinen on kirjoittanut kokonaisen kirjan Toriin liittyen. Joihinkin tuoreimpiin tai suomalaisiin tapauksiin liittyen aihepiiriistä ei ole tehty tutkimuksia, minkä vuoksi jouduin monin paikoin käyttämään lähteinä uutisia. Tämä korostaa työni tärkeyttä ja ajankohtai-

suutta, koska moniin käsittelemiini aiheisiin ei ole paneuduttu tarkemmin, vaikka ne ovat olleet mediassa esillä lähes päivittäin.

Seuraavaksi esittelen tutkimuskysymykseni ja -tavoitteeni sekä lyhyesti tutkimusmenetelmäni. Teoriaosuudessa tarkastelen Internet-sensuuria ja -seuraamista sekä Torin toimintaa, riskejä ja ohjelmistoja. Tämän jälkeen esittelen tarkemmin tutkimuksen toteutuksen ja tulokset. Lopuksi vastaan tutkimuskysymyksiin Pohdinta-osuudessa ja tarkastelen tutkimustani kokonaisuutena Yhteenveto-kappaleessa.

1.1 Tutkimuksen tavoitteet ja rajaus

Opinnäytetyössä tarkastellaan Internet-sensuurin ja -seurannan toimintaa ja tekniikoita. Lisäksi Torin toiminnasta ja Tor-ohjelmistoista kerätään kattava kokonaiskuva. Työn tarkoituksena on selvittää Tor-ohjelmistojen soveltuvuutta tavallisille tietokoneen käyttäjille, jotka käyttävät Internetiä. Soveltuvuutta selvitetään tutkimuskysymyksien pohjalta, jotka ovat:

1. Yleistyvätkö Tor-ohjelmistot maailmanlaajuisesti yksityishenkilöiden käytössä?
2. Onko Tor-ohjelmistojen käyttö tarpeellista suomalaisille yksityishenkilöille?
3. Osaavatko suomalaiset yksityishenkilöt käyttää Tor-ohjelmistoja turvallisesti?

Uskoisin, etteivät Tor-ohjelmistot sovellu tavallisille Internetin käyttäjille, koska he eivät oletettavasti osaa käyttää Tor-ohjelmistoja turvallisesti ja eivät ole valmiita muuttamaan Internetin käyttötapojaan. Perustan oletukseni siihen, että tavallinen Internetin käyttäjä ei välttämättä tiedosta Tor-ohjelmistojen mahdollisia turvallisuusriskejä, eikä tavallinen suomalainen Internetin käyttäjä häiriinny häneen kohdistuvasta Internetissä tapahtuvasta seurannasta ja sensuurista.

Opinnäytetyössä rajataan pois muut kuin Tor-ohjelmistot, koska Tor on tällä hetkellä mahdollisesti käytetyin anonyymi verkko (Ziccardi 2013, 175) ja tiedossani ei ole muita vastaavanlaisia ohjelmistoja. Opinnäytetyössä ei tutkita Internetin tekniikoita ja toimintaa laajemmin, vaan ainoastaan niiltä osin, miten Tor niihin vaikuttaa. Kyseisessä opinnäytetyössä ei käsitellä Torin piilotettuja palveluita eikä mobiilia, koska tutkimus koskee

yksityisiä tietokoneiden käyttäjiä ja näistä kumpikaan ei liity normaaliin Internetin käyttöön tietokoneella.

1.2 Tutkimusmenetelmät

Opinnäytetyön tutkimusosuus toteutettiin kahdessa eri osassa. Tutkimuksen ensimmäisessä osassa käytettiin kvalitatiivista eli laadullista tutkimusmenetelmää, jossa aineisto kerättiin kyselynä asiantuntijoilta. Ensimmäisen osan tavoitteena oli saada Internet-sensuurista ja -seurannasta sekä Torin nykytilanteesta mahdollisimman kattava kuva. Tutkimuksen toinen osa toteutettiin kvantitatiivisena eli määrällisenä tutkimuksena, jossa kerättiin empiiristä aineistoa suomalaisilta yksityishenkilöiltä testin muodossa. Testin tarkoituksena oli saada käytännön kokemuksia Tor-ohjelmistoista. Testillä selvitettiin tavallisen tietokoneen käyttäjän kyvykkyyttä asentaa ja käyttää Tor-ohjelmistoja turvallisesti. Valitsin käyttöönottotestin tutkimusmenetelmäksi, koska näin pystyin käytännössä parhaiten havainnoimaan tavallisten tietokoneen käyttäjien kykyä asentaa ja käyttää Tor-ohjelmistoja. Asiantuntijoiden vastauksien avulla sain alan asiantuntijoilta perehtyneempiä näkemyksiä Tor-ohjelmistoista sekä Internet-sensuurista ja -seurannasta. Tarkemmin käytännön tutkimuksesta kerrotaan Tutkimuksen toteutus -kappaleessa. Seuraavaksi siirryn käsittelemään työni teoriataustaa.

2 Internet-sensuuri

Tässä kappaleessa käsitellään Internet-sensuuria yleisellä tasolla ja sen tekniikoita. Kappaleessa annetaan esimerkkejä Internet-sensuurista Suomessa, Turkissa ja Kiinassa.

2.1 Internet-sensuurista yleisesti

Sensuurilla tarkoitetaan valtioiden ja muiden organisaatioiden harjoittamaa valvontaa ja ennakkotarkastusta. Valtiot voivat tarkastaa julkista materiaalia muun muassa painotuotteita, näytelmiä, elokuvia ja Internetissä olevaa materiaalia. Valtioilla on myös mahdollisuus sensuurin nimissä poistaa materiaaleista haluamiaan kohtia. (Aikio & Vornanen 2000, 555.) Internetin kasvun myötä myös Internet-sensuuri on kasvanut ympäri maailmaa.

Valtiot käyttävät Internet-sensuuria tarkoituksenaan estää verkonkäyttäjältä vahingollisen tai laittoman materiaalin käyttämisen (Ziccardi 2013, 75–76). Suomessa on asetettu Internet-sensuuria koskeva laki, joka koskee lapsipornografiaa (1068/2006), mutta muualla Euroopassa Internet-sensuuri on ulottunut lapsipornografian lisäksi muun muassa kulttuuriin, politiikkaan, viharikoksiin, rasismiin, terrorismiin, tekijänoikeuksiin ja uhkapeleihin (Ziccardi 2013, 195), esimerkiksi Turkissa on noussut vuoden 2014 aikana pinnalle tapaukset, joissa on kielletty videopalvelu YouTube ja yhteisö- ja mikroblogipalvelu Twitter (Sezer 2014). Muualla maailmassa on lisäksi sensuroitu uskontoon ja aikuisviihteeseen liittyvää materiaalia (Ziccardi 2013, 188–189).

2.2 Internet-sensuurin tekniikat

Valtioiden Internet-sensuuria voidaan ylläpitää ja valvoa valtionsisäisen verkkoliikenteen laajuisena viranomaisten toimesta tai ne voidaan delegoida verkonpalveluntarjoajille. Internet-sensuuri voidaan myös asettaa esimerkiksi yrityksien, kirjastojen ja nettikahviloiden sisäiseen verkkoon, mutta myös yksittäisten henkilöiden tietokoneissa voi olla oma Internet-sensuurinsa. (Ziccardi 2013, 202.)

Sensuroinnin suodatustekniikat voidaan jakaa sisällönanalyysiin ja estämiseen (Hamilton 2004, 156). Sisällönanalyysissä tutkitaan Internet-yhteyksissä liikkuvaa dataa. Kielle-

tyn materiaalin löytyessä datasta esimerkiksi koko Internet-yhteys Internet-sivustolle voidaan estää tai kielletyt sanat, lauseet tai kappaleet voidaan poistaa tekstistä. Kyseistä teknologiaa kutsutaan nimellä Deep Packet Inspection (DPI). Sisällönanalyysiä pidetään tehokkaana suodatustekniikkana, joka on käytössä muun muassa Kiinassa, jota pidetään Internet-sensuurin edelläkävijänä. (Wagner 2009, 3, 5, 8.)

Murdoch ja Anderson (2008, 59–63) esittelevät kolme erilaista estotoimenpidettä: Tiettyjen palvelimien IP-osoitteiden estäminen, DNS-suodatus tai välityspalvelinsuodatus. IP-osoitteiden estäminen ei salli yhteyttä kiellettyyn IP-osoitteeseen. DNS-suodatuksessa nimipalvelinjärjestelmä ei palauta kielletyn verkkotunnuksen IP-osoitetta. Välityspalvelinsuodatuksessa Internet-sivustot ohjataan välityspalvelimen läpi, jolloin välityspalvelin estää kielletyt Internet-sivut. Välityspalvelinsuodatuksen etuna on yksittäisten Internet-sivujen estäminen, koska silloin koko WWW-palvelinta ei tarvitse estää ja muilla WWW-palvelimella olevilla sallituilla Internet-sivuilla on mahdollisuus käydä. (Murdoch & Anderson 2008, 59–63; Ziccardi 2013, 201.) Jotkin valtiot ovat myös tehneet yhteistyötä hakukoneyhtiöiden kanssa, jottei heidän valtioidensa sisällä hakukonehauissa tulisi kiellettyä tai ei-haluttua materiaalia (Ziccardi 2013, 201).

Seuraavat kappaleet käsittelevät Suomessa, Turkissa ja Kiinassa esiintyvää Internet-sensuuria. Internet-sensuuria esiintyy laajalti ympäri maailmaa Suomen, Turkin ja Kiinan lisäksi, mutta näitä maita tarkastelemalla saadaan käsitys sekä Euroopan että globaalin Internet-sensuurin tilanteesta.

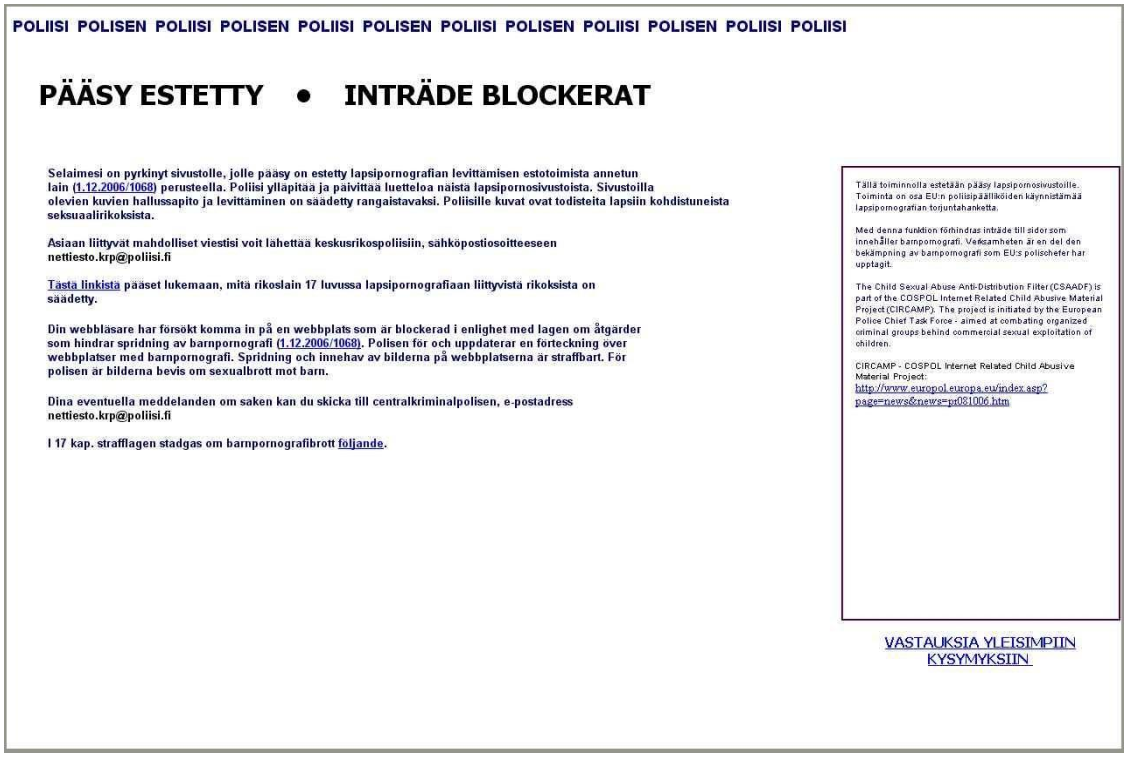
2.3 Suomen Internet-sensuuri

Suomessa näkyvillä Internet-sivustoilla pätee Suomen lait. Suomen poliisilla on Internetissä Nettivinkki-palvelu, jolla pystytään ilmoittamaan Internetissä havaituista rikosepäilyistä tai laittomaksi epäillystä materiaalista, joihin lukeutuu muun muassa huumausaineet, petokset, rasistiset ilmiöt, väkivalta ja muut turvallisuusuhat. Kaikki ilmoitukset analysoidaan ja jatkokäsitellään. (Poliisi 2014c.) Suomessa on myös säädetty vuonna 2006 laki, jonka mukaan Internetissä ei saa jakaa tekijänoikeuden suojaamaa aineistoa ilman tekijän lupaa (Poliisi 2014b). Helsingin käräjäoikeus määräsi vuosina 2011 ja 2012 osaa suomalaisista palveluntarjoajista estämään The Pirate Bay -sivuston, koska käräjä-

oikeus katsoi sen rikkovan tekijänoikeuksia. (Elisa Oyj 2011; HS 2012; Salokorpi 2013.) Suomessa on myös laitonta markkinoida vahvoja alkoholijuomia, joten Suomessa esimerkiksi Koskenkorvan Internet-sivusto on estetty (Järvinen 2014a, 248–249).

Vuonna 2007 Suomessa otettiin käyttöön laki lapsipornografian levittämisen estotoimista (1068/2006). Lain 1 §:n mukaan ”tarkoituksena on lasten ja heidän perusoikeuksiensa suojaamiseksi edistää toimenpiteitä, joiden avulla voidaan estää pääsy ulkomailla ylläpidettäviin lapsipornosivustoihin.” Poliisi ylläpitää salaista estolistaa, jonka pitäisi sisältää vain lapsipornosivustoja (Tarvainen 2008). Lain 4 §:n (1068/2006) perusteella poliisi kartoittaa salaiseen estolistaan tarvittavat tiedot muun muassa teleyrityksiltä, kansalaisjärjestöiltä, viranomaisilta ja yksityisiltä henkilöiltä. Kyseistä estolistaa ei pakoteta käytettäväksi, vaan Internetin palveluntarjoajilla on mahdollisuus vapaaehtoisesti ottaa estolista käyttöön (HE 99/2006, luku 1 § 3; Railas 2005, 1; Poliisi 2014a). Myös osa Internetin palveluntarjoajista antaa asiakkailleen mahdollisuuden itse valita, onko estolista heidän käytössään vai ei, mutta oletuksena estolista on käytössä (Juutilainen 2008). Suomessa käytetään DNS-suodatusta ja välityspalvelinsuodatusta (Poliisi 2014a).

Lain 5 §:ssä (1068/2006) määrätään laittoman Internet-sivuston tiedottamisvelvollisuudesta. Jos verkonkäyttäjä yrittää päästä estetylle Internet-sivustolle, käyttäjä ohjataan tiedotesivustolle, jossa kerrotaan sivuston estosta ja perusteista pääsyn estämiselle sekä annetaan tiedot tahoista, joihin voidaan tarvittaessa olla yhteydessä. Seuraavassa kuviossa esimerkki poliisin tiedotesivustosta (Kuvio 2).



Kuvio 2. Poliisin tiedotesivusto estetystä Internet-sivusta (Poliisi 2014a)

Kyseinen estolista on saanut myös osakseen kritiikkiä. Turun yliopisto (HE 99/2006, luku 5.2) ja kansalaisten sähköisiä oikeuksia puolustava Electronic Frontier Finland ry (Effi) (Tarvainen 2008) pitävät estolistaa perustuslain kieltämänä ennakkosensuurina ja sananvapauden vastaisena. Helsingissä järjestettiin vuonna 2008 Internet-sensuurin vastainen mielenosoitus, johon osallistui noin 500 mielenosoittajaa. Mielenosoittajat olivat myös sitä mieltä, ettei Internet-sensuuri auta poistamaan lapsipornoa Internetistä, vaan se lakaisee ongelman pois näkyvistä. (Poropudas 2008.)

Estolistat sisältävät joidenkin lähteiden mukaan Internet-sivustoja, jotka eivät täytä laittomuuden rajoja (Tarvainen 2008). Esimerkiksi thaimaalainen sananvapausjärjestö vaati syytteiden nostamista Suomen hallitusta vastaan, koska listalle oli asetettu thaimaalainen sivusto, jossa on kuva edesmenneestä prinsessasta (Linnake 2008). Lisäksi Scorpions -yhtyeen Virgin Killer -levyn Wikipedia-sivu asetettiin listalle, koska levynkannessa on alaston tyttö, jonka epäiltiin olevan alaikäinen (Mannila 2008).

Muualla Euroopan alueella on otettu laajamittaisemmin käyttöön Internet-sensuuria. Seuraavassa kappaleessa kerrotaan Turkin Internet-sensuurista, joka on noussut mediassa esille vuoden 2014 aikana.

2.4 Turkin Internet-sensuuri

Suomeen verrattuna Turkin Internet-sensuurin huomiota ei ole kerännyt pelkästään lapsipornografiaan liittyvät sivustot, vaan myös poliittinen materiaali. Euroopan turvallisuus- ja yhteistyöjärjestö väittää, että Turkissa oli vuonna 2010 noin 3 700 sivustoa, jotka oli sensuroitu mielivaltaisista ja poliittisista syistä. Sensuroitujen sivujen joukoissa oli muun muassa maan kurdivähemmistöön liittyviä uutissivustoja ja ulkomaisia sivustoja. (Reporters without borders 2010, 58.) Engelli Web -sivuston (2014) mukaan Turkissa oli vuonna 2014 noin 50 000 estettyä sivustoa. Turkissa sivustojen sensurointiin vaaditaan oikeuden päätös tai hallinnollinen päätös tietoliikenteen ja informaatioteknologian korkealta neuvostolta (Reporters without borders 2010, 58).

Turkin Internet-sensuuri nousi näkyvämmin mediaan, kun Turkki esti pääsyn YouTubeen vuonna 2008, koska siellä levitettiin videoita, joiden koettiin olevan epäkunnioittavia Turkin kansaa kohtaan. Myös samana vuonna yhteisöpalvelu MySpace asetettiin sensuurilistalle, koska sen katsottiin rikkovan immateriaalioikeuksia, mutta se poistettiin listalta vuotta myöhemmin. (Reporters without borders 2010, 58.) Sittemmin myös YouTuben esto on otettu pois käytöstä, koska YouTuben sensuroiminen nousi uudelleen esille vuonna 2014. YouTubeen ja Twitteriin pääsy estettiin Turkin alueella, koska YouTubessa ja Twitterissä oli jaettu äänitteitä, joiden koettiin olevan haitallisia Turkille. Twitterissä jaettujen äänitteiden epäiltiin sisältävän todisteista mahdollisesta korruptiosta Turkin korkea-arvoisten poliitikkojen keskuudessa. (Christie-Miller 2014; LiveLeak 2014; Sezer 2014; Toivonen 2014.) YouTubessa olevissa äänitteissä puolestaan keskusteltiin mahdollisista sotatoimista Syyriassa (BBC 2014a; Toivonen 2014). Kaksi viikkoa tapauksen jälkeen oikeus antoi päätöksen, jossa poistettiin Twitterin esto, sillä oikeuden päätöksen mukaan kyseinen esto rikkoi maan sananvapautta. (BBC 2014a; Ozvilgin & Coskun 2014.) Muutamaa kuukautta myöhemmin oikeus poisti myös YouTuben eston samasta syystä (BBC 2014b; Toivonen 2014).

Seuraava kappale käsittelee Kiinan Internet-sensuuria, jota pidetään yhtenä teknillisesti kehittyneimpänä (Bambauer ym. 2005, 3).

2.5 Kiinan Internet-sensuuri

Kiinan ollessa väkiluvultaan maailman suurin valtio on Kiina myös verkonkäyttäjämäärältään maailman suurin. Vuonna 2010 verkonkäyttäjien määrän arveltiin olevan noin 380 miljoonaa. (Reporters without borders 2010, 8.) Vuonna 2012 Kiina ylitti puolen miljardin verkonkäyttäjän rajan. Yhdysvalloissa on toiseksi eniten verkonkäyttäjiä maailmassa. Yhdysvalloissa oli vuonna 2012 noin 250 miljoonaa verkonkäyttäjää, joka on vasta puolet Kiinassa oleviin verkonkäyttäjiin verrattuna. (Internet World Stats 2012.)

Kiinan Internet-sensuuria pidetään edelläkävijänä, koska se on kehittynyt vuosien saatossa yhdeksi teknillisesti kehittyneimmäksi Internet-sensuuriksi (Bambauer ym. 2005, 3; Human Rights Watch 2006, 3; Reporters without borders 2010, 8). Internet-sensuuri koskee kaikkia aina yrityksistä yksityishenkilöihin. Internet-sensuuria ylläpitää pääosin Kiinan hallitus, mutta on myös yrityksiä, joilla on käytössään oma Internet-sensuurinsa. Yrityksien omat Internet-sensuurit sensuroivat hallituksen sensuroimia sivuja, mutta myös sivustoja, joita yritys kuvittelee hallituksen haluavan sensuroida. (Human Rights Watch 2006, 3–4.)

Kiina sensuroi omien sanojensa mukaan verkonkäyttäjille vahingollista materiaalia, joihin lukeutuu muun muassa aikuisviihde sekä poliittinen ja rikollinen aineisto (Reporters without borders 2010, 9). Kiinan Internet-sensuuri koskee monia suosittuja sivustoja. Suomen ja maailman 20 suosituimman sivuston joukosta löytyvät yhteisöpalvelu Facebook.com, Twitter.com, hakukone Google.com, Internet-palvelu Yahoo.com ja YouTube.com (Alexa 2014), jotka ovat kaikki sensuroitu Kiinassa (Greatfirewallofchina.org 2014; Reporters without borders 2010, 8, 10).

Kiinan hallitus on ilmoittanut kiinalaisille ja ulkomaalaisille tietokoneiden valmistajille, että valmistajien pitäisi esiasentaa Kiinaan myytäviin tietokoneisiin suodatusohjelmisto nimeltä Green Dam Youth Escort. Sovelluksen tarkoituksena on suojata nuoria verkonkäyttäjiä vahingolliselta materiaalilta peittämällä vahingollisen materiaalin Internet-sivulta. (Reporters without borders 2010, 9; OpenNet Initiative, 21.) Tarvittaessa ohjelmisto voi myös sulkea selaimen välilehtiä tai koko selaimen (OpenNet Initiative, 22).

Kiinan tiedetään myös yrittävän aktiivisesti torjua Torin käyttöä estämällä käyttäjiä yhdistämästä Tor-verkkoon (Winter & Lindskog 2012, 1).

Kiinalla on kymmeniä tuhansia viranomaisia, jotka valvovat verkkoa, verkon käyttöä ja käyvät muun muassa verkonkäyttäjien sähköposteja läpi (Human Rights Watch 2006, 3; Reporters without borders 2010, 11), esimerkiksi nettikahviloiden asiakkaiden verkonkäyttöä seurataan tarkasti. Nettikahviloiden asiakkaiden henkilöllisyys tarkistetaan ja heistä otetaan kuva, ennen kuin he saavat käyttää verkkoa. Nettikahviloiden asiakkaiden verkkoon kirjautumista hallinnoidaan viranomaisten toimesta, ja nettikahvilan ylläpitäjä seuraa asiakkaan verkonkäyttöä reaaliaikaisesti, jottei asiakas käytä verkko väärin. (Reporters without borders 2010, 11.) Kiinassa on ollut tapauksia, joissa yksityishenkilöitä on vangittu Internetin väärinkäytön vuoksi, muun muassa protestoimisesta ihmisoikeuksien puolesta (Reporters without borders 2010 8–11; Ziccardi 2013, 258–259).

3 Internet-käyttäjien seuraaminen

Edellisessä kappaleessa käsiteltiin Internet-sensuuria ja miten Internet-käyttäjien liikkuvuutta Internetissä yritetään estää. Tämä kappale käsittelee sitä, miten eri tahot seuraavat Internetin käyttöämme ja keräävät siitä tietoa. Kappaleessa kerrotaan yleisellä tasolla Internet-käyttäjien seuraamisesta ja Internetin käytön kautta tapahtuvasta tietojen keräämisestä. Kappaleessa käydään myös läpi Yhdysvaltojen tiedusteluorganisaatioiden seurantatekniikoita ja seurannan laajuutta, suomalaisiin kohdistuvaa Internetin seurantaa sekä kahden käydyimmän Internet-sivuston, Internet-palveluita tarjoavan Googlen ja yhteisöpalvelu Facebookin tietojen keräämistä.

3.1 Internet-käyttäjien seuraamisesta yleisesti

Moni Internetin käyttäjä voisi miettiä, kuka häntä voisi seurata ja miksi. Järvinen (2014a, 176–178) listaa neljä eri tahoa, jotka voivat mahdollisesti seurata jokaista Internetin käyttäjää. Nämä tahot ovat perhe, työpaikka, Internet-yritykset ja valtiolliset toimijat. Vaikka Suomessa luottamuksellisen viestinnän seuraaminen on kiellettyä, sitä pidetään yhtenä yleisimpänä Suomessa tehtävänä rikkomuksena. Useassa perheessä perheenjäsenten Internetin käyttöä seurataan, esimerkiksi vanhemmat seuraavat lapsiensa Internetin käyttöä, vaikka se on laitonta. Samankaltaista seurantaa tapahtuu myös työpaikoilla, joissa esimiehet voivat seurata alaistensa Internetin käyttöä. Moni Internet-yritys seuraa Internetin käyttöämme ja kerää Internetin ja palvelujen käytöstä tietoa. Samaa tekevät myös valtioiden tiedusteluorganisaatiot, joiden päätavoitteena on rikollisuuden vähentäminen. (Järvinen 2014a, 176–178.)

Suuri osa tiedon keräämisestä perustuu suurten massojen seuraamiseen, eikä vain yksittäisten henkilöiden seuraamiseen. Mahdollisiin seurantalistoihin, joissa seurataan yksittäisiä ihmisiä voi joutua esimerkiksi ammatin tai Internet-toiminnan myötä. Monien valtioiden tiedusteluorganisaatiot voivat kiinnostua poliitikoista, valtioiden keskeisistä virkamiehistä tai journalisteista. (Järvinen 2014a, 174–176.) Internet-käyttäjien toiminta Internetissä, kuten kuuluminen johonkin tiettyyn järjestöön tai tiettyjen hakujen tekeminen Internetissä, voi myös johtaa seurantalistoille joutumiseen (Brunila 2014; Järvinen 2014a, 175).

Moni saattaisi vähätellä ajatusta seuraamisesta ja tietojen keräämisestä ajattelemalla, ettei heillä ole mitään salattavaa. Usealla on kuitenkin salaisuuksia, joita ei välttämättä halua jakaa kaikille, kuten pankkitilin tiedot, sairaudet, rakkaussuhteet ja salasanat. Osa nuorista on hyvin avoimia käyttäessään Internetiä, eikä tiedosta sitä, että heidän Internetin käytöstä kerättyä tietoa voidaan käyttää heitä vastaan myöhemmin, esimerkiksi heidän hakiessaan johonkin poliittiseen ammattiin tai matkustaessaan ulkomaille. (Järvinen 2014a, 179.) Nuori englantilaispariskunta ei varmasti olisi arvannut, että pariskunnan miehen Twitteriin laittamat kaksi viestiä olisivat voineet aiheuttaa käännytyksen Yhdysvaltojen lentokentällä. Twitter-viesteissä mies oli kirjoittanut juhlivansa niin, että Yhdysvallat tuhoutuvat ja julistanut kaivavansa Marilyn Monroen haudastaan. Nämä viestit aiheuttivat sen, että pariskuntaa pidettiin maan turvallisuuden uhkana, eikä heitä päästetty Yhdysvaltoihin. (Järvinen 2014a, 278.)

Vaikka monen tahon tarkoitusperää voidaan pitää hyväntahtoisena, osa tiedosta kerätään laittomuuksien rajoja hipoen ja kansalaisten yksityissuojaa venyttäen (Järvinen 2014a, 30–31). Seuraava kappale käsittelee Yhdysvaltojen Internetin tiedustelua, jota pidetään yhtenä maailman kehittyneimpänä.

3.2 Yhdysvallat Internet-käyttäjien seuraajana

Yksi Yhdysvaltojen tiedusteluorganisaatioista on vuonna 1952 perustettu NSA (National Security Agency). NSA:n tehtäviin kuuluu muun muassa verkkoliikenteen seuraaminen, tiedon kerääminen ja sen analysointi. NSA:n rooli on laajentunut Yhdysvaltalaisessa tiedustelussa Internetin kasvun myötä. NSA:n kannatus kasvoi Yhdysvalloissa 11.9.2001 tehtyjen terrori-iskujen jälkeen. NSA:n roolin kasvaessa vuosien saatossa on sen näkyvyyskin noussut suuremmaksi, ja Snowdenin vuonna 2013 tekemien tietopaljastuksien myötä sen toiminta on noussut huomion keskipisteeksi. (Järvinen 2014a, 32–33, 157.) Snowdenin tietovuodoista on ilmennyt paljon asioita muun muassa NSA:n toiminnan laajuudesta ja sen käyttämistä seurantatekniikoista. (Greenwald 2014, 12–13; Järvinen 2014a, 13–15, 20–21.)

Snowdenin tietopaljastuksissa tuli ilmi monia työkaluja, jotka auttoivat NSA:ta keräämään ja analysoimaan tietoa, kuten DNI Presenter -ohjelma, PRISM-vakoiluohjelmisto ja Xkeyscore-hakuohjelmisto (Järvinen 2014a, 22–23, 71, 74–75; Loshin 2013, 1; The Guardian 2013). DNI Presenter -ohjelmalla oli mahdollista lukea esimerkiksi sähköposteja ja Facebookin sisällä käytyjä ihmisten välisiä kahdenkeskisiä chat-keskusteluja (Järvinen 2014a, 75). PRISM-vakoiluohjelmaa pidettiin yhtenä tärkeimmistä tietolähteistä, joka mahdollisti NSA:lle pääsyn esimerkiksi Microsoftin, Yahoon, Googlen, Facebookin, Skypen ja Applen palvelinten tiedostoihin, joista he pystyivät keräämään palveluiden käyttäjien tietoja omiin tarpeisiinsa. Kaikki yritykset ovat kiistäneet julkisuudessa antaneensa NSA:lle mahdollisuuden päästä palvelimilleen ja väittäneet olleensa PRISM-ohjelmasta täysin tietämättömiä. (Greenwald 2014, 138–141; Järvinen 2014a, 22–23, 71; Loshin 2013, 1.) XKeyscore-hakuohjelma on hakuohjelma, joka kerää yhteen eri lähteistä kerätyt tiedot, kuten sähköposteista, Internet-sivustojen historioista, chat-keskusteluista ja muista Internet-toimista. Kerätyistä tiedoista voidaan hakea tietoa käyttäen hakukriteereinä muun muassa IP-osoitetta, sähköpostiosoitetta, nimeä, kieltä, maata, osoitetta, puhelinnumeroa tai selaimen merkkiä. (Greenwald 2014, 182–190; Järvinen 2014a, 74; The Guardian 2013.) Yhdysvallat on antanut muillekin maille, kuten Saksan tiedusteluorganisaatioille ja Ruotsin signaalitiedustelulle (FRA) mahdollisuuden käyttää Xkeyscore-hakuohjelmaa (Järvinen 2014a, 128, 145).

NSA:n tiedetään myös asentaneen vakoiluohjelmia eri valmistajien reitittimiin ja mahdollisesti myös kovalevyihin. Vakoiluohjelmien asentaminen voi tapahtua tehtaalla, varastossa tai kuljetus- ja logistiikkayritysten avulla, jolloin NSA:n on mahdollista päästä esimerkiksi yritysten sisäiseen Internet-verkkoon, kun laite otetaan käyttöön. (Greenwald 2014, 177–179; Järvinen 2014a, 88–90.) Vastaavanlaista tapaa on käytetty esimerkiksi Yhdysvaltojen seuratessa Kiinan yliopistoverkkojen Internet-toimintaa (Järvinen 2014a, 139).

Yksi Yhdysvaltojen tiedusteluorganisaatioiden tavoitteista on torjua terrorismia. Yhdysvallat on kertonut torjuneensa tiedustelunsa ansiosta 54 iskua vuoden 2001 terroriiskujen jälkeen (Elliott & Meyer 2013). Iskuista osa on ollut mahdollisesti todellisia uhkia, mutta joidenkin iskujen torjumista voidaan pitää kyseenalaisena, kuten sodan aloittaminen Irakissa vuonna 2003, koska Irakissa epäiltiin olevan laittomia aseohjelmia.

Tiedusteluorganisaatioiden mukaan Irakin laittomista aseohjelmista oli täysin varmaa tietoa, mutta sodan lopputuloksena oli yli 4 000 kuollutta Yhdysvaltojen sotilasta, yli 100 000 kuollutta irakilaista ja totuus siitä, ettei mitään laittomia aseohjelmia löytynyt-kään. Yhdysvalloissa on vuoden 2001 jälkeen tapahtunut yksi terrori-isku, joka on vaatinut ihmishenkiä. Kyseinen terrori-isku tapahtui vuoden 2013 Bostonin maratonissa, jossa Tsarnajevin veljekset räjäyttivät kaksi omatekoista pommia katsomossa vahingoittaen 264 ihmistä ja surmaten kolme. Yhdysvallat oli saanut Venäjän FSB:ltä (Venäjän federaation turvallisuuspalvelu) vihjeen vanhemman veljen kytköksistä radikaaliin äärislamilaisjärjestöön, mutta siitä huolimatta isku onnistui, koska Yhdysvaltojen tiedusteluorganisaatiot eivät nähneet hänessä mitään epäilyttävää. (Järvinen 2014a, 165–169.)

Yhdysvalloilla ei ole lain mukaan oikeutta seurata omien kansalaistensa viestintää. NSA:n tulkinnan mukaan tämä tarkoittaa sitä, että jos Internet-yhteyden toinen osapuoli on vähintään 51 prosentin todennäköisyydellä maan rajojen ulkopuolella, viestintää saa seurata. (Järvinen 2014a, 68.) NSA:n toiminta vaikuttaa myös monen suomalaisen Internetin käyttöön. Suuri osa palveluistamme sijaitsee Yhdysvalloissa, kuten Google, Facebook ja Twitter, mutta myös osa liikenteestämme ohjataan Yhdysvaltojen läpi, vaikka emme olisikaan yhteydessä Yhdysvalloissa olevaan palveluun (Järvinen 2014a, 66, 68). Tämä johtuu siitä, että monella mantereella on nopeimmat yhteydet Yhdysvaltoihin, jolloin yhteyden on nopeampi mennä Yhdysvaltojen kautta, vaikka etäisyys Yhdysvaltojen kautta olisikin paljon pidempi (Järvinen 2014a, 66). Tästä syystä monen suomalaisenkin Internet-toimintaa voidaan seurata NSA:n toimesta.

NSA:n arvellaan keräävän Internet-liikenteestä vuorokaudessa noin 29 000 teratavua tietoa, joka käsittää 1,6 prosenttia koko maailman Internet-liikenteestä vuorokaudessa. Prosenttiluku voi kuulostaa pieneltä, mutta koska Internetissä liikkuvasta tiedosta yli 95 prosenttia on sellaista, mikä ei välttämättä NSA:ta kiinnosta, kuten YouTuben videoiden katsomista. Tästä syystä ei NSA:n edes tarvitse yrittää seurata kaikkea Internet-liikennettä. (Järvinen 2014a, 76.) Noin 90 prosenttia NSA:n keräämistä tiedoista on tavallisten Internet-käyttäjien, joita voidaan pitää niin sanotusti sivullisina ja viattomina, mutta NSA säilyttää tietoja käyttääkseen niitä mahdollisesti myöhemmin (Digitoday 2014; Järvinen 2014a, 274).

Yhdysvaltojen ja muiden valtioiden tiedusteluorganisaatioiden levitessä päivittäisiin Internet-palveluihimme on Suomessa tiedustelu pysynyt vähäisenä. Seuraava kappale käsittelee tiedustelua Suomessa ja miten tiedustelu kohdistuu Suomen kansalaisiin.

3.3 Internetin käytön seuranta Suomessa

Suomella ei ole vastaavanlaista tiedusteluorganisaatiota käytössä kuin esimerkiksi Yhdysvaltojen NSA. Suomella ei ole ulkomaalaista tiedustelutoimintaa, vaan Suomen tiedustelu perustuu naapurivaltioiden kuunteluun radioteitse ja yhteistyönä ulkomaalaisten tiedustelupalveluiden kanssa. Suomella ei myöskään ole tällä hetkellä käytössä laajaa Internetin valvontaa. (Järvinen 2014a, 306, 309.)

Vuonna 2009 Suomessa täydennettiin vuoden 2004 tietosuojalakia niin sanotulla Lex Nokia -lainsäädöksellä, joka antaa työnantajalle oikeudet käsitellä yrityksen tietokoneelta lähetettyjen sähköpostiviestien tunnistamistietoja (HE 48/2008). Vuonna 2015 Suomeen on tulossa uusi Tietoyhteyskuntakaari-lakisäädös, joka ei näillä näkymin tuo suuria muutoksia Internetin valvontaan, mutta sen on tarkoitus selkeyttää lainsäädäntöä ja lisätä Internet-käyttäjien yksityisyyden suojaa esimerkiksi luottamuksellisiin viesteihin sosiaalisessa mediassa (Valtioneuvosto 2014). Tietoyhteyskuntakaari-lakisäädös saattaa vielä muuttua, ja vielä on epäselvää, tuleeko Lex Nokia -lakitäydennys pysymään uudessa Tietoyhteyskuntakaari-lakisäädöksessä. Lex Nokia -lakitäydennys on aiheuttanut paljon keskustelua työntekijöiden yksityisyyttä koskien, mutta tämän hetkisillä ennakkotiedoilla se pysyy uudessa lakisäädöksessä. (Lehto 2013; Sajari 2008; Valtioneuvosto 2014.)

Suomen tiedustelun minimaalinen luonne ei poista sitä mahdollisuutta, ettei muiden maiden tiedustelu voisi valvoa Suomea ja sen kansalaisia, minkä myös ulkoministeriö sai huomata vuonna 2013. Suomen ulkoministeriöstä löydettiin lokakuussa 2013 vieraan valtion vakoiluohjelma, joka oli ottanut ulkoministeriön Internet-verkon täysin hallintaansa ja valvonut ulkoministeriön toimintaa neljän vuoden ajan. Kyseinen tapaus paljastui vasta, kun ystävämielinen valtio antoi vinkin asiasta. (Järvinen 2014a, 307–308.) Kyseinen ystävämielinen valtio on voinut olla Ruotsi, jonka vuoden 2007 lakimuutos antoi Ruotsin FRA:lle luvan kuunnella rajat ylittävää teleliikennettä. Tämä tele-

liikennettä koskeva laki kattaa muun muassa puhelut, tekstiviestit, sähköpostit ja Internet-liikenteen. Tämä tarkoittaa sitä, että vaikka suomalaisten Internetin käyttöä ei valvota Suomessa, sitä valvotaan Suomen rajojen ulkopuolella. Suomen ulkomaanliikenteestä 95-prosenttia kulkee Ruotsin läpi, minkä vuoksi Ruotsi pystyy seuraamaan kaikkia suomalaisia, kunhan vain Internet-liikenteen toinen osapuoli on Suomen rajojen ulkopuolella ja Internet-liikenne menee Ruotsin läpi. (Järvinen 2014a, 140.) FRA:n tiedetään myös tehneen yhteistyötä NSA:n kanssa, jolloin myös NSA:n on mahdollista saada suomalaisten tietoja, vaikka suomalaiset eivät olisi suoraan yhteydessä Internet-palveluihin, joista NSA pystyy keräämään tietoa. (Järvinen 2014a, 145–146.) Valtioiden lisäksi monet yritykset keräävät käyttäjistään tietoa, kuten Google (2014) ja Facebook (2014), joita käsitellään seuraavassa kappaleessa.

3.4 Facebook ja Google tietojen kerääjänä

Monen palvelun käyttäminen voi tuntua toimivan ilmaiseksi, mutta aina asia ei ole näin yksinkertainen. Tämän kaltaisissa palveluissa maksuvälineenä ei toimi raha, vaan esimerkiksi henkilökohtaiset tietomme, joita palvelut keräävät. (Järvinen 2014a, 178.) Hyviä esimerkkejä tästä ovat Google ja Facebook, jotka ovat vuonna 2014 kaksi Suomen ja koko maailman käydyintä Internet-sivua (Alexa 2014). Google (2014) ja Facebook (2014) kertovat avoimesti omissa tietosuojakäytännöissään keräävänsä käyttäjistään tietoa, minkä tavoitteena heidän mukaansa on esimerkiksi palveluiden parantaminen ja mainoksien kohdentaminen.

Facebookin (2014) ja Googlen (2014) palveluiden käyttäjät antavat palveluille henkilökohtaisia tietojaan, jotka palveluiden on helppo ottaa talteen, esimerkiksi rekisteröitymissään tai käyttämällä palveluita. Facebook pystyy keräämään käyttäjistään henkilökohtaista tietoa, koska sosiaalisen median palvelut yleensä perustuvat henkilökohtaisten tietojen ja verkostojen jakamiseen. Harva pystyy käyttämään valehenkilöllisyyttä sosiaalisessa mediassa, koska esimerkiksi Facebookin käyttö perustuu oikeiden henkilötietojen kanssa toimimiseen. (Järvinen 2014a, 273.) Järvisen (2014, 265) mukaan Googlen toiminta on vieläkin laajempaa kuin Facebookin, koska Googlen toiminta on vuosien saatossa laajentunut yli 160 palveluun aina hakukoneesta YouTubeen. Järvinen jopa vertaa Googlen toimintaa kaupalliseksi NSA:ksi, koska moni Googlen palveluista pe-

rustuu juuri tietojen keräämiseen. Google on vuosien saatossa kerännyt hakuhistoriamme lisäksi suojaamattomien wlan-verkkojen dataliikennettä ja tutkinut koneellisesti käyttäjiensä sähköposteja (Järvinen 2014a, 23, 92, 235, 265).

Vaikka olemme valmiita luovuttamaan tietojamme yrityksille, joiden toimintaa pidämme moitteettomana ja joiden palvelut käyttäisivät tietojamme mielestämme oikein, ei se poista mahdollisuutta, jossa jokin toinen taho voisi päästä palvelussa tietoihimme käsiksi. Kyseinen toinen taho voisi käyttää palveluiden keräämiä tietoja omiin tarkoituksiinsa ilman, että palvelut tai me itse tiedämme siitä. Tämä on tapahtunut esimerkiksi kun NSA:n käyttämällä PRISM-vakoiluohjelmalla on päästy Facebookin ja Googlen palvelimille ja jonka toiminnasta eivät palvelut eivätkä käyttäjät tietäneet. (Greenwald 2014, 138–141; Järvinen 2014a, 22, 178.)

Nykypäivänä monien tahojen yrittäessä seurata jokapäiväistä Internetin käyttöämme on hyvä tietää, miten siltä pystyy tarvittaessa suojautumaan ja saamaan haluamansa yksityisyyden (Järvinen 2014a, 173). Seuraava kappale käsittelee Tor-ohjelmistoja, joilla oikein käytettynä voi saavuttaa haluamansa yksityisyyden. Tor-ohjelmistojen käytettävyydestä kertoo paljon se, että Snowdenin tiedetään käyttäneen Tor-ohjelmistoa vuotaessaan salaisia dokumentteja (Finley 2014; Musil 2014). Lisäksi yhdysvaltalainen sotilas Manning on käyttänyt Tor-ohjelmistoa lähettäessään salaisia dokumentteja paljastussivusto Wikileaksille suoraan Yhdysvaltojen armeijan tukikohdasta, jolloin hän on pystynyt kiertämään tukikohdan sisäisen valvonnan (Järvinen 2014a, 63).

4 Tor

Internetin sensuroinnin ja seuraamisen myötä osa käyttäjistä haluaa saada käyttää Internetiä vapaasti. Tästä syystä osa käyttäjistä on alkanut käyttää Toria (The Onion Router), joka antaa mahdollisuuden käyttää Internetiä anonyymisti. Tässä kappaleessa tarkastellaan Torin kehitystä, toimintaa ja käyttöä sekä siihen lukeutuvia ohjelmistoja ja ominaisuuksia.

4.1 Anonymiteetti

Anonymiteetti on tuntemattomuutta tarkoittava käsite (Aikio & Vornanen 2000, 45), jota jo aikoinaan Suomen presidentti Urho Kekkonen on käyttänyt hyödykseen kirjoittaessaan kirjoja ja kirjeitä monilla eri nimimerkeillä, kuten Mies suomalainen ja Esaijas Kohennuskeppi. Jotkin tahot pitävät anonyymiyttä Internetissä uhkana, kun taas toiset pitävät sitä mahdollisuutena sananvapauteen ja yksityisyyteen. (Karhula & Ekholm 2011, 1–2.)

Käyttäjiä on mahdollista tunnistaa Internetissä, jolloin heidän anonymiteettinsä voi olla uhattuna. Käyttäjän tunnistamiseen Internetissä voidaan käyttää muutamia eri tapoja, muun muassa yksilöityä IP-osoitetta, selaimen evästeitä tai järjestelmän profilointia. Käyttäjän yhdistäessä Internetiin palveluntarjoaja jakaa tietokoneelle yksilöidyn IP-osoitteen, jonka avulla tietokone pystytään tunnistamaan Internetissä. IP-osoitteesta voidaan päätellä esimerkiksi tietokoneen sijainti. Jotkin Internet-palvelut tallentavat käyttäjän tietokoneelle istunnoissa käytettäviä evästeitä, jotka sisältävät järjestelmän tunnistamistietoja. Mahdolliset salakuuntelijat voivat kyseisistä evästeistä tunnistaa käyttäjän, joka kirjautuu esimerkiksi sosiaaliseen mediaan tai sähköpostiinsa, vaikka käyttäjä kirjautuisikin palveluihin jostain muualta kuin kotoaan, kuten nettikahvilasta, hotellista tai jonkin toisen henkilön tietokoneelta. Järjestelmien profilointi sisältää tietoja järjestelmästä, esimerkiksi mitä selainta ja käyttöjärjestelmää käytetään, asennetut fontit, lisäosat ja muita ohjelmistoja. (Loshin 2013, 4.)

Jotkin käyttäjät kuvittelevat käyttävänsä Internetiä anonyymisti, kun selaavat Internetiä Google Chrome -selaimen incognito-tilalla tai Mozilla Firefoxin yksityisellä ikkunalla.

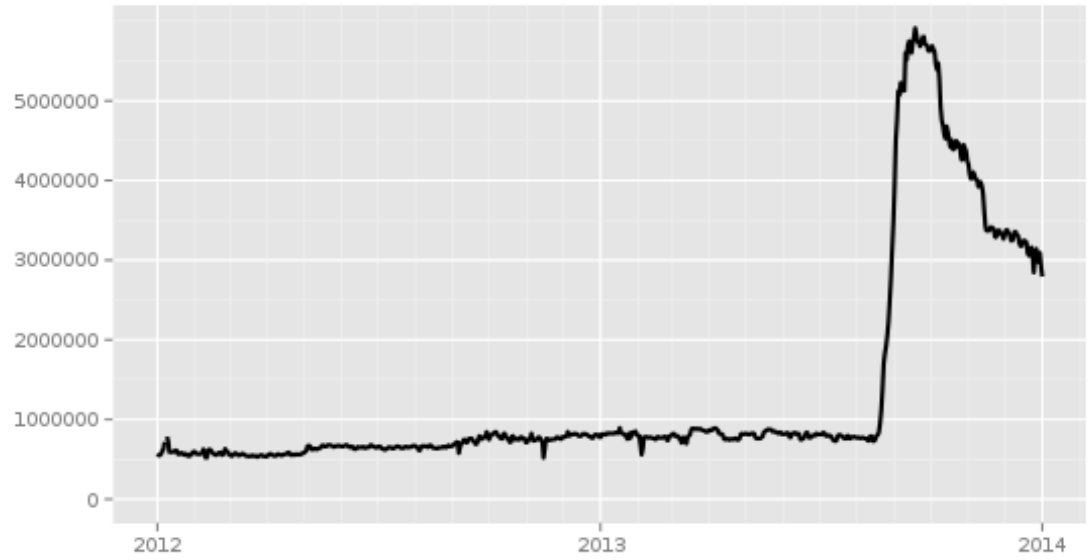
Todellisuudessa näillä selaimen yksityisyystiloilla käyttäjä käyttää Internetiä salaisesti vain lokaalisti, jolloin käytetyltä selaimelta ei nähdä, millä sivustoilla käyttäjä on käynyt, mutta Internetissä yksityisyystilan käyttäjä on yhtä helppo tunnistaa kuin tavallisen selauksen käyttäjät. (Järvinen 2014a, 249–251; Loshin 2013, 1.)

Anonyymit ohjelmistot, kuten Tor, eivät anna kuvitteellista anonymiteettiä niin kuin edellä mainitut yksityisyystilat selaimissa, vaan oikein käytettynä se antaa käyttäjälle mahdollisuuden käyttää Internetiä anonyymisti. Torin käyttö on kasvanut muutamassa vuodessa huomattavasti, ja seuraavassa kappaleessa käsitelläänkin sitä kehittävää Tor-projektia.

4.2 Tor-projekti

Vuonna 1995 Yhdysvaltojen armeija alkoi kehittää Tor-ohjelmistoa, jonka suunniteltiin suojaavan valtion kommunikaatiota. Vuodesta 2001 Torin kehittäminen siirtyi Tor-projektille (Tor Project), joka on kehittänyt Toria vapaana ohjelmistona kaikille Internetin käyttäjille. (Syverson 2005; Tor Project 2014g; Tor Project 2014h.) Tor-projekti toimii suurimmaksi osaksi vapaaehtoistyöllä ja sen toiminta on voittoa tavoittelematonta. Tor-projekti on saanut toimiakseen sponsoritukea muun muassa yli neljältä tuhannelta Internetin käyttäjältä ja monenlaisilta yrityksiltä aina Googlesta Kansalliseen tiedesäätiöön (NSF) (Tor Project 2014i; Tor Project 2014j). Tor-projektin alaisuudessa kehitetään noin kymmentä eri ohjelmistoa, kuten Tor Browseria ja Tailsia, joita käsitellään myöhemmissä kappaleissa (Tor Project 2014k).

Torin kehittäminen ja kasvava suosio perustuu käyttäjien tarpeeseen selata Internetiä veloituksetta anonyymisti ja ilman Internet-sensuurin asettamia rajoja (Loshin 2013, 9). Torin suosio on kasvanut vuosien 2012 ja 2013 välissä huomattavasti, minkä seuraava kuvio osoittaa (Kuvio 3).



Kuvio 3. Torin käyttäjämäärän kehitys vuosina 2012–2013 (Tor Project 2014l)

Kuviosta voi nähdä, kuinka vuoden 2013 puolenvälin aikoihin Torin käyttäjämäärä kasvoi moninkertaisesti alle miljoonasta käyttäjästä yli viiteen miljoonaan käyttäjään. Tähän voi olla monia syitä, mutta Snowdenin vuonna 2013 tekemät salaisten asiakirjojen paljastukset ovat tulleet ilmi käyttäjämäärän kasvun aikoihin (Greenwald 2014, 257, 297), mikä on mahdollisesti saanut käyttäjät hakeutumaan anonyymeihin verkkoihin ja siten käyttämään Toria. Käyttäjämäärän moninkertaisen kasvun jälkeen käyttäjämäärät ovat vähentyneet tasaiseen tahtiin, minkä todellista syytä on vaikea arvata, mutta se voi liittyä mahdollisesti Tor-ohjelmistojen käyttämisen rajoituksiin ja todellisen tarpeen vähyyteen. Toriin ja sen toimintaan tutustutaan tarkemmin seuraavassa kappaleessa.

4.3 Toiminta

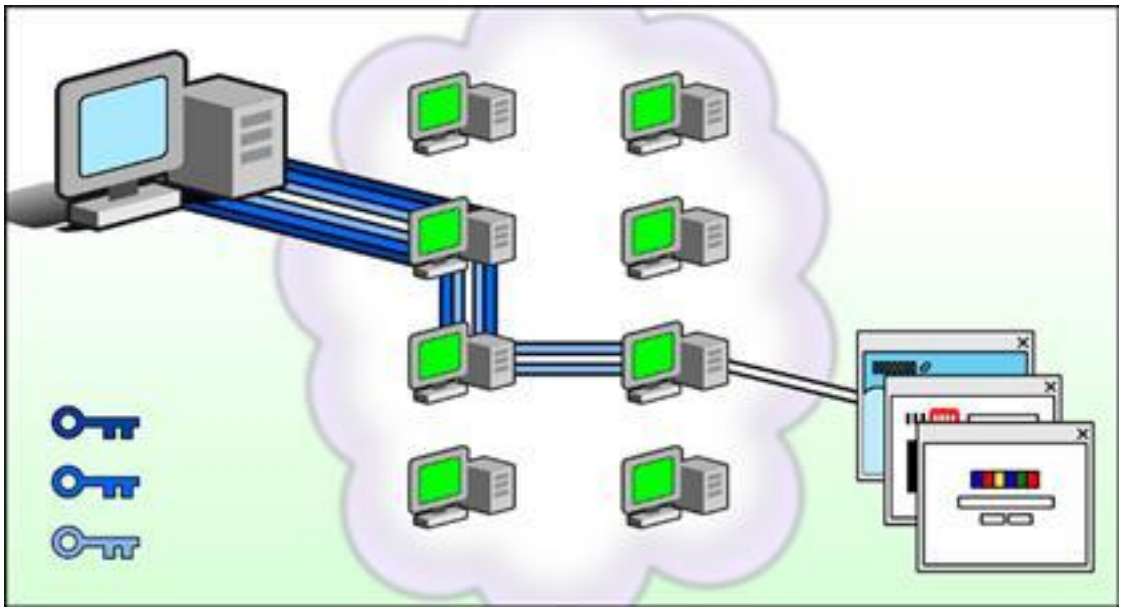
Tor on vapaa ohjelmisto, joka antaa sen käyttäjälle mahdollisuuden käyttää Internetiä anonyymisti ja kiertäen maansa asettaman Internet-sensuurin (Loshin 2013, 5). Tor-verkko rakentuu lähtökohtaisesti välityspalvelimista, joita on tällä hetkellä noin 5 000 (Tor Project 2014l). Näitä välityspalvelimia kutsutaan solmuiksi (node) ja ne luovat yhteyden käyttäjän ja Internet-sivuston välille. Nämä solmut ovat käytännössä tietokoneita, joihin on asennettu Tor-ohjelmisto. Solmut määritetään vastaanottamaan Tor-liikennettä ja lähettämään sitä eteenpäin. Solmuja voidaan myös kutsua nimellä relay. (Järvinen 2014a, 261; Loshin 2013, 5–9.)

Ylläpidetyt solmut voidaan karkeasti jakaa kolmeen eri kategoriaan: transit, exit ja bridge -solmut (nodes). Transit-solmut toimivat Tor-verkossa ensimmäisenä tai toisena solmuna. Exit-solmut voivat toimia Tor-verkossa ensimmäisenä, toisena tai kolmantena solmuna. Bridge-solmun eli sillan tehtävänä on toimia ensimmäisenä solmuna, jos valtio yrittää sensuroida Tor-verkkoa. (Loshin 2013, 5–7, 14–15.)

Osa organisaatiosta on päättänyt yrittää estää Torin käytön. Tor-ohjelmiston luodessa Internet-yhteyttä haetaan julkinen lista kaikista Tor-verkon solmuista. Koska lista on julkinen ja kaikkien haettavissa, voivat organisaatiot hakea listan ja estää listalla olevat solmut. Tällöin Tor-verkkoon yhdistäminen ei onnistu. Tässä tapauksessa Torissa olevat sillat (Bridges Relays tai Bridges) ovat toimiva ratkaisu, koska sillat eivät löydy julkiselta listalta. Sillat ovat piilotettuja solmuja, jotka toimivat kuin transit-solmut. (Loshin 2013, 69–74; Tor Project 2014f.)

Käyttäjän avatessa Internet-yhteyttä Tor-verkkoon käyttäjän Tor-ohjelmisto tarvitsee listan aktiivisista solmuista. Tor-ohjelmisto ottaa Internet-yhteyden Torin hakemistopalveluun (directory service), joka ylläpitää listaa aktiivisista solmuista ja josta Tor-ohjelmisto hakee listan ja valitsee satunnaisesti kolme solmua. Käyttäjän Tor-ohjelmisto myös vaihtaa solmuja noin kymmenen minuutin välein, jolloin Internet-yhteys ei mene koko ajan samojen solmujen läpi. Näin Internet-yhteyttä on vaikeampi seurata ja estää palomuureilla. (Järvinen 2014a, 261; Loshin 2013, 5–9, 14–18, 43.)

Solmujen valinnan jälkeen käyttäjän ottaessa Internet-yhteyttä Tor-verkon läpi Internet-sivustoon Internet-yhteys menee entry-solmuun, joka on Internet-yhteyden ensimmäinen solmu. Entry-solmu ohjaa Internet-yhteyden tämän jälkeen toisen solmun kautta kolmanteen solmuun eli exit-solmuun, josta Internet-yhteys ohjataan käyttäjän haluamalle Internet-sivustolle. Tämä näyttää kyseiselle Internet-sivustolle siltä, että exit-solmu olisi Internet-sivustoon yhteydessä oleva käyttäjä, eikä suinkaan käyttäjä itse. Tämän jälkeen Internet-sivusto lähettää exit-solmulle käyttäjän pyytämät tiedot. (Järvinen 2014a, 261; Loshin 2013, 17–18.) Seuraavasta kuviosta selviää, kuinka Internet-yhteys kulkee käyttäjän tietokoneelta Tor-verkon läpi Internet-sivustolle ja myös kuinka jokaisessa solmussa puretaan yksi salauskerros pois (Kuvio 4).



Kuvio 4. Käyttäjän yhdistäminen Tor-verkon läpi Internet-sivustolle (Tor Project 2014n)

Torin nimi The Onion Router juontaakin juurensa juuri siitä, että Torin sisällä menevää Internet-yhteyden salattuja kerroksia kuoritaan kerros kerrokselta kuin sipulia. Käyttäjältä Tor-verkkoon lähtevä Internet-yhteys on salattu kolmeen kertaa. Jokaisen solmun kohdalla yksi kerros salauksesta puretaan, kunnes salattu Internet-yhteys saapuu exit-solmuun. Tästä eteenpäin ei Tor huolehdi salauksesta. Kun Internet-yhteys tulee takaisinpäin Internet-sivustolta käyttäjälle, liikenne ohjataan ja salataan päinvastaisessa järjestyksessä. Solmut salaavat ne kerrokset, jotka aikaisemmin purettiin, ja liikenne ohjataan exit-solmun kautta keskimmäiselle solmulle. Tästä Internet-yhteys etenee entry-solmuun ja käyttäjälle, minkä jälkeen käyttäjä purkaa kaikkien kerroksien salaukset. (Järvinen 2014a, 261; Loshin 2013, 14–16.)

Internetin käyttö Tor-verkon läpi voi olla hitaampaa kuin ilman Tor-verkkoa. Tämä johtuu Torin toiminnasta, jossa Internet-yhteys ei mene suorinta tietä käyttäjältä Internet-sivustolle niin kuin normaalisti, vaan kiertää kolmen solmun kautta. Internet-yhteys myös salataan aluksi ja sen jälkeen salausta puretaan jokaisella solmulla. Internet-yhteyttä saattaa myös hidastaa se, että solmuilla voi olla muitakin käyttäjiä, joiden liikennettä solmut toimittavat. (Loshin 2013, 33.)

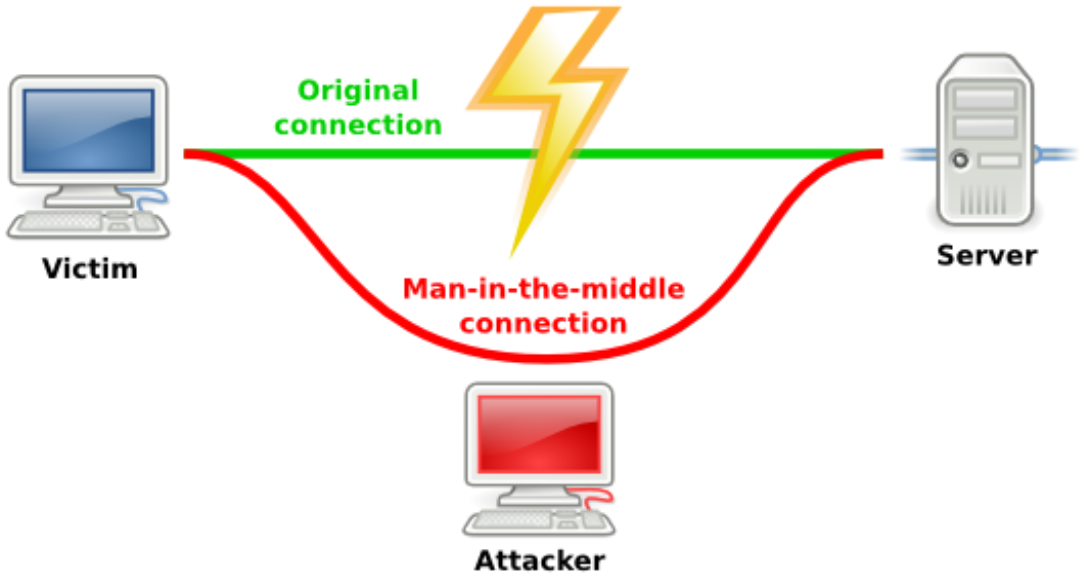
Käyttäjällä on suora Internet-yhteys vain hakemistopalveluun ja entry- tai exit-solmuun, riippuen toimiiko käyttäjä lähettäjänä vai vastaanottajana. Tällöin Internet-yhteys pysyy turvallisena Tor-verkossa, koska ensimmäinen solmu tietää ainoastaan Internet-yhteyden lähtöpisteen ja seuraavan solmun, mutta ei lopullista päämäärää. Toinen solmu tietää ainoastaan, mistä solmusta Internet-yhteys tulee ja mihin solmuun Internet-yhteys on menossa. Kolmas solmu tietää vain lopullisen päämäärän ja toisen solmun, mutta ei Internet-yhteyden alkuperää. Mahdollinen salakuuntelija pystyy näin ollen yhdistämään käyttäjän ja entry-solmun toisiinsa sekä päämäärän ja exit-solmun toisiinsa. Salakuuntelija ei kuitenkaan pysty yhtäaikaisesti yhdistämään, kuka käyttäjä on ja mikä on käyttäjän Internet-yhteyden päämääränsä, elleivät seuraavassa kappaleessa esiteltävät riskit esiinny. (Loshin 2013, 7–9, 16–18.)

4.4 Riskit

Käyttäjän halutessa pysyä anonyyminä vaarantamatta omaa tietoturvallisuuttaan täytyy hänen myös tiedostaa Torin käytössä piilevät riskit. Järvisen (2014, 264) mukaan edes NSA ei ole pystynyt suoraan murtamaan Toria. Tor-ohjelmisto pitää olla asennettu oikein ja asetukset määritelty turvallisiksi, jotta Toria pystytään käyttämään riskittömästi (Loshin 2013, 14). Oletusasetukset Tor-ohjelmissa on määritelty mahdollisimman turvallisiksi ja hyödyllisiksi kehittäjien toimesta. Tästä syystä on suositeltavaa, että käyttäjä pitää asetukset oletuksena, eikä muuttele niitä. (Loshin 2013, 49.) Tor-ohjelmistojen suurimpia riskejä ovat esimerkiksi ”mies välissä -hyökkäys”, kirjautuminen henkilökohtaisiin palveluihin, ladattujen tiedostojen avaaminen, käytettävän tietokoneen tai oheisten ohjelmistojen turvattomuus, ”päästä päähän ajoitus -hyökkäys” ja käyttäjämäärien vähentyminen. Näitä edellä mainittuja riskejä käsitellään seuraavaksi tarkemmin.

Toria käyttäessä täytyy muistaa, että Tor salaa Internet-yhteyden exit-solmuun asti. Tällöin exit-solmun ja päämäärän välillä oleva Internet-yhteys on Torin osalta salaamaton. (Loshin 2013, 12–13; Tails 2014c.) Exit-solmun ja päämäärän välissä olevaan Internet-yhteyteen voidaan tehdä niin sanottu ”mies välissä -hyökkäys” (man-in-the-middle attack), jossa salakuuntelija asettuu Internet-sivuston ja exit-solmun väliin tai exit-solmun ylläpitäjä voi salakuunnella Internet-yhteyttä. Näin kävi vuonna 2007, kun exit-solmun ylläpitäjä ruotsalainen Egerstad onnistui keräämään muun muassa suurlähetystöjen ar-

kaluontoisten sähköpostiosoitteiden käyttäjätunnuksia ja salasanoja. (Tails 2014c; The Sydnet Morning Herald 2007.) Mies välissä -hyökkäyksiä vastaan pystytään suojautumaan käyttämällä salattua HTTPS-protokollaa, jolloin välissä oleva hyökkääjä kuuntelee pelkästään salattua Internet-yhteyttä ja esimerkiksi salasanat eivät päädy hyökkääjälle salaamattomana. (Tails 2014c.) Seuraava kuvio osoittaa miltä ”mies välissä -hyökkäys” näyttää tehtynä tavalliseen Internet-yhteyteen (Kuvio 5).



Kuvio 5. "Mies välissä -hyökkäys" Internet-yhteyteen (Tails 2014c)

Käyttäjän ei suositella kirjautuvan Tor-verkon läpi henkilökohtaisiin palveluihinsa, esimerkiksi sähköpostiin tai sosiaaliseen mediaan, koska näin käyttäjä itse luovuttaa tietonsa mahdolliselle salakuuntelijalle ja vaarantaa oman anonymiteettinsä Tor-verkossa (Loshin 2013, 12–13). Käyttäjän ei myöskään ole suositeltavaa avata ladattuja tiedostoja tietokoneella, joka on yhdistettynä Internetiin, koska kyseiset dokumentit voivat lähettää tunnistettavia tietoja tietokoneesta. (Loshin 2013, 27–28.)

Käytettävää tietokonetta pitää olla turvallista käyttää. Tor koskee vain käyttäjältä exit-solmuun olevaa Internet-yhteyttä, eikä pysty vaikuttamaan siihen, onko käyttäjän tietokone turvallinen. Käyttäjän tietokoneeseen voi olla asennettuna esimerkiksi jokin haittaohjelma, joka valvoo tai estää tietokoneen toimintaa, tai tietokoneessa voi olla keylogger, joka tallentaa kaiken, mitä tietokoneen näppäimistöllä tehdään. (Loshin 2013, 12.)

Joillakin valtioilla tai vastaavilla tahoilla, joilla on paljon valtaa ja resursseja, voi olla mahdollisuus käyttää ”päästä päähän ajoitus -hyökkäystä” (end-to-end timing attack), jossa hyökkääjä voi valvoa käyttäjältä lähtevää Internet-yhteyttä ja saapuvaa Internet-yhteyttä Internet-sivustolle, johon käyttäjä ottaa yhteyttä. Tämän kaltaisissa tilanteissa kyseinen taho voi nähdä, että tietokoneesta on lähetetty saman verran dataa kuin on saapunut Internet-sivustolle. Tästä voidaan päätellä, mihin käyttäjä on ollut yhteydessä, vaikka Internet-yhteys olisikin salattu. (Loshin 2013, 12–13.) Tämän kaltaisia hyökkäyksiä Torin käyttäjiä kohtaan ei ole tullut julki, mutta niiden teoreettinen toteuttaminen on mahdollista.

Toriin liittyvistä sovelluksista voi löytyä mahdollisia riskejä, jotka vaarantavat käyttäjän anonymiteetin ja turvallisuuden. Ohjelmisto Tor Browser ja käyttöjärjestelmä Tails, joita käsitellään tarkemmin myöhemmin, käyttävät selaimenaan muokattua Firefoxia, jonka tiedetään sisältäneen haavoittuvuuksia, joiden avulla NSA on saanut paljastettua Torin käyttäjien oikeita IP-osoitteita. (Järvinen 2014a, 264.)

Riskiksi voi myös nousta Torin käyttäjien väheneminen, koska Torissa käyttäjämäärät avustavat luomaan turvallisen ja anonyymin Internetin käytön (Loshin 2013, 13). Hypoteettisessa tilanteessa, jossa Internetissä olisi kymmenen käyttäjää ja näistä kymmenestä käyttäjästä vain yksi käyttäisi salattua ja anonyymiä verkkoa, ei tämä yksi käyttäjä pysyisi anonyyminä, koska kaikki salattu tiedonsiirto olisi hänen, jolloin tiedettäisiin, mihin käyttäjä on ollut yhteydessä. Ainoana salatun tiedonsiirron käyttäjänä hän myös herättäisi mahdollisten salakuuntelijoiden huomion, jolloin häntä mahdollisesti alettaisiin seurata enemmän kuin muita. Tilanteessa, jossa kaikki kymmenen käyttäjää käyttäisivät salattua Internet-yhteyttä, eivät salakuuntelijat pystyisi tietämään, mikä salattu Internet-yhteys on kenenkin ja mitä Internet-yhteyksien sisällä tapahtuu. (Dingledine & Mathewson 2006, 4–5.) Seuraava kappale käsittelee, kuinka Tor-ohjelmistoja olisi suositeltavaa käyttää, jotta niiden käyttö tapahtuu mahdollisimman turvallisesti.

4.5 Torin käyttäminen

Aikaisemmin käsiteltiin Torin käytössä olevia mahdollisia riskejä, joita käyttäjän on hyvä tiedostaa. Tämän lisäksi käyttäjän on suotavaa tarkastella Internetin käyttötapojaan, jotta Torin käyttäminen tapahtuu turvallisesti. Käyttäjän käyttäessä Tor-ohjelmistoja väärin voi hän esimerkiksi asettaa omat salasanansa tai oman turvallisuutensa vaaraan. Seuraavassa listassa on ohjeita turvalliseen Torin käyttämiseen (Loshin 2013, 12–14, 27–28, 49; Tails 2014c; Tor Project 2014m), joita käyttäjän olisi syytä noudattaa:

- Tor-ohjelmisto on asennettu oikein.
- Käytettävä tietokone on turvallinen, eikä siihen ole asennettu esimerkiksi haitta-ohjelmistoja.
- Torin tai sen osien asetuksia ei suositella muutettavaksi.
- Torrent-tiedostoja ei saa ladata Tor-verkon läpi.
- Torin selaimiin ei saa asentaa lisäosia.
- Selaimen lisäosille, jotka eivät kuulu Tor-ohjelmistoon ei saa antaa toimintalupaa, kuten Flash, RealPlayer ja Quicktime.
- Palveluihin, jotka eivät käytä HTTPS-protokollaa ei saa kirjautua.
- Maissa, joissa Tor on kielletty ohjelmisto, on suositeltavaa käyttää siltoja Internet-yhteyden luomiseksi Tor-verkkoon.

Osalle käyttäjistä voi riittää se, että käyttää Tor-ohjelmia turvallisesti, mutta osa haluaa käyttää Internetiä anonyymisti. Käyttäjän, joka haluaa pysyä Internetissä anonyyminä, on suositeltavaa noudattaa seuraavia ohjeita (Loshin 2013, 12–14, 27–28, 49; Tails 2014c; Tor Project 2014m):

- Käytetään vain Toriin kehitettyjä selaimia esimerkiksi Tor Browseria tai Tailsissä olevaa Iceweasel Web Browser -selainta.
- Ei saa kirjautua henkilökohtaisiin palveluihin, jotka sisältävät käyttäjän henkilökohtaisia tietoja.
- Mitään henkilökohtaisia tietojaan ei saa antaa Internet-sivustoille.
- Vältä Internet-sivustoja, jotka eivät käytä HTTPS-protokollaa.
- Ladattuja tiedostoja ei saa avata niin, että Internet-yhteys on auki.

Torin käyttämisessä on myös hyvä tiedostaa se, että yhdistäessä Internet-sivustolle Tor-verkon läpi voi sivuston latautuminen olla hitaampaa kuin yhdistäessä sivustolle ilman Tor-verkkoa (Loshin 2013, 33). Seuraavassa kappaleessa käsitellään Tor Browseria, joka voidaan asentaa yleisimmille käyttöjärjestelmille.

4.6 Tor Browser

Tor Browser (Tor Browser Bundle tai Bundle) on ohjelmisto, jolla pystytään käyttämään Toria suoraan tietokoneen käyttöjärjestelmässä, kuten Microsoft Windowsissa, Apple OS X:ssä tai Linuxissa (Loshin 2013, 29; Tor Project 2014d). Tor Browser koostuu neljästä pääkomponentista, jotka ovat Vidalia, Tor, Mozilla Firefox ESR ja Torbutton (Loshin 2013, 29; Tor Project 2014c).

Vidalia on ohjauspaneeli Torille. Käyttäjä voi Vidalialla määritellä Torin asetuksia esimerkiksi palomuurien kiertämiseksi tai ylläpitämässään solmussa. Vidalialla käyttäjä pystyy seuraamaan Tor-verkkoa, kuten mitä solmuja Tor-verkossa on ja minkä maiden kautta käyttäjän Internet-yhteys kiertää. Vidalian toimintoihin ei ole välttämätöntä puuttua, mutta se on tällä hetkellä paras tapa tarvittaessa hallita Toria. (Loshin 2013, 29–30; Tor Project 2014b.)

Tor Browserissa Tor on ydinkomponentti, joka hallitsee Tor-verkon yhteyttä. Siihen lukeutuu verkkoon yhdistäminen, solmujen selvittäminen ja valitseminen. Tor toimii taustalla, ja näin ollen käyttäjä ei normaalisti edes huomaa Torin toimintaa. (Loshin 2013, 31.)

Mozilla Firefox ESR (Extended Support Release) on Tor Browserin käyttämä selain (Loshin 2013, 31). Tämä helpottaa monia Tor Browserin käyttäjiä, koska Mozillan Firefox -selain on ollut viimeisen kymmenen vuoden aikana yksi suosituimmista selaimista, joten sen käyttäminen on monille käyttäjille valmiiksi tuttua (Loshin 2013, 49; W3Schools 2014a). Mozilla Firefox ESR on suunniteltu organisaatioille, jotka tarvitseva pidempää tukea, tasapainoisempia päivityksiä ja haluavat muokata selainta tarpeidensa mukaan (Loshin 2013, 31; Mozilla 2014). Tor Browserin mukana on komponentti Tor-

button, jonka tehtävänä on huolehtia sovellustason turvallisuudesta ja yksityisyydestä poistamalla aktiivista sisältöä Mozilla Firefox ESR:ssä (Tor Project 2014a). Mozilla Firefox ESR:n on asennettu HTTPS Everywhere- ja NoScript-lisäosat, jotka lisäävät turvallisuutta. (Loshin 2013, 32).

Tor Browserin asentaminen (liite 1) onnistuu tietokoneen omalle kovalevylle tai ulkoiseen asemaan esimerkiksi USB-muistitikulle. Moni käyttäjä suosiikin ulkoista asemaa, jolloin Tor Browserin käyttäminen onnistuu muilla tietokoneilla helpommin, koska sitä ei tarvitse asentaa aina uudestaan. Riittää, että liittää tietokoneeseen ulkoisen aseman, jossa Tor Browser on asennettuna. Toisena syynä ulkoisen aseman käytön suosioon voidaan pitää sitä, että joissakin maissa Tor Browserin löytymistä tietokoneelta voidaan pitää rikkomuksena. Tällaisissa tilanteissa ulkoisen aseman piilottaminen tai tuhoaminen onnistuu helpommin kuin tietokoneen sisällä olevan kovalevyn. (Loshin 2013, 33.) Sellainen tietokoneen käyttäjä, jolle Tor Browserin tuomat ominaisuudet eivät riitä, voi käyttää Tails-käyttöjärjestelmää, jota käsitellään seuraavassa kappaleessa.

4.7 Tails

Tor Browserin ollessa ohjelmisto, joka voidaan asentaa eri käyttöjärjestelmiin (asennusohjeet liitteessä 2), on Tails itsessään käyttöjärjestelmä, jossa on Tor mukana. Tails on Linux-pohjainen käyttöjärjestelmä, joka on räätälöity Debian-jakelupaketista. Tailsin etuna Tor Browseriin verrattuna on se, että kaikki tietokoneen Internet-liikenne pakotetaan yhdistettäväksi Tor-verkon läpi. Jos Internet-yhteys ei mene Tor-verkon läpi, se estetään. (Loshin 2013, 53–54; Tails 2014a.) Tämä parantaa käyttäjien yksityisyyttä esimerkiksi käyttäjän ladatessa tiedostoja. Tilanteessa, jossa käyttäjä lataa tiedoston käyttäen Tor Browseria, lataaminen tapahtuu Tor-verkon läpi. Käyttäjän avatessa tiedostoa voi tiedosto kuitenkin hakea dataa käytetyltä palvelimelta ilman Tor-verkkoa ja näin paljastaa käyttäjän oikean IP-osoitteen ilman, että käyttäjä itse edes tiedostaa sitä. Tämän kaltainen tilanne ei pitäisi olla mahdollista Tailsillä, koska kaikissa tilanteissa Internet-liikenne ohjataan Tor-verkon läpi. Tails sisältää Unsafe Web Browser -selaimen, joka ei poikkeuksellisesti ohjaa Internet-liikennettä Tor-verkon läpi. Kyseistä selainta voidaan käyttää esimerkiksi Internet-verkoissa, joiden aktivointiin tarvitaan kirjautumi-

nen tai rekisteröityminen, jotta Tails pystyy luomaan Internet-yhteyden Tor-verkkoon. (Loshin 2013, 53–54.)

Tails sisältää tyypillisimmät ominaisuudet, joita käyttäjä voi tarvita, kuten selaimen, sähköpostin, pikaviestinohjelman, toimisto-ohjelmiston, äänieditorin ja kuvankäsittelyohjelman (Tails 2014a). Tailsin selaimena käytetään Iceweaselia, joka on Firefoxista muokattu selain, josta on Tailsissa kaksi eri versiota. Toinen versio on Tor-verkkoa käyttävä Iceweasel Web Browser ja toinen on Unsafe Web Browser, joka ei käytä Tor-verkkoa. Tails sisältää samoja ohjelmistoja kuin Tor Browser, esimerkiksi Torin, Vidalian, Torbuttonin, HTTPS Everywheren ja NoScriptin. Käyttäjien turvallisuuden ja anonymiteetin luomisen takia Tailsistä löytyy muun muassa salaukseen tarkoitettuja sovelluksia, salasanojen generointisovellus sekä hiirellä käytettävä näppäimistö, jos fyysiseen näppäimistöön on asennettu näppäimiä tallentava keylogger. (Loshin 2013, 54–55; Tails 2014b.)

Tailsin eroavaisuus totuttuihin käyttöjärjestelmiin on siinä, ettei sitä ole tarkoitettu asennettavaksi tietokoneen kovalevylle, vaan käyttöjärjestelmää ajetaan reaaliaikaisesti DVD-levyltä, USB-muistitikulta tai SD-muistikortilta. Käyttöjärjestelmän asentaminen siis tapahtuu polttamalla DVD-levylle, asentamalla USB-muistitikulle tai SD-kortille ja käynnistämällä tietokone sitä kautta. Ei ole väliä, mikä käyttöjärjestelmä tietokoneeseen on asennettu, koska Tails ei käytä tietokoneen kovalevyä. Tämä helpottaa käyttöjärjestelmän käyttämistä muillakin tietokoneilla, koska sitä ei tarvitse erikseen asentaa käytetylle tietokoneelle. Normaalisti Tailsia ei asenneta tietokoneen kovalevylle, joten se ei tallenna käytetyn tietokoneen kovalevylle lokeja, evästeitä tai mitään muutakaan, jotka jättäisivät todistusaineistoa sen käytöstä tai käyttötarkoituksesta. Tails käyttää tallennukseen keskusmuistia, joka tyhjennetään tietokoneen sammuessa. Tästä syystä kaikki käyttäjän tekemät muutokset ja lataamat tiedostot poistuvat tietokoneen sammuessa, jolloin uudelleen käynnistettäessä Tails on jälleen oletusasetuksilla. Poikkeuksena tähän on se, että Tails on mahdollista asentaa USB-muistitikulle tai SD-muistikortille, jotta käyttöjärjestelmän muutokset pysyvät tallessa. (Loshin 2013, 56; Tails 2014a). Tailsiin on mahdollista asentaa uusia sovelluksia ja määritellä asetuksia, mutta tämä ei ole suositeltavaa, koska tämä voi tehdä Tailsistä turvattomamman ja uhata käyttäjän yksityisyyttä

(Loshin 2013, 65). Tor-ohjelmistoja käyttävät monenlaiset tahot, joita käsitellään seuraavassa kappaleessa.

4.8 Torin käyttäjäkunta

Torin käyttämistä voidaan pitää vääränä tai rikollisena, koska se antaa käyttäjälle mahdollisuuden kiertää maansa asettamia Internet-sensuureja. Toria voidaan käyttää esimerkiksi siten, että lapsi kiertää vanhempien laittamat estot tai työntekijä menee yrityksensä kieltämille Internet-sivustoille. Tor avaa myös käyttäjilleen mahdollisuuden anonyymisti julkaista materiaalia Internetissä ilman, että lainvalvojat tarkastavat sitä. Joidenkin mielestä Tor on rikollisuuteen tarkoitettu työkalu, mutta asia ei ole aivan näin mustavalkoinen. Yhtälailla henkilö, joka on valmis käyttämään Toria rikollisiin tarkoituksiin, voisi myös olla valmis varastamaan toisen henkilön tietokoneen tai puhelimen ja näin saada saman turvan kuin Tor hänelle antaisi. (Loshin 2013, 18–24.)

Toria käyttävät monet tahot, joiden tarkoituksena ei ole käyttää Toria rikollisiin tarkoituksiin. Journalistit voivat käyttää Toria raportoidessaan paikoista, joissa ei ole turvallista yhteyttä Internetiin tai ollessaan yhteydessä tietolähteeseen, joka haluaa pysyä tuntemattomana. Aktivistit käyttävät Toria toimiessaan ihmisoikeuksien puolesta. Tor antaa tietovuotajille, ilmiantajille ja poliisien tietolähteille mahdollisuuden toimia Internetissä asettamatta itseään vaaraan. Tor-ohjelmistoilla diplomaatit, korkeat tahot ja liikemiehet voivat käyttää Internetiä luotettavasti ilman, että heitä valvotaan valtion tai yhtiöiden puolesta. Yksityiset henkilöt käyttävät Toria, koska he haluavat kiertää maidensa Internet-sensuurin etsiessään esimerkiksi tietoa maansa ihmisoikeuksista tai välttääkseen kohdennetun mainonnan. Toria käyttää mahdollisesti myös Yhdysvaltojen armeija, jonka käyttöön Tor alun perin kehitettiin. Lainvalvojat saattavat myös käyttää Toria salaisissa tutkimuksissaan. Torin laajan käyttäjäkunnan takia on mahdotonta sanoa, onko käyttäjä rikollinen vai esimerkiksi peitetehtävässä oleva viranomainen. (Loshin 2013, 1–3, 18–23; Tor Project 2014e.)

4.9 Sähköpostin käyttäminen anonyymisti

Sähköpostin käyttäminen on yleistynyt Internetin käytön lisääntymisen myötä. Käyttäjä, joka haluaa käyttää Internetiä anonyymisti voi tarvita myös sähköpostin, jota voi käyt-

tää turvallisesti ja anonyymisti. Tähän on muutamia eri tapoja riippuen siitä, mihin tarkoitukseen sähköpostia käytetään. Jokaisessa eri tavassa on samat turvallisen käytön ohjeet. Sähköpostia käytetään aina Tor-verkon läpi myös rekisteröinnissä. Sähköpostipalvelun on oltava luotettava ja siinä on oltava HTTPS-protokolla käytössä. Lisäksi käyttäjän tulee salata kaikki sähköpostiviestinsä ja välttää anonymiteettinsä vaarantuminen siten, ettei anna sähköpostipalvelimelle omia tietojaan, kuten puhelinnumeroaan tai osoitettaan. (Loshin 2013, 110–112.)

Sähköpostin käyttämiseen voidaan käyttää muun muassa kertakäyttöisiä, tavallisia ja piilotettuja sähköpostipalveluja. Vain hetken käytössä olevat kertakäyttösähköpostit toimivat hyvin palveluissa, joissa ei tarvitse kuin hetkellisesti sähköpostia, esimerkiksi kommentoidessa jotakin julkaisua (Loshin 2013, 104–105). Normaalisti käytössä olevia sähköpostipalveluja, kuten Google Gmail tai Yahoo! voidaan käyttää anonyymisti ja luotettavasti, kunhan turvallisen käytön ohjeita noudatetaan (Loshin 2013, 105–107). Piilotettujen palveluiden joukosta löytyy myös sähköpostipalveluita, mutta niiden luotettavuudesta on vaikea mennä takuuseen, siten niiden käyttöä ei suositella, jos ei tiedä sähköpostipalvelun olevan luotettava (Loshin 2013, 108).

Teoriaosuudessa käsiteltiin muun muassa Tor-ohjelmistojen käyttäjämäärän kasvua ja ohjelmistojen tarpeellisuutta. Tor-ohjelmistoille voidaan nähdä tarvetta, kun esimerkiksi Kiina rajoittaa kansalaistensa Internetin käyttöä, tai Yhdysvallat tarkkailee muiden maiden kansalaisia. Tor-ohjelmistojen tarpeellisuutta ja käyttäjämäärien kasvua selvitetään tarkemmin tutkimusosuudessa. Seuraavaksi siirrytään käsittelemään tutkimuksen toteutusta, missä kerrotaan tarkemmin tutkimuksen toteutuksen eri vaiheista.

5 Tutkimuksen toteutus

Tutkimus toteutettiin kaksiosaisena. Tutkimuksen ensimmäinen osa tehtiin laadullisena tutkimuksena, jossa aineisto koostui asiantuntijoille suunnatusta kyselystä. Kyselyn tavoitteena oli saada Internet-sensuurin ja -seurannan sekä Torin nykytilanteesta mahdollisimman kattava kuva. Tutkimuksen toinen osa tehtiin empiirisenä ja niin ikään määrällisenä tutkimuksena, jossa aineisto kerättiin suomalaisilta yksityishenkilöiltä testin muodossa. Torin käyttöönoton testauksen tarkoituksena oli saada käytännön kokemuksia Tor-ohjelmistoista. Testillä selvitettiin lisäksi tavallisen tietokoneen käyttäjän kyvykkyyttä asentaa ja käyttää Tor-ohjelmistoja turvallisesti.

5.1 Asiantuntijakysely

Kysely lähetettiin IT-alan ammattilaisille, joilla on asiantuntijaomaista tietoa Internetin sensuureista, Internetin käyttäjien seuraamisesta Internetissä, Torin ohjelmien käytöstä ja Torin toimivuudesta. Asiantuntijat valittiin eri organisaatioista ja lähtökohdista niin, että Internet-seurannan ja -sensuurin sekä Torin nykytilanteesta saataisiin mahdollisimman monipuolinen näkemys.

Kyselyyn valittiin tietotekniikka-asiantuntija ja tietokirjailija Petteri Järvinen, jonka kirjaa (2014a) käytettiin lähteenä teoriaosuudessa, Effin varapuheenjohtaja Ville Oksanen, F-Securen Security Response -osaston johtaja Antti Tikkanen ja Internet-aktivisti Matti Nikki. Kysymykset lähetettiin myös liikenne- ja viestintäministeriöön, jonka edustajan mukaan vastaukset kerättiin yksittäisiltä virkamiehiltä, ja vastaukset ovat yksittäisten henkilöiden mielipiteitä. Lisäksi yksi kyselyyn valituista asiantuntijoista halusi pysyä tuntemattomana, joten häntä kutsutaan tutkimuksessa Nimettömäksi.

Asiantuntijoille esitetyt kysymykset valikoitiin teoriataustassa käsitellyistä asioista niin, että kysymykset kattoivat Torin käyttöön johtavia syitä ja Torin käytön periaatteita. Asiantuntijoille esitettiin seuraavat kysymykset:

1. Mitä mieltä olet Internet-sensuurista? (esim. onko Internet-sensuurissa hyötyjä tai haittoja, millaista Internet-sensuuri on tulevaisuudessa jne.)

2. Mitä mieltä olet käyttäjien seuraamisesta Internetissä ja siitä, että heistä kerätään tietoa? (esim. onko tietojen keräämisessä hyötyjä tai haittoja, mikä on seuraamisen tuleva suunta jne.)
3. Mitä mieltä olet anonyymeistä verkoista, kuten Torista?
4. Tulevatko Internetin käyttäjät siirtymään enemmän anonyymeihin verkkoihin, kuten Toriin?
5. Onko Torin käytöstä hyötyä tai haittaa?
6. Ovatko Tor-ohjelmistot luotettavia ja antavatko ne toivotun anonymiteetin?
7. Onko Torin käytössä joitain riskejä tai tietoturvauhkia?
8. Sopiiko Tor yksityishenkilön käyttöön ja osaako hän käyttää Toria turvallisesti?

Kysely toteutettiin sähköpostiviestien välityksellä, jotta vastaukset välittyivät tutkimukseen mahdollisimman muuttumattomina ja asiantuntijat pystyivät vastaamaan kyselyyn oman aikataulunsa mukaisesti. Samat kysymykset esitettiin kaikille asiantuntijoille, jotta jokaiseen kysymykseen saataisiin mahdollisimman monipuolinen perspektiivi. Tutkimusten tuloksiin koottiin kyselyn vastauksista keskeisimmät asiat (vastaukset löytyvät kokonaisuudessaan liitteestä 6).

Seuraavassa kappaleessa kerrotaan, miten tutkimustuloksien taustalla olevat testit toteutettiin.

5.2 Torin käyttöönoton testaus

Tässä kappaleessa käydään läpi Tor-ohjelmistojen käyttöönoton testauksen toteuttamista. Tutkimuksessa toteutettiin testausosio, jotta saatiin käsitys tavallisen tietokoneen käyttäjän kyvystä asentaa Tor-ohjelmistoja ja käyttää niitä turvallisesta. Lisäksi kerättiin testihenkilöiden mielipiteitään kyseisistä ohjelmistoista. Kappaleissa käsitellään testauksen toteutuksen yleisiä asioita, testin eri osiot ja testihenkilöihin liittyvät valintakriteerit.

5.2.1 Testi yleisesti

Testi jaettiin viiteen erilliseen osioon: Tor Browserin asentaminen, Tails-käyttöjärjestelmän asentaminen, Tor-ohjelmistojen turvallinen käyttäminen, käyttöjakso ja palaute. Testissä havainnoitiin testihenkilöiden kykyä asentaa Tor-ohjelmistoja ja

käyttää niitä turvallisesti. Testihenkilöiltä kerättiin myös palaute Torin käytöstä ja siitä, näkevätkö he Tor-ohjelmistot hyödylliseksi ja tulevatko he käyttämään niitä vastaisuudessa.

Testiin osallistui viisi henkilöä. Testi toteutettiin yksitellen jokaiselle testihenkilölle, jolloin testihenkilöiden valvominen ja tulosten kerääminen testistä oli helpompaa. Testihenkilöt toimivat osioissa omatoimisesti, eivätkä he saaneet ohjeistusta osioita tehdessään. Testin alussa testihenkilöille annettiin testiohjeet, joiden mukaan testihenkilöiden tuli toimia (liite 4). Testin osioissa testihenkilöitä ei perehdytetty mitenkään, vaan he toimivat testeissä täysin omien taitojensa ja tietojen mukaan, jolloin testistä saatiin luotettavampi ja että testitulokset kuvastavat normaalin tietokoneen käyttäjän käyttötaitoja.

Tilanteessa, jossa testihenkilö ei onnistunut toteuttamaan jotakin testin osiota, testin teettäjä ohjeisti testihenkilöä eteenpäin, jolloin tämä testin osio merkittiin epäonnistuneeksi. Testin osiot toteutettiin kokonaisuuksina, poikkeuksena testin ensimmäinen ja toinen osio, jotka toteutettiin yhtenä kokonaisuutena. Osiokokonaisuuksien jälkeen testihenkilölle kerrottiin hänen mahdollisesti tekemänsä virheet ja testihenkilöä opastettiin tarvittaessa niin, että mahdolliset virheet eivät aiheuta vaaratilanteita myöhemmin. Tilanteessa, jossa testihenkilön toimet saattoivat aiheuttaa yhtäkkisen vaaratilanteen, oli testin teettäjä velvollinen toimimaan testihenkilön hyväksi, jotta vaara vältettiin. Vaaratilanteiksi laskettiin esimerkiksi tilanteet, joissa testihenkilön salasana oli uhattuna tai testihenkilö käytti tietokonetta niin, että tietokone vioittuisi. Mahdolliset vaaratilanteet tai virheelliset toimet otettiin tutkimuksessa huomioon.

5.2.2 Tor-ohjelmistojen asentaminen

Testin ensimmäisessä osiossa testihenkilöt asensivat Tor Browser -selaimen tietokoneelleen ja menivät Tor Browseria käyttäen Tor-projektin Internet-sivustolle. Osiossa havainnoitiin selaimen lataamista sekä sen eheyden tarkistamista ja onnistunutta käynnistämistä (liite 1). Testin ensimmäisestä osiosta saatiin tietoa testihenkilöiden kyvykkyydestä asentaa Tor Browser tietokoneelle turvallisesti, joka on lähtökohtana Tor Browserin turvalliseen käyttöön Internetiä selatessa.

Toisessa osiossa testihenkilöt asensivat Tails-käyttöjärjestelmän tyhjälle DVD-levylle ja käynnistivät Tails-käyttöjärjestelmän. Käyttöjärjestelmän käynnistyksen jälkeen testihenkilöt tekivät tarvittavat toimenpiteet, jotta he pystyivät käynnistämään Iceweasel Web Browser -selaimen ja menemään onnistuneesti Tor-projektin Internet-sivustolle. Osiossa havainnoitiin Tails-käyttöjärjestelmän lataamista, eheyden tarkistamista, DVD-levylle polttamista, käynnistämistä ja onnistunutta käyttämistä niin, että testihenkilöt pääsivät Internetiin (liite 2). Tails asennettiin tyhjälle DVD-levylle, eikä USB-muistitikulle sen takia, koska Tailsin kehittäjät suosittelevat tätä toimenpidettä (Tails 2014d). Osiossa ei myöskään tarjota tyhjiä DVD-levyjä testihenkilöille, elleivät he erikseen sitä pyydä. Testin toisessa osiossa saatiin tietoa testihenkilöiden kyvykkyydestä asentaa Tails-käyttöjärjestelmä ja ottaa se käyttöön tietokoneelle turvallisesti, mikä on lähtökohtana Tails-käyttöjärjestelmän turvalliselle käytölle. Tor Browser -selain ja Tails-käyttöjärjestelmä valittiin asennettaviksi ohjelmistoiksi, koska ne ovat ainoat tietokoneohjelmistot, jotka soveltuvat Internetin käyttämiseen Tor-verkon läpi.

5.2.3 Tor-ohjelmistojen turvallinen käyttäminen

Kolmannessa osiossa testihenkilöiltä selvitettiin Torin turvalliseen käyttöön liittyviä asioita. Osiossa otettiin selvää siitä, tiedostavatko testihenkilöt Torin käytössä piileviä riskejä, tietävätkö he entuudestaan joitain turvallisuusohjeita, löytävätkö he turvallisen käytön ohjeet Internetistä ja ymmärtävätkö he turvallisen käytön ohjeet sekä osaisivatko he käyttää Toria turvallisesti.

Testihenkilöiltä kysyttiin Tor-ohjelmien asennuksen jälkeen, olisivatko he tiedostaneet Tor-ohjelmien mahdollisia riskejä ja tiesivätkö he turvallisen käytön ohjeita. Testihenkilön tietäessä tiettyjä turvallisen käytön ohjeita entuudestaan näitä verrattiin turvallisen käytön ohjeissa oleviin kohtiin (liite 5). Tämän jälkeen testihenkilö etsi listaa turvallisen käytön ohjeista Internetistä. Tilanteessa, jossa testihenkilö ei löytänyt turvallisen käytön ohjeita, hänet opastettiin Tor-projektin Internet-sivustolle, jolta ohjeet löytyvät. Testihenkilöltä kysyttiin kohta kohdalta, ymmärsikö hän, mitä ohjeissa neuvottiin ja miten niitä noudatettiin. Testihenkilö vastasi kysymyksiin suullisesti. Kolmannella osiolla saatiin tietoa siitä, osaisivatko testihenkilöt käyttää turvallisesti Tor-ohjelmistoja ennen neljännen osion omatoimisen käyttöjakson aloittamista.

5.2.4 Käyttöjakso ja palautteen kysymykset

Neljäs osio tapahtui testihenkilöiltä itsenäisesti. Osiossa testihenkilöt käyttivät Tor-ohjelmistoja kahden päivän ajan. Kahden päivän käyttöjakson aikana testihenkilöt noudattivat turvallisen käytön ohjeita päivittäisessä Internetin käytössään (liite 5). Kyseinen osio toteutettiin siksi, että testihenkilöt saivat käyttökokemuksia Tor-ohjelmistoista vastatakseen viidennen osion palautteeseen. Käyttöjakson aikana testihenkilöjä suositeltiin pitämään muistiinpanoja viidennen osion kysymyksiä koskien, jotta palautteeseen saatiin kattavat mielipiteet käyttöjaksolta.

Käyttöjakson jälkeen testihenkilöt vastasivat viidennen osion kysymyksiin (liite 4) kirjallisesti (vastaukset löytyvät kokonaisuudessaan liitteestä 7).

Osiot järjestettiin kyseiseen järjestykseen, jotta jokaisesta osiosta saatiin luotettavat tulokset. Testihenkilö asensi ensimmäisessä osiossa Tor-ohjelmistoja ja avasi Tor-ohjelmistoilla ensimmäiset Internet-sivut, jolloin vähäinen käyttökokemus oli jo saavutettu. Tämän jälkeen saatiin selvitettyä ymmärtäisikö testihenkilö, että Tor-ohjelmistoja pitäisi käyttää turvallisten käytön ohjeiden mukaisesti. Näin myös varmistettiin turvallinen käyttöjakso. Käyttöjakson aikana testihenkilöille muodostui mielipide Tor-ohjelmistoista, joten käyttöjakson jälkeen palautteesta saatiin mahdollisimman totuudenmukainen. Koko testin tavoitteena oli saada kattava kokonaiskuva testihenkilöiden kyvystä asentaa Tor-ohjelmistoja ja käyttää niitä turvallisesti sekä saada heidän mielipiteensä ohjelman toimivuudesta.

5.2.5 Testihenkilöt ja laitteisto

Valitsin lähipiiristäni viisi henkilöä, jotka olivat iältään 26- ja 27-vuotiaita ja täyttivät tietyt kriteerit. Testihenkilöt on valittu ikäluokasta 18–34, sillä se on aktiivisin Internetin käyttäjäryhmä (Lebo 2013, 20; Statista 2011; Statista 2014). Testihenkilöt valittiin niin, että heidän tietokoneen käyttötaitoaan voitiin pitää keskivertona, esimerkiksi testihenkilöt eivät työskennelleet IT-alalla tai eivät ole saaneet IT-alan koulutusta, mutta käyttivät tietokonetta lähes päivittäin. Testihenkilöt eivät olleet käyttäneet aikaisemmin Tor-ohjelmistoja, mutta olivat saattaneet kuulla niistä. Testihenkilöiden valintakriteeri-

nä oli myös oma tietokone, jossa on Windows-käyttöjärjestelmä. Testihenkilöillä täytyi olla oma tietokone sen takia, että testihenkilöt käyttivät testissä omaa konettaan, jotta testissä käytetyn tietokoneen käyttö oli tuttua, jolloin testeissä saadut tuloksetkin olivat myös luotettavampia. Testihenkilön oma tietokone luonnehti myös aidompaa tilannetta, koska todellisessakin tilanteessa testihenkilöt käyttäisivät oletuksena omaa tietokonettaan ottaessaan käyttöön Tor-ohjelmistoja. Testissä käytetyissä tietokoneissa oli myös jokin Windows-käyttöjärjestelmä, mikä on valittu sillä perusteella, että Internetissä käytetyistä käyttöjärjestelmistä yli 80 prosenttia on Windows-käyttöjärjestelmiä (W3Schools 2014b). Loshinin (2013, 53) mukaan Tailsin käyttämistä tulisi välttää Applen tietokoneilla, koska se saattaa olla ajoittain ongelmallista. Tästä syystä testissä ei edes harkittu Applen OS X -käyttöjärjestelmän käyttämistä, joka olisi ollut toiseksi suosituin käyttöjärjestelmä tietokoneissa (W3Schools 2014b). Testihenkilöiden tietokoneessa täytyi myös olla polttava DVD-asema, jotta Tailsin polttaminen DVD-levylle oli mahdollista. Jokaista testihenkilöä kohden oli varattu yksi tyhjä DVD-levy.

6 Tutkimuksen tulokset

Asiantuntijoiden vastaukset ja testin tulokset on kerätty tähän kappaleeseen. Käsittelen ensiksi asiantuntijoiden vastaukset ja sen jälkeen Torin käyttöönoton testauksen tulokset.

6.1 Asiantuntijakyselyn tulokset

Tähän kappaleeseen on koottu asiantuntijoille suunnatun kyselyn keskeisiä asioita liittyen tutkimukseen (asiantuntijoiden vastaukset löytyvät kokonaisuudessaan liitteestä 6).

6.1.1 Internet-sensuuri

Yksikään asiantuntijoista ei selkeästi kannattanut Internet-sensuuria. Suuri osa asiantuntijoista oli sitä mieltä, että Internet-sensuurin hyödyt ovat pienet, koska kunnollista Internet-sensuuria on vaikea toteuttaa ja sen kiertäminen on helppoa, esimerkiksi Oksanen viittasi siihen, että Internetin käyttäjä pääsee halutessaan Kiinankin hyvin tehokkaasta palomuurista läpi. Nikin mielestä Internet-sensuurin kasvaminen saattaisi johtaa Internetin pirstaloitumiseen, jossa Internet ei ole enää neutraali ja kaikille samalla lailla toimiva kommunikaatioväline. Internet-sensuurin nähtiin sensuroivan monia Internet-sivustoja, joiden ei tarvitsisi olla sensuroituna. Liikenne- ja viestintäministeriön mukaan Internetin käytön pitäisi olla mahdollisimman vapaata, mutta voi olla tilanteita, joissa Internetin käyttöä voidaan perustellusti rajoittaa.

Osa asiantuntijoista oli sitä mieltä, että tulevaisuudessa Internet-sensuuri saattaa kasvaa ympäri maailma, jopa EU-maiden alueilla, mutta Internet-sensuurin tulevaisuuden suuntaa on vaikea ennustaa. Järvisen mielestä parasta sensuuria olisi itsesensuuri, jossa Internet-käyttäjä itse miettisi omaa toimintaansa ja sitä, kannattaako kaikkea julkaista Internetissä, vaikka siihen olisikin mahdollisuus.

6.1.2 Internet-käyttäjien seuraaminen

Oksanen totesi vastauksessaan, että osa Internet-palveluista perustuu käyttäjiltä kerättävien tietojen taloudelliseen arvoon, nimittäin palvelun ollessa maksuton on käyttäjä

palvelun tuote. Moni Internet-käyttäjä saattaisi pitää tätä Internetin seurantaa ja tiedonkeräämistä hyvänä asiana, koska se auttaisi parantamaan käyttäjien käyttämiä palveluita. Osa Internetin käyttäjistä ei kuitenkaan haluaisi, että heidän Internetin käyttöään seurataan. Liikenne- ja viestintäministeriön mukaan Suomen perustuslaki edellyttää, että jokaisen ihmisen yksityiselämä ja luottamuksellinen viestintä pitää olla turvattuna. Koska osa Internetin käyttäjistä hyväksyy tiedon keräämisen ja osa ei, pitäisi Internetin käyttäjillä olla mahdollisuus valita, saako häntä seurata vai ei. Nikin mielestä Internet-käyttäjiin kohdistuva seuranta on yksityisyyden loukkaamista, ja Tikkasen mukaan seuranta lisää tietoturvariskejä. Toisaalta Liikenne- ja viestintäministeriö ja Nimetön pitävät seurantaa joidenkin palveluiden osalta tiettyyn pisteeseen saakka tarpeellisena, koska osa palveluista vaatii seurantaa toimiakseen. Internetin seuraamisen ja tietojen keräämisen tulevaisuuden tulee näyttämään se, kiinnostaako Internetin käyttäjiä oman yksityisyyden suojaaminen vai ei. Nikki totesi myös, kuinka valtiollisella tasolla esimerkiksi NSA on hyödyntänyt palveluiden käyttämiä seurantamekanismeja. Tikkasen mielestä ennen Snowdenin tietopaljastuksia moni Internet-käyttäjä luuli käyttävänsä Internetiä anonyymisti, kunnes esimerkiksi NSA:n todellinen kyky seurata Internet-liikennettä tuli julki. Nikki kertoi, että esimerkiksi Tor-ohjelmistojen käyttäminen lienee vastareaktio konkreettisiin oikeudenloukkauksiin ja uhkiin. Liikenne- ja viestintäministeriön mukaan kehityksen mahdollisen jarruttamisen sijaan tulisi keskittyä ilmiön sekä sen avaamiin mahdollisuuksien ja riskien ymmärtämiseen. Seuraavassa kappaleessa käsitellään asiantuntijoiden näkemyksiä Torin hyödyistä ja haitoista.

6.1.3 Torin hyödyt ja haitat

Asiantuntijat pitivät Torin kaltaisia ohjelmistoja lähes välttämättöminä, koska Internet-käyttäjillä on hyvä olla mahdollisuus käyttää Internetiä anonyymisti. Liikenne- ja viestintäministeriön mukaan anonymiteetin tulisi olla yhteiskunnassa sallittua. Ihmisellä on esimerkiksi oikeus kävellä anonyymisti kaduilla ja tehdä ostoksia, niin miksei samantasoista oikeutta olisi myös Internetissä. On toki ymmärrettävää, että joissakin luottamuksellisissa asioissa anonymiteettiä ei sallita. Asiantuntijoiden mielestä Torin käyttämisen hyötynä voidaan pitää sitä, että joillakin Internetin käyttäjillä voi olla tarve käyttää Internetiä anonyymisti ja suojata oma identiteettinsä. Internetin käyttäjät voivat esimerkiksi anonyymeinä ilmaista mielipiteitään, tutkia tai julkaista arkaluontoista ai-

neistoa. Tikkanen myös mainitsi, että osa Internetin käyttäjistä voi tarvita Tor-ohjelmistoja työssään tutkiessaan esimerkiksi haittaohjelmia ja rikollisten toimintaa.

Torin käyttäjiin kohdistuvana haittana pidettiin sitä, että käyttäjä voi asettaa itsensä vaaratilanteeseen, jos käyttäjä ei tiedosta Torin käytön riskejä ja sitä, mihin Tor pystyy ja mihin ei. Oksanen myös pohti, että Tor-ohjelmistojen käyttäminen saattaisi herättää huomiota ja Internetin käyttäjä voisi joutua esimerkiksi NSA:n tarkkailun kohteeksi. Yhteyskunnallisena haittana Torin käytössä pidettiin laittomuuksien kasvamista liittyen esimerkiksi lapsipornoon tai huumekauppaan. Sitä ei pidetty niin suurena riskinä, koska isoimpiin tekijöihin voidaan päästä käsiksi muuta kautta, ja tällä hetkellä laittomuuksien määrä on pysynyt suhteellisen pienenä. Tikkanen piti Toria monikäyttöisenä työkaluna, jota pystytään käyttämään sekä hyvään että pahaan. Seuraavaan kappaleeseen on koottu asiantuntijoiden mietteitä koskien Tor-ohjelmistojen turvallisuutta.

6.1.4 Tor-ohjelmistojen turvallisuus

Järvinen piti Toria tällä hetkellä kaikkein luotettavimpana tapana säilyttää oma anonymiteettinsä, ja muidenkin asiantuntijoiden mielestä Tor-ohjelmistoilla voidaan tehokkaasti ja luotettavasti suojata Internetin käyttäjän identiteetti. Joidenkin asiantuntijoiden mielestä tarpeeksi kiinnostavia Tor-ohjelmistojen käyttäjiä voidaan mahdollisesti jäljittää muulla tavoin, kuten selaimen haavoittuvuuksia hyödyntämällä. Tästä huolimatta normaaleille Internetin käyttäjille Toria pidettiin tehokkaana ja turvallisena työkaluna, mutta joissakin tapauksissa tulisi huomioida, keneltä suojaudutaan ja miksi, koska esimerkiksi Tikkasen mukaan täydellistä suojaa on mahdotonta saavuttaa. Turvallisuutta pidettiin suhteellisena käsitteenä, koska jokaisessa ohjelmistossa on haavoittuvaisuuksia ja niitä tulee koko ajan lisää. Torin turvallisuudesta kärsii myös se, että käyttäjä voi käyttää Tor-ohjelmistoja väärin, jolloin käyttäjä voi altistaa itsensä vaaratilanteelle.

6.1.5 Tor-ohjelmistojen yleistyminen

Tikkasen mukaan Torin kaltaiset ohjelmistot ovat alkaneet kiinnostaa Internet-käyttäjiä yhä enemmän, ja osa asiantuntijoista uskoi siihen, että anonyymien ohjelmistojen käyttö saattaa yleistyä. Asiantuntijat kokivat, että Tor-ohjelmistojen mahdollinen yleistyminen tapahtunee hitaasti ja että ne eivät saavuta suurta suosiota lähiaikoina. Järvisen ja Ni-

mettömän mukaan tähän oli syynä se, että suuri osa Internet-käyttäjistä on mukavuudenhaluisia, eivätkä halua muuttaa vakiintuneita Internetin käyttörutiinejaan. Tor-ohjelmistojen käyttöönoton vaikeus ja Tor-verkon hitaus voivat myös vaikuttaa ohjelmistojen käyttöönottoon. Internetin käyttäjät saattavat myös kokea anonyymien ohjelmistojen hyödyt minimaalisina, vaikka tiedostaisivatkin, että heistä kerätään tietoa.

Asiantuntijat arvelivat, että anonyymien ohjelmistojen käyttäjäkunta saattaa kasvaa tulevaisuudessa, mutta se on yhteydessä siihen, kuinka paljon ihmisiä seurataan ja sensuroidaan tulevaisuudessa. Nikin mukaan käyttäjämäärät eivät tule kasvamaan, ellei kyseisille ohjelmistoille nähdä tarvetta. Seuraavaksi koostan yhteenvedon asiantuntijoiden mielipiteistä liittyen Torin sopivuuteen yksityishenkilön käytössä.

6.1.6 Torin sopivuus yksityishenkilölle

Asiantuntijoiden mielestä Tor-ohjelmistojen käyttöönotto vaatii oma-aloitteista asioiden opiskelua, jotta tavalliset Internet-käyttäjät tiedostavat, miten Tor-ohjelmistoja käytetään, mihin Tor-ohjelmistot pystyvät ja mihin eivät. Nämä asiat tiedostava Torin käyttäjä osaa käyttää Tor-ohjelmistoja turvallisesti. Nikin mielestä ilman tätä ymmärrystä Tor ei ole turvallinen käyttää, vaan pikemminkin äärimmäisen vaarallinen käyttäjänsä tietoturvalle ja yksityisyydelle. Järvisen mukaan Tor-ohjelmistojen käyttäjältä vaaditaan myös huolellisuutta ja varovaisuutta, lisäksi käytettävän tietokoneen pitää olla turvallinen käyttää. Seuraavaksi käsittelen testihenkilöiden käyttöönottotestauksen tulokset.

6.2 Torin käyttöönoton testauksen tulokset

Tähän kappaleeseen on kerätty Torin käyttöönoton testauksen tulokset. Lisäksi testihenkilöiden kirjallisista palautteista (liite 7) on koottu yhteenveto tähän kappaleeseen. Tulokset on jaettu kappaleen sisällä omiksi kokonaisuuksiksi, jotta niiden hahmottaminen on helpompaa. Kappaleissa käsitellään Tor-ohjelmistojen asennuksen tuloksia, turvallista käyttämistä, käyttöjaksoa ja palautetta. Testin tuloksia on koottu taulukoihin. Taulukoiden vasemmassa sarakkeessa kerrotaan testiin kuuluvia toimenpiteitä ja riveissä testihenkilöiden suoriutuminen kyseisistä toimenpiteistä. Lisäksi taulukoiden ylin rivi näyttää testihenkilöiden sukupuolen (M/N) ja iän.

6.2.1 Tor-ohjelmistojen asennuksen tulokset

Tässä kappaleessa esitetään Tor Browserin ja Tails-käyttöjärjestelmän asennukseen liittyvät tulokset, jotka muodostivat testin ensimmäisen ja toisen osion. Oheisesta taulukosta selviää Tor-ohjelmistojen asennuksen tulokset.

Taulukko 1. Tor-ohjelmistojen asennuksen tulokset

	Hlö 1 M/27	Hlö 2 N/26	Hlö 3 M/26	Hlö 4 M/27	Hlö 5 M/27
Latasi Tor Browserin	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä
Tarkasti Tor Browserin eheyden	Ei	Ei	Ei	Ei	Ei
Asensi Tor Browserin	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä
Käynnisti Tor Browserin	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä
Pääsi Internet-sivustolle käyttäen Tor Browseria	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä
Latasi Tailsin	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä
Tarkasti Tailsin eheyden	Ei	Ei	Ei	Kyllä	Ei
Pyysi DVD-levyn polttamista varten	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä
Poltti Tailsin DVD-levylle	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä
Käynnisti Tailsin	Kyllä	Kyllä	Kyllä	Kyllä	Ei
Pääsi Internet-sivustolle käyttäen Tailsia	Kyllä	Kyllä	Kyllä	Kyllä	Ei

Kuten taulukosta käy ilmi, ohjelmistojen asennuksessa esiintyi isoimpana ongelmana ohjelmistojen eheyden tarkastaminen. Tämä johtui eheyden tarkastamisen vaikeudesta ja asennusohjeiden epäselvyydestä, esimerkiksi osalle testihenkilöistä asennusohjeissa käytetyt termit eivät olleet tuttuja. Testihenkilöt eivät myöskään ymmärtäneet ohjelmistojen eheyden tarkastamisen tärkeyttä, koska he eivät tienneet, mitä eheyden tarkastaminen tarkoittaa. Testihenkilöt eivät pitäneet asennusta mahdottomana, mutta eheyden tarkastamisen takia kuitenkin todella vaikeana prosessina keskiverto tietokoneen käyttäjälle. Tor-ohjelmistojen asentamisen muut osa-alueet onnistuivat pääsääntöisesti kaikilta hyvin, lukuun ottamatta yhtä testihenkilöä, joka ei onnistunut itsenäisesti käynnistämään Tailsia ja käyttämään sitä Internetin selailuun. (Taulukko 1; Liite 7.)

6.2.2 Tor-ohjelmistojen turvallisen käyttämisen tulokset

Tässä kappaleessa havainnollistetaan tuloksia koskien testihenkilöiden kyvykkyyttä käyttää Tor-ohjelmistoja turvallisesti. Tämä oli testin osioista kolmas, jonka tarkoituksena oli selvittää, tiedostavatko testihenkilöt Torin käytössä piileviä riskejä, tietävätkö he entuudestaan joitain turvallisuusohjeita, löytävätkö he turvallisen käytön ohjeet Internetistä ja ymmärtävätkö he turvallisen käytön ohjeet. Oheisen taulukon vasemmassa sarakkeessa on lueteltu Tor-ohjelmistojen turvallisen käytön ohjeet (liite 5), lisäksi taulukko osoittaa testihenkilöiden Tor-ohjelmistojen turvallisen käyttämisen tulokset.

Taulukko 2. Tor-ohjelmistojen turvallisen käyttämisen tulokset

	Hlö 1 M/27	Hlö 2 N/26	Hlö 3 M/26	Hlö 4 M/27	Hlö 5 M/27
Olisiko testihenkilö tiedostanut riskit	Ei	Ei	Kyllä	Kyllä	Kyllä
Tiesikö turvallisen käytön ohjeet jo valmiiksi	Ei	Ei	Ei	Ei	Ei
Löysikö turvallisen käytön ohjeet	Osan	Kyllä	Kyllä	Kyllä	Osan
Tietää, ettei Tor-ohjelmistojen asetuksia ole suositeltavaa muuttaa	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä
Tietää, mikä on Torrent-tiedosto	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä
Tietää, ettei Torrent-tiedostoja saa ladata	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä
Tietää, ettei lisäosia saa asentaa	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä
Tietää, ettei lisäosia saa sallia	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä
Tietää, mikä on HTTPS	Kyllä	Kyllä	Kyllä	Ei	Ei
Osaa tarkastaa HTTPS:n käytön	Kyllä	Kyllä	Kyllä	Kyllä	Ei
Tietää, miksei ladattuja tiedostoja saa avata	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä

Kolme viidestä testihenkilöstä olisi tiedostanut Tor-ohjelmistojen käytössä olevat riskit, mutta yksikään testihenkilö ei tiennyt etukäteen turvallisen käytön ohjeita. Kahdella testihenkilöllä oli vaikeuksia löytää Torin turvallisen käytön ohjeet kokonaisuudessaan, mutta turvallisen käytön ohjeet kuitenkin ymmärrettiin hyvällä menestyksellä. (Taulukko 2.)

6.2.3 Käyttöjakson tulokset ja palaute

Tässä kappaleessa käsitellään testihenkilöiden käyttöjaksoa ja käyttöjakson jälkeen pyydettyä kirjallista palautetta (liite 7).

Testihenkilöt olivat sitä mieltä, että Tor-ohjelmistoille löytyy tarvetta, etenkin maissa, joissa valvotaan ja rajoitetaan kansalaisten Internetin käyttöä, esimerkiksi yksi testihenkilö nosti esille NSA-tiedusteluskandaalit sekä Turkin ja Kiinan hallituksien rajoitukset Internetissä. Testihenkilöt kokivat Tor-ohjelmistoissa olevan sekä haittoja että hyötyjä, esimerkiksi Tor-ohjelmistojen isoimpana haittana pidettiin sitä, että niitä voidaan käyttää laittomiin toimiin, mutta sitä pidettiin pienenä haittana verrattuna siihen, kuinka paljon siitä voi olla joillekin tahoille hyötyä. Hyötyinä testihenkilöt pitivät suojautumista rikollisuutta ja valtioita vastaan, sekä sitä, että asiallisilla Internet-sivustoilla voi käydä, vaikka ne olisivatkin estetty jonkin tahon toimesta.

Testihenkilöiden mielestä anonyymien ohjelmistojen käyttö lisääntyy eri puolilla maailmaa. Käyttäjämäärän lisääntymiseen vaikuttaa valtioiden historia, nykytilanne ja Internetiin kohdistuvat toimet. Käyttäjämäärän lisääntymiseen vaikuttaa lisäksi tiedon ja asioinnin siirtyminen yhä enemmän Internetiin. Testihenkilöt eivät näe länsimaissa niin suurta tarvetta anonyymeille ohjelmistoille kuin esimerkiksi Aasiassa, jossa Internetin käyttöä seurataan ja sen käyttö on rajatumpaa. Oheinen taulukko näyttää testihenkilöiden käyttöjakson tulokset.

Taulukko 3. Tor-ohjelmistojen käyttäminen

	Hlö 1 M/27	Hlö 2 N/26	Hlö 3 M/26	Hlö 4 M/27	Hlö 5 M/27
Käytti onnistuneesti Tor-ohjelmistoja	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä
Tulee vastaisuudessa käyttämään Toria	Ei	Ei	Ei	Ei	Ei

Jokainen testihenkilö käytti Tor-ohjelmistoja kahden päivän ajan ongelmitta, mutta yksikään testihenkilö ei nähnyt itselleen tarvetta jatkaa Tor-ohjelmistojen käyttöä testin jälkeen (Taulukko 3). Tähän oli syynä se, että testihenkilöiden mielestä Tor-ohjelmistot

haittasivat heidän Internetin käyttöään enemmän kuin hyödyttivät. Tor-ohjelmistojen hyötyjä pidettiin vähäisinä, koska Suomessa Internet-sensuurin kiertämistä ei pidetty oleellisena ja koska testihenkilöt pääsevät haluamilleen Internet-sivustoille ilman Tor-ohjelmistoja. Testihenkilöt eivät myöskään pitäneet omaa Internetin käyttöään niin salaisena, että sen seuranta ja valvonta häiritsisi heitä. Yhtenä syynä tähän oli se, että he jakavat jo osan tiedoistaan omatoimisesti Internetissä, kuten sosiaalisessa mediassa.

Tor-ohjelmistojen hitaus ja testihenkilöiden omien Internetin käyttötapojen muuttaminen ei ollut testihenkilöille mieluisaa, koska turvallisen käytön ohjeet rajoittaisivat liikaa heidän päivittäistä Internetin käyttöään. Muutama testihenkilö oli myös sitä mieltä, että he käyttävät Internetiä jo tarpeeksi turvallisesti, eivätkä tunne tarvitsevansa Tor-ohjelmistojen tarjoamaa lisäturvaa Internetin käytölleen.

7 Pohdinta

Tässä kappaleessa vastataan tutkimuskysymyksiin ja pohditaan Tor-ohjelmistojen sopivuutta yksityishenkilöille, mikä oli tutkimuksen aiheena. Tutkimuskysymykset olivat seuraavat: Yleistyvätkö Tor-ohjelmistot maailmanlaajuisesti yksityishenkilöiden käytössä? Onko Tor-ohjelmistojen käyttö tarpeellista suomalaisille yksityishenkilöille? Osaavatko suomalaiset yksityishenkilöt käyttää Tor-ohjelmistoja turvallisesti? Kappaleessa pohditaan vastauksia tutkimuskysymyksiin käyttäen tukena teoriataustaa, kyselyyn osallistuneiden asiantuntijoiden (Petteri Järvinen, Ville Oksanen, Antti Tikkanen, Matti Nikki, Liikenne- ja viestintäministeriö ja Nimetön) vastauksia (liite 6), Torin käyttöönoton testituloksia ja testihenkilöiden palautteita (liite 7).

7.1 Yleistyvätkö Tor-ohjelmistot maailmanlaajuisesti yksityishenkilöiden käytössä?

Tämä kappale vastaa ensimmäiseen tutkimuskysymykseen ja käsittelee Internet-sensuurin ja Internetissä tapahtuvan seurannan mahdollisia tulevaisuudennäkymiä ja sitä, miten ne vaikuttavat Tor-ohjelmistojen käyttöön.

Tor-ohjelmistojen käyttäjäkunnan mahdolliseen kasvuun vaikuttanee tavallisten Internet-käyttäjien tarve kyseisille ohjelmistoille. Kuten aikaisemmin on käynyt ilmi, tällä hetkellä Tor-ohjelmistoja käytetään pääasiassa Internet-sensuurien kiertämiseen ja Internetissä tapahtuvan seurannan välttämiseksi. Siten näen näiden tekijöiden suuresti vaikuttavan siihen, kasvavatko Tor-ohjelmistojen käyttäjämäärät yksityishenkilöiden käytössä.

Vaikka moni organisaatio onkin ottanut Internet-sensuurin käyttöön, eivät asiantuntijat näe Internet-sensuurin hyötyjä kovin suurina. Vuosien saatossa Internet-sensuurit ovat tulleet tehokkaammiksi, ja uusia sensuuritekniikkoja on kehitetty, koska erinäiset tahot eivät halua sallia vapaata pääsyä kaikkialle Internetissä. Internet-sivustojen estämiselle voi olla monia syitä, mutta esimerkiksi Internet-sivuilla oleva rikollisuus on yksi syy joidenkin Internet-sivujen estämiseen. Monet valtiot, kuten Suomi, Turkki ja Kiina, ovatkin ottaneet erilaisia sensuuritekniikkoja käyttöön, mutta näissä valtioissa on myös

tapauksia, joiden vuoksi Internet-sensuurin laatu on noussut kyseenalaiseksi, koska osa estetyistä Internet-sivustoista ei välttämättä sisällä mitään laitonta. Näitä tapauksia ovat olleet esimerkiksi vuonna 2014 Turkissa tapahtuneet YouTuben ja Twitterin estäminen. Osa asiantuntijoistakin myöntää, että Internet-sensuurit saattavat sensuroida liikaa ja näin estää hyväksyttäviäkin Internet-sivuja.

Kiinassa olevaa Internet-sensuuria pidetään edelläkävijänä (Wagner 2009, 8), mutta Oksasen mielestä sekään ei riitä estämään Internetin käyttäjiä käymästä sensuroiduilla Internet-sivustoilla, koska Internet-sensuurien kiertäminen on suhteellisen helppoa. Tämä osoittaa myös sen, että vaikka Kiinan valtio on panostanut huomattavasti resursseja, kuten kymmeniä tuhansia viranomaisia, verkon valvontaa varten, ei Internet-sensuurin kiertäminen välttämättä ole täysin mahdotonta. Tutkimuksessani en kokeillut, pystyykö Kiinan Internet-sensuuria kiertämään Tor-ohjelmistoilla, mutta osa testihenkilöistä onnistui uteliaisuuttaan käymään Suomessa estetyllä koskenkorva.com-sivustolla käyttäen Tor-ohjelmistoja. Tämä ei kuulunut itse testiin, mutta osa testihenkilöistä raportoi kyseisestä kokeilusta myöhemmin. Kävin myös itse kyseisellä Internet-sivustolla, joten ainakin joitakin Suomen Internet-sensuurin estämiä Internet-sivustoja on mahdollista kiertää Tor-ohjelmistoilla.

Moni asiantuntija oli sitä mieltä, että Internetin sensurointi saattaa kasvaa tulevaisuudessa, koska osa valtioista mahdollisesti haluaa rajoittaa Internetissä olevaa tietoa, jopa Euroopan maissa. Tulevaisuutta on kuitenkin vaikeaa ennustaa. Lähdekirjallisuuden perusteella ei ole ollut merkkejä siitä, että lähitulevaisuudessa Internet-sensuurit tulisivat poistumaan käytöstä tai edes vähenevän huomattavasti, sen sijaan sen voidaan olettaa kasvavan.

Internet-sensuurit vaikuttavat olevan suhteellisen tehottomia, vaikka niihin käytettäisiin paljon resursseja, mikä saattaisi olla syynä Internet-sensuurin vähenemiseen. Internet-sensuurit myös sensuroivat Internet-sivustoja, joita ei tarvitsisi estää. Tällä hetkellä ei myöskään näytä siltä, että organisaatiot lopettaisivat Internetin sensuroimisen. Mielestäni Järvinen antaa oivallisen neuvon Internetin käyttäjille, kun hän kehottaa Internetin käyttäjiä itse miettimään sitä, mitä julkaisevat Internetissä ja mitä eivät, koska tällöin Internet-sensuureille ei välttämättä olisi tulevaisuudessa tarvetta.

Tiedon ja arkisten asioiden siirtyessä yhä enemmän Internetiin on myös Internetissä tapahtuva käyttäjien seuranta ja heidän tietojensa kerääminen lisääntynyt. Yritykset ovat alkaneet hyödyntää palveluissaan käyttäjistä keräämiään tietoja palveluidensa parantamiseksi ja mainoksien kohdentamiseksi. Oksasen mielestä osa Internet-palveluista perustuu käyttäjiltä kerättävien tietojen taloudelliseen arvoon, nimittäin palvelun ollessa maksuton on käyttäjä itsessään palvelun tuote. Tästä syystä myös jotkin yritykset pystyvät tarjoamaan ilmaisia palveluita käyttäjilleen, koska tuotot tulevat esimerkiksi palveluissa olevista mainoksista. Tähän on hyvänä esimerkkinä Facebook ja Google, jotka ovat maailman kaksi käydyintä Internet-sivustoa. Molempien yritysten palveluita pystyy käyttämään ilmaiseksi ja molemmat palvelut kertovat avoimesti keräävänsä käyttäjistään tietoa. Järvinen (2014a, 265) jopa vertaa Googlen toimintaa kaupalliseksi NSA:ksi, koska moni Googlen palveluista perustuu juuri tietojen keräämiseen.

Tietojen keräämiseen ja käyttäjien seurantaan Internetissä on myös osallistunut valtioiden tiedusteluorganisaatiot, kuten Yhdysvaltojen NSA. Snowdenin tietopaljastukset vuoden 2013 kesällä toivat esille, kuinka laajalle NSA:n tiedustelu todellisuudessa ulottuu. Snowdenin tietopaljastuksissa ilmeni NSA:n käyttämiä ohjelmistoja, kuten PRISM-vakoiluohjelma, jonka avulla NSA pystyi keräämään tietoa monesta eri suositusta palvelusta, esimerkiksi Googlesta, Facebookista, Microsoftista ja Applesta. NSA:n yhtenä tavoitteena on suojella omia kansalaisiaan torjumalla esimerkiksi terrorismia (Järvinen 2014a, 166), mikä lienee monen muunkin tiedusteluorganisaation yksi tavoite.

Internet-seuraamisen ja käyttäjiin kohdistuvan tietojen keräämisen tulevaisuus on epävarmaa, koska esimerkiksi Snowdenin tekemät tietopaljastukset ovat suhteellisen tuoreita ja koska isot muutokset vievät aikaa myös nopeasti kehittyvässä Internetissä. Nikki pitää Tor-ohjelmistojen käyttämistä vastareaktiona Internetin-käyttäjien seuraamiselle ja tietojen keräämiselle. Tämän pystynee mielestäni päättelemään myös vuoden 2013 puolenvälin aikoihin tapahtuneesta Torin käyttäjämäärän kasvusta (Kuvio 3 s. 21), joka todennäköisesti johtui Snowdenin tekemistä tietopaljastuksista. Internet-seurannan ja tietojen keräämisen tulevaisuus riippunee paljolti siitä, tulevatko Internetin käyttäjät hyväksymään seurannan vai ei. Asiantuntijoiden mielestä tällä hetkellä näyttäisi siltä,

että osa Internetin käyttäjistä hyväksyy seuraamisen ja osa ei, ja tästä syystä Internet-käyttäjillä pitäisi olla mahdollisuus valita, saako heistä kerätä tietoa vai ei.

On vaikea uskoa, että muutaman vuoden sisällä Internet-palveluissa tapahtuva seuranta tai tietojen kerääminen loppuisi kokonaan tai edes vähentyisi radikaalisti, koska se saattaisi tarkoittaa suuria muutoksia Internet-palveluissa. Moni yritys saa rahansa juuri tietojen keräämisestä ja käyttäjiensä seurannasta, jolloin sen poistuessa pitäisi yrityksien keksiä muita tapoja saada tuottonsa, mikä voisi tarkoittaa esimerkiksi sitä, että osasta palveluista tulisi maksullisia. Harva varmaankin käyttäisi esimerkiksi Googlen hakukonetta, jos joutuisi maksamaan jokaisesta hausta. Tämä voisi johtaa myös siihen, että hakukoneen haut eivät olisi yhtä täsmällisiä, koska palvelun kehittäminen voisi kärsiä ilman käyttäjistä kerättyä tietoa. On hankala kuvitella valtioiden tiedusteluorganisaatioiden vähentävän seurantaa ja tietojen keräämistä, koska sehän on kyseisten organisaatioiden tehtävä. Valtioiden tiedusteluorganisaatiot toteuttavat varmasti vastaisuudessakin tehtäväänsä. Arveluttavaa on se, seuraavatko ne tulevaisuudessa vähemmän tavallisia ihmisiä ja keskittävät sitä kautta saadut resurssit todellisiin uhkiin ja laittomuuksien pois kitkemiseen.

Tikkasen mielestä Internetin käyttäjien kiinnostus on kasvanut koskien ohjelmistoja, joilla on mahdollista kiertää Internet-sensuureja ja välttää Internetin seurantaa. Asiantuntijoiden mielestä Tor-ohjelmistojen käyttäjämäärät saattavat kasvaa tulevaisuudessa, mutta se tulee tapahtumaan heidän mukaansa hitaasti. Internet-käyttäjien päätökseen aloittaa käyttää Tor-ohjelmistoja vaikuttanee Internetin-käyttäjän asuinmaa, jolloin kyseisessä maassa käytetyllä Internet-sensuurilla ja Internetissä tapahtuvalla seurannalla voi olla iso merkitys käyttämisen aloittamisessa. Mielestäni niissä maissa, joissa seurataan ja valvotaan Internetiä paljon, kuten Kiinassa, eivät Tor-ohjelmistojen käyttöönoton vaikeus, hitaus tai käyttötapojen muuttaminen juurikaan vaikuta Tor-ohjelmistojen käyttöönottoon, koska Tor-ohjelmistojen käyttäminen voi pitää Internetin käyttäjän vapaalla jalalla. Viittaan tällä siihen, että Kiinassa on ollut tapauksia, joissa yksityishenkilöitä on vangittu Internetin väärin käytön vuoksi, muun muassa protestoimisesta ihmisoikeuksien puolesta (Reporters without borders 2010 8–11; Ziccardi 2013, 258–259). Testihenkilöt olivat myös sitä mieltä, että Tor-ohjelmistoille löytyy tarvetta etenkin maissa, joissa rajoitetaan ja valvotaan kansalaisten Internetin käyttöä.

Internet-sensuurin saralta näkisin, että lähitulevaisuudessa Tor-ohjelmistoja käytetään edelleen Internet-sensuurien kiertämiseen yhtä paljon kuin tänä päivänä, koska tällä hetkellä ei ole selkeää syytä siihen, miksi kyseisten ohjelmistojen käyttäminen loppuisi Internet-sensuurin myötä. Kuten yllä toin esille, Internet-käyttäjien seuranta ja heidän tietojensa kerääminenkään ei ole yrityksen eikä valtioiden organisaatioiden osalta vähenemässä ainakaan huomattavissa määrin, minkä vuoksi en usko Torin käyttäjien vähenevän. Tällä hetkellä ei ole myöskään tarjolla ohjelmistoa, joka olisi ilmainen ja yhtä suosittu kuin Tor ja joka olisi lähivuosina syrjäyttämässä Toria.

Arvelujeni mukaan Torin käyttäjämäärät tuskin lähtevät huomattavaan laskuun lähitulevaisuudessa, ellei Tor-ohjelmistoista löytyisi jotakin, joka vaikuttaisi niiden luotettavuuteen tai Torin käyttäjien turvallisuuteen. En myöskään usko Tor-ohjelmistojen käyttäjämäärän saavan suurempaa suosiota lähiaikoina, ellei maailmalla ilmene lisää Snowdenin kaltaisia henkilöitä, jotka paljastavat jotakin vieläkin arkaluontoisempaa tietomateriaalia. Mikäli mitään mullistavaa ei tule tapahtumaan, uskon, ettei Torin käyttäjämäärissä tapahdu radikaaleja muutoksia puoleen eikä toiseen.

7.2 Onko Tor-ohjelmistojen käyttö tarpeellista suomalaisille yksityishenkilöille?

Tässä kappaleessa vastataan toiseen tutkimuskysymykseen ja selvitetään, onko suomalaisilla yksityishenkilöillä tarvetta Tor-ohjelmistoille. Kappaleessa käsitellään Suomen Internet-sensuuria, suomalaisiin kohdistuvaan Internetin seurantaa sekä asiantuntijoiden ja testihenkilöiden mielipiteitä Tor-ohjelmistojen tarpeellisuudesta Suomessa.

Suomessa Internet-sensuuri estää enimmäkseen lapsipornoon liittyviä Internet-sivustoja, mutta osa estetyistä Internet-sivustoista on estetty, koska niiden on katsottu rikkovan Suomen lakeja. Suomen Internet-sensuuria voidaan pitää suhteellisen vähäisenä verrattuna esimerkiksi Kiinaan tai Turkkiin, koska Suomessa ei ole estetty missään vaiheessa mitään suosittuja Internet-sivustoja, kuten YouTubea, joka on ollut estettynä Kiinassa sekä Turkissa. Suomen Internet-sensuuri ei tiedettävästi ole suuremmin haitannut tavallisten suomalaisten Internetin käyttöä, minkä myös testihenkilöt toteavat,

joten en usko Internet-sensuurin olevan Suomessa syynä Tor-ohjelmistojen käyttöönotolle. Tästä huolimatta Suomen Internet-sensuuri on saanut osakseen kritiikkiä, koska Internet-sensuuria pidetään perustuslain kieltämänä ennakkosensuurina ja sanavapauden vastaisena, eikä Internet-sensuurin nähdä poistavan laittomia Internet-sivustoja, vaan lakaisevan laittomat Internet-sivustot pois näkyvistä. Suomen Internet-sensuurin katsotaan myös sensuroivan Internet-sivustoja, joiden ei katsota täyttävän laittomuuden rajoja. (Poropudas 2008, Tarvainen 2008.) Suomen tulevaisuuden Internet-sensuuria on vaikea ennustaa, mutta jos lapsipornon Internet-sensurointi on aiheuttanut Suomessa kritiikkiä, on vaikea uskoa, että Suomessa Internet-sivustojen sensurointi kasvaisi lähiaikoina radikaalisti. Tähän spekulaatioon täytyy myös sisällyttää se, että Suomi kuuluu EU:n maihin, koska asiantuntijoiden mielestä on mahdollista, että EU:n maiden Internet-sensuuri saattaa kasvaa. Nikki ei pidä ajatusta mahdottomana, että EU:n maille tulisi yhteneväinen Internet-sensuurikäytäntö, jota valvottaisiin koko EU:n alueella. Tässä tilanteessa Internet-sensuurin osalta Tor-ohjelmistot voisi tulla tarpeeseen myös Suomessa.

Tiedettävästi Suomi ei seuraa kansalaistensa Internetin käyttöä ainakaan siinä suhteessa kuin esimerkiksi Ruotsin FRA tai NSA seuraa suomalaisia. Ruotsin FRA:n tiedetään seuraavan suomalaisia, koska sillä on lupa kerätä kaikki Internet-liikenne, joka menee Ruotsin läpi, mikä tarkoittaa sitä, että FRA voi kuunnella valtaosaa suomalaisten ulkomaalaisesta Internet-liikenteestä. Tämän lisäksi monen suomalaisen käydyimmät Internet-sivut ovat yhdysvaltalaisia (Alexa 2014), jolloin myös NSA:lla on mahdollisuus kerätä suomalaisista tietoa. FRA:n tiedetään myös tehneen yhteistyötä NSA:n kanssa, jolloin kaikki FRA:n keräämät tiedot suomalaisista saattavat päätyä NSA:lle. (Järvinen 2014a, 145.) Suomella ei ole käytössä vastaavanlaisia tiedusteluorganisaatioita, kuten FRA tai NSA, niin mielestäni Suomen tiedusteluorganisaatiot eivät ole varteenotettava syy ottaa Tor-ohjelmistoja käyttöön Suomessa. Suomalaisten tavallisten Internetin käyttäjien pitäisi tästä syystä huomioida se, hyväksyvätkö he sen, että vieraiden maiden tiedusteluorganisaatiot keräävät heistä tietoa. Testihenkilöt eivät ainakaan mieltäneet omaa Internetin käyttöään niin salaisena, että heitä häiritsisi NSA:n kaltaisten organisaatioiden seuranta.

Mielestäni tavallisten Internetin-käyttäjien suurimpana huolenaiheena ei ole Internet-palveluiden tekemä tiedon kerääminen, koska osa testihenkilöistä kertoi jakavansa jo osan tiedoistaan omatoimisesti Internetissä, kuten sosiaalisessa mediassa. Edellisessä kappaleessa käsiteltiin sitä, että osa Internet-palveluista saattaisi olla maksullisia, jos Internet-palvelut eivät keräisi tietoa, joten uskon monen suomalaisen hyväksyvän tiedon keräämisen, jos he saavat ilmaisia Internet-palveluita.

Asiantuntijoiden mielestä Tor-ohjelmistot ovat tarpeellisia yksityishenkilöille, joilla on tarvetta suojata oma identiteettinsä Internetissä. Suomalaisille yksityishenkilöille tämän kaltaisia tilanteita Internetissä saattavat olla esimerkiksi omia mielipiteitä ilmaistaessa, arkaluontoista materiaalia tutkiessa tai julkaistaessa. Liikenne- ja viestintäministeriön mukaan Suomessa jokaisella on oikeus turvattuun yksityiselämään, johon liittyvät henkilötiedot ja viestinnän luottamuksellisuuden suoja. Anonyymien ohjelmistojen tarve saattaa kasvaa tulevaisuudessa, mutta se on yhteydessä siihen, kuinka paljon ihmisiä seurataan ja sensuroidaan tulevaisuudessa. Asiantuntijat toteavat, että Tor-ohjelmistojen käyttöönoton vaikeus ja Tor-verkon hitaus voivat myös vaikuttaa ohjelmistojen käyttöönottoon. Asiantuntijoiden ja testihenkilöiden mielestä suomalaiset Internetin käyttäjät saattavat myös kokea Tor-ohjelmistojen hyödyn minimaalisena, vaikka tiedostaisivatkin, että heistä kerätään tietoa.

Yksikään testihenkilöistä ei kokenut Tor-ohjelmistoille olevan Suomessa kovin suurta tarvetta, koska testihenkilöt eivät pitäneet Internet-sensuuria, Internetin seurantaa tai tiedon keräämistä suurena haittana. Käyttöjakson jälkeen ainutkaan testihenkilö ei ollut halukas käyttämään Tor-ohjelmistoja vastaisuudessa, koska testihenkilöt pitivät käyttötapojen muuttamista liian suurena vaivana ja Tor-ohjelmistoja liian hitaina. Osa testihenkilöistä koki myös käyttävänsä Internetiä jo tarpeeksi turvallisesti, eivätkä tunne tarvitsevansa Tor-ohjelmistoista lisäturvallisuutta Internetin käytölleen.

Mielestäni Suomessa kovinkaan oleellisena syynä Tor-ohjelmistojen käyttöön ei ole Internet-sensuuri tai Internet-palveluiden tietojen kerääminen. Tor-ohjelmistojen tarpeellisuus Suomessa kohdistuu Internetin käyttäjiin, jotka kokevat valtioiden tiedusteluorganisaatioiden seuraamisen olevan heille haittana. Internetin käyttäjän täytyy myös huomioida se, että käyttämällä Tor-ohjelmistoja voi myös herättää enemmän huomiota

ja saattaa tästä syystä joutua esimerkiksi NSA:n tarkkailun kohteeksi. Suomessa ei ole kovinkaan suurta tarvetta Tor-ohjelmistoille. Näkisin Tor-ohjelmistojen tarpeen koskevan sellaisia suomalaisia Internetin käyttäjiä, joita valtioiden tiedusteluorganisaatiot häiritsevät ja henkilöitä, jotka tarvitsevat anonymiteettiä Internetissä esimerkiksi ammatistaan johtuen.

7.3 Osaavatko suomalaiset yksityishenkilöt käyttää Tor-ohjelmistoja turvallisesti?

Tämä kappale vastaa kolmanteen tutkimuskysymykseen ja tarkastelee sitä, onko suomalaisilla yksityishenkilöillä kykyä käyttää Tor-ohjelmistoja turvallisesti. Kappaleessa pohditaan testin osioiden onnistuneisuutta, asiantuntijoiden mielipiteitä ja mitkä seikat vaikuttavat turvalliseen käyttämiseen.

Tor-ohjelmistojen asennuksessa testihenkilöille vaikein osuus oli ohjelmistojen eheyden tarkistaminen. Kukaan testihenkilöistä ei tarkastanut Tor Browserin eheyttä, ja ainoastaan yksi testihenkilö onnistui tarkastamaan Tails-käyttöjärjestelmän eheyden. Tails-käyttöjärjestelmän eheyden tarkastamisen vaikeus johtui osaksi haastavista asennusohjeista ja osaksi siitä, ettei kyseinen toimenpide ollut heille valmiiksi tuttu. Tor Browserin eheyden tarkastamisen tekemättä jättäminen johtui siitä, että asennusohjeet ovat muuttuneet, ja ohjeissa ei neuvota enää kyseistä toimenpidettä, vaan eheyden tarkastamisen ohjeet pitää etsiä muualta Tor-projektin Internet-sivuilta. Tämä saattaa johtaa siihen, että joissakin tapauksissa Internetin käyttäjät voivat asentaa Tor-ohjelmistoja, joiden käyttö ei ole edes turvallista. Tätä voi pitää turvallisuusriskinä, koska oikein asennettuna Tor-ohjelmisto on lähtökohtana turvalliseen käyttämiseen. Hyvänä asiana pitäisin sitä, että kaikki testihenkilöt tiedostivat eheyden tarkastamisen tärkeyden, mutta sen suorittaminen osoittautui haastavaksi.

Kaksi testihenkilöä eivät olisi tiedostaneet Tor-ohjelmistojen käytössä mahdollisia riskejä ja he olisivat saattaneet hyvinkin käyttää käyttöjakson ajan Tor-ohjelmistoja turvattomasti. Molemmat testihenkilöt olivat sitä mieltä, että jos käyttävät ohjelmistoa, jonka pitäisi lisätä turvallisuutta, täytyisi sen myös ohjata käyttäjiään niin, etteivät he aseta itseään vaaratilanteeseen. Tor Browserin myös näyttäessä tavalliselta Internet-selaimelta

hämäsi se kyseisiä testihenkilöitä niin, että he kuvittelivat, että sitä voisi käyttää niin kuin täysin tavallista Internet-selainta. Yksikään testihenkilöistä ei tiennyt etukäteen turvallisen käytönohjeita, mistä voi olettaa, ettei kellekään heistä Tor-ohjelmistojen käyttäminen ollut valmiiksi kovin tuttua. Testihenkilöt löysivät Tor-ohjelmistojen turvallisen käytön ohjeet. – vaikkakin kaksi löysi vain osan ohjeista, löysivät he kuitenkin niistä oleellisimmat, jotka mielestäni olisivat riittäneet turvalliseen käyttämiseen. Turvallisen käytön ohjeissa ei myöskään ollut suuria epäselvyyksiä ja ne ymmärrettiin hyvällä menestyksellä. Käyttöjakso onnistui testihenkilöiltä ongelmitta ja heidän mielestään turvallisen käytön ohjeiden mukaisesti.

Tor-ohjelmien käytön suurimpia turvallisuusuhkia on se, jos käyttäjä ei tiedosta Tor-ohjelmistojen riskejä sekä Tor-ohjelmistojen rajoitteita. Nikin mielestä ilman tätä vaadittua ymmärrystä Tor-ohjelmistot eivät ole turvallisia käyttää, vaan pikemminkin äärimmäisen vaarallisia käyttäjänsä tietoturvalle ja yksityisyydelle. Asiantuntijoiden mukaan Tor-ohjelmistojen käyttöönotto vaatii oma-aloitteista asioiden opiskelua, jotta tavalliset Internet-käyttäjät tiedostavat, miten Tor-ohjelmistoja käytetään turvallisesti. Osa testihenkilöistä totesi saman asian ilmoittaessaan, jos he tarvitsisivat Tor-ohjelmistoja turvaamaan omaa Internetin käyttöään, esimerkiksi työpaikallaan tai kotonaan, niin he tutustuisivat ohjelmistoihin tarkemmin ennen niiden käyttöönottoa. Järvisen mukaan Tor-ohjelmistojen käyttäjältä vaaditaan myös huolellisuutta ja varovaisuutta, lisäksi käytettävän tietokoneen pitää olla turvallinen käyttää.

Turvallisuutta uhkaavimmat tilanteet vaikuttaisivat ilmaantuvan, jos Tor-ohjelmistojen käyttäjä ei tarkista Tor-ohjelmistojen eheyttä ja asentaa turvattoman Tor-ohjelmiston, tai jos käyttäjä ei tiedosta ohjelmistojen mahdollisia riskejä. Uskon käyttäjien tutustuvan Tor-ohjelmistoihin tarkemmin ennen asennusta ja käyttöönottoa, jos he näkisivät Tor-ohjelmistoille todellista tarvetta. Tilanteessa, jossa Internetin käyttäjä toteaisi, ettei osaa toteuttaa jotakin tärkeää toimenpidettä, joka liittyy ohjelmiston turvallisuuteen, jättäisi hän todennäköisesti ohjelmiston käyttöönottamatta tai opettelisi asian niin, että se varmasti onnistuisi turvallisesti. Tor-ohjelmistojen käyttämisellä yritetään tavoitella lisäturvallisuutta, joten mielestäni tavallinenkin Internetin käyttäjä opettelisi käyttämään ohjelmistoja turvallisesti. Testi myös osoitti, että tavallisilla Internetin käyttäjillä on kyky ymmärtää, miten Tor-ohjelmistoja käytetään turvallisesti. Liikenne- ja viestintäministe-

riön mukaan osaavissa käsissä Tor-ohjelmistoja voidaan pitää turvallisina. Tavallinen tietokoneen käyttäjä kykenee käyttämään Tor-ohjelmistoja turvallisesti, jos hän on valmis opettelemaan Tor-ohjelmistojen turvallisen käytön ja haluaa käyttää niitä turvallisesti, mikä olisi mielestäni suotavaa ottaessa käyttöön ohjelmistoja, joiden tavoitteena on lisätä turvallisuutta. Liikenne- ja viestintäministeriön mukaan Tor-ohjelmistojen käyttäjän täytyy myös huomioida, minkä tasoista turvallisuutta hän tavoittelee, koska täydellistä turvallisuutta ei ole olemassa.

7.4 Soveltuvatko Tor-ohjelmistot yksityishenkilöille

Tämä kappale käsittelee tutkimuksen lopullista päämäärää, joka oli tutkimuskysymyksien avulla selvittää Tor-ohjelmistojen soveltuvuutta yksityishenkilöille. Kappaleeseen on koottu tutkimuskysymyksiä koskevista kappaleista pohdintoja, joiden perusteella vastataan siihen, soveltuvatko Tor-ohjelmistot yksityishenkilöille.

Aikaisemmassa kappaleessa todettiin, että tällä hetkellä Tor-ohjelmistojen tarve näyttäisi olevan Suomessa todella vähäistä. Testihenkilöt eivät kokeneet tarvetta Tor-ohjelmistoille, ja suomalainen Internetin käyttäjä, joka voisi tarvita Tor-ohjelmistoja, käyttäisi Tor-ohjelmistoja mahdollisesti estääkseen valtioiden tekemää Internet-seuraamista. Lähiaikoina ei näyttäisi Suomessa Tor-ohjelmistoille olevan suurtakaan tarvetta, mutta tilanne voi muuttua. Maailmalla Tor-ohjelmistojen käyttäjämäärät saattavat kasvaa, mistä voisi päätellä, että niille nähdään tarvetta ulkomailla.

Tor-ohjelmistojen isoimmat riskit vaikuttivat koostuvan siitä, että Tor-ohjelmistojen käyttäjä ei ole tutustunut tarpeeksi hyvin käyttämiinsä ohjelmistoihin, kuten miten Tor-ohjelmistoja käytetään, mihin Tor-ohjelmistot pystyvät ja mihin eivät. Testihenkilöt mainitsivat, että perehtyisivät Tor-ohjelmistoihin tarkemmin, jos näkisivät ohjelmistoille tarvetta. Uskoisin Internetin käyttäjän, joka tuntee tarvitsevansa Tor-ohjelmistoja, olevan tarpeeksi valveutunut myös opiskelemaan tarvittavat asiat, jotta pystyisi käyttämään Tor-ohjelmistoja oikein ja turvallisesti. Testi osoitti, että käyttäjillä on kyky omaksua Tor-ohjelmistojen riskejä, joten heillä olisi mahdollisuus oppia käyttämään Tor-ohjelmistoja riskittömästi. Tietääkseni Tor-ohjelmistot ovat tällä hetkellä ainoita ilmaisia työkaluja anonyymiin Internetin käyttöön, myös muun muassa Snowdenin ja Man-

ningin tiedetään käyttäneen kyseisiä ohjelmistoja (Finley 2014; Järvinen 2014a, 63; Musil 2014). Asiantuntijatkin pitivät Tor-ohjelmistoja tehokkaana ja luotettavana tapana suojata Internetin käyttäjän identiteettiä, joten Internetin-käyttäjät voivat mielestäni käyttää Tor-ohjelmistoja, jos tarvitsevat anonymiteettiä Internetissä. Tietenkin Tor-ohjelmistojen turvallisuudessakin täytyy huomioida se, että turvallisuutta voidaan pitää suhteellisena käsitteenä, koska asiantuntijoiden mielestä täydellistä turvallisuutta on lähes mahdotonta saavuttaa. Ohjelmistoista löytyy useasti haavoittuvuuksia, ja vanhoja haavoittuvuuksia paikatessa voi syntyä uusia. Tästä syystä on suositeltavaa, ettei ohjelmistoihin luotettaisi täydellisesti, vaan ohjelmistoja käytettäisiin huolellisuutta ja varovaista työtapaa noudattaen.

Tor-ohjelmistojen käytössä voi tulla vastaan tilanteita, joissa joiltakin Internet-sivustoilta puuttuu HTTPS-protokolla, videoiden katsominen ei onnistu tai Tor-verkot ovat hitaita. Nämä tilanteet voivat vaikuttaa Tor-ohjelmistojen käyttöönottoon, koska Internetin käyttäjä joutuu muuttamaan omia Internetin käyttötapojaan. Ainakin osa testihenkilöistä koki näiden tilanteiden haittaavan heidän Tor-ohjelmistojen käyttöään. Tulevaisuudessa nämä tilanteet tulevat mahdollisesti vähenemään, jos tai kun Tor-ohjelmistojen käyttäminen helpottuu. Videoiden katsominen ei aina onnistu Tor Browser -selaimella, koska moni video saattaa käyttää toisto-ohjelmana Adobe Flash Playeriä, jota ei suositella asennettavaksi Tor Browser –selaimeen. Näillä näkymin HTML5-kielen yleistyminen vähentää Flash-videoita Internet-sivustoilla, jolloin Internet-käyttäjät tarvitsevat Adobe Flash Playeriäkin yhä vähemmän (Vaughan-Nichols 2011). HTTPS-protokollan käyttö saattaa tulla yleistymään Internet-sivustoilla, koska ainakin Googlen hakukonetta on optimoitu suosimaan HTTPS-protokollaa tukevia Internet-sivustoja (Bahajji & Illyes 2014), ja tällä hetkellä moni suosittu Internet-sivusto tukee jo HTTPS-protokollaa (Alexa 2014). Tor-ohjelmistoilla Internetin käyttö voi tuntua välillä hitaalta, mikä johtuu Tor-verkon toiminnasta, jossa monta käyttäjää käyttää samoja solmuja ja Internet-yhteys kiertää monen solmun kautta. Tekniikan kehittyessä Internet-verkkojen nopeudet kasvavat, ja solmujen määrät (Tor Project 2014o) ja nopeudet ovat myös kasvaneet vuosien saatossa (Tor Project 2014p). Nämä vaikuttavat myönteisesti Tor-verkkoihin, jolloin Tor-verkon käyttö saattaa nopeutua. Toisaalta tällä hetkellä Tor-ohjelmistojen käyttäjämäärät ovat kasvaneet samaan tahtiin kuin Tor-verkon nopeus ja tämä on vaikuttanut asiaan niin, ettei Tor-verkkojen nopeus ole kas-

vanut vuosien aikana yhtään per Tor-ohjelmiston käyttäjä (Tor Project 2014q). Tämä saattaa tarkoittaa tulevaisuudessa myös sitä, että Tor-ohjelmistojen hitaus edelleen saattaa haitata joitakin sen käyttäjiä.

Mielestäni Tor-ohjelmistot soveltuvat tavallisille Internetin käyttäjille, jos he näkevät Tor-ohjelmistoille tarvetta ja ovat valmiita opiskelemaan, miten Tor-ohjelmistoja käytetään oikein ennen niiden käyttöönottoa, etteivät vahingossakaan aseta omaa tietoturvaansa vaaraan. Tämän kaltaisen Internetin käyttäjän täytyy myös olla valmis muuttamaan Internetin käyttötapojaan, jos aikoo käyttää pelkästään Tor-ohjelmistoja Internetin käytössään. Suosittelisin sellaiselle Internetin käyttäjälle, jota valtioiden tiedustelu häiritsee, mutta joka ei ole valmis muuttamaan käyttötapojaan ja käyttämään Tor-ohjelmistoja kaikkeen Internetin selaamiseen, jättämään Tor-ohjelmistot asentamatta, koska tällöin Internetin käyttäjä vain herättää isompaa huomiota valtioiden tiedustelussa ja häntä saatetaan seurata yhä enemmän Internetissä.

Suosittelisin Tor-ohjelmistojen opiskelua ja asennusta sellaisille tavallisille Internetin käyttäjille, jotka pitävät itseään kyvykkäänä omaksumaan Tor-ohjelmistojen turvallisen käytön ja jota ei häiritse mahdollinen valtioiden Internet-seuranta, koska ikinähän ei voi tietää, tuleeko kyseisille ohjelmistoille tarvetta esimerkiksi tulevaisuudessa tai ulkomailla. Näin Internetin käyttäjä olisi valmiiksi tietoinen siitä, miten Tor-ohjelmistoja käytetään ja niiden käyttäminen olisi helppo aloittaa, jos sille näkee tarvetta myöhemmin. Tämän kaltainen Internetin käyttäjä pystyy myös halutessaan tukemaan muita Tor-ohjelmistojen käyttäjiä käyttämällä satunnaisesti Tor-ohjelmistoja, koska mitä enemmän Tor-verkoissa on käyttäjiä, sitä vaikeampaa Tor-ohjelmistojen käyttäjiä on identifioida. Tällöin ne, jotka todella tarvitsevat ohjelmistoja saavat siitä tarvitsemansa turvan. Asiantuntijoiden ja testihenkilöiden vastausten perusteella vaikuttaisi siltä, että Tor-ohjelmistojen hyödyt koetaan haittoja tärkeämmäksi, minkä vuoksi mielestäni Tor-ohjelmistojen käyttäjien tukemista voidaan pitää hyvänä asiana.

8 Yhteenveto

Tämän opinnäytetyön tavoitteena oli selvittää, soveltuvatko Tor-ohjelmistot yksityisille tietokoneen käyttäjille. Opinnäytetyön tavoitteeseen pyrittiin vastaamaan seuraavia teemoja käsittelevien tutkimuskysymyksien pohjalta: Tor-ohjelmistojen käyttäjämäärän mahdollinen tuleva suunta, Tor-ohjelmistojen tarpeellisuus suomalaisille Internetin käyttäjille ja osaavatko suomalaiset käyttää Tor-ohjelmistoja turvallisesti. Vastaavanlaista tutkimusta ei ole aikaisemmin toteutettu, ja koska Tor-ohjelmistojen käyttäjämäärät ovat kasvaneet viime vuosien aikana Internetin sensuroinnin ja seuraamisen takia, on syytä selvittää soveltuvatko Tor-ohjelmistot yksityisille tietokoneen käyttäjille.

Teoriataustassa tarkasteltiin Internet-sensuuria, Internetin käyttäjien seuraamista ja tietojen keräämistä ja Tor-ohjelmistoja. Tutkimuksessa toteutettiin asiantuntijoille suunnattu kysely ja Tor-ohjelmistojen käyttöönottotestaus viidelle testihenkilölle. Tutkimuksessa saatiin selville, että Tor-ohjelmistojen käyttäjämäärissä ei ole lähitulevaisuudessa odotettavissa radikaaleja muutoksia, tosin käyttäjämäärät saattavat tulevaisuudessa kasvaa, jos Tor-ohjelmistoille nähdään suurempaa tarvetta. Tutkimuksessa selvisi, ettei Tor-ohjelmistoja koeta Suomessa kovinkaan tarpeellisina, mutta tarve mahdollisesti kasvaa tulevaisuudessa riippuen siitä, tuleeko Internetin sensurointi ja seuraaminen kasvamaan Suomen tai EU-maiden alueilla. Vaikka Suomessa Tor-ohjelmistojen tarvetta ei koeta kovinkaan suureksi, voivat jotkin tahot pitää Tor-ohjelmistoja tarpeellisena esimerkiksi Internet seuraamisen vuoksi. Sellaisten henkilöiden, jotka tuntevat tarvitsevansa Tor-ohjelmistoja, pitää huomioida se, minkä takia käyttäisivät Tor-ohjelmistoja, kuten keneltä olisivat suojautumassa ja miksi. Tämä on tärkeää siksi, että täydellistä turvaa on mahdotonta saavuttaa ja joissakin tapauksissa käyttäjä voi olla mahdollista selvittää. Tor-ohjelmistojen turvallisuutta ja luotettavuutta voidaan pitää suhteellisen hyvinä, mutta isoimpana turvallisuusuhkana voidaan pitää käyttäjää, joka ei ole perehtynyt ohjelmistojen toimintaan ja käyttöön. Tor-ohjelmistojen käyttäminen onnistuu tavalliselta Internetin käyttäjältä turvallisesti, kunhan vain Internetin käyttäjä tutustuu huolellisesti Tor-ohjelmistoihin ennen niiden käyttöönottoa, jotta osaa varmasti käyttää Tor-ohjelmistoja oikein. Sellainen Internetin käyttäjä, joka ei ymmärrä, miten Tor-ohjelmistoja käytetään turvallisesti, asettaa oman tietoturvansa vaaraan, jolloin Tor-ohjelmistojen käytöstä voi olla enemmän haittaa kuin hyötyä. Tor-ohjelmistojen käyttä-

jältä vaaditaan ymmärrystä siitä, mihin Tor-ohjelmistot pystyvät ja mihin eivät sekä sitä, että he ovat tarvittaessa valmiita muuttamaan Internetin käyttötapojaan.

Työn alussa esitin hypoteesin siitä, etteivät Tor-ohjelmistot sovellu tavallisille Internetin käyttäjille, koska he eivät oletettavasti osaa käyttää Tor-ohjelmistoja turvallisesti ja eivät ole valmiita muuttamaan Internetin käyttötapojaan. Perustin oletukseni siihen, että tavallinen Internetin käyttäjä ei välttämättä tiedosta Tor-ohjelmistojen mahdollisia turvallisuusriskejä, eikä tavallinen suomalainen Internetin käyttäjä häiriinny häneen kohdistuvasta Internetissä tapahtuvasta seurannasta ja sensuurista. Työni tulokset eivät täysin tukeneet hypoteesiani, koska Tor-ohjelmistojen käyttäminen voi onnistua tavalliseltakin Internetin käyttäjältä turvallisesti. Hypoteesiani toisaalta tuki se, etteivät ainakaan käyttöönoton testihenkilöt olleet valmiita muuttamaan Internetin käyttötapojaan, osaksi siksi, ettei heitä häirinnyt Internetissä tapahtuva seuranta ja sensuuri.

Mielestäni Internet-sensuuri on hyväksyttävä asia, jos sillä tavoitellaan valtion laittomien Internet-sivustojen estämistä, kuten lapsiporno-sivustot, mutta en näe Internet-sensuuria lopullisena ratkaisuna tälle ongelmalle. Internet-sensuuria on tällä hetkellä suhteellisen helppoa kiertää ja sillä mielestäni yritetään vain nopeasti lakaista ongelmat pois näkyvistä, vaikka ongelma silti pysyy. Pidän myös Internetin käyttäjien seuraamista joissakin määrin hyväksyttävänä, mutta mielestäni sitä ei saisi tehdä tavallisten kansalaisten kustannuksella. Ymmärrän, että valtioilla on tahto seurata esimerkiksi muiden valtioiden johtohenkilöiden tai rikollisjärjestöjen toimia, mutta en ymmärrä, miksi tavallisista kansalaisista kerätään tietoa. Mielestäni tämä vaikeuttaa todellisten rikosten estämistä, koska tiedon määrän kasvaessa on vaikeampaa löytää todellisia uhkia tai rikollisia. Spekulaatioitani tukee myös se, ettei lähdekirjallisuudessa, asiantuntijoiden vastauksissa tai testihenkilöiden palautteessa ollut selkeitä viitteitä siihen, että he pitäisivät Internet-sensuurin ja -seurannan tilannetta hyvänä. Tällä hetkellä Internetissä toimii omin päin monia organisaatioita, jotka yrittävät löytää Internetistä rikollisia tai estää rikollista toimintaa Internetissä. Mielestäni näiden organisaatioiden pitäisi tehdä yhteistyötä ja sopia yhteiset säännöt Internetiin, koska näin Internet pysyisi maailmanlaajuisena. Organisaatioiden yhdistämisellä saataisiin Internetiin niin sanottu maailmanlaajuinen ylläpitäjä, joka pitäisi Internetistä rikollisuuden poissa ja näin Internet-sivustojakaan ei tar-

vitsisi estää jokaisessa maassa yksitellen, vaan sivut olisi mahdollista sulkea kokonaan Internetin ylläpitäjän toimesta.

Pidän Tor-ohjelmistoja hyvänä asiana, koska niiden avulla Internetin käyttäjillä on mahdollisuus yksityisyyteen. Suomessa on mahdollista esimerkiksi äänestää vaaleissa anonyymisti, joten miksei vastaavaa anonyymiä mahdollisuutta voisi olla käyttäessä Internetiä? Vaikka moni Internetin käyttäjä saattaa ajatella, että häntä ei Internet-seuranta haittaa, voi jotakin toista henkilöä tämä haitata. Suomessa kaikilla aikuisilla kansalaisilla on äänioikeus, vaikka kaikki eivät kuitenkaan äänestä, joten miksei anonyymiyden mahdollisuutta annettaisi Internetissä, vaikka kaikki sitä ei välttämättä tarvitsisikaan? Ihmiset, joita tietojen kerääminen ei haittaa, voivat mielestäni jakaa tietonsa Internetissä vapaasti, mutta niille ihmisille, jotka eivät tätä halua tehdä, pitäisi olla mahdollisuus pitää tietonsa itsellään. Oletettavaa on, etteivät kaikki Internetin käyttäjät ole valmiita ottamaan Toria käyttöön. Mielestäni olisi hyvä, jos Torin ominaisuuksia pystyttäisiin integroimaan tuotteisiin jo valmiiksi niin, ettei niiden käyttämiseen tarvitsisi perehtyä, vaan tuotteet hoitaisivat käytön turvallisesti käyttäjän puolesta. Vaikka Tor-ohjelmistot mahdollistavatkin laittomuuksien tekemisen, ei se tarkoita sitä, että niitä pitäisi käyttää siihen. Näin ollen toivon, että kaikki Tor-ohjelmistojen käyttäjät noudattavat maansa asettamia lakeja.

8.1 Tutkimuksen hyödyllisyys

Tutkimuksen tulokset ovat hyödyllisiä Tor-ohjelmistojen kehittäjille ja käyttäjille, koska tuloksia huomioimalla voidaan lisätä ohjelmistojen turvallisuutta. Käyttöönottotestauksessa selvisi, että Tor-ohjelmistojen eheyden tarkastaminen ja turvallinen käyttäminen olivat käyttäjille suurimmat kompastuskivet. Tämä voisi viitata siihen, että käyttäjät tarvitsevat helpomman tavan tarkistaa eheyden ja selkeämmät ohjeet tämän toteuttamiseen. Turvallisessa käyttämisessä oli haastavinta löytää ohjeet siihen, miten Tor-ohjelmistoja käytetään turvallisesti, koska ohjeiden löytymisen jälkeen testihenkilöt kuitenkin ymmärsivät hyvällä menestyksellä Tor-ohjelmistojen turvallisen käytön ohjenuorat. Kyseisen riskitekijän kehittäjät pystyvät eliminoimaan ohjaamalla Tor-ohjelmistojen käyttäjiä niin, että heidän on pakko tutustua turvallisen käytön ohjeisiin ennen ohjelmistojen käyttämistä. Nämä seikat olisivat kehittäjien osalta suhteellisen

pieniä toimenpiteitä, joilla he pystyisivät edesauttamaan Tor-ohjelmistojen käyttämisen turvallisuutta.

Työni avulla tavallisilla tietokoneen käyttäjilläkin on mahdollisuus paremmin arvioida omaa tilannettaan ja sitä, onko heillä tarvetta Tor-ohjelmistoille. Lisäksi työni antaa hyvät perustiedot Internetin käyttäjälle Internet-sensuurista ja -seuraamisesta, jolloin Internetin käyttäjä voi harkita, näkeekö tarvetta Tor-ohjelmistoille. Tutkimuksesta hyötyy myös Tor-ohjelmistojen käyttäjät ja tavalliset tietokoneen käyttäjät, jotka ottavat Tor-ohjelmistoja käyttöön, koska tutkimuksessa käsitellään Tor-ohjelmistojen toimintaa, käyttöä ja riskejä, joiden ymmärtämisellä saa hyvät valmiudet käyttöönottaa ja käyttää Tor-ohjelmistoja. Kokonaisuutena työstäni voi olla apua mahdollisten tietoturvauhkien minimoimisessa, varsinkin jos Tor-ohjelmistojen käyttäjämäärät tulevaisuudessa kasvavat.

8.2 Tutkimuksen haasteet

Tutkimuksessa nousi esille, ettei kukaan testihenkilöistä nähnyt tarvetta Tor-ohjelmistoille, tutkimus on toteutettu suomalaisilla Internetin käyttäjillä ja vielä lisäksi suomeksi. Testiosioon olisi ollut mielenkiintoista saada tutkimustuloksia ja mielipiteitä testihenkilöiltä, jotka olisivat nähneet Tor-ohjelmistoille tarvetta käyttöönoton jälkeen. Tämän kaltaisten testihenkilöiden saaminen olisi ollut toisaalta suhteellisen haastavaa, koska tutkimuksen pohdinnassa todettiin, ettei Suomessa ole Tor-ohjelmistoille kovinkaan suurta tarvetta, jolloin testihenkilöiden määrää olisi joutunut kasvattamaan suuremmaksi. Toisaalta tämä toi tutkimuksessa esille yhdenmukaisuutta Tor-ohjelmistojen tarpeesta Suomessa, koska yksikään ei nähnyt tarvetta Tor-ohjelmistoille, vaikka testihenkilöt oli valittu suhteellisen satunnaisesti, kuitenkin tietynlaiset kriteerit täyttäen. Tällä hetkellä Suomessa Tor-ohjelmistojen tarpeen ollessa suhteellisen pieni olisi esimerkiksi englanniksi kirjoitetulla ja toteutetulla tutkimuksella voitu saada suurempi hyöty, koska kohdeyleisö olisi isompi. Toisaalta tästä ei ollut haittaakaan, koska suomalaisten tarvetta Tor-ohjelmistoille tulevaisuudessa on mahdoton ennustaa.

Testin tuloksia ei voi yleistää koskemaan kaikkia Internetin käyttäjiä, koska testihenkilöt olivat valittu pienestä ikähaarukasta ja heitä oli vain viisi. Asiantuntijoille esitetystä kyse-

lystä ilmeni myös, ettei kukaan asiantuntijoista ollut selkeästi Internet-sensuurin ja -seurannan puolella, mikä saattoi vääristää kyselyn tuloksia. Toisaalta teoriaosuudessa käytetystä lähdemateriaalistakin huomasi saman, että Internet-sensuurin ja -seurannan puolustajia oli haastavaa löytää, mikä tuo kyselyn tuloksiin enemmän luotettavuutta. Tutkimukseen olisi pitänyt saada suurempi otanta testihenkilöitä ja asiantuntijoita, jotta työn tulokset olisivat olleet täsmällisempiä. Tässäkään tapauksessa työn tuloksia ei olisi voinut yleistää maailmanlaajuiseksi, vaikka Internet on maailmanlaajuinen, koska jokaisella Internetin käyttäjällä on eri lähtökohdat eri maissa.

8.3 Jatkotutkimusehdotukset

Tässä kappaleessa esitetään neljä mahdollista jatkotutkimuskohdetta, joita anonyymin Internetin käytön kannalta olisi suositeltavaa tutkia: anonyymin Internetin käyttö mobiililaitteilla, Tor-ohjelmistojen sopivuus yrityskäyttöön, Tor-verkon solmut ja Tor-ohjelmistojen käyttäjät.

Mielestäni hyvä olisi perehtyä siihen, miten Internetiä voidaan käyttää anonyymisti mobiililaitteilla. Suomalaisista yli 60 prosenttia omistaa älypuhelimen (Sutinen 2013). Näissä älypuhelimissa käytetään samoja Internet-palveluita, joita käytetään tietokoneellakin, jolloin Internetissä tapahtuva seuranta ja sensuuri kohdistuvat myös mobiililaitteisiin (Järvinen 2014a, 292, 294, 296–297) ja jolloin Internetin käyttäminen anonyymisti voi tulla kysymykseen mobiililaitteillakin. Tällä hetkellä mobiililaitteisiin on kehitetty erilaisia ohjelmistoja, kuten Tor projektin Orbot ja Orweb sekä F-Securen Freedome (F-Secure 2014; The Guardian Project 2014a; The Guardian Project 2014b). Tällaisella tutkimuksella olisi mahdollista selvittää, mitä eri ohjelmistoja mobiililaitteille on ja miten ne eroavat toisistaan esimerkiksi hinnan, toimivuuden ja ominaisuuksien suhteen.

Osa asiantuntijoista ja testihenkilöistä mainitsi Tor-ohjelmistojen käytöstä yrityksissä. Hyvä olisi siis tutkia myös Tor-ohjelmistojen sopivuutta yrityskäyttöön. Tutkimuksessa selvitettäisiin, minkälaiset yritykset voisivat tarvita Tor-ohjelmistoja ja mihin käyttöön sekä mitä hyötyjä Tor-ohjelmistojen käyttö toisi yritykselle.

Kolmas jatkotutkimusehdotukseni on edellä mainittuja hieman teknillisempi. Tutkimuksessa käsiteltiin Tor-verkkojen toimintaa, joten mielestäni aiheellista olisi tutkia myös Tor-verkkoa tarkemmin. Työssä tutkittaisiin tarkemmin Tor-verkon solmujen toimintaa, kuten mitä vaatimuksia Tor-verkon solmujen ylläpitoon on, esimerkiksi laitteistoon ja Internet-yhteyden nopeuteen liittyen, sekä millaisia Tor-verkon solmujen ominaisuudet ovat, esimerkiksi niiden piilotetut palvelut ja sillat. Tutkimuksessa voitaisiin myös käyttöönottaa Tor-verkon solmu ja tehdä käyttöönotosta selvitys.

Työni tuloksissa selvisi, että tavallisella tietokoneen käyttäjällä voi olla haasteita asentaa ja käyttää Tor-ohjelmistoja oikein. Tästä syystä olisi tärkeää tutkia tavallisten tietokoneiden käyttäjien käyttökokemuksia laajemmin. Tutkimuksessa voisi tutkia tavallisia tietokoneen käyttäjiä, jotka käyttävät Tor-ohjelmistoja. Tor-ohjelmistojen käyttäjistä olisi mahdollisuus tutkia esimerkiksi seuraavia asioita: Käyttävätkö he Tor-ohjelmistoja oikein ja turvallisesti, miksi ja mihin he käyttävät Tor-ohjelmistoja sekä miten he kehittäisivät ohjelmistoja heille sopivammiksi esimerkiksi käytettävyydeltä, toiminnalta ja ominaisuuksilta. Tämänkaltainen jatkotutkimus jatkaisi eteenpäin siitä, mihin tämä tutkimus jäi, tutkimalla sellaisia Tor-ohjelmistojen käyttäjiä, joille ohjelmistot ovat jo valmiiksi tuttuja ja joilla on jokin seikka motivoimassa kyseisten ohjelmien käyttöä. Tutkimuksessa pystyisi hyödyntämään työssäni saatuja tuloksia ja huomioimaan niitä asioita mitkä nousivat työssäni esille esimerkiksi Tor-ohjelmistojen turvalliseen käyttöön liittyen.

Lähteet

Aikio, A. & Vornanen, R. 2000. Uusi sivistysanakirja. 19. uudistettu painos. Otava. Keuruu.

Akdeniz, Y. & Altiparmak, K. 2008. Internet: Restricted Access A Critical Assessment of Internet Content Regulation and Censorship in Turkey. Luettavissa: http://www.cyber-rights.org/reports/internet_restricted_colour.pdf. Luettu: 1.11.2014.

Alexa 2014. The top 500 sites on the web. Luettavissa: http://www.alexa.com/topsites. Luettu: 1.11.2014.

Bahajji, Z.A. & Illyes, G. 2014. HTTPS as a ranking signal. Google Online Security Blog. Luettavissa: http://googleonlinesecurity.blogspot.in/2014/08/https-as-ranking-signal_6.html. Luettu: 1.11.2014.

Bambauer, D.E., Deibert, R.J., John G. Palfrey Jr., Rohozinski, R., Villeneuve, R. & Zittrain, J. 2005. Internet Filtering in China in 2004-2005: A Country Study. Luettavissa: https://opennet.net/sites/opennet.net/files/ONI_China_Country_Study.pdf. Luettu: 1.11.2014.

BBC 2014a. Officials in Turkey 'lift Twitter ban'. Luettavissa: http://www.bbc.com/news/world-europe-26873603. Luettu: 1.11.2014.

BBC 2014b. Turkish court orders YouTube access to be restored. Luettavissa: http://www.bbc.com/news/technology-27623640. Luettu: 1.11.2014.

Brunila, M. 2014. Onko NSA-vuotajia kaksi? Digitoday. Luettavissa: http://www.digitoday.fi/yhteiskunta/2014/07/04/onko-nsa-vuotajia-kaksi/20149405/66. Luettu: 1.11.2014.

Christie-Miller, A. 2014. Turkey bans Twitter - and Turks make it trend worldwide. The Christian Science Monitor. Luettavissa: http://www.csmonitor.com/World/Middle-East/2014/0321/Turkey-bans-Twitter-and-Turks-make-it-trend-worldwide. Luettu: 1.11.2014.

Digitoday 2014. Snowdenin pommi: 90 % NSA:n urkkimista sivullisia, NSA säilyttää viestit ja tuhmat kuvat. Luettavissa: http://www.digitoday.fi/tietoturva/2014/07/07/snowdenin-pommi-90--nsan-urkkimista-sivullisia-nsa-sailyttaa-viestit-ja-tuhmat-kuvat/20149488/66. Luettu: 1.11.2014.

Dingledine, R. & Mathewson, N. 2006. Anonymity Loves Company: Usability and the Network Effect. The Free Haven Project. Luettavissa: http://freehaven.net/anonbib/cache/usability:weis2006.pdf. Luettu: 1.11.2014.

EFF 2014. HTTPS Everywhere. Luettavissa: https://www.eff.org/https-everywhere. Luettu: 1.11.2014.

Elisa Oyj 2011. Elisa tulee valittamaan väliaikaisesta Pirate Bay -määräyksestä. Luettavissa: http://elisa.fi/ir/pressi/index.cfm?t=100&o=5120&did=17563. Luettu: 1.8.2014.

Elliott, J. & Meyer, T. 2013. Claim on "Attacks Thwarted" by NSA Spreads Despite Lack of Evidence. ProPublica. Luettavissa: http://www.propublica.org/article/claim-on-attacks-thwarted-by-nsa-spreads-despite-lack-of-evidence. Luettu: 1.11.2014.

Engelli Web 2014. Luettavissa: http://engelliweb.com/. Luettu: 1.11.2014.

Facebook 2014. Tietojenkäyttökäytäntö. Luettavissa: https://www.facebook.com/about/privacy/your-info. Luettu: 1.11.2014.

Finley, K. 2014. Out in the Open: Inside the Operating System Edward Snowden Used to Evade the NSA. Wired. Luettavissa: http://www.wired.com/2014/04/tails/. Luettu: 1.11.2014.

F-Secure 2014. Freedome. Luettavissa: https://www.f-secure.com/en/web/home_global/freedome. Luettu: 1.11.2014.

GNU 2014. What is free software? Luettavissa: http://www.gnu.org/philosophy/free-sw.html. Luettu: 1.11.2014.

Google 2014. Tietosuojakäytäntö. Luettavissa: https://www.google.com/intl/fi/policies/privacy/. Luettu: 1.11.2014.

Gpg4win 2014. Download. Luettavissa: http://gpg4win.org/download.html. Luettu: 1.11.2014.

Greatfirewallofchina.org 2014. Luettavissa: http://www.greatfirewallofchina.org/index.php. Luettu: 1.11.2014.

Greenwald, G. 2014. Edward Snowden - Ei pakopaikkaa. Gummerus Kustannus Oy. Tanska.

Hallituksen esitys Eduskunnalle laiksi lapsipornografian levittämisen estotoimista (HE 99/2006).

Hallituksen esitys Eduskunnalle sähköisen viestinnän tietosuojalain ja eräiden siihen liittyvien lakien muuttamisesta (HE 48/2008).

Hamilton, S. 2004. To what extent can libraries ensure free, equal and unhampered access to Internet-accessible information resources from a global perspective. IFLA. Luettavissa: http://archive.ifla.org/faife/report/StuartHamiltonPhD.pdf. Luettu: 1.11.2014.

HS 2012. TeliaSonera esti pääsyn Pirate Bay -nettipalveluun. Luettavissa: http://www.hs.fi/talous/a1305588140275. Luettu: 1.11.2014.

Human Right Watch 2006. Race to the Bottom: Corporate Complicity in Chinese Internet Censorship. Luettavissa: http://www.hrw.org/sites/default/files/reports/china0806webwcover.pdf. Luettu: 1.11.2014.

Internet World Stats 2012. Top 20 countries with the highest number of Internet users. Luettavissa: http://www.internetworldstats.com/top20.htm. Luettu: 1.11.2014.

Juutilainen, V. 2008. Kiistelty lapsipornosuodatus osittain vapaaehtoiseksi. Helsingin Sanomat. Luettavissa: http://www.hs.fi/kotimaa/artikkeli/+/1135235278283. Luettu: 16.7.2014.

Järvinen, P. 2014a. NSA - Näin meitä seurataan. Docendo. Jyväskylä.

Järvinen, P. 14.8.2014b. Tietotekniikka-asiantuntija. Sähköposti.

Karhula, P. & Ekholm, K. 2011. Onko anonyymiys uhka? Luettavissa: http://ojs.tsv.fi/index.php/signum/article/download/4582/4324. Luettu: 1.11.2014.

Laki lapsipornografian levittämisen estotoimista (1068/2006).

Lebo, H. 2013. Surveying The Digital Future. Luettavissa: http://www.worldinternetproject.net/_files/_Published/_oldis/713_2013_digital_future_report_usa.pdf. Luettu: 1.11.2014.

Lehto, T. 2013. Laaja lakiuudistus romuttaa Lex Nokian. It-viikko. Luettavissa: http://www.itviikko.fi/uutiset/2013/04/05/laaja-lakiuudistus-romuttaa-lex-nokian/20134956/7. Luettu: 1.11.2014.

Liikenne- ja viestintäministeriö. 10.9.2014. Sähköposti.

Linnake, T. 2008. Suomi leimasi prinsessan muistosivun lapsipornoksi. It-viikko. Luettavissa: http://www.itviikko.fi/tietoturva/2008/02/22/suomi-leimasi-prinsessan-muistosivun-lapsipornoksi/20085474/7. Luettu: 1.11.2014.

LiveLeak 2014. Turkish Prime Minister Erdogan's phone talks with his son Bilal, about where to hide the money (english translation). Luettavissa: http://www.liveleak.com/view?i=9f6_1393289511. Luettu: 1.11.2014.

Loshin, P. 2013. Practical Anonymity: Hiding in Plain Sight Online. Elsevier. Yhdysvallat

Mannila, M. 2008. Scorpions-kansi vapautui sensuurista. It-viikko. Luettavissa: http://www.itviikko.fi/tietoturva/2008/12/10/scorpions-kansi-vapautui-sensuurista/200831842/7. Luettu: 1.11.2014.

Mitchell, B. 2014a. DNS - Domain Name System. About.com. Luettavissa: http://compnetworking.about.com/cs/domainnamesystem/g/bldef_dns.htm. Luettu: 1.11.2014.

Mitchell, B. 2014b. HTTP. About.com. Luettavissa: http://compnetworking.about.com/od/networkprotocols/g/bldef_http.htm. Luettu: 1.11.2014.

Mozilla 2014. Mozilla Firefox ESR Overview. Luettavissa: https://www.mozilla.org/en-US/firefox/organizations/faq/. Luettu: 1.11.2014.

Murdoch, S.J. & Anderson, R. 2008. Tools and Technology of Internet Filtering. Teoksessa Deibert, R., Palfrey, J., Rohozinski, R. & Zittrain, J. (toim.) Access Denied: The Practice and Policy of Global Internet Filtering, s. 57–72. The MIT Press. Yhdysvallat. Luettavissa: http://www.cl.cam.ac.uk/~sjm217/papers/opennet08tools.pdf. Luettu: 1.11.2014.

Musil, S. 2014. Anonymous OS reportedly used by Snowden reaches version 1.0. CNET. Luettavissa: www.cnet.com/news/anonymous-os-reportedly-favored-by-nsa-whistle-blower-edward-snowden-reaches-version-1-0/. Luettu: 1.11.2014.

Nikki, M. 8.8.2014. Internet-aktivisti. Sähköposti.

Nimetön. 18.8.2014. Sähköposti.

NoScript 2014. What is it? Luettavissa: http://noscript.net/. Luettu: 1.11.2014.

Oksanen, V. 21.8.2014. Varapuheenjohtaja. Effi. Sähköposti.

OpenNet Initiative. Internet Filtering in China. Luettavissa: https://opennet.net/sites/opennet.net/files/ONI_China_2009.pdf. Luettu: 1.11.2014.

Opensource.com 2014. What is open source? Luettavissa: http://opensource.com/resources/what-open-source. Luettu: 1.11.2014.

Ozvilgin, O. & Coskun, O. 2014. Turkey lifts Twitter ban after court ruling. Reuters. Luettavissa: http://www.reuters.com/article/2014/04/03/us-turkey-twitter-idUSBREA320E120140403. Luettu: 1.11.2014.

Poliisi 2014a. Lapsipornografiasivuille pääsyn estäminen. Luettavissa: https://www.poliisi.fi/poliisi/krp/home.nsf/pages/A12612E6A0B3A1EBC2257549003F446E?opendocument. Luettu: 1.11.2014.

Poliisi 2014b. Tietotekniikkarikosten tunnusmerkistöjä. Luettavissa: https://www.poliisi.fi/poliisi/krp/home.nsf/pages/C2315A82BE4616A1C225783E0056EDE0. Luettu: 1.11.2014.

Poliisi 2014c. Tietotekniikkarikollisuus. Luettavissa: https://www.poliisi.fi/poliisi/krp/home.nsf/pages/63B3FC75928EFB7EC2256C8B0043A41E?opendocument. Luettu: 1.11.2014.

Poropudas, T 2008. Sensuurimielenosoitus keräsi 500 osanottajaa. Taloussanomat. Luettavissa: http://www.taloussanomat.fi/it-viikko/2008/03/04/sensuurimielenosoitus-kerasi-500-osanottajaa/20086603/133. Luettu: 1.11.2014.

Railas, L. 2005. Selvitys lainsäädännöllisistä esteistä ja muutostarpeista rikollisen ja lapsille haitallisen sisällön estokeinojen velvoittavuuteen liittyen. LVM Hanke: 42976, Dno: 1394/92/2005. Luettavissa: http://www.lvm.fi/fileserver/upl973-Railaksen%20selvitys.pdf. Luettu: 1.11.2014.

Reporters without borders 2010. Enemies of the Internet - Contries under Surveillance. Luettavissa: http://en.rsf.org/IMG/pdf/Internet_enemies.pdf. Luettu: 1.11.2014.

Rouse, M. 2014. Proxy server. WhatIs.com. Luettavissa: http://whatis.techtarget.com/definition/proxy-server. Luettu: 1.11.2014.

Sajari, P. 2008. Oikeusoppineet: Lex Nokia rikkoo perustuslakia. HS. Luettavissa: http://www.hs.fi/talous/artikkeli/Oikeusoppineet+Lex+Nokia+rikkoo+perustuslakia/1135241246344. Luettu: 16.7.2014.

Salokorpi, J. 2013. Myös TeliaSoneran Pirate Bay -esto pysyi hovioikeudessa. Yle. Luettavissa: http://yle.fi/uutiset/myos_teliasoneran_pirate_bay_-esto_pysyi_hovioikeudessa/6490873. Luettu: 1.11.2014.

Sezer, S. 2014. Turkey Twitter accounts appear blocked after Erdogan court action. Reuters. Luettavissa: http://www.reuters.com/article/2014/04/20/us-turkey-twitter-idUSBREA3J0ET20140420. Luettu: 1.11.2014.

Statista 2011. Average daily internet use of Americans in 2010, by age group. Luettavissa: http://www.statista.com/statistics/191552/average-daily-internet-use-of-us-americans-in-2010-by-age-group/. Luettu: 1.11.2014.

Statista 2014. Age distribution of internet users worldwide as of September 2013. Luettavissa: http://www.statista.com/statistics/272365/age-distribution-of-internet-users-worldwide/. Luettu: 1.11.2014.

Sutinen, R. 2013. Arki muuttuu yhä mobiilikeskeisemmäksi. TNS Gallup. Luettavissa: http://www.tns-gallup.fi/uutiset.php?aid=14935&k=14320. Luettu: 1.11.2014.

Syverson, P. 2005. Brief Selected History. Onion Routing. Luettavissa: http://www.onion-router.net/History.html. Luettu: 1.11.2014.

Tails 2014a. About. Luettavissa: https://tails.boum.org/about/index.en.html. Luettu: 1.11.2014.

Tails 2014b. Features and included software. Luettavissa: https://tails.boum.org/doc/about/features/index.en.html. Luettu: 1.11.2014.

Tails 2014c. Warning. Luettavissa: https://tails.boum.org/doc/about/warning/index.en.html. Luettu: 1.11.2014.

Tails 2014d. Installing onto a USB stick or SD card. Luettavissa: https://tails.boum.org/doc/first_steps/installation/index.en.html. Luettu: 1.11.2014.

Tails 2014e. Verify the ISO image using the command line. Luettavissa: https://tails.boum.org/doc/get/verify_the_iso_image_using_the_command_line/index.en.html. Luettu: 1.11.2014.

Tails 2014f. Download, verify and install. Luettavissa: https://tails.boum.org/download/. Luettu: 1.11.2014.

Tarvainen, T. 2008. Effin kantelu nettisensuurista oikeuskanslerille. Effi. Luettavissa: http://www.effi.org/blog/sensuurikantelu.html. Luettu: 1.11.2014.

The Guardian 2013. XKeyscore presentation from 2008. Luettavissa: http://www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-program-full-presentation. Luettu: 1.11.2014.

The Guardian Project 2014a. Orbot: Mobile Anonymity + Circumvention. Luettavissa: https://guardianproject.info/apps/orbot. Luettu: 1.11.2014.

The Guardian Project 2014b. Orweb: Private Web Browser. Luettavissa: https://guardianproject.info/apps/orweb/. Luettu: 1.11.2014.

The New Yorker 2014. Strongbox. Luettavissa: https://projects.newyorker.com/strongbox/. Luettu: 1.11.2014.

The Sydnet Morning Herald 2007. The hack of the year. Luettavissa: http://www.smh.com.au/articles/2007/11/12/1194766589522.html. Luettu: 1.11.2014.

Tikkanen, A. 25.8.2014. Security Response -osaston johtaja. F-Secure. Sähköposti.

Toivonen, T. 2014. Turkkilaisoikeus kumosi myös YouTube-kiellon. Yle. Luettavissa: http://yle.fi/uutiset/turkkilaisoikeus_kumosi_myos_youtube-kiellon/7173970. Luettu: 1.11.2014.

Tor Project 2014a. Torbutton. Luettavissa: https://www.torproject.org/torbutton/. Luettu: 1.11.2014.

Tor Project 2014b. Vidalia. Luettavissa: https://www.torproject.org/projects/vidalia.html.en. Luettu: 1.11.2014.

Tor Project 2014c. Tor Browser Bundle: Details. Luettavissa: https://www.torproject.org/projects/torbrowser-details.html.en#contents. Luettu: 1.11.2014.

Tor Project 2014d. What is the Tor Browser? Luettavissa: https://www.torproject.org/projects/torbrowser.html.en. Luettu: 1.11.2014.

Tor Project 2014e. Inception. Luettavissa: https://www.torproject.org/about/torusers.html.en. Luettu: 1.11.2014.

Tor Project 2014f. Tor: Bridges. Luettavissa: https://www.torproject.org/docs/bridges.html.en. Luettu: 1.11.2014.

Tor Project 2014g. Tor: Overview. Luettavissa: https://www.torproject.org/about/overview.html.en. Luettu: 1.11.2014.

Tor Project 2014h. Tor FAQ. Luettavissa: https://www.torproject.org/docs/faq. Luettu: 1.11.2014.

Tor Project 2014i. Tor: Sponsors. Luettavissa: https://www.torproject.org/about/sponsors.html.en. Luettu: 1.11.2014.

Tor Project 2014j. Core Tor People. Luettavissa: https://www.torproject.org/about/corepeople.html.en. Luettu: 1.11.2014.

Tor Project 2014k. Software & Services. Luettavissa: https://www.torproject.org/projects/projects.html.en. Luettu: 1.11.2014.

Tor Project 2014l. Tor Metrics: Users. Luettavissa: https://metrics.torproject.org/users.html. Luettu: 1.11.2014.

Tor Project 2014m. Want Tor to really work? Luettavissa: https://www.torproject.org/download/download.html.en. Luettu: 1.11.2014.

Tor Project 2014n. The Short User Manual. Luettavissa: https://www.torproject.org/dist/manual/short-user-manual_en.xhtml. Luettu: 1.11.2014.

Tor Project 2014o. Tor Metrics: Servers. Luettavissa :https://metrics.torproject.org/network.html. Luettu: 1.11.2014.

Tor Project 2014p. Tor Metrics: Bandwidth. Luettavissa: https://metrics.torproject.org/bandwidth.html. Luettu: 1.11.2014.

Tor Project 2014q. Tor Metrics: Performance. Luettavissa: https://metrics.torproject.org/performance.html. Luettu: 1.11.2014.

Tor Project 2014r. Tor Metrics: Performance. Luettavissa: https://www.torproject.org/docs/verifying-signatures.html.en. Luettu: 1.11.2014.

Valtioneuvosto 2014. Tietoyhteiskuntakaari eduskunnan käsiteltäväksi. Liikenne- ja viestintäministeriön tiedote. Luettavissa: http://valtioneuvosto.fi/ajankohtaista/tiedotteet/tiedote/fi.jsp?oid=407475. Luettu: 1.11.2014.

Vaughan-Nichols, S.J. 2011. Flash is dead. Long live HTML5. ZDNet. Luettavissa: http://www.zdnet.com/blog/networking/flash-is-dead-long-live-html5/1633. Luettu: 1.11.2014.

Viestintävirasto 2014. Evästeet. Luettavissa: https://www.viestintavirasto.fi/tietoturva/palveluidenturvallinenkaytto/evasteet.html. Luettu: 1.11.2014.

Wagner, B. 2008. Deep Packet Inspection and Internet Censorship: International Convergence on an 'Integrated Technology of Control'. Luettavissa: http://advocacy.globalvoicesonline.org/wp-content/uploads/2009/06/deeppacketinspectionandinternet-censorship2.pdf. Luettu: 1.11.2014.

Winter, P. & Lindskog, S. 2012. How China is Blocking Tor. Karlstad University. Luettavissa: http://arxiv.org/pdf/1204.0447v1.pdf. Luettu: 1.11.2014.

W3Schools 2014a. Browser Statistics Luettavissa:
http://www.w3schools.com/browsers/browsers_stats.asp. Luettu: 1.11.2014.

W3Schools 2014b. OS Platform Statistics. Luettavissa:
http://www.w3schools.com/browsers/browsers_os.asp. Luettu: 1.11.2014.

Ziccardi, G. 2013. Resistance, Liberation Technology and Human Rights in the Digital Age. Springer. Milano.

Liitteet

Liite 1. Tor Browserin asennusohje Windows 7-käyttöjärjestelmälle

Tässä asennusohjeessa käytetään Windows 7-käyttöjärjestelmää, mutta samat ohjeet toimivat muillakin Windowsin käyttöjärjestelmillä, kuten Windows 8 ja Windows Vista (Tor Project 2014d; Tor Project 2014r).

Asennustiedoston lataus

Tor Browser asennustiedosto ja ohjelmiston allekirjoitus löytyvät Tor-projektin Internet-sivustolta https://www.torproject.org/projects/torbrowser.html.en. Tor Browserin asennustiedosto on torbrowser-install-3.6.3_en-US.exe ja ohjelmiston allekirjoitus torbrowser-install-3.6.3_en-US.exe.asc. Tiedostojen nimissä saattaa olla eroavaisuuksia, koska versionumerot ja ohjelmiston kieli saattavat vaihdella, mutta tiedostonimien päätteet ovat aina samat.

Eheyden tarkastaminen

Ohjelmiston eheyden voi tarkastaa esimerkiksi GnuGP-ohjelmistolla (asennusohjeet GnuGP-ohjelmistoon löytyvät liitteestä 3).

GnuGP-ohjelmistoa käytetään komentotulkista (cmd.exe).
Avain allekirjoituksen tarkistamista varten ladataan komennolla, jossa "C:\polku \gpg2.exe" on hakemistopolku, johon GnuPG-ohjelmisto on asennettu:

```
"C:\polku\gpg2.exe" --keyserver x-hkp://pool.sks-keyservers.net --recv-keys 0x416F061063FEE659
```

Avaimen aitous tarkastetaan komennolla:

```
"C:\polku\gpg2.exe" --fingerprint 0x416F061063FEE659
```

Komennon jälkeen tulostuu seuraavanlaiset rivit:

```
pub   2048R/63FEE659 2003-10-16
    Key fingerprint = 8738 A680 B84B 3031 A630  F2DB 416F 0610 63FE E659
```

uid Erinn Clark <erinn@torproject.org>
uid Erinn Clark <erinn@debian.org>
uid Erinn Clark <erinn@double-helix.org>
sub 2048R/EB399FD7 2003-10-16

Ohjelmiston allekirjoitus tarkistetaan seuraavalla komennolla, jossa "C:\polku\" on hakemistopolku, missä tiedostot sijaitsevat:

"C:\polku \gpg2.exe" –verify "C:\polku\torbrowser-install-3.6.3_en-US.exe.asc"
"C:\polku\torbrowser-install-3.6.3_en-US.exe"

Komennon jälkeen pitäisi tulostua seuraavat rivit, joissa mainitaan Good signature. Tekstistä "WARNING: This key is not certified with a trusted signature!" ei tarvitse välittää. Varoitus johtuu siitä, että avainta ei ole asetettu luotettavien avainten joukkoon.

gpg: Signature made 07/25/14 20:19:46 FLE Daylight Time using RSA key ID 63FEE659
gpg: Good signature from "Erinn Clark <erinn@torproject.org>"
gpg: aka "Erinn Clark <erinn@debian.org>"
gpg: aka "Erinn Clark <erinn@double-helix.org>"
gpg: WARNING: This key is not certified with a trusted signature!
gpg: There is no indication that the signature belongs to the owner.
Primary key fingerprint: 8738 A680 B84B 3031 A630 F2DB 416F 0610 63FE E659

Näillä toimilla ohjelmisto on todettu eheäksi ja sen voi asentaa.

Asennus ja käynnistäminen

Avaamalla asennustiedoston torbrowser-install-3.6.3_en-US.exe asennus käynnistyy. Asennuksen jälkeen Tor Browser on valmis käynnistettäväksi. Ensimmäisellä käynnistyskerralla Tor Browser kysyy, halutaanko asetuksia muutella vai yhdistetäänkö suoraan. Koska Suomessa Tor Browseria ei ole estetty, riittää, kun painaa Connect-nappulaa ja Tor Browser yhdistää Tor-verkkoon. Onnistuneen asennuksen ja käynnistyksen jälkeen pitäisi avautua sivusto, jossa onnitellaan Torin käytöstä.

Ongelmatilanteissa voi kääntyä Tor-projektin sivustojen puoleen, josta löytyy ohjeita ongelmatilanteisiin ja kuvalliset asennusohjeet.

Liite 2. Tails-käyttöjärjestelmän asentaminen DVD-levylle käyttäen Windows 7-käyttöjärjestelmää

Asennusohjeet ovat tarkoitettu Windows 7-käyttöjärjestelmälle. Muita käyttöjärjestelmiä käyttäessä tai ongelmatilanteissa voi kääntyä Tailsin Internet-sivuston puoleen, josta löytyy lisää ohjeita. (Tails 2014d; Tails 2014e.)

Asennustiedoston lataus

Tails-käyttöjärjestelmä, Tailsin allekirjoitus ja allekirjoitusta varten tarkoitettu avain löytyvät Tailsin kotisivuilta https://tails.boum.org/download/.

Tails-käyttöjärjestelmän ISO-tiedoston nimi on tails-i386-1.1.iso, Tails-käyttöjärjestelmän allekirjoitustiedoston nimi on tails-i386-1.1.iso.sig ja allekirjoitusta varten tarkoitetun avaimen nimi on tails-signing.key. Nimissä saattaa olla eroavaisuuksia kielestä ja versioista johtuen, mutta tiedostojen nimien päätteet ovat aina samat.

Eheyden tarkastaminen

Tails-käyttöjärjestelmän eheyden voi tarkastaa esimerkiksi GnuGP-ohjelmistolla (asennusohjeet GnuGP-ohjelmistoon löytyvät liitteestä 3).

GnuGP-ohjelmistoa käytetään komentotulkista (cmd.exe). Tailsin allekirjoitusavain tuodaan GnuPG-ohjelmiston avaimiin komennolla, jossa "C:\polku \gpg2.exe" on hakemistopolku, johon GnuPG-ohjelmisto on asennettu:

```
"C:\polku\gpg2.exe" --keyid-format long --import "C:\polku\tails-signing.key"
```

Komennon jälkeen tulee ilmoitus onnistuneesta avaimen tuonnista:

```
gpg: key 1202821CBE2CD9C1: public key "Tails developers (signing key) <tails@boum.org>" imported
gpg: Total number processed: 1
gpg:               imported: 1  (RSA: 1)
gpg: no ultimately trusted keys found
```

Tämän jälkeen käyttöjärjestelmän eheys vahvistetaan komennolla, jossa "C:\polku\" on hakemistopolku, jossa tiedostot sijaitsevat:

"C:\polku \gpg2.exe" --keyid-format long --verify "C:\polku\tails-i386-1.1.iso.sig" "C:\polku\tails-i386-1.1.iso"

Komennon jälkeen pitäisi tulostua seuraavat rivit, joissa mainitaan Good signature. Tekstistä "WARNING: This key is not certified with a trusted signature!" ei tarvitse välittää. Varoitus johtuu siitä, että avainta ei ole asetettu luotettavien avainten joukkoon.

gpg: Signature made 07/22/14 18:30:31 FLE Daylight Time
gpg: using RSA key 1202821CBE2CD9C1
gpg: Good signature from "Tails developers (signing key) <tails@boum.org>"
gpg: WARNING: This key is not certified with a trusted signature!
gpg: There is no indication that the signature belongs to the owner.
Primary key fingerprint: 0D24 B36A A9A2 A651 7878 7645 1202 821C BE2C D9C1

Näillä toimilla käyttöjärjestelmä on todettu eheäksi ja sen voi asentaa DVD-levylle.

Asennus ja käynnistäminen

Tails-käyttöjärjestelmän tiedosto tails-i386-1.1.iso poltetaan tyhjälle DVD-levylle käyttäen Windows Disc Image Burneria. Suositeltavaa on rastittaa tiedoston tarkistaminen polttamisen jälkeen.

Onnistuneen DVD-levyn polttamisen jälkeen tietokone käynnistetään uudelleen niin, että se käynnistyy DVD-levyltä. Tails-käyttöjärjestelmän käynnistyttyä tietokone yhdistetään Internetiin.

Tails-käyttöjärjestelmä on onnistuneesti asennettu DVD-levylle ja käynnistetty siltä. Tilanteessa, jossa tietokone ei käynnisty automaattisesti Tails-käyttöjärjestelmään täytyy tietokoneen BIOS-asetuksia muuttaa. BIOS:n asetusten muuttamisesta löytyy tarkemmat ohjeet Ubuntun Internet-sivuilta: https://help.ubuntu.com/community/BootFromCD.

Liite 3. GnuPG:n asentaminen

Asennusohjeet toimivat Windows-käyttöjärjestelmillä (Gpg4win 2014).

GnuPG-ohjelmisto tulee Gpg4win-ohjelmiston asennuksen yhteydessä.

Gpg4win-ohjelmiston asennustiedosto löytyy Internet-osoitteesta: http://gpg4win.org/download.html.

Asennustiedoston lataamisen jälkeen Gpg4win-ohjelmiston eheyden tarkistaminen on suositeltavaa. Ohjelmiston eheys tarkistetaan asennustiedoston allekirjoituksesta. Ohjeita tähän toimenpiteeseen löytyy asennussivustolta.

Ladatun asennustiedoston nimi voi olla esimerkiksi gpg4win-2.2.1.exe. Avaamalla ladatun asennustiedoston ohjelmiston asennus alkaa. Asennusohjelmassa valitaan haluttu kieli ja halutut ohjelmistot, johon pelkästään GnuPG-ohjelmisto riittää, koska sillä voi tarkistaa ohjelmistojen eheyden. Asennuksen päätyttyä GnuPG-ohjelmisto on valmis käytettäväksi.

Liite 4. Testiohjeet testihenkilölle

Testissä asennetaan ja käytetään itsenäisesti Tor-ohjelmistoja. Oikein asennettuna ja käytettynä Tor-ohjelmistoilla voidaan käyttää Internetiä anonyymisti ja kiertäen Internet-sensuurit, välttäen näin kolmansien osapuolien, kuten yritysten tai valtioiden, tiedon keräämisen ja seuraamisen. Testin osioissa tullaan asentamaan käyttöä varten Tor-ohjelmistot Tor Browser -selain ja Tails-käyttöjärjestelmä.

Testin aikana etsitään omatoimisesti Internetistä tarvittavaa tietoa, jotta testit saadaan suoritettua onnistuneesti. Testihenkilö vastaa testin teettäjälle kolmannen osion kysymyksiin suullisesti ja viidenteen osioon kirjallisesti. Muut osiot toteutetaan itsenäisesti. Testin teettäjä valvoo koko testin ajan testihenkilön toimia ja kirjaa ylös **testin vaiheita**.

Suorita seuraavat osiot järjestyksessä:
Ensimmäinen osio, Tor Browserin asennus: Tee tarvittavat toimenpiteet, jotta pääset turvallisesti Tor Browserilla osoitteeseen www.torproject.org.

Toinen osio, Tails-käyttöjärjestelmän asennus: Tee tarvittavat toimenpiteet, jotta pääset turvallisesti osoitteeseen www.torproject.org käyttäen Tails-käyttöjärjestelmää.

Kolmas osio, Tor-ohjelmistojen turvallinen käyttäminen:
Tiesitkö ennen Torin käyttöönottoa, että selaimen tai käyttöjärjestelmän käyttämiseen on olemassa turvallisen käytön ohjeita, joita tulisi noudattaa Toria käyttäessä?

- **Kyllä**: Kerro turvallisen käytön ohjeista.

Hae turvallisen käytön ohjeita. Käy löytämäsi ohjeet läpi kohta kohdalta testin teettäjän kanssa.

Neljäs osio, käyttöjakso: Käytä Tor-ohjelmistoja kahden päivän ajan noudattaen turvallisen käytön ohjeita (liite 5). Käyttöjakson aikana on suositeltavaa ottaa muistiinpanoja viidennen osion palautetta koskien.

Viides osio, palaute:

1. Mitä mieltä olet Tor-ohjelmistoista?
2. Oliko Tor-ohjelmistojen käytössä tai asennuksessa ongelmia? Minkälaisia?
3. Onko Tor-ohjelmistojen käytöstä mielestäsi hyötyä tai haittaa?
4. Tuletko vastaisuudessa käyttämään Tor-ohjelmistoja? Miksi/miksi et?
5. Tulevatko Internetin käyttäjät mielestäsi siirtymään enemmän anonyymeihin verkkoihin, kuten Toriin? Miksi / miksi ei?

Liite 5. Turvallisen käytön ohjeet

Seuraavassa listassa on ohjeita turvalliseen Torin käyttämiseen (Loshin 2013, 12–14, 27–28, 49; Tails 2014c; Tor Project 2014m), joita käyttäjän olisi syytä noudattaa:

- Tor-ohjelmisto on asennettu oikein.
- Käytettävä tietokone on turvallinen, eikä siihen ole asennettu esimerkiksi haitta-ohjelmistoja.
- Torin tai sen osien asetuksia ei suositella muutettavaksi.
- Torrent-tiedostoja ei saa ladata Tor-verkon läpi.
- Torin selaimiin ei saa asentaa lisäosia.
- Selaimen lisäosille, jotka eivät kuulu Tor-ohjelmistoon ei saa antaa toimintalupaa, kuten Flash, RealPlayer ja Quicktime.
- Palveluihin, jotka eivät käytä HTTPS-protokollaa ei saa kirjautua.
- Maissa, joissa Tor on kielletty ohjelmisto, on suositeltavaa käyttää siltoja Internet-yhteyden luomiseksi Tor-verkkoon.

Osalle käyttäjistä voi riittää se, että käyttää Tor-ohjelmia turvallisesti, mutta osa haluaa käyttää Internetiä anonyymisti. Käyttäjä, joka haluaa pysyä Internetissä anonyyminä, on suositeltavaa noudattaa seuraavia ohjeita (Loshin 2013, 12–14, 27–28, 49; Tails 2014c; Tor Project 2014m):

- Käytetään vain Toriin kehitettyjä selaimia esimerkiksi Tor Browseria tai Tailsissä olevaa Iceweasel Web Browser -selainta.
- Ei saa kirjautua henkilökohtaisiin palveluihin, jotka sisältävät käyttäjän henkilökohtaisia tietoja.
- Mitään henkilökohtaisia tietojaan ei saa antaa Internet-sivustoille.
- Vältä Internet-sivustoja, jotka eivät käytä HTTPS-protokollaa.
- Ladattuja tiedostoja ei saa avata niin, että Internet-yhteys on auki.

Liite 6. Asiantuntijakyselyn vastaukset

1. **Mitä mieltä olet Internet-sensuurista? (esim. onko Internet-sensuurissa hyötyjä tai haittoja, millaista Internet-sensuuri on tulevaisuudessa jne.)**

Petteri Järvinen:

Internet-sensuuri on laaja käsite. Perinteistä valtiollista sensuuria on vaikea toteuttaa, sillä sen kiertäminen on helppoa, mutta silti on toivottavaa, että esimerkiksi lapsiporno tai luvatta levitettävät henkilötiedot voidaan poistaa netistä tai ihmisten pääsy niille estää. Valtiollisen sensuurin merkitys on vähentynyt, koska nykyinen internet tarjoaa niin helppoja keinoja teknisten estojen kiertämiseen. Parasta sensuuria on itsesensuuri – käyttäjien tulisi tarkkailla omaa toimintaansa ja miettiä, kannattaako kaikkea julkaista vaikka se teknisesti onkin mahdollista.

Ville Oksanen (Effi)

Sensuuri ei yleensä toimi ts. jopa Kiinan hyvin tehokkaasta "great firewall of Chinasta" pääsee läpi. Lisäksi sensuuri yleensä ylisensuroi ja alisensuroi samaan aikaan. Tämä on nähty konkreettisesti esimerkiksi lapsipornosuoduksen kanssa ([http://]www.lapsiporno.info Suomen osalta)

Antti Tikkanen (F-Secure)

Tietyissä maissa Internetiä sensuroidaan tai sen käyttöä pyritään estämään. Nykymaailmassa tietoa tuottavat uutismedioiden lisäksi kaikki internetin käyttäjät, ja millään valtiolla ei ole mahdollisuutta kontrolloida uutisten lähteitä. Tämä johtaa siihen että tiedon välitykseen käytettyjä verkkoja pyritään sensuroimaan. Tämä kehitys tulee epäilemättä jatkumaan tulevat vuosikymmenet.

Matti Nikki:

Internet-sensuuri tuhoaa Internetin.

Sensuuri on vain yksi ilmentymä isosta jutusta nimeltä "internet governance". Nettisensuurin jujunahan on se että ulkomaiset palvelimet ovat virkavallan toimintavaltuuksien ulkopuolella, joten tarvitaan valtamekanismi niiden kommunikointiin puuttumiseen. Yksittäiset valtiot näin kaappaavat väkivalloin itselleen valtaa Internetin hallin-

taan jotta voisivat omien rajojensa sisällä ikäänkuin määrätä internet governancesta ominpäin.

Tämähän vääjäämättä johtaa Internetin pirstaloitumiseen, jossa Internet ei enää olekaan neutraali ja kaikille samallatapaa toimiva kommunikaatioväline. Äärimmäisenä kehityksenä saattaa tulla eteen valtioiden rajoille nousevat palomuurit suodattamaan kiellettyä liikennettä, ja dystopisena tulevaisuudenkuvana voisi nähdä mahdollisuuden siitä että nämä palomuurit käännetäänkin toimivaan whitelist-periaatteella, että valtiorajojen yli kommunikointiin vaaditaan erikseen lupa joka myönnetään vain suuryrityksille ja jota koskee tiukat ehdot. Ehkäpä tulevaisuudessa tietoliikenneyhteyksien salakuljettaminen on rikos.

Internet-sensuurin tulevaisuudesta on ihan mahdoton sanoa. Sitä kun ei tiedä, ehkä EU herää valtataisteluun ja vaatii yhtenäistä sensuurikäytäntöä jonkin EU-viranomaisen valvontaan. Tekijänoikeusteollisuus on jo pitkään hamuillut saada lusikkansa kunnolla tähän soppaan, ehkä lopulta nähdään laaja-alaista liikehdintää silläkin rintamalla, ks. http://www.dw.de/eu-verdict-rekindles-internet-censorship-debate/a-17526954

Liikenne- ja viestintäministeriö

Sananvapaus on yksi perustuslaissamme turvatuista perusoikeuksista. Viranomaisten ei tule ainoastaan pidättäytyä perusoikeuksien loukkauksilta vaan viranomaisten lakisääteisenä velvollisuutena on myös aktiivisesti edistää sananvapauden ja muiden perusoikeuksien toteutumista. Sananvapauteen sisältyy oikeus ilmaista, julkistaa ja vastaanottaa tietoja, mielipiteitä ja muita viestejä kenenkään ennakolta estämättä.

Kaikkien käytettävissä olevalla avoimella ja luotettavalla internetillä on huomattava merkitys kansantaloudelle, kilpailukyvylle, investoinneille, työllisyydelle, hyvinvoinnille ja perusoikeuksien toteutumiselle. Internetin käytön tulisikin olla mahdollisimman vapaata ja siksi olisi hyvä pidättäytyä kaikenlaisesta sensuurista.

On kuitenkin tilanteita, joissa internetin käyttöä voi olla perusteltua rajoittaa, mutta näitten perusteiden tulee kestää erittäin tarkkaa arviointia ja olla myös tehokkaita tietyn ongelman ratkaisemiseksi. Sananvapautta, kuten muitakin perusoikeuksia, voi siis teori-

assa rajoittaa, mutta vain jos se on tarpeen perusoikeuksien toteutumisen tai muiden painavien yhteiskunnallisten intressien turvaamiseksi. Perusoikeuksien rajoitukset tulee säätää lailla; niiden tulee olla täsmällisesti ja tarkkarajaisesti määriteltyjä; niiden tulee perusoikeusjärjestelmän kannalta hyväksyttäviä ja painavan yhteiskunnallisen tarpeen vaatimia; rajoituksilla ei saa kajota perusoikeuden ydinalueelle; rajoitusten tulee olla välttämättömiä hyväksyttävän tavoitteen saavuttamiseksi ja oikeassa suhteessa perusoikeuden suojaamaan oikeushyvään ja rajoituksen taustalla olevan yhteiskunnallisen intressin painoarvoon. Lisäksi perusoikeuksia rajoitettaessa on turvattava kansalaisille riittävät ja tehokkaat oikeusturvakeinot. Rajoitukset eivät saa myöskään olla ristiriidassa Suomen hyväksymien kansainvälisten ihmisoikeusvelvoitteiden kanssa.

Usein internetin rajoittaminen tai sen yrittäminen ei välttämättä osoittaudu kovin tehokkaaksi toimenpiteeksi tietyn ongelman poistamiseksi. Päinvastoin maailmalla on nähty lukuisia esimerkkejä siitä, kuinka sananvapauden rajoitukset internetissä ovat johtaneet kansalaisille elinkeinoelämälle ja jopa viranomaisille vahingollisiin seurauksiin.

Nimetön:
Periaatteessa olen kaikenlaista nettisensuuria vastaan, sillä hyvätkin aikomukset esimerkiksi lapsipornon torjumiseksi ovat osoittautuneet Suomessa(kin) teknisesti vaikeiksi toteuttaa niin, että toimista olisi jotain todellista hyötyä – tai niin, ettei samalla aiheuteta haittaa viattomalle nettikäytölle. Lisäksi pelkona on ollut, että yhden asian sensurointi laskee kynnystä sensuroida jotain muuta myöhemmin. Ja Pirate Bay -estojen myötä näin näyttäisi jo tapahtuneen.

Euroopassa kysymys nettisensuurista on entistäkin ajankohtaisempi EU-oikeuden keväisen päätöksen myötä. Päätös liittyi laajempaan kysymykseen kansalaisten oikeudesta tulla unohdetuksi internetissä ja nyt muun muassa Googlen täytyy tarjota kansalaisille mahdollisuus anoa tiettyjen hakutulosten poistamista tietyissä tilanteissa. Tässä ovat vastakkain tietosuoja ja sananvapaus. Ja minusta jälkimmäinen ajaa edelle.

2. **Mitä mieltä olet käyttäjien seuraamisesta Internetissä ja että heistä kerätään tietoa? (esim. onko tietojen keräämisessä hyötyjä tai haittoja, mikä on seuraamisen tuleva suunta jne.)**

Petteri Järvinen:

Monet kuluttajat tuntuvat pitävän nettikäyttönsä seuraamista hyvänä asiana, koska se mahdollistaa palveluiden kehittämisen, räätälöinnin ja mainosten paremman kohdistamisen. Niillä, jotka näin haluavat, tulee olla oikeus se tehdä, koska tieto ihmisen nettikäytöstä on hänen henkilökohtaista omaisuuttaan ja se tulee voida myydä esimerkiksi ilmaispalvelua vastaan. Toisaalta niillä, jotka haluavat pitää kiinni yksityisyydestään, tulisi olla keinot suojata omia toimiaan netissä. Tällä hetkellä suojaus vaatii omatoimisuutta ja erilaisia teknisiä järjestelyjä, eikä se näytä lähiaikoina muuttuvan.

Ville Oksanen (Effi)

Suuri osa Internetistä perustuu käyttäjiltä kerättävien tietojen taloudelliseen arvoon. "Jos palvelu ei ole maksulinen, sinä olet sen tuote." Varsinkin Internet of Thingsin myötä tässä mennään nopeasti kohtuuttomuuksiin. Tällä hetkellä MyData-liike näyttää potentiaalisimmalta vastareaktiolta.

Antti Tikkanen (F-Secure)

Ennen viime kesää moni luuli, että verkossa surffaaminen on anonyymiä. Paljastukset Yhdysvaltojen turvallisuusvirasto NSA:n kyvystä seurata liikennettä herättivät todellisuuteen. Se paljasti, että tunnetut ja paljon käytetyt palvelut, esimerkiksi Google ja Apple, ovat tarkkailun kohteina. Lisäksi se kohdistui myös valtioiden johtohenkilöihin, kuten Saksan liittokansleri Angela Merkeliin (http://www.hs.fi/ulkomaat/a1382665750413). Vastaavaa tiedustelua harjoittavat kaikki siihen kykenevät valtiot, kukin omien mahdollisuuksiensa puitteissa.

Yritykset ja kuluttajat ovat kiinnostuneempia yksityisyydestään ja siitä, mitä heidän tiedoilleen tapahtuu. Lisäksi monimutkaisista teknologia-,turvallisuus- ja yksityisyyskysymyksistä käydään globaalia keskustelua.

Seuranta lisää tietoturvariskejä, mielestämme tietoturvayhtiönä meillä on nyt velvollisuus palvella maailmanlaajuisesti asiakkaita, jotka haluavat mieluiten olla tekemisissä yksityisyyttä suojaavien kuin seurantaa harjoittavien yritysten kanssa.

Yksityisyys on aina ollut keskeinen osa F-Securen toimintaa ja se näkyy monissa tuotteissamme.

Matti Nikki:
Seuranta on periaatteessa yksityisyyden loukkaamista, ja ties mihin käyttöön tiedot lopulta päätyvät. Mainostajien käyttämiä seurantamekanismeja hyödynnetään myös valtiollisella tasolla, muunmuassa NSA oli seurannut (ja seuraa kai vieläkin) googlen tracking cookieita ja nyysinyt tiedot omaan käyttöönsä.

Käytännössä yksityisyydestään välittävät tahot leimaantuvat ennenpitkää suoraan potentiaalisiksi rikollisiksi kun seurannan kattavuus lähestyy täydellistä. Tällä voi olla melko brutaaleja seurauksia mikäli hallitus ei ole sellainen "kiltti" niinkuin suomessa, maailmallahan monet hallitukset käyttävät kansalaistensa seurantaa kontrolloidakseen poliittista oppositiota...

Ihmisoikeuksien toteutumisen takaamiseksi kommunikaation yksityisyys on välttämätöntä ja Internet-käyttäjien seuranta on sen suora vihollinen.

Liikenne- ja viestintäministeriö
Viime vuosina internetin ja sen palvelujen käyttäjistä kerättävä tieto ja tämän tiedon arvo on räjähdysmäisesti kasvanut. Tietojen keräämisestä on varmasti sekä hyötyä että haittaa. Suoria hyötyjä käyttäjille itselleen voi tulla esim. siitä, että tutkimalla asiakkaiden käyttäytymistä yritykset voivat tarjota yhä parempia ja personoidumpia palveluita. Haittoja on selkeästi vaikeampi vielä konkretisoida, mutta pitkälle vietynä esimerkiksi profilointi voi johtaa esimerkiksi hintasyrjintään. Lisäksi on hyvä muistaa, että kerättyjen tietojen päätyminen vääriin käsiin, esim. rikollisille, voi johtaa huomattaviinkin vahinkoihin.

Jokaisella on Suomessa oikeus turvattuun yksityiselämään, johon sisältyy myös henkilötietojen nauttima suoja. Henkilöihin yhdistettävissä olevia tietoja syntyy erittäin paljon aivan arkisissa yhteyksissä. Tätä kehitystä kiihdyttävät erilaista digitaalista tietoa tuottavien sensorien yleistyminen tietokoneissa, matkapuhelimissa, televisioissa, maksuvälineissä, ajoneuvoissa ja lukemattomissa muissa niin sanotuissa ”älytuotteissa”, kuten

esim. internetiin kytkeytyvissä älyjääkaapeissa. Useimmiten tietojen kerääminen tapahtuu laitteen tai palvelun käyttäjien suostumuksella (käyttäjäehdot). Monesti käyttäjät altistavatkin itsensä yksityisyyttänsä koskevien tietojen keräämisen kohteeksi, koska kokevat saavansa näin heidän tarpeitaan vastaavan palvelun, jopa ”ilmaiseksi”.

Kehityksen jarruttamisen sijaan tulisi keskittyä ilmiön sekä sen avaamien mahdollisuuksien ja riskien ymmärtämiseen. Siksi osaamista ja ymmärrystä olisi syytä parantaa esimerkiksi kehittämällä digitaalisten hyödykkeiden tietosuoja- sekä tietosuojaominaisuuksien läpinäkyvyyttä, todennettavuutta ja vertailtavuutta. Lisäksi olisi varmasti hyvä, että markkinat tarjoaisivat käyttäjille erilaisilla rahoitustavoilla toimivia palveluita. On myös varmasti olemassa sellaisia yhteiskunnallisia palveluita, joiden maksamista käyttäjien yksityiselämää kuvaavilla tiedoilla ei voida pitää lainkaan hyväksyttävänä. Olisi esimerkiksi vaikea nähdä, että pakollisen liikennevakuutuksen saamisen ehtona olisi luovutettava vakuutusyhtiölle vaikkapa viestintäänsä tai ostoskäyttäytymistään koskevia tietoja.

Tahdonvastaiseen henkilötietojen tai luottamuksellista viestintää koskevien tietojen keräämiseen on suhtauduttava huomattavasti tiukemmin kuin suostumukseen perustuvaan tietojen keräämiseen. Jo perustuslaki edellyttää, että jokaisen yksityiselämä ja luottamuksellinen viestintä ovat turvattuja. Tämän oikeuden rajoittamista arvioitaessa tulee noudattaa huolellisesti ensimmäisessä vastauksessa kuvattua menettelyä ja intressipunnintaa.

Nimetön:
Käyttäjien seuraaminen internetissä ja tietojen kerääminen on tiettyyn pisteeseen saakka tarpeellista, jotta vaikkapa mobiilit paikkatietopalvelut pystyvät tarjoamaan kuluttajille ja miksei yrityksillekin niitä palveluja, joita he odottavat. Toisaalta on tullut selväksi, että tämän varjolla on monissa tapauksissa kerätty turhan paljon tietoa enemmän tai vähemmän vahingossa.

Tulevaisuus riippuu siitä, kuinka valppaasti käyttäjät alkavat katsoa tietojensa keräämisen perään ja vaatia tietosuojaa. Välillä näyttää siltä, että suuri yleisö suhtautuu asiaan melko apaattisesti, kuten Facebook on todistanut. Se on jatkanut kasvuaan siitä huolimatta, että palvelu on käynyt läpi useita käyttäjien tietoja koskevia selkkauksia.

3. **Mitä mieltä olet anonyymeistä verkoista, kuten Torista?**

Petteri Järvinen:

Kuten kaikki anonymiteetti, Torin liittyy hyviä ja huonoja puolia. Se on monissa maissa ainoa melko turvallinen keino netissä liikkumiseen, toisaalta etenkin länsimaissa se tarjoaa keinon laittomuuksiin ja toisten häiriköintiin. Anonymiteettiä on ollut aina, myös nettimaailman ulkopuolella, joten tällä hetkellä Tor ei ole mikään ongelma. Tilanne voi muuttua, jos nettimaailman rikolliset alkavat toden teolla hyödyntää sitä. Oleellista on, että rikoksiin syyllistyviltä jää jatkossakin jälkiä, jotta riittävän moni (ei kaikkia) heistä voidaan jäljittää.

Ville Oksanen (Effi)

Välttämätön työkalu, mikäli haluaa suojata identiteettinsä.

Antti Tikkanen (F-Secure)

Monet haluavat pysyä anonyymina verkossa. Tällainen teknologia on alkanut kiinnostaa myös yrityksiä ja muita korkeaa tietoturvaa arvostavia organisaatioita. Tor tarjoaa ihmisille ja organisaatioille erään tehokkaan tavan pysyä anonyyminä. Sitä käyttävät monet ihmiset monista eri syistä: journalistit pitääkseen lähteensä piilossa, aktivistit pysyäkseen turvassa vihamielisiltä valtioilta, viranomaiset toimiessaan peitetehtävissä ja rikolliset peitelläkseen jälkiään. Kuten niin moni muukin teknologia, Tor on monikäyttöinen ja sitä käytetään sekä hyvään että pahaan.

Matti Nikki:

Anonyymit verkot ovat välttämätön ja todennäköisesti tulevaisuudessa kasvava mekanismi yksityisyyden suojaamiseksi tulevaisuudessa. Niitä luonnollisesti käytetään myös laittomaan toimintaan ja se on hinta jonka yhteiskunta maksaa suurten väkijoukkojen yksityisyyden loukkaamisesta. Nämä verkot kun eivät kasva mikäli niille ei nähdä tarvetta, ja käyttäjämäärät nousevat nimenomaan vastareaktiona konkreettisiin oikeudenloukkauksiin ja uhkiin.

Sikäli kun anonyymejä verkkoja käytetään välityspalvelimina julkiseen verkkoon, syntyy monimutkaisia ongelmia sekä verkon ylläpitäjälle, sen käyttäjälle että viranomaisille. Arvostan niitä jotka jaksavat ylläpitää näitä palvelimia ja tapella siihen liittyvien ongelmien kanssa.

Liikenne- ja viestintäministeriö

Internetin alkuaikoina oli selkeästi yleisempää käyttää nimimerkkejä ja toimia ns. anonyymisti. Sosiaalisen median kehityttyä on kuitenkin ryhdytty käyttämään internetissä yhä enemmän palveluita omalla nimellä. Mitä tulee Tor-verkkoselailuun, se on yksi tapa suojautua henkilötietojen keräämiseltä tai viestinnän luottamuksellisuuden suojan loukkauksilta verkossa, mutta tietysti Tor:iin liittyy myös negatiivisia lieveilmiöitä, kun se mahdollistaa anonymiteetin, niin hyvässä kuin pahassakin.

Asiaa voisi lähestyä netin ulkopuolisesta yhteiskunnasta katsoen. Anonymiteetti on yhteiskunnassa sallittua, muttei rajattomasti. Kaduilla saa kävellä, kaupoissa tehdä ostoksia, mielipiteitään ilmaista ja esim. yhdistystoimintaan osallistua ilman erityistä velvoitetta toimia omalla nimellään. Sen sijaan erityisissä luottamusta edellyttävissä yhteyksissä on luonnollista, ettei anonyymisyys toimi. Luottokortit, pankkitilit, passit, sairaskertomukset ja monet muut on luonnollisestikin voitava yhdistää tiettyyn henkilöön. Niinpä luottamusta erityisesti edellyttäviin palveluihin kehitetään ja tulee entisestään kehittää riittävän vahvoja tunnistautumismenetelmiä. Se ei kuitenkaan tarkoita sitä, että esimerkiksi netin keskustelupalstoilla tulisi välttämättä edellyttää esiintymistä omalla nimellään.

Lopuksi on hyvä huomata, että lainsäädäntömme (sähköisen viestinnän tietosuojalaki 6 §) mahdollistaa viestintäpalvelujen käyttäjiä suojaamaan viestinsä ja tunnistamistietonsa haluamallaan tavalla käyttäen hyväksi sitä varten tarjolla olevia teknisiä mahdollisuuksia, jollei laissa toisin säädetä.

Nimetön:

Teoriassa hyvä idea, mutta on epäselvää, miten hyvin anonymiteetti toteutuu käytännössä.

4. **Tulevatko Internetin käyttäjät siirtymään enemmän anonyymeihin verkkoihin, kuten Toriin?**

Petteri Järvinen:
Anonyymipalvelujen ja salauksen käyttö on yleistynyt koko ajan, joskin varsin hitaasti. Enemmistö käyttäjistä on liian laiskoja ja mukavuudenhaluisia asentaakseen mitään suojausohjelmia, joten en usko että siitä tulee valtavirtaa vielä pitkään aikaan.

Ville Oksanen (Effi)
Tavallinen käyttäjä ei ole niin kiinnostava joten hyödyn koetaan olevan (ihan perustellusti) pieni. Tuotteet otetaan käyttöön, jos se on helppoa, kuten Tor-Firefoxilla se on.

Antti Tikkanen (F-Secure)
Erilaiset teknologiat, jotka mahdollistavat anonyymiteetin verkossa kiinnostavat yhä enemmän kuluttajia. Tapa käyttää Internetiä on muuttunut. Kuvia, viestejä ja dokumentteja tallennetaan pilveen, ja suuri osa digitaalisesta elämästä tapahtuu mobiililaitteilla pilviympäristössä. Tarvitaan myös uusia suojausratkaisuja ja kiinnostusta ovat herättäneet uudenlaiset yksityisyyssuojasovellukset, joilla voi tehdä itsensä verkossa näkymättömäksi hakkereilta, estää seuranta tai asettaa virtuaalinen sijainti minne tahansa maahan. Virtuaalisesta sijainnista voi hyötyä esim. verkko-ostoksissa (lentoliput, hotellit, Amazon), tai matkustaessaan voi käyttää kotimaan palveluita tai päästä käsiksi sisältöön, joka muuten on rajoitettua.

Käyttäjiä profiloidaan ja heitä seurataan verkossa sivustoilla, missä he liikkuvat tai mitä tahansa sovelluksia tai hakukoneita he käyttävät. Anonyymina mainostajat eivät saa tietoja käyttäjästä. Lisäksi ei ole varmuutta mihin kaikkialle kerättyjä tietoja käytetään. Tiedot voivat päätyä myös rikollisten käsiin, joilla he yrittävät hankkia taloudellista hyötyä. Yrityksille on tärkeää suojata liiketoimintaansa ja suojautua tietovuodoilta, tästä syystä ne suhtautuvat asiaan ilmeisen vakavasti.

Tor verkkona on hyvä tapa pysyä anonyyminä. Sen käyttöä rajoittavat usein verkon hitaus ja käyttöönoton helppous. On siis hyvä että sen rinnalla on myös muita vaihtoehtoja erilaisille käyttäjille.

Matti Nikki:

Riippuu ihan yleisestä Internetin ja lakiympäristön kehityksestä ja siitä onko anonyymiydelle käytännön tarvetta. Tekijänoikeusrintamalla on ehkä konkreettisin vaikutus tähän. Toistaiseksi on melko turvallista ladata netistä mitä vaan sisältöä ilman pelkoa seurauksista, mutta mikäli tämä muuttuu niin anonyymiverkkojen käyttö kasvaa heti ja se on sitten trendi joka ei ihan heti palaudu vaikka lait muuttuisivat takaisin aiempaan suuntaan.

Toistaiseksi suurin rajoittava tekijä on Internet-yhteyksien hitaus, joka ei mahdollista kovin nopeita anonyymiverkkoja. Japanissa jossa on paljon nopeita verkkoyhteyksiä tarjolla ollaan tälläkin rintamalla edellä, ks. esim legendaarinen p2p-ohjelma Winny jolla oli satoja tuhansia käyttäjiä jo kymmenen vuotta sitten.

Mikäli jokin tämmöinen saa kriittisen massan kasaan, käyttö räjähtää, mutta se ei korvaa tavallista julkista Internettiä mitenkään. Facebook sun muut julkisen verkon palvelut pitävät käyttäjät tiukasti kiinni perinteisessä verkossa ja näitä ei todennäköisesti käytetä anonyymiverkkojen läpi isoissa määrin pitkään aikaan. Ei niin kauan kuin Internet käyttää mitään salaamattomia protokollia...

Liikenne- ja viestintäministeriö

Varmasti erilaisten välityspalvelimien ja muilla tavoin toimivien anonyymien verkkojen käyttö tulee lisääntymään jonkin verran, mutta myös muunlainen suojautuminen tietojen keräämiseltä. On myös oletettavaa, että palveluntarjoajat tulevat rakentamaan palveluita yhä enemmän privacy by design -periaatteen mukaan ja myös markkinoimaan tuotteitaan tietosuojalla ja -turvalla. Tätä nähdään jo nyt (esim. F-Securen Younited ja Freedome). Toisaalta voi olla, että vaikka käyttäjien tietoisuus asioista nousee, kaikki eivät silti tule näkemään ylimääräistä vaivaa välttääkseen tietojen keruuta. Tässä mielessä tuotteisiin integroitu tietosuoja ja -turva on tärkeää.

Nimetön:

Ehkä tietyt käyttäjäsegmentit, jotka haluavat syystä tai toisesta pysytellä poissa netin valtaväyliltä. Mutta en ole huomannut merkkejä, että Tor tai muut houkuttelisivat suu-

ria massoja. Syynä voi olla vaikkapa se, että ihmisiä on vaikea kammeta pois vakiintuneista nettirutiineista – vaikka he tiedostaisivatkin sen mahdollisuuden, että heidän toimintaansa tarkkaillaan. Viittaan myös siihen apatiaan, mistä minulla ei ole suoria todisteita, mutta minkä voi välillisesti aistia vaikka juuri Facebookista.

5. Onko Torin käytöstä hyötyä tai haittaa?

Petteri Järvinen:

Jokaisella on joskus tilanteita, jolloin haluaisi liikkua netissä tuntemattomana. Tor mahdollistaa tämän, jos vaikka haluaa selata kilpailevan yrityksen rekrytointi-ilmoituksia tai kysyä neuvoa jossain arkaluontoisessa asiassa. Haittana ovat kyseenalaiset palvelut, joissa levitetään tietoa rikollisuudesta, myydään laittomasti hankittuja henkilötietoja tai levitetään esimerkiksi lapsipornoa. Yleensä näihin tekijöihin päästään kuitenkin kiinni muuta kautta, sillä kukaan ei voi elää täysin nettimaailmassa.

Ville Oksanen (Effi)

Tor hidastaa verkkoliikennettä ja sen käyttäminen on automaattisesti epäilyttävää esim. NSA:n silmissä, eli sillä pääsee helposti tarkkailun kohteeksi. Toisaalta oikein käytettynä Tor suojaa varsin tehokkaasti käyttäjän yksityisyyttä.

Antti Tikkanen (F-Secure)

Torin käytöstä on varmasti sekä hyötyä että haittaa. Se tarjoaa monille käyttäjille elintärkeän tavan pysyä anonyyminä verkossa (journalistit, aktivistit, viranomaiset). Samalla se tarjoaa rikollisille tavan peittää jälkensä. Moni teknologia on luonteeltaan juuri tällaista -- sitä voidaan käyttää sekä hyvään että pahaan.

Matti Nikki:

Tor:n käytöstä on ehdottomia hyötyjä sen käyttäjälle, kunhan ymmärtää mitä työkalu tekee ja mitä se ei tee. Haittaa siitä on myös valtavasti, mikäli sitä käyttää ymmärtämättä täsmälleen mitä se tekee. Kun Tor:ia käyttää avoimen netin selaamiseen, jokin ventovieras kolmas osapuoli (exit node) välittää liikenteen ja pääsee lukemaan sen. Suojaamattoman liikenteen osalta tämä tarkoittaa salasanojen ja muiden arkaluontoisten tietojen varastamisen uhkaa.

Tor:sta on hyötyjä myös yhteiskunnalle, koska se mahdollistaa arkaluontoisenkin keskustelun joka tuo oman panoksensa yhteiskunnalliseen kehitykseen. Myös tietojen vuotaminen onnistuu Tor:n avulla ja Tor pitää huolen että vuodetut tiedot pysyvät saatavilla eikä mikään viranomainen voi niitä poistaa netistä. Esimerkiksi korruptoituneen lääkeyhtiön salatessa lääkkeen hengenvaarallisia sivuvaikutuksia, yhteiskunnalle on ERITTÄIN hyödyllistä että on mahdollista vuotaa asiakirjoja niin että yhtiöllä ei ole mitään mahdollisuuksia hiljentää tietojen vuotajaa. (Ks. Eli Lilly ja Zyprexa, tuomioistuin määräsi vuodetut asiakirjat salaisiksi jonka jälkeen ne vuodettiin kaikelle kansalle muun muassa Tor:n avulla uhmaten tuomioistuimen määräystä)

Yhteiskunnalliset haitat Tor:sta eivät ole nekään täysin mitättömiä, Tor kun mahdollistaa monenlaiset laittomat palvelut ja Tor heikentää viranomaisten kontrollia rikollisten kommunikaatiomahdollisuuksiin. Oikeutetutkaan pakkokeinot eivät ole aina mahdollisia kun tekijä on Tor:n avulla tuntematon ja jäljittämättömissä. Käytännössä tämä on rajoittunut lähinnä huumekauppaan, lapsipornoon, ja perättömiin uhkauksiin joita poliisi joutuu sitten setvimään ilman helppoja oikoteitä tekijöiden jäljittämiseksi.

Liikenne- ja viestintäministeriö

Katsoisin asiaa laajemmin kuin juuri TOR-verkon näkökulmasta. Julkisuudessa on ollut tietoja siitä, kuinka esimerkiksi toimittajat ovat pyrkineet turvaamaan lähdesuojaa käyttämällä anonyymejä viestipalveluja. Myös sananvapauden käyttöä ja yksityisyyden suojaa loukkaavissa/rajoittavissa maissa kansalaisten mahdollisuus turvallisesti ilmaista mielipiteitään ja osallistua yhteiskunnallista päätöksentekoa koskevaan keskusteluun voi edellyttää valtion turvallisuuspalvelujen valvonnan välttämistä viestinnän suojaamisella anonyymiksi.

Nimetön:

Hyötyä voisin kuvitella vaikkapa toisinajattelijoille, jotka pelkäävät tuoda ajatuksiaan esiin normaalin verkon kautta. Haittaa on puolestaan siitä, että Torin nimettömyys houkuttelee mukaan tietenkin myös rikollisia.

6. **Ovatko Tor-ohjelmistot luotettavia ja antavatko ne toivotun anonymiteetin?**

Petteri Järvinen:
Snowdenin paljastuksista voi päätellä, että NSA on tehnyt työtä Torin murtamiseksi, mutta mitään selvää aukkoa ei ole löytynyt. Selaimen haavoittuvuuksia hyödyntämällä käyttäjä voidaan ehkä paljastaa, kuten FBI:n tekemä Silkroadin ratsia osoitti. Tällä hetkellä Toria voitaneen pitää kaikkein luotettavimpana tapana säilyttää oma anonymiteetti.

Ville Oksanen (Effi)
Tor tarjoaa hyvän suojan "normaaleja" tahoja kohtaan. Mikäli oma päätelaite on kuitenkin murrettu, se ei tarjoa mitään suojaa. Lisäksi tarpeeksi kiinnostavat kohteet kyetään teknisesti yleensä jäljittämään Torin käytöstä huolimatta.

Antti Tikkanen (F-Secure)
Tor-ohjelmistot auttavat ihmisiä pysymään anonyymeinä. Uhkakuvissa täytyy ottaa huomioon aina se, keneltä ollaan suojautumassa. Tor on varmasti tehokas suoja useimpia hyökkääjiä vastaan, mutta täydellistä suojaa on mahdotonta saavuttaa.

Matti Nikki:
Tor:n luotettavuus on rajallinen, ja riippuu siitä ymmärtääkö käyttäjä mitä ohjelma tarjoaa. Tor:ia ei voi suositella tänäpäivänä jokapäiväiseen käyttöön johtuen exit-nodejen mahdollisuudesta vakoilla ja muuttaa välitettäviä tietoja.

Virheitä on myös helppo tehdä joka johtaa anonyymiyden murtumiseen. Jos sivusto vaikka vaatii javascriptiä ja selain antaa sitä käyttää, käyttäjä vuotaa helposti valtavasti tietoa itsestään ja koneestaan niin että jäljitys on mahdollista. Monimutkaisemmat hyökkäykset pystyvät kalastamaan tietoa muunmuassa viiveistä ja muusta ajoitustiedoista, ja Tor-verkkoon kohdistuu jatkuvasti uhkia johtuen järjestelmän suunnittelu- ja toteutusvirheistä. Oman ongelmansa tuo selainten haavoittuvuudet joiden avulla käyttäjän kone voidaan kaapata, käytti Tor:ia tai ei, ks.
http://www.wired.com/2013/09/freedom-hosting-fbi/

Joka kerta kun haavoittuvuus korjataan, järjestelmästä tulee astetta turvallisempi, mutta jos Tor:ia haluaa käyttää jatkuvasti kehittyvän web-sisällön selaamiseen, tämähän ei riitä. Niitä uusia haavoittuvuuksia kun tulee jatkuvasti lisää.

Tor:n käyttö ei myöskään onnistu näkymättömästi ihan suoraan. Mikäli vastassa on valtio, pelkästään se että käyttää Tor:ia voi johtaa televalvontaan joutumiseen jolloin salaamattomat viestit (esim. puhelimessa) joutuvat syynätyksi, vaikka ne olisivat jääneet huomiotta mikäli Tor:ia ei olisi käyttänyt.

Liikenne- ja viestintäministeriö

Riippuu varmasti siitä minkä tasoisen anonymiteetin toivoo saavuttavansa. 100 %:sta tietoturvaa ei ole olemassa. Tor-verkko kuten kaikki muukin tietotekniikka ja digitaaliset palvelut toimivat juuri siten, kuin ne on ohjelmoitu toimimaan. Samoin niihin liittyvät kaikki ne tietoturvahaavoittuvuudet, joita ohjelmoinnissa ei ole osattu tai haluttu huomioida.

Nimetön:

Pakko sanoa, että eivät välttämättä. Katso vastaukseni seuraavaan kysymykseen.

7. Onko Torin käytössä joitain riskejä tai tietoturvauhkia?

Petteri Järvinen:

Tor vaatii käyttäjältä huolellisuutta, koska omia henkilötietoja tulee helposti kirjoitettua puoli vahingossa. Selaimen laajennukset ja koneen muut sovellukset voivat niin ikään paljastaa tärkeitä tietoja vahingossa. Ja jos koneelle on saatu ujutettua haittaohjelma, mistään salausohjelmasta tai Torista ei ole sen jälkeen apua. Oleellista on, että käyttäjä ymmärtää mitä Tor tekee (ja erityisesti, mitä se ei tee).

Ville Oksanen (Effi)

Vrt. 5.

Antti Tikkanen (F-Secure)

Viitaten edelliseen kysymykseen, tietyssä tapauksissa kyllä. Riskejä löytyy varmasti sekä liikennettä suojaavasta algoritmista ja siihen liittyvistä ohjelmistoista. Isojen, ja mahdollisesti vähän pienempienkin maiden viranomaiset ja tiedustelupalvelut omaavat erilaisia teknisiä keinoja joilla Tor-käyttäjiä voidaan seurata. Ks esimerkiksi haittakoodin käyttö Firefox-selainta vastaan rikostutkinnassa (http://www.wired.com/2013/09/freedom-hosting-fbi/) tai "confirmation attack" -hyökkäykset (https://blog.torproject.org/blog/tor-security-advisory-relay-early-traffic-confirmation-attack).

Matti Nikki:

Katso edellinen vastaus.

Liikenne- ja viestintäministeriö

Kaikkien tietoteknisten laitteiden, ohjelmistojen ja palveluiden käyttöön liittyy varmasti positiivisia mahdollisuuksia. Vastaavasti niiden kaikkien käyttöön liittyy myös riskejä, jotka tulisi ymmärtää ja hallita paremmin (kts. vastaus nro 2).

Nimetön:

Vanhana uhkana on ollut pelko, että esimerkiksi NSA pystyy kaivautumaan suojatun verkon saloihin käsiksi. On ollut puhetta, että tämä olisi osoittautunut vaikeaksi.

Mutta tuoreena tapauksena on Torin ilmoittama hyökkäys, missä yritettiin mahdollisesti selvittää anonyymejä käyttäjiä. Saattaa olla, että koko hyökkäys oli kahden tietoturvatutkijan projekti ilman sen vakavampia aikomuksia, mutta tapaus teki loven Torin uskottavuuteen ja luotettavuuteen.

8. **Sopiiko Tor yksityishenkilön käyttöön ja osaako hän käyttää Toria turvallisesti?**

Petteri Järvinen:

Nykyiset Tor-paketit ovat erittäin helppokäyttöisiä, mutta ne vaativat hieman vaivaa ja omaa varovaisuutta. Kyse on pikemminkin huolellisuudesta kuin tiedosta. Tor on saa-

tavilla kaikille käyttöjärjestelmille ja jopa älypuhelimille (Android, iPhone), joten käyttö onnistuu keneltä tahansa – jopa ilman tietokonetta.

Ville Oksanen (Effi)

Torin käyttäminen intregoidulla selaimella on yhtä helppoa kuin tavallisen selaimen käyttö. Selaimessa on kuitenkin todennäköisesti aina tiedustelupalveluiden tuntemia ns. nollapäiväaukkoja, joita voidaan hyödyntää tarpeksi kiinnostavia kohteita kohtaan.

Antti Tikkanen (F-Secure)

Tor, kuten monet muutkin tietoturva- ja salaustuotteet eivät vielä ole "kaiken kansan" tuotteita. On hyvä että tähän ongelmaan on herätty, ja tarjolle on tulossa yhä helppo-käyttöisempiä ratkaisuja.

Matti Nikki:

Suurin osa yksityishenkilöistä ei varmasti osaa käyttää Toria turvallisesti. Se ei ole millään tapaa itsestäänselvää, ja hyökkäyksen kohteeksi joutuessaan Tor-verkko piilottaa joskus myös hyökkääjän identiteetin. Tor:ia olisi turvallisinta käyttää virtuaalikoneessa tai livecd:ltä (esim. Tails), mutta silloinkin täytyy pitää mielessä että kolmas osapuoli pystyy vakoilemaan liikennettä vaikka ei tiedäkään kenen liikennettä se on. Käyttäjän ei myöskään pidä kirjautua mihinkään palveluun joka yksilöi tai paljastaa käyttäjän julkisen identiteetin, tai anonyymiys saattoi mennä siinä heti samantien metsään.

Tor:n oikeaoppinen käyttö vaatii että ymmärtää miten se toimii ja mitä se tekee, ja mikäli tämä ehto täyttyy niin Tor soveltuu yksityishenkilön käyttöön. Ilman tätä vaadittua ymmärrystä Tor ei ole turvallinen käyttää vaan pikemminkin äärimmäisen vaarallinen käyttäjänsä tietoturvalle ja yksityisyydelle.

Liikenne- ja viestintäministeriö

Yksiselitteistä vastausta on mahdotonta antaa. Vastaavasti voisi kysyä, sopiiko kiipeilyköysi yksityishenkilön käyttöön? Osaavissa ja riskit ymmärtävissä käsissä ainakin kiipeilyköyden käyttö lienee turvallisuutta lisäävä tekijä. Toisaalta köyden huolimaton käyttö vuorilla tai väärinkäyttö vaikkapa rikollisen käsissä saattavat johtaa varsin vakaviin seurauksiin. Kenties sama koskee anonymiteetin tarjoavia viestintäsovelluksiakin.

Nimetön:

Turvallinen käyttö on viimeistään äskettäisen tietoturvakohun jälkeen suhteellinen käsite jopa anonymiteettiä lupaavien palvelujen kohdalla.

Liite 7. Testihenkilöiden palaute

1. **Mitä mieltä olet Tor-ohjelmistoista?**

Henkilö 1:
Luettuani uutisia NSA-tiedusteluskandaaleista ja esimerkiksi Turkin ja Kiinan hallitusten rajoituksista kansalaistensa Internetin käytölle, näen Torin kaltaisille ohjelmistoille selkeää tarvetta.

Henkilö 2:
En koe niitä tarpeellisiksi suomalaiselle internetin käyttäjälle, koska maassamme ei juurikaan ole tavallista netin käyttäjää rajoittavaa sensuuria ja valvontaa. Tiukkaa valvontaa ja sensuuria harjoittavissa maissa Tor-ohjelmistot lienevät tarpeeseen.

Henkilö 3:
Ihan hyvä idea ja tarkoitus. Tor-selaimen käyttö on hieman rajattua kaikkien kieltojen vuoksi, muuta Tailsin käyttö mitätöi nämä ongelmat. Itse en ehkä näe näille ohjelmistoille vielä käyttöä päivittäisessä nettisurfailussani.

Henkilö 4:
Ammattimaisemmassa käytössä varmaankin hyötyä, jos kokee tietosuoja-asiat erittäin tarpeellisiksi, mutta peruskäyttäjälle en näe ohjelmassa juurikaan lisäarvoa.

Henkilö 5:
Hidas, ei varsinaista hyötyä normi käytössä, tavalliselle netin käyttäjälle. Ideana hyvä ja kiinnostava.

2. **Oliko Tor-ohjelmistojen käytössä tai asennuksessa ongelmia? Minkälaisia?**

Henkilö 1:
Asennus on keskivertokuluttajalle suhteellisen vaikea prosessi. Erityisesti Tor Browserin ja Tailsin varmentaminen asentaessa vaatii jo pidempää asiaan paneutumista ja to-

dellista tarvetta ohjelmistoille. Ylitsepääsemättömältä asentaminen ei tuntunut, jos miettii että tarvitsisin anonyymia selainta työssäni tai jopa oman turvallisuuteni takaamiseksi.
Käyttö sinänsä vaikuttaa suoraviivaisemmalta. Silmiinpistävää on tosin Tailsin hitaus verrattuna tietokoneen normaaliin käynnistämiseen. Lisäksi minulle entuudestaan tuntemattomat rajoitukset anonyymille selaamiselle, vaikka käytössä olisikin jo Tor selain, luovat ison kynnyksen käytölle. Käyttäjänä joutuisin muuttamaan rajusti selaamistapojani ja luomaan esimerkiksi erilliset sähköpostit anonyymiä netin käyttöä varten. Lisäksi pelkästään https-protokollaa käyttävien sivustojen käyttäminen ja varovaisuus ladattujen tiedostojen avaamisessa vaikeuttavat päivittäistä tietokoneen käyttöäni jo liiallisesti.

Henkilö 2:
Tor Browserin asentaminen ja käyttö oli helppoa. Tailsin asentamisohjeet saivat tällaisen keskinkertaisen koneen käyttäjän ymmyrkäiseksi, koska ohjeissä käytetty tietokonetermistö ei ole minulle tuttua. Tailsin käyttäminen sen sijaan oli helpompaa, muttei kuitenkaan sujunut ilman ohjeita.

Henkilö 3:
Ainoa ongelma oli tarkistusavaimen käytössä - ohjeikkuna ei avautunut oletetusti, jolloin avaimen varmistus jäi tekemättä. Ei muita ongelmia.

Henkilö 4:
Itse ohjelman asentamisessa ei juurikaan ollut vaikeuksia, mutta turvallisen käytön testaukset ja verifioinnit olivat melko haastavia toteuttaa ja ymmärtää, mitä ne oikeastaan tekevät tai tuoko tämän vahvistuksen tekeminen oikeasti lisää luotettavuutta.

Henkilö 5:
Selaimen asennuksessa ei ollut. Toki kannattaa lukea ennen asennusta mikä Tor on ja mikä sen tarkoitus on

3. Onko Tor-ohjelmistojen käytöstä mielestäsi hyötyä tai haittaa?

Henkilö 1:

Ohjelmistoista voi olla haittaa tai hyötyä, riippuen tilanteesta. En pidä hyvänä ohjelmistojen kehittämistä jotka helpottavat rikollisten viestintää tai esimerkiksi lapsipornon levittämistä anonyymisti.

Toisaalta nykymaailmassa ollaan jo tilanteessa, jossa yritykset, tiedusteluviranomaiset tai muut tahot seuraavat ihmisten toimintaa ja ostotottumuksia tavalla, joka rikkoo omia yksityisyyden rajojani. Mielestäni on erittäin hyödyllistä, että esimerkiksi turkkilaiset, syyrialaiset, pohjoiskorealaiset, venäläiset tai kiinalaiset ihmisoikeuksia puolustavat tahot voivat viestiä muun maailman kanssa, ilman että heidän turvallisuutensa on uhattuna.

Kokonaisuutena olen anonyymin selaamisen kannattaja, sillä rikollisia ja moraalisesti arveluttavia ihmisiä tulee aina olemaan, eikä kaikkien ihmisten vapauksia ja oikeuksia pidä rajoittaa vain näiden harvojen ihmisten kiinnisaamiseksi.

Henkilö 2:

Lienevät hyödyllisiä niille, joilla on tarvetta - hyödyllisiä siis, jos pääsy estetyille asiallisille sivuistoille mahdollistuu. Haittana voisin mainita sen, että sensuuriton internetin selaus saattaa johdattaa asiattomille sivustoille.

Henkilö 3:

Tor-selaimen ja Tailsin karu ulkoasu eivät varmaankaan herätä normaalien netin käyttäjien mielenkiintoa käyttää ohjelmistoja, samoin Tailsin yksinkertaisten asennusohjeiden puute voi vaikuttaa käyttäjien päätökseen negatiivisesti. Hyötyähän ohjelmistoista on kyberrikollisuuden ja tietomurtojen lisääntyessä, samoin kuin valtioiden harrastama normaalien netinkäyttäjien liikkeiden seuranta.

Henkilö 4:

Ammattimaisessa käytössä varmasti hyötyä mm. estämään salaisen tiedon leviämistä, tuotekehityksen vakoilua tai muuta vastaavaa. Peruskäyttäjälle varsinkin turvallisen käytön noudattaminen tuo enemmänkin haittaa ja rajoituksia, koska normaaliin internetkäyttäytymiseen kuuluva tiedostojen ja lisäosien lataaminen ja asentaminen on kiellet-

tyä. Myöskään esim. monella usein käyttämälläni sivustolla esim. keskustelufoorumeilla ei ollut olemassa suojattua https -osoitetta, joten peruskäyttäjää turvallisuusohjeiden noudattaminen rajoittaa huomattavasti. En myöskään koe esim. sensuurin kiertämisen olevan monessakaan tapauksessa kovin oleellista esimerkiksi Suomessa.

Henkilö 5:
Hyötyä on jos haluaa käyttää selainta siihen mihin tarkoitettu. Haittoja ei hitauden lisäksi mielestäni ole.

4. Tuletko vastaisuudessa käyttämään Tor-ohjelmistoja? Miksi/miksi et?

Henkilö 1:
En usko, että tulen käyttämään Tor ohjelmistoja tulevaisuudessa. Olen mielestäni jo valmiiksi riittävän varovainen siitä, mitä jaan Internetissä. Tämän takia minua ei häiritse ajatus siitä, että tekemisiäni saattaa seurata jokin taho.
Ohjelmistojen hitaampi käyttäminen, omien toimintatapojeni muutos ja jatkuva varovaisuus käytettäessä vaikuttavat minusta liian suurelta muutokselta. Olisin valmis noudattamaan anonyymin selaamisen ohjeita vain, jos minulla olisi painava syy toimintatapojeni muuttamiseksi. Tällä hetkellä en näe itselläni tarvetta ohjelmistojen käytölle sekä toimintatapojeni muuttamiselle.

Henkilö 2:
En, koska en koe sitä tarpeelliseksi, koska pääsen kaikille tarvittaville sivustoille, enkä häiriinny minuun kohdistuvasta valvonnasta. Lisäksi Tor-ohjelmistot rajoittaisivat internetin käyttöäni, koska en pystyisi käyttämään sellaisia sivustoja, joilla yleensä käyn (tietoturvariskialttiit sähköposti, facebook jne).

Henkilö 3:
Luultavasti en. Oma netissä surffailu on sen verran mielenkiinnotonta, etten usko kenenkään hyötyvän nettikäyttöni seurannasta.

Henkilö 4:

En ainakaan normaalissa kotikäytössä juuri edellämainittujen rajoituksien vuoksi. Jos joskus ammatissa tarvitsen tällaista salausta, voin olla kiinnostuneempi ottamaan tarkemmin selvää mahdollisuuksista.

Henkilö 5:

En, sillä se on suht verkkainen käyttää. En usko myöskään saavani hyötyä sen käytöstä. Lisäksi tottunut käyttämään muita selaimia.

5. **Tulevatko Internetin käyttäjät mielestäsi siirtymään enemmän anonyymeihin verkkoihin, kuten Toriin? Miksi / miksi ei?**

Henkilö 1:

Uskon, että anonyymien selaajien määrä tulee kasvamaan. Esimerkiksi Saksassa, NSA uutiset otettiin paljon vakavammin vastaan kuin oletin. Taustalla on varmaan myös muisto DDR aikojen Stasi ajoista, joissa kansalaisten jokapäiväistä toimintaa seurattiin sairaalloisella tarkkuudella. Jopa nuorienkin saksalaisten asenteet ja varovaisuus esimerkiksi Facebookin käytössä olivat selkeästi erilaiset kuin minulla.
Riippuen eri maiden nykytilanteista ja historiasta, tarpeet anonyymille selaamiselle ovatkin siis hyvin erilaiset maailmanlaajuisesti tarkasteltuna. Kokonaisuutena uskon, että Tor ohjelmistoille on siten aina olemassa tarvetta jossakin päin maailmaa, minkä takia ohjelmistojen käyttäjämäärä tulee lisääntymään

Henkilö 2:

Kyllä ja ei. Riippunee paljolti mm. käyttäjän asuinmaan hallinnollisesta suunnasta sekä poliittisesta ja uskonnollisesta ilmapiiristä. Euroopan demokraattisissa hyvinvointivaltioissa anonyymeille verkoille tuskin tulee koskaan olemaan aitoa tarvetta, mutta esim. itäblokin maat ovat asia erikseen.

Henkilö 3:

Hyvin mahdollista lähitulevaisuudessa, kun normaalien ihmisten elämä asioinnin ja tiedonvaihdon osalta siirtyy entista enemmän nettiin. Suuri osa normaaleista netin käyttäjistä ei luultavasti tiedosta, kuinka suuriin ongelmiin voi ajaantua, jos henkilökohtaiset

tiedot ja salasanat joutuvat vääriin käsiin. Muutos kuitenkin vaatii asian herättävän valtamedioiden suuremman mielenkiinnon ja sitä myötä ihmisten valistuken sekä koulutuksen.

Henkilö 4:

Vahvan sensuurin maissa, kuten esimerkiksi Aasian maissa, joissa teknologian ja internetin käyttö yleistyy koko ajan, tällaiset mahdollisuudet varmastikin yleistyvät, koska monet länsimaisten normaaliin internet-sivujen käyttöön kuuluvat palvelut on estetty valtion toimesta. Myös ammattimaisessa käytössä tietosuojan merkitys tulee varmasti kasvamaan. Normaalin länsimaisen internetin käyttäjän trendi on kuitenkin enemmän siihen suuntaan, että kaikki asiat jaetaan jo omatoimisesti sosiaalisen median kautta, joten en usko tällaiselle palvelulle olevan tarvetta suurissa massoissa.

Henkilö 5:

Eivät: Tietoisuus verkon vaaroista, tietotaito ja kiinnostus ihmisillä vähäistä. Hyödyt perus netin käyttäjälle mielestäni suht vähäiset. Jos olet facebookista susta tiedetään kaikki jokatapauksessa.