SEINÄLLE NAULATTU HYYTELÖ

Valtiollisen internet-sensuurin menetelmät ja niiden kiertäminen

HAMK
HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Ammattikorkeakoulututkinnon opinnäytetyö

Tietojenkäsittelyn koulutus
syksy, 2023

Mikko Paakkanen

HAMK
HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Tietojenkäsittelyn koulutus Tiivistelmä

Tekijä Mikko Paakkanen Vuosi 2023

Työn nimi Seinälle naulattu hyytelö – Valtiollisen internet-sensuurin menetelmät ja niiden kiertäminen

Ohjaaja Ismo Turve

TIIVISTELMÄ

Opinnäytetyön aiheena oli valtioiden harjoittama internet-sensuuri, joka tätä nykyä koskee jo valtaosaa maailman internetiä käyttävästä väestöstä. Tavoitteena oli selvittää, mitä teknisiä menetelmiä valtiot käyttävät estääkseen alueillaan olevien ihmisten pääsyä internet-sisältöihin, millä menetelmillä estoja kierretään ja miten estot vaikuttavat ihmisten ja yritysten toimintaan internetiä sensuroivissa maissa.

Opinnäytetyön tietopohja koostuu pääosin kirjallisuuslähteistä. Tutkimuslähteiden perusteella selvitettiin, mitä teknisiä menetelmiä internetin sensurointiin käytetään, kuinka tehokkaita ne ovat, sekä millä keinoin ja kuinka tehokkaasti estoja kierretään. Taustaksi selvitettiin myös internet-sensuurin laajuutta ja sitä, minkä tyyppistä aineistoa sensuroidaan.

Opinnäytetyö on lähinnä tutkimuksellinen. Tutkimusstrategiana oli tapaustutkimus, jossa pyrittiin löytämään ja ymmärtämään sensuuriin liittyviä tekniikoita ja asettamaan niitä viitekehykseensä. Opinnäytetyössä on myös toiminnallinen osuus, jossa perustetaan sensuurin kiertämisjärjestelmä Saksassa sijaitsevaa virtuaalipalvelinta hyödyntäen.

Tutkimuksessa havaittiin, että moni merkittävä valtio sensuroi verkkosisältöjä erittäin kehittyneillä ja hyvin toimivilla teknisillä ratkaisuilla. Myös sensuurin kiertämiseen on tarjolla kehittyneitä menetelmiä, ja niitä kehitetään kilpaa sensuurimenetelmien kehittämisen kanssa. Lisäksi kävi ilmi, että internet-sensuuri ei ole vain tiedon saatavuusongelma, vaan myös merkittävä tietoturvaongelma ihmisille ja yrityksille, jotka toimivat sensuurimaissa.

Avainsanat tietoverkot, tietoverkkotekniikka, sensuuri, sananvapaus, kyberturvallisuus

Sivut 133 sivua ja liite 1 sivu

HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Degree Program in Business Information Technology Abstract

Author Mikko Paakkanen Year 2023

Subject The Jell-O on the Wall – Methods of state-sponsored internet censorship and how to circumvent them

Supervisor Ismo Turve

ABSTRACT

The subject of the thesis was internet censorship, which now affects most of the world's internet-connected population. The purpose was to find out, what kind of technologies states use to prevent people from accessing certain content on the internet, how to circumvent these technologies, and what effects censorship has on people and companies.

Main sources of information are research papers and articles. The thesis sought to analyze, how effective the current state censorship technologies are, and how successfully these methods can be circumvented. The study also investigated the prevalence of internet censorship in the world and what kind of material is censored in general.

The study is mostly theoretical, with case study as the research strategy. The main objective was to find and understand current censorship and censorship-circumvention technologies, and to set them in a broader framework. In the thesis, there is also a practical chapter where a censorship-circumvention tool is set up, using a virtual server located in Germany.

The research demonstrates that several noteworthy states censor the internet successfully with very advanced technologies. The censorship can be circumvented with similarly advanced technologies, which are developed in competition with the censorship. The study also revealed that internet censorship is not only a problem of information accessibility but also a significant cyber security problem for people and companies located in censoring countries. The study offers some recommendations for action for this situation.

Keywords data networks, censorship, freedom of speech, cyber security

Pages 133 pages and appendix 1 page

Sanasto

TCP/IP, Transmission Control Protocol / Internet Protocol	Joukko standardoituja sääntöjä, jotka mahdollistavat tiedonsiirron verkossa.
Datapaketti	Internetissä liikkuvan tiedon yksikkö, kun tieto liikkuu jaettuna osiin. Sisältää varsinaisen lähetettävän tiedon eli hyötykuorman lisäksi otsikkotietoja.
DPI, deep packet inspection	Datapakettien syvätutkimus. Tietoliikenteen tutkimisen ja suodattamisen edistynyt menetelmä, joka pääse käsiksi myös datapakettien hyötykuormaan.
VPN, virtual private network	Virtuaalinen yksityisverkko. Salattu yhteys avoimen verkon yli, muodostaen eräänlaisen putken, jonka sisältö on salattu.
Sensuuri	Pääsyn rajoittaminen johonkin aineistoon, yleensä viranomaisten tekemänä, tarkoituksena estää tietojen tai ajatusten leviäminen.
GFW, Great Firewall (of China)	Kiinan palomuuri. Järjestelmä, jolla Kiina sensuroi ulkomaista verkkosisältöä. Maailman laajin ja kehittynein internet-sensuurijärjestelmä.
BGP, Border Gateway Protocol	Tietoliikenneprotokolla, jolla internetin autonomiset järjestelmät ovat yhteydessä toisiinsa.
Peittely, obfuscation	Erilaiset menetelmät, joilla kielletyn tyyppinen tietoliikenne, kuten VPN-liikenne, saadaan näyttämään sallitulta liikenteeltä.
Tiedonsiirtoprotokolla	Yhteyskäytäntö. Sovittu säännöstö, jota kahden tai useamman laitteen on noudatettava, jotta niiden välille voidaan muodostaa yhteys.

Sisällys

Komennot, kuvat, ohjelmakoodit ja taulukot

Liitteet

1 Johdanto

Demokraattisissa länsimaissa moni on tottunut ajattelemaan, että internet on vapaa ja että lähes kaikki avoimessa internetissä oleva tieto on vapaasti kenen tahansa saatavilla. Suurinta osaa maailman ihmisistä tämä vapaus ei kuitenkaan todellisuudessa koske, sillä monet maat käyttävät teknisiä menetelmiä, joilla ne rajoittavat pääsyä kotimaan verkosta tiettyihin ulkomailla oleviin tiedon lähteisiin. Ehkäpä tunnetuin internetin rajoittaja on Kiina.

Kiina on myös osoittanut, että internetin rajoittaminen on ylipäätään mahdollista. Vielä tämän vuosituhannen alussa sitä pidettiin melko toivottomana. Esimerkiksi Yhdysvaltojen silloinen presidentti Bill Clinton sanoi vuonna 2000 naureskelevaan sävyyn, että Kiinan yritykset rajoittaa internetiä ovat ”kuin yrittäisi naulata hyytelöä seinälle” (Clinton, 2000).

Nykyisin kuitenkin yhä useampi maa haluaa hallita informaatiotilaa oman maan rajojen sisällä, ja internetin rajoitukset ovat maailmalla yleistymässä. Yhdysvaltalaisen Freedom House -järjestön uusimman vuosiraportin mukaan internetin vapaus on maailmassa vähentynyt jo 12:tta peräkkäistä vuotta, ja yli kaksi kolmasosaa maailman väestöstä elää maissa, joissa internet ei ole vapaa kuin korkeintaan osittain (Freedom House, 2022i, s. 5).

Tässä opinnäytetyössä tutkitaan valtioiden asettamia teknisiä internet-rajoituksia. Rajoituksista käytetään tässä nimitystä sensuuri, koska ne täyttävät yleisimmät sensuurin määritelmät. Tarkoitus on tutkia, millaisia yleisimpiä teknisiä keinoja maat käyttävät internetin sensurointiin ja millaisin keinoin näissä maissa matkustavat tai työskentelevät, avointa internetiä tarvitsevat ihmiset voivat kiertää näitä rajoituksia. Tarkoitus on myös testi- ja demonstraatiotarkoituksessa rakentaa järjestelmä, jonka avulla ulkomailla sensuroivassa maassa oleskeleva voisi kiertää sensuuria.

Opinnäytetyön tavoitteet voidaan tiivistää kolmeen tutkimuskysymykseen:

- Millaisilla tekniikoilla valtiot nykyisin rajoittavat internetin käyttöä?
- Millaisilla ajantasaisilla tekniikoilla näitä rajoituksia voi kiertää tietoturvallisesti?
- Miten rajoitukset vaikuttavat rajoittavassa maassa työskentelyyn?

2 Lähestymistapa ja tutkimusmenetelmä

Tämän opinnäytetyön lähestymistapana eli tutkimusstrategiana on tapaustutkimus, jossa tavoitteena on internet-sensuuriin liittyvien ilmiöiden ja tekniikoiden ymmärtäminen ja selittäminen. Suomessa paljon käytetyn määritelmän mukaan tapaustutkimuksessa tarkastellaan yhtä tai useampaa tapausta, ja tutkimuksen keskeisimpänä tavoitteena on näiden tapausten määrittely, analysointi ja ratkaisu (Eriksson & Koistinen, 2014, s. 4).

2.1 Tapausten määrittely

Tapaustutkimuksessa tutkittava tapaus voi olla esimerkiksi prosessi, ilmiö tai ohjelma. Usein tapaustutkimuksessa tapausta pyritään ymmärtämään osana jotain ympäristöä eli kontekstia. Tapauksen analysoiminen kontekstissaan on tärkeää, koska konteksti selittää tapausta ja usein juuri konteksti tekee tapauksen ymmärrettäväksi. (Eriksson & Koistinen, 2014, s. 5–7)

Tässä opinnäytetyössä tapauksia on useita. Ne voidaan jakaa kolmeen luokkaan:

- internetin sensurointimenetelmät
- sensuurin kiertomenetelmät
- käytännöt, joilla sensuurin voi huomioida työelämässä

Kussakin luokassa voi olla useita tapauksia. Esimerkiksi sensurointimenetelmiä ja sensuurin kiertomenetelmiä on useita, ja jokainen niistä voidaan ajatella tapaustutkimusmielessä tapaukseksi. Tapaukseksi voidaan määritellä myös jonkin maan käyttämä menetelmien kokonaisuus. Käsiteltävien tapausten lukumäärä ja rajaukset tarkentuvat tutkimuksen edetessä.

Tavoitteena on selittää ja ymmärtää näitä tapauksia – menetelmiä, joilla valtiot sensuroivat internetiä, menetelmiä, joilla sensuuria voi kiertää ja käytäntöjä, joilla sensuuri voidaan ottaa huomioon työssä.

Kontekstina tapauksille on sensuuri kokonaisuutena maailmassa ja siihen liittyvät lähinnä poliittiset ja yhteiskunnalliset taustatekijät. Myös sensuurista aiheutuvat seuraukset ovat osa

kontekstia. Ilman sensuurin kokonaisuuden huomioimista sensuurin menetelmät jäisivät irrallisiksi ja mahdollisesti myös osin selittämättömiksi, tai vähintäänkin niiden merkitystä olisi vaikea hahmottaa. Yhteiskunnallinen analyysi kuitenkin rajataan tässä tarkoituksella lähinnä sen tarkasteluun, mikä on sensuurin suhde sananvapauteen ja demokratiaan. Koska kyse on tietojenkäsittelyn eikä yhteiskuntatieteen opinnäytetyöstä, painopisteenä ovat tietotekniset ratkaisut ja tavat reagoida ilmiöön työelämässä.

2.2 Aineisto ja sen analysoiminen

Pääasiallisena aineistona käytetään kirjallisuuslähteitä, joissa tutkitaan ja selitetään sensuuriin ja sen kiertämiseen liittyviä menetelmiä. Valtiot pitävät sensuurin tekniset ratkaisunsa salassa, eikä niistä ole julkaistu virallisia käsikirjoja tai oppaita. Sensuurimenetelmiä on kuitenkin tutkittu paljon, ja niistä on julkaistu melko runsaasti tutkimuskirjallisuutta, konferenssiesityksiä ja asiantuntijoiden laatimia blogikirjoituksia. Myös kiertomenetelmistä on julkaistu kirjallisuutta, ja osasta niistä on käytettävissä jopa oppaita, etenkin silloin, kun kyse on kaupallisista tuotteista.

Kirjallisuuslähteitä luetaan siten, että niistä pyritään etsimään tapauskokonaisuuksia, joiden pääasialliset toimintaperiaatteet voidaan selittää. Eri lähteitä yhdistellen pyritään saamaan kokonaiskuva kustakin menetelmästä. Tutkimusote voidaan ajatella monimenetelmäiseksi sikäli, että mitä tahansa luotettavina pidettäviä tietolähteitä voidaan käyttää, jos ne auttavat selittämään tapauksia (Eriksson & Koistinen, 2014, s. 9–10).

Pienessä osassa tässä työssä käytetyistä kirjallisuuslähteistä kirjoittajat tai osa kirjoittajista ovat anonyymejä tai he esiintyvät pelkillä etunimillään. Yleensä missä tahansa tutkimuksessa vähimmäisvaatimus uskottavuudelle on, että tutkija esiintyy omalla nimellään ja hänen mahdolliset taustatahonsa ja sidonnaisuutensa ovat selvitettävissä. Tähän työhön on kuitenkin tarkoin harkiten hyväksytty mukaan muutamia anonyymejä tai osittain anonyymejä lähteitä. Edellytyksenä näiden lähteiden hyväksymiselle on ollut, että tutkijoiden anonymiteetille on tunnistettavissa hyväksyttävä syy ja lähteiden julkaisijat tai taustaorganisaatiot ovat uskottavia. Näissä lähteissä esitellään autoritaaristen valtioiden sensuurimenetelmistä tietoja, joita kyseiset maat todennäköisesti eivät haluaisi julkisuuteen. Syy anonymiteetille on näissä tapauksissa se, että tällaisten tietojen julki tuominen voi

altistaa tutkijat häirinnälle, ongelmille urakehityksessä tai jopa väkivallalle – etenkin, jos tutkijat ovat kyseisten maiden kansalaisia (esim. McNeill, 2021; Roy, 2019; Scholars at Risk, 2023). Tässä käytettyjen anonyymien lähteiden taustatahot ovat esimerkiksi yliopistoja, kansalaisjärjestöjä tai tietoturva-alan konferensseja. Lisäksi mukana on joitakin lähteitä, joissa tekijäksi on merkitty vain jokin suuri kansainvälinen yritys. Näissä lähteissä käsitellään lähinnä yleisesti tiedossa olevia verkkoteknisiä asioita, jotka ovat helposti tarkistettavissa useista lähteistä.

2.3 Näkökulman valinnasta

Opinnäytetyön tarkoituksena on lisätä ymmärrystä valtiollisten internet-rajoitusten nykytilasta. Näkökulmana työssä on avoimesta demokratiasta, esimerkiksi Suomesta, tulevan ihmisen tai yrityksen näkökulma. Tarkoitus ei ole tarkastella sitä, kuinka internetiä sensuroivien maiden omat kansalaiset voisivat kotimaassaan käyttää avointa ja vapaata internetiä, vaan kuinka sensuroivissa maissa olevien ulkomaalaisten tulisi toimia. Sensuroivan maan omat kansalaiset voivat toki käytännössä käyttää samoja menetelmiä kuin ulkomailta tulevat, mutta rajoitusten laajempi merkitys sananvapaudelle ja rajoittavien maiden väestön toimintaedellytyksille rajataan tämän tutkimuksen ulkopuolelle.

Opinnäytetyöstä hyötyy periaatteessa kuka tahansa, joka aikoo matkustaa internetiä rajoittavaan maahan. Pääkohderyhmänä ovat kuitenkin ulkomailla toimivat suomalaiset yritykset ja niiden lähettämät työntekijät, jotka tarvitsevat pääsyn länsimaalaisiin internet-palveluihin tai jotka haluavat varmistaa oman tietoturvansa.

3 Konteksti: Internet-rajoitusten tausta ja nykytila

Internetiä ei sensuroida tyhjiössä, vaan sensuurilla on oma kontekstinsa. Ennen kuin mennään sensuurin tekniikoihin, on syytä taustoittaa, kuinka paljon ja miksi valtiot rajoittavat internetin käyttöä ja mitä merkitystä rajoittamisella on. Tämä asettaa koko opinnäytetyön kontekstiinsa, jolloin voidaan arvioida myös työn merkitystä.

3.1 Rajoitukset ovat verkkosensuuria

Rajoituksista käytetään tässä opinnäytetyössä nimitystä sensuuri tai verkkosensuuri, koska ne täyttävät yleiset sensuurin määritelmät. Sensuurille ei ole yksiselitteistä määritelmää, mutta yleensä sillä tarkoitetaan minkä tahansa tiedon, aineiston tai ajatuksen leviämisen rajoittamista. Perinteisen määritelmän mukaan sensuuri on viranomaisten tekemää aineiston poistamista yleisesti saatavilta. Tällöin tarkoitetaan aineiston poistamista nimenomaan siitä syystä, että halutaan estää ihmisiltä pääsy aineistossa olevien tietojen tai ajatusten pariin, koska tietojen tai ajatusten vapaata leviämistä pidetään jollain tavoin haitallisena tai riskialttiina. Sensuuria ei ole esimerkiksi tiedon poistaminen siitä syystä, että tieto on vanhentunutta tai epärelevanttia tai sen säilyttämisestä koituu liikaa kustannuksia. (McDonald, 1993, s. 52.)

Verkkosensuuri voi sisältää paljon muutakin kuin tiedon saatavuuden kontrollointia. Verkossa sensuuri voi kohdistua mihin tahansa sisältöihin, ja se voi olla myös yhteyksiin tai käyttäjiin kohdistuvaa kontrollia (Ekholm & Karhula, 2015, s. 208). Päivikki Karhulan (2013) mukaan voidaan sensuurin ohella puhua myös tietovalvonnasta, joka kohdistuu käyttäjiin. Tietovalvonnalla voidaan seurata, millaisista sisällöistä käyttäjä on kiinnostunut ja millaista tietoa hän on kerännyt.

3.2 Internetin rajoittaminen yleistyy

Vuosi vuodelta useammassa valtiossa internetin vapautta rajoitetaan. Demokratian tilaa maailmassa seuraavan yhdysvaltalaisen Freedom House -järjestön tuoreimman Freedom on the Net - vuosiraportin mukaan internetin vapaus maailmassa oli vuonna 2022 heikentynyt jo 12 vuotta peräkkäin (Freedom House, 2022i, s. 5). Heikentyminen ei kuitenkaan ole täysin

suoraviivaista. Raportin mukaan internetin vapaus oli heikentynyt 28 maassa, mutta samaan aikaan se oli kuitenkin parantunut 26 maassa. Internetin vapautta rajoitetaan järjestön mukaan hyvin monenlaisilla tavoilla. Sitä voidaan rajoittaa esimerkiksi vangitsemalla ihmisiä, jotka julkaisevat sosiaalisissa medioissa politiikkaa, uskontoa tai sosiaalisia kysymyksiä koskevaa sisältöä tai manipuloimalla internetissä käytäviä keskusteluja. Monet maat myös käyttävät teknisiä estomenetelmiä rajoittaakseen pääsyä tiettyihin internet-palveluihin. Tässä opinnäytetyössä käsitellään näitä teknisiä rajoituksia.

Deibert ym. (2012) ovat määritelleet internetin kehityksestä neljä vaihetta, jotka eroavat toisistaan rajoitusten suhteen.

Ensimmäinen vaihe alkoi internetin keksimisestä 1960-luvulla ja jatkui noin vuoteen 2000 asti. Sitä kirjoittajat kuvaavat nimellä ”avoin yhteismaa” (open commons). Tuolloin internet miellettiin eräänlaiseksi muusta elämästä erilliseksi saarekkeeksi, ”kybertilaksi”, ja useimmat maat joko eivät välittäneet internetissä tapahtuvasta toiminnasta tai pyrkivät sääntelemään sitä hyvin kevyesti. Toinen vaihe, ”pääsy kielletty” (access denied) -vaihe kattoi noin vuodet 2000–2005. Tuolloin valtiot katsoivat, että internetissä tapahtuvaa toimintaa pitää jotenkin rajoittaa, ja ne alkoivat ottaa käyttöön suodatuksia, joilla pääsy estettiin tiettyihin palveluihin. Esimerkki näistä estoista ovat vaikkapa Kiinan käyttöön ottamat ulkomaisten palvelujen estot. Kolmas vaihe, ”kontrolloitu pääsy” (access controlled) kattoi noin vuoden 2005–2010, ja sille oli leimallista tarkempi ja monimuotoisempi internetin valvonta ja kontrolli. Siihen sisältyy selkeiden pääsyn estojen lisäksi valvontaa, rekisteröitymispakkoja ja jopa kybervakoilua. Etenkin vaatimalla internet-liittymien ja erilaisten nettipalvelujen käyttäjiltä rekisteröitymistä saadaan autoritaarisissa maissa luotua internetiin itsesensuurin ilmapiiri, jossa käyttäjät itse rajoittavat toimintaansa rangaistusten tai vaikeuksien pelossa. (Deibert ym., 2012, s. 6–14)

Neljäs, vuoden 2010 jälkeen alkanut vaihe on Deibertin ja muiden mukaan ”kiistellyn pääsyn” (access contested) vaihe, jossa aiempien vaiheiden keskeiset osat ovat yhä käytössä, mutta jossa kiista internetin hallinnasta on avointa ja näkyvää. Sekä vapaan ja avoimen internetin että kontrollin kannattajat kamppailevat siitä, kumpi linja voittaa. Valtioiden aiemmissa vaiheissa asettamia rajoituksia kyseenalaistavat sekä toiset valtiot että kansalaisyhteiskunta ja yritykset. Rajoitusten kannattajista puolestaan valtaosa on valtioita,

mutta joukossa on myös yrityksiä. Kiistellyn pääsyn vaiheeseen tultaessa internet on myös militarisoitunut, kun valtiot ovat kehittäneet kykyään informaatiosodankäyntiin internetissä. (Deibert ym., 2012, s. 14–18.)

Viime vuosina internetiä on alettu kuvata myös jakautuneeksi tai pirstaleiseksi (esim. Council on Foreign Relations, 2022; Komaitis, 2023). Internetin vapautta ajava kansainvälinen järjestö Internet Society kuvaa nykyistä internetiä sanalla splinternet, joka on muunnos sirpaletta tarkoittavasta englannin kielen sanasta splinter (Internet Society, 2022). Internetin pirstaloitumisesta on käytetty myös nimitystä balkanisaatio (balkanization). Tällä tarkoitetaan internet-palvelujen jakautumista aiempaa pienempinä yksikköinä toimiviin, toisilleen vihamielisiin alueisiin (Goud, 2018). Venäjän helmikuussa 2022 aloittama hyökkäyssota Ukrainassa on entisestään lisännyt internetin sirpaloitumista (Meinel & Hagebölling, 2023).

Internetin sirpaloituminen voidaan nähdä myös osana kansainvälisten suhteiden ja kansainvälisen politiikan laajempaa kehitystä, jossa koko kansainvälinen järjestelmä on muuttumassa yhä pirstaleisemmaksi (Komaitis, 2023). Myös muut ovat havainneet korrelaatiota valtioiden internetin sensurointitapojen ja poliittisten liittoutumisten välillä (esim. Merrill & Weber, 2020). Kybertilasta on tullut yhä enemmän valtioiden välisen geopoliittisen kilpailun kohde, ja erilaisten internet-palvelujen suodattaminen on osa tätä kilpailua, jossa valtiot pyrkivät rajaamaan hallinnoimiensa alueiden interneteistä eräänlaisia kansallisia saarekkeita tai etupiirejä (Deibert ym., 2012, s. 4).

Internetiä pyrkivät rajoittamaan myös muut toimijat kuin valtiot. Tätä kehitystä esimerkiksi yhdysvaltalainen kansalaisoikeusjärjestö ACLU kuvaa niin ikään jakamalla kehityksen eri vaiheisiin. ACLU:n mukaan internet on nykyisin vapauden suhteen kehityksensä kolmannessa vaiheessa. Tämän näkemyksen mukaan ensimmäisessä vaiheessa eli modeemiyhteyksien aikana internet oli vapaa ja avoin, noudattaen niin sanottua verkon neutraaliusperiaatetta. Se paljolti pysyi sellaisena myös toisessa vaiheessa eli varhaisena laajakaista-aikana, vaikka valtiot ja yritykset tuolloin pyrkivätkin ottamaan internetiä yhä enemmän hallintaansa. Nyt kolmannessa vaiheessa sen sijaan suuret internet-yhtiöt pyrkivät yhä enemmän kontrolloimaan sitä, kuinka internetiä käytetään, ja tähän hallintaan ne käyttävät myös teknisiä keinoja. (Stanley, 2010.)

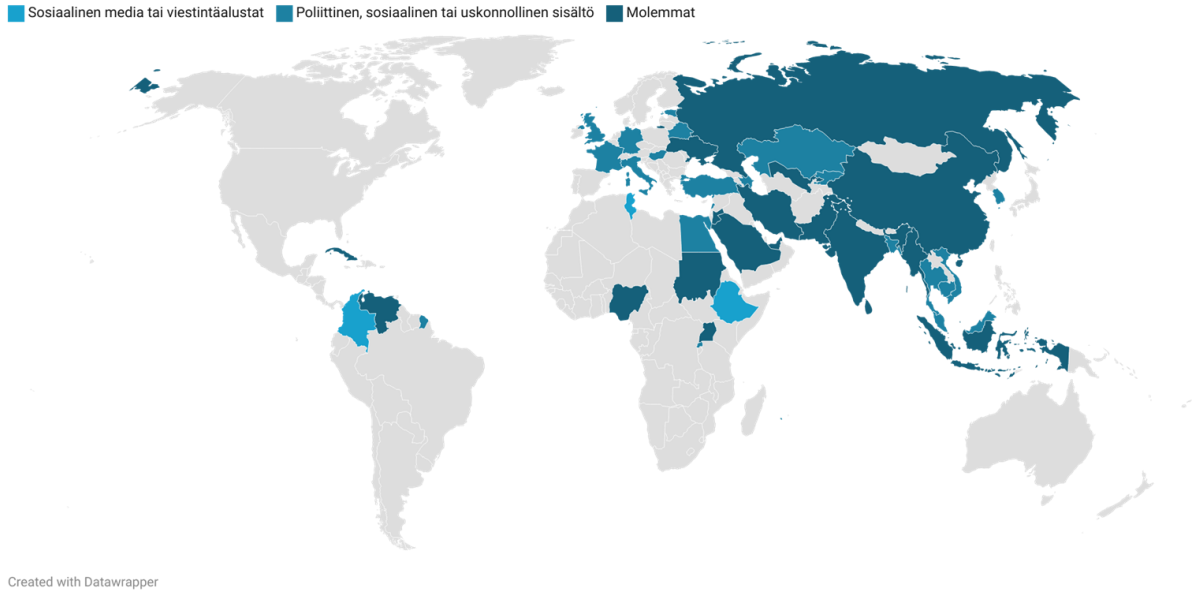
Toisaalta valtiot pyrkivät vastaamaan internet-yhtiöiden pyrkimyksiin yrittämällä rajoittaa eräiden yhtiöiden toimintaa lainsäädännöllä. Esimerkiksi Yhdysvallat on pyrkinyt toistuvasti kieltämään kiinalaisen Bytedance-yhtiön omistaman Tiktok-sovelluksen siihen liittyvine internet-palveluineen, koska yhtiön on arveltu välittävän sovelluksen keräämiä käyttäjätietoja Kiinan hallinnolle (esim. Paul, 2023).

3.3 Maat, jotka sensuroivat internetiä

Runsaan kahden vuosikymmenen kehityksen tuloksena internet-sisältöjen ja -palvelujen sensurointi on nykyisin erittäin yleistä. Freedom Housen mukaan maailman väestöstä 64 prosenttia elää maissa, jotka rajoittavat pääsyä internetissä oleviin poliittisiin, sosiaalisiin tai uskonnollisiin sisältöihin. Maailman ihmisistä 51 prosenttia puolestaan elää maissa, joissa pääsy sosiaalisiin medioihin tai viestintäalustoihin on ollut rajoitettua vähintään tilapäisesti. Useat maat rajoittavat molempia: sekä sisältöjä että sosiaaliseen mediaan tai viestintään liittyviä alustapalveluja. Freedom Housen vuoden 2022 vuosiraporttia varten tutkituista maista peräti kaksi kolmasosaa rajoitti jollain tavalla pääsyä ulkomaisiin tietolähteisiin. (Freedom House, 2022i)

Pääsyä internet-palveluihin rajoitti vuonna 2022 Freedom Housen mukaan 34 maata (Kuva 1). Pääsyä sosiaalisen median palveluihin tai viestintäalustoihin rajoittivat Etiopia ja Tunisia. Pääsyä poliittiseen, sosiaaliseen tai uskonnolliseen sisältöön rajoittivat Britannia, Etelä-Korea, Italia, Kazakstan, Kirgisia, Libanon, Malesia, Ranska, Ruanda, Saksa, Singapore, Thaimaa, Turkki, Unkari, Vietnam ja Viro. Pääsyä molempiin rajoittivat Arabiemiraatit, Indonesia, Intia, Iran, Jordania, Myanmar, Nigeria, Pakistan, Saudi-Arabia, Sri Lanka, Sudan, Uganda, Ukraina, Uzbekistan, Venezuela ja Venäjä (Freedom House, 2022i).

Kuva 1: Internetiä rajoittavat maat kartalla (Freedom House, 2022i)



Freedom Housen tarkastelussa on mukana kaikkiaan 70 maata. Järjestö on määritellyt maiden internet-vapaudelle indeksin, jossa arvo 100 vastaa kaikkein suurinta vapautta ja arvo 0 kaikkein vähäisintä vapautta. Maat, joiden indeksin arvo on vähintään 70 on määritelty vapaiksi. Indeksin arvoilla 40—69 maa on osittain vapaa, ja alle 40 tarkoittaa ei-vapaata maata. (Freedom House, 2022b.)

Ei-vapaiksi määriteltyjä maita oli 21 Freedom Housen mukaan vuonna 2022. Internetin näkökulmasta osittain vapaita puolestaan oli 32 maata (Taulukko 1).

Taulukko 1: Internetiä sensuroivia maita (Freedom House, 2022i)

Ei vapaa internet	
Thaimaa	39
Azerbaidžan	38
Ruanda	37
Kazakstan	32
Turkki	32
Venezuela	30
Bahrain	29
Sudan	29
Valko-Venäjä	28
Arabiemiirikunnat	28
Egypti	27
Etiopia	27
Uzbekistan	27
Pakistan	26
Saudi-Arabia	24
Venäjä	23
Vietnam	22
Kuuba	20
Iran	16
Myanmar	12
Kiina	10

Osittain vapaa internet	
Unkari	69
Kenia	68
Etelä-Korea	67
Brasilia	65
Filippiinit	65
Kolumbia	64
Ecuador	64
Ghana	64
Angola	61
Meksiko	61
Tunisia	61
Malesia	59
Ukraina	59
Sambia	58
Malawi	57
Nigeria	57
Gambia	56
Singapore	54
Kirgisia	53
Intia	51
Libanon	51
Marokko	51
Uganda	50
Indonesia	49
Zimbabwe	49
Sri Lanka	48
Jordania	47
Nicaragua	45
Libya	44
Bangladesh	43
Kambodža	43
Irak	42

Yhdysvaltalainen lehdistönvapausjärjestö Committee to Protect Journalists puolestaan laati vuonna 2019 listan kymmenestä maailman sensuroiduimmasta maasta (Taulukko 2).

Taulukko 2: Kymmenen sensuroiduinta maata (CPJ, 2019)

Järjestys	Maa
1	Eritrea
2	Pohjois-Korea
3	Turkmenistan
4	Saudi-Arabia
5	Kiina
6	Vietnam
7	Iran
8	Päiväntasaajan Guinea
9	Valko-Venäjä
10	Kuuba

Näistä maista Eritrea näyttää Committee to Protect Journalistsin mukaan rajoittavan pääsyä internet-sisältöihin melko satunnaisesti, koska internet on Eritreassa vain harvojen käytettävissä ja hallinto on niin brutaali ja sen valta niin laajalle ulottuvaa, että internetin rajoittaminen on käytännössä tarpeetonta. Pohjois-Koreassa puolestaan pääsy maailmanlaajuiseen internetiin on annettu vain poliittiselle eliitille, ja muut pääsevät vain tiukasti kontrolloituun Pohjois-Korean sisäiseen verkkoon nimeltä Kwangmyong. Myös Turkmenistanissa pääsy internetiin ylipäätään on vain melko pienellä osalla väestöstä, ja riippumattomiin internet-julkaisuihin pääsy sekä ainakin joidenkin VPN-palvelujen käyttö on estetty. (CPJ, 2019.)

On hyvä pitää mielessä, että pääsyä internet-palveluihin eivät rajoita ainoastaan autoritaarisesti hallitut maat, vaan yhä useammin myös länsimaiset demokratiat (Rytinki, 2014). Alaluvussa 3.3 mainittujen poliittisen, sosiaalisen tai uskonnollisen sisällön rajoittajien joukossa on avoimia demokratioita kuten Britannia, Italia, Ranska, Saksa ja Viro, jotka esimerkiksi Freedom House kaikesta huolimatta luokittelee vapaan internetin maiksi. Näissä maissa rajoitukset koskevat esimerkiksi disinformaatiota levittäviä Venäjän valtiollisia tiedotusvälineitä. Näissä maissa rajoitukset ovat periaatteellisesti erilaisia kuin autoritaarisissa maissa, sillä demokratioissa myös rajoituksista ovat päättäneet demokraattisesti valitut päätöksentekoelimet. Avoimien demokratioiden internet-sensuuria käsitellään tarkemmin jäljempänä alaluvussa 3.4.

Kun puhutaan internetin käytön rajoittamisesta, on syytä huomioida sekin, että merkittävää osaa maailman väestöstä rajoitukset eivät koske siitä syystä, että he eivät käytä

minkäänlaista internetiä, edes sensuroitua tai rajoitettua. Pienelle osalle heistä kyse voi olla omasta valinnasta, mutta hyvin monilla ei olisi pääsyä verkkoon, koska verkkoa ei ole tai heillä ei ole siihen varaa. (ITU, 2023.)

Kansainvälisen telealan järjestön ITU:n mukaan vuonna 2022 maailman väestöstä arviolta 66 prosenttia käytti internetiä. Noin joka kolmas ihminen maailmassa ei siis käyttänyt lainkaan internetiä. Internet voidaan ajatella maailman mittakaavassa jossain määrin etuoikeutettujen ihmisten toimintaympäristönä, sillä kaikkein köyhimmissä maissa vain 36 prosenttia väestöstä käytti internetiä ITU:n mukaan vuonna 2022. Lisäksi internetin käyttö on selkeästi sukupuolittunutta etenkin köyhimmissä maissa. Köyhimpien maiden naisista 30 prosenttia käytti internetiä, kun samojen alueiden miehistä osuus oli 43 prosenttia. Köyhimmissä maissa nuoret käyttävät internetiä enemmän kuin väestö keskimäärin, sillä köyhimpien maiden 15–24-vuotiaista internetin käyttäjiä oli 48 prosenttia. Köyhimmissä maissa internetin käytön rajallisuutta selittänee ainakin osittain se, että niissä 3g- ja 4g-mobiiliverkkojen peitto on ITU:n mukaan vähemmän kattava kuin kehittyneissä maissa, vaikka kuitenkin käytännössä kaikilla maailman urbaaneilla alueilla on jonkinlainen mobiililaajakaistaverkko käytettävissä. (ITU, 2023.)

3.4 Mitä internetistä sensuroidaan

Sensuurin ymmärtämisen kannalta on olennaista tietää myös, millaisia asioita internetistä yleensä sensuroidaan. Kaikkien maiden kaikkea sensuuria ei tässä kattavasti selosteta, koska internetiä enemmän tai vähemmän sensuroivia maita on erittäin suuri määrä ja niiden sensuuritoimet sekä -tarpeet vaihtelevat eri aikoina. Mukaan on poimittu tyypillisiä tapauksia esimerkinomaisesti.

3.4.1 Suomi

Suomi on vakaa ja avoin eurooppalainen maa, jonka sananvapaustilanne on kansainvälisesti vertaillen hyvä (esim. OECD, 2021), mutta Suomikin rajoittaa pääsyä tiettyihin internet-sisältöihin. Suomessa on pyritty rajoittamaan pääsyä internetissä etenkin tekijänoikeuksien suojaamaan aineistoon sekä lapsipornoa sisältävään aineistoon (Rytinki, 2014).

Sensuuri Suomessa ei ole kuitenkaan ollut aina kovin tehokasta. Lapsipornon sensuroimiseksi internetistä säädettiin Suomessa erillinen laki vuonna 2006, mutta laki menetti melko nopeasti merkityksensä, koska sensuurin käytännön toteutus osoittautui odotettua vaikeammaksi. Laki lapsipornografian levittämisen estotoimista (1068/2006) tuli voimaan vuoden 2007 alussa. Laissa mahdollistetaan se, että teleyritykset määrätään estämään pääsy lapsipornosivustoille internetissä. Lain tultua voimaan poliisi laati ja päivitti listoja sivustoista, jotka teleyritysten piti estää. Lopulta poliisi kuitenkin lakkasi päivittämästä listoja ja teleyritykset lakkasivat estämästä listoilla olleita osoitteita, koska kävi selväksi, etteivät estot olleet tehokkaita (Opetus- ja kulttuuriministeriö, 2013).

3.4.2 Euroopan unioni

Myös Euroopan unioni on päätynyt rajoittamaan tiettyjä internet-sisältöjä. Nämä säännökset ovat voimassa myös Suomessa Suomen omien lakien lisäksi, koska Suomi on EU:n jäsenmaa. Maaliskuussa 2022 Euroopan unionin neuvosto kielsi pääsyn venäläisen RT- eli Russia Today -median eri kielisiin eurooppalaisiin uutiskanaviin sekä Sputnik-kanavaan. Kesäkuussa 2022 neuvosto lisäsi kieltolistalle Rossija-kanavan eri versioita sekä TV Centre International -kanavan. Kielto oli seurausta täysimittaisesta hyökkäyssodasta, jonka Venäjä aloitti Ukrainassa 24. helmikuuta 2022. Kiellot koskivat kaikkea näiden medioiden jakelua, myös internetissä tapahtuvaa. Käytännössä kielto tarkoittaa internetin osalta, että internet-palvelujen tarjoajat velvoitetaan suodattamaan tällaiset sisällöt pois asiakkaidensa tai käyttäjiensä saatavilta. Kielloilla pyritään estämään Venäjän propagandaoperaatioita EU-maissa. Kieltojen on määrä olla voimassa, ”kunnes aggressio Ukrainaa vastaan lopetetaan ja kunnes Venäjän federaatio sekä siihen kytkeytyvät mediaorganisaatiot lakkaavat toteuttamasta propagandatoimia unionia ja sen jäsenvaltioita vastaan”, todetaan asiaa koskevassa neuvoston päätöksessä. (Fathaigh, 2022.)

EU-maissa lisäksi syksyllä 2022 voimaan tullut digitaalisten palvelujen asetus velvoittaa joukon internetissä palveluja tarjoavia yhtiöitä moderoimaan palvelujaan niin, ettei niissä ole laittomia sisältöjä, kuten vihapuhetta. Samalla asetus kuitenkin velvoittaa palveluntarjoajat antamaan yleisölle mahdollisuuden valittaa tällaisista moderointipäätöksistä. Velvoite koskee esimerkiksi tietyt kriteerit täyttäviä verkkokauppoja ja sosiaalisen median palveluja. (Hartmann, 2023.)

Suomen lisäksi myös monet yksittäiset Euroopan unionin jäsenmaat ovat asettaneet erilaisia pääsyrajoituksia internet-sisältöihin, vaikka lähes kaikki unionin maat ovatkin sananvapautta kunnioittavia demokratioita. Usein rajoitukset koskevat rikollista tai haitallista aineistoa kuten lapsipornoa, mutta mailla on myös omia yksilöllisiä näkemyksiään sensuuritarpeesta. Esimerkiksi Saksassa on pyritty rajoittamaan natsiaineiston leviämistä. Nordhein-Westfalenin osavaltiossa määrättiin vuonna 2002 internet-palveluntarjoajat estämään pääsy kahdelle ulkomaiselle äärioikeistosivustolle (Dornseif, 2003).

3.4.3 Kiina

Todennäköisesti tunnetuin internetiä sensuroiva valtio on Kiina, joka aloitti internetin sensuroimisen 1990-luvulla. Kiinalla tarkoitetaan tässä yhteydessä Kiinan kansantasavallan faktisesti hallitsemia alueita. Esimerkiksi Taiwan toimii käytännössä kuten itsenäinen valtio, vaikka Kiina katsookin sen yhdeksi maakunnistaan. Taiwanin internet on yksi Aasian vapaimmista, eivätkä sen sensuurikäytännöt mainittavasti eroa demokraattisten maiden käytännöistä (Freedom House, 2022g).

Kiina on parin vuosikymmenen aikana kehittänyt erittäin tehokkaita tekniikoita pääsyn estämiseksi Kiinasta tiettyihin ulkomaisiin internet-sisältöihin. Kiinan vaikutus internet-sensuuriin ei rajoitu ainoastaan maan sisälle, sillä se myös levittää internetin sensuuri- ja tarkkailumenetelmiä ulkomaille myymällä tätä varten kehittämiään ohjelmistoja, laitteita ja osaamista. Kiina on vuonna 2011 esimerkiksi myynyt Iranille laajan internet-liikenteen tarkkailujärjestelmän, joka sisälsi sekä laitteistoa että ohjelmistoja myös länsimaalaisilta valmistajilta (Stecklow, 2012).

Freedom Housen mukaan Kiinassa oli vuonna 2022 kahdeksatta vuotta peräkkäin ”maailman huonoin” tilanne internetin vapauden suhteen (Freedom House, 2022i, s. 9). Tässä tosin on huomioitava, että Freedom Housen selvitykseen ei ollut lainkaan otettu mukaan sellaisia erittäin rajoittavia maita kuin esimerkiksi Pohjois-Korea, Turkmenistan tai Eritrea.

Kiinaa johtava kommunistinen puolue pyrkii käytännössä pitämään käytännössä kaiken julkisen informaatiotilan hallinnassaan, ja puolue on alusta asti katsonut, että internetillä on tässä erittäin tärkeä rooli (Benetti, 2022, s. 89). Kiinan kommunistisen puolueen pääsihteeri

Xi Jinping on pitänyt esillä internet-sensuurin tärkeyttä, käyttämättä kuitenkaan sanaa sensuuri. ”On elintärkeää säilyttää puolueen hallinta internet-sektorilla”, hän ilmoitti esimerkiksi heinäkuussa 2023 Pekingissä pidetyssä kyberturvallisuuskonferenssissa (Xinhua, 2023). Sensuroinnin motiivina Kiinalla on lähinnä halu muokata mielipideilmastoa hallinnolle suotuisaksi sekä ehkäistä näkyviä mielenilmauksia ja sosiaalista epävakautta, ja mahdollisesti myös halu antaa kiinalaisille teknologiayrityksille kilpailuetua ulkomaisiin yrityksiin nähden (Y. Wang, 2020).

Kiina sensuroi ulkomaisia verkkosisältöjä ja -palveluja järjestelmällä, josta tässä käytetään suomenkielistä nimitystä Kiinan palomuuri. Järjestelmän alkuperäinen kiinankielinen nimitys 防火长城, pinyin-järjestelmällä translitteroituna Fánghuǒ Chángchéng, ja englanninkielinen nimitys Great Firewall (GFW) ovat johdoksia nimityksistä, joita käytetään Pohjois-Kiinassa sijaitsevasta joukosta muinaisia rakennelmia. Rakennelmat ovat kiinaksi万里长城 (Wànlǐ Chángchéng), englanniksi Great Wall [of China] ja suomeksi Kiinan muuri. Tällöin on luontevaa johtaa Kiinan sensuurijärjestelmän nimitys myös suomeksi samojen rakennelmien nimestä, joten järjestelmää voi sanoa Kiinan palomuuriksi.

Kiinan palomuuri otettiin käyttöön viime vuosituhannen vaihteessa osana Kiinan turvallisuusministeriön käynnistämää, Kultainen kilpi -projektiksi (Golden Shield Project / 金盾工程 / Jīndùn Gōngchéng) nimettyä laajamittaista valvonta- ja sensuuriohjelmaa. Aluksi Kiinan palomuuri esti pääsyn vain rajalliselle määrälle kiinankielisiä, kommunistista puoluetta vastustaneita verkkosivustoja, joiden rajoitukset oli melko helppo kiertää, mutta sittemmin järjestelmä on laajentunut erittäin kattavaksi. Kiina täydentää Kiinan palomuuria maan sisäisellä valvonta- ja sensuurijärjestelmällä sekä lainsäädännöllä, joka rajoittaa verkkojulkaisemista. (Y. Wang, 2020.)

Nykyisellään Kiinan palomuuri on yksi maailman laajimmista internet-sensuurijärjestelmistä. Kiina on estänyt pääsyn erittäin suureen määrään ulkomaisia sisältöjä, esimerkiksi käytännössä kaikkiin länsimaalaisiin sosiaalisen median palveluihin, blogialustoihin ja viestintäsovelluksiin sekä lukuisiin uutismedioihin, videontoistopalveluihin ja käytännössä kaikkiin pornosivustoihin. Sensuroiduista internet-sivustoista tai palveluista on vaikea laatia kattavaa listaa, koska sensuuritilanne muuttuu aika ajoin, eikä sensuuri perustu pelkästään

palvelujen osoitteisiin, vaan myös sisältöjen suodattamiseen. Lisäksi Kiina pyrkii teknisesti estämään sensuurin kiertämismenetelmien, kuten VPN-yhteyksien käyttöä. (Benetti, 2022, s. 89; Y. Wang, 2020; Yuan, 2018)

Kiinan estämiä ulkomaisia sivustoja voi listata esimerkinomaisesti käyttämällä Comparitech-sivustolla (Comparitech, ei pvm.) olevaa palvelua (Taulukko 3). Palvelussa voi testata, onko jokin verkko-osoite kielletty Kiinassa. Kattavaa listaa palvelusta ei saa.

Taulukko 3: Esimerkkejä Kiinassa estetyistä palveluista (Comparitech, ei pvm.)

Sosiaalinen media ja blogialustat	**Media- ja uutispalvelut**	**Viestisovellukset**	**Muita palveluja**
Instagram	The New York Times	WhatsApp	Dropbox
Facebook	Washington Post	FB Messenger	Google Drive
Twitter	Financial Times	Viber	Google Search
TikTok	BBC	Signal	DuckDuckGo
Wordpress	Reuters	Telegram	
Blogspot	Le Monde	Discord	
Blogger	Süddeutsche Zeitung		

Kiina rajoittaa myös joidenkin kiinalaisten yhtiöiden ulkomailla toimivien palvelujen käyttöä Kiinassa. Esimerkiksi kiinalaisen Bytedance-yhtiön kansainvälisille markkinoille suunnattu lyhytvideopalvelu TikTok ei toimi Kiinassa (Taulukko 3), vaikka saman yhtiö tuottama, Kiinan markkinoille tarkoitettu vastaavanlainen palvelu Douyin toimii (Lin, 2021). Lisäksi Kiina vaatii maan rajojen sisällä toimivilta ulkomaisilta yhtiöiltä Kiinan sensuurisääntöjen noudattamista. Esimerkiksi Kiinassa toimiva versio yhdysvaltalaisen Microsoftin Bing-hakukoneesta sensuroi laajalti hakutuloksiaan (Knockel ym., 2023).

Bingiä vastaava, yhdysvaltalaisen Google-yhtiön hakukone puolestaan ei toimi Kiinassa, koska Google ei ole suostunut sensuroimaan hakutuloksia. Tästä syystä Kiina on vuodesta 2014 asti estänyt Kiinan palomuurilla pääsyn käytännössä kaikkiin Googlen palveluihin, kuten Gmailiin, Google Mapsiin ja Google Scholariin sekä Android-sovelluskauppa Google Playhin. (Sheehan, 2018.)

Kiinan erityishallintoalueilla Hongkongissa ja Macaossa pätevät eri säännöt kuin manner-Kiinassa. Esimerkiksi Hongkongissa on oma lainsäädäntö, joka takaa teoriassa sananvapauden, mutta sielläkin sananvapauden rajat ovat tiukentuneet viime vuosina,

etenkin vuoden 2019 demokratiamielenosoitusten jälkeen. Vuonna 2020 voimaan tulleen turvallisuuslain on tulkittu periaatteessa mahdollistavan Kiinan palomuurin ulottamisen myös Hongkongiin, mutta toistaiseksi näin kattavaa verkkosensuuria ei ole Hongkongissa otettu käyttöön (Freedom House, 2022c; Von Kalkhof, 2021). Internet on Hongkongissa silti edelleen huomattavasti vapaampi kuin muualla Kiinassa. Esimerkiksi heinäkuussa 2023 paikallinen tuomioistuin esti paikallisia viranomaisia kieltämästä demokratiamielistä internet-sisältöä (May, 2023).

3.4.4 Pohjois-Korea ja muut suljetut valtiot

Kaikkein suljetuimmissa valtioissa internet-sensuuri ei vaadi kovin monimutkaista tekniikkaa, koska pääsy kansainväliseen internetiin on rajattu vain tarkoin valikoiduille kansalaisille, tai koska valvontayhteiskunta on niin tehokas, ettei internetiä uskalleta käyttää tavoilla, jotka hallinto voisi kokea uhkaavaksi.

Mahdollisesti tunnetuin kansalaisvapauksia rajoittava valtio, noin 26 miljoonan asukkaan Pohjois-Korea, on totalitaarinen diktatuuri, jossa valtio hallitsee kaikkea tiedonvälitystä ja valvoo kansalaisten keskinäistä viestinvaihtoa. Pohjois-Koreassa tavalliset kansalaiset eivät pääse kansainväliseen internetiin lainkaan. Pääsy internetiin on rajattu vain muutamalle tuhannelle poliittiseen eliittiin kuuluvalle ihmiselle. Pohjois-Koreassa toimii kuitenkin tavallisille kansalaisille tarkoitettu, valtion ylläpitämä oma internet, joka on eräänlainen maan sisäinen intranet. Enemmistöllä väestöstä ei ole kuitenkaan pääsyä siihenkään. (Burgess, 2023; Freedom House, 2022e.)

Vapauden suhteen suunnilleen samalla tasolla Pohjois-Korean kanssa on Eritrea. Internetin kontrollointi hoidetaan Eritreassa lähinnä internet-kahviloita valvomalla ja tarvittaessa sulkemalla hallintoa arvostelevia verkkosivustoja. Internet-sensuurin tarvetta vähentää se, että pääsy internetiin on vain parilla prosentilla väestöstä, ja hallinto on niin alistava, että internetin käyttäminen hallintoa kyseenalaistavalla tavalla on erittäin riskialtista. (CPJ, 2019; Freedom House, 2022a; RSF, 2021.)

Vielä Pohjois-Koreaakin vähemmän kansalaisvapauksia on Freedom Housen mukaan Turkmenistanissa, joka sijaitsee Keski-Aasiassa. Turkmenistan sai vuonna 2022 Freedom

Housen Freedom in the World -raportissa vain kaksi pistettä sadasta, kun Pohjois-Korea sai kolme. Internetin rajoittamisen suhteen Turkmenistan ei teknisesti ole kovin edistynyt, mutta rajoituksia on melko kattavasti. Turkmenistanissa toimii yksi valtiollinen internet-palveluntarjoaja, joka rajoittaa kansalaisten pääsyä esimerkiksi riippumattomiin uutislähteisiin ja moniin muihin internet-sivustoihin. Viranomaisten on raportoitu salakuuntelevan internet-puheluja, tallentavan näppäimistöjen käyttöä ja kaappaavan tietokoneisiin kytkettyjä kameroita. Viranomaisilla saattaa olla vain rajallinen kyky estää rajoitusten kiertäminen teknisin keinoin. Tähän viittaa se, että viranomaisten on raportoitu pakottaneen koti-internet-yhteyksiä hankkineita ihmisiä vannomaan Koraanin nimiin, etteivät he käytä VPN:ää, kun kehittyneemmissä maissa VPN-estot hoidetaan teknisin keinoin. Koti-internet-yhteyden saaminen on Turkmenistanissa vaikeaa ja vie aikaa. (Freedom House, 2022h; RFE/RL, 2021.)

3.4.5 Iran

Myös shiiaislamistinen teokratia Iran kuuluu aktiivisiin internetin sensuroijiin. Iranin ylin hengellinen johtaja Ali Khamenei on pyrkinyt valtakaudellaan lisäämään internetin kontrollia ja keskittämään siihen liittyvää valtaa itselleen. Käytännössä hän johtaa perustamaansa Kyberavaruuden ylintä neuvostoa, tiedustelupalveluja ja Vallankumouskaartia, jotka vastaavat internetin kontrolloinnista Iranissa (Center for Human Rights in Iran, 2018, s. 18–20). Internet-arkkitehtuurinsa erityispiirteiden ansiosta Iran kykenee katkaisemaan lähes kokonaan internet-yhteydet ulkomaille siten, että maan sisäinen internet kuitenkin toimii. Ulkomaanyhteydet katkaistiin esimerkiksi vuonna 2019, kun Iranissa oli mielenosoituksia (Salamatian ym., 2021).

Iranilla oli alun perin pyrkimyksenä rakentaa maahan hieman Pohjois-Korean tapaan eräänlainen maan sisäverkko, valtion kontrolloiman ”kansallisen internet”, joka olisi ollut erillään kansainvälisestä internetistä. Tällöin iranilaiset olisivat päässeet verkossa käsiksi vain hallinnon hyväksymään tietoon. Viranomaiset eivät kuitenkaan lopulta pitäneet tällaista järjestelmää mahdollisena, koska se olisi hallinnon mielestä liikaa haitannut esimerkiksi yliopistojen, pankkien, muiden yritysten ja valtion virastojen toimintaa. Sen sijaan Iraniin perustettiin ”kansallinen informaatioverkko” (National Information Network, NIN).

Järjestelmää on otettu käyttöön vaiheittain. (Center for Human Rights in Iran, 2018, s. 26–28.)

NIN-verkon on Iranin viranomaisten mukaan tarkoitus olla ”puhdas” sekä ”uskonnollisten ja vallankumouksellisten arvojen mukainen” (Citizen Lab, 2012) ja ”vapaa läntisistä ajatuksista ja ihanteista” (Stone, 2023). Kyseessä on valtion kontrolloima Iranin sisäinen verkko, jossa voi käyttää iranilaisia palveluja ja iranilaista sisältöä, mutta jonka kautta pääsee myös kansainväliseen internetiin. Käytännössä tämä tarkoittaa, että Iranin sisäinen ja ulkoinen internet-liikenne on eriytetty, mikä mahdollistaa Iranin irrottamisen kansainvälisestä internetistä aina, kun hallinto katsoo sen tarpeelliseksi. NIN:ssä on paikalliset versiot merkittävimmistä kansainvälisistä internet-palveluista, kuten YouTubea vastaava Aparat. NIN:n tiedonsiirtonopeus on parempi kuin kansainvälisen verkon ja sen käyttö on halvempaa. Iran kykenee myös halutessaan hidastamaan ulkomaan yhteyksiä entisestään, kuten se teki esimerkiksi joulukuun 2017 levottomuuksien aikana (Center for Human Rights in Iran, 2018, s. 26–27, 33.)

Raja pohjoiskorealaistyyppisen maan sisäisen intranetin ja NIN-järjestelmän välillä on pitkälti määrittelykysymys. Osa tutkijoista katsoo, että Iran on kehittämässä verkkoaan kohti maan sisäistä intranetiä, joka voitaisiin nähdä eräänlaisena islamistisena ”halal-internetinä” (esim. Salamatian ym., 2021, s. 12).

NIN-verkko on suunniteltu vaatimaan käyttäjiltä vahva tunnistautuminen, ennen kuin verkkoa pääsee käyttämään. Tätä ominaisuutta ei kuitenkaan aivan alussa otettu käyttöön (Center for Human Rights in Iran, 2018, s. 37). Verkon on Iranin viranomaisten mukaan määrä olla kokonaan valmis ja kaikkien ominaisuuksien käytössä viimeistään keväällä 2024 (Stone, 2023). Tavoitteena on, että valtaosalla iranilaisista olisi käytettävissään vain NIN, ja laajemmat käyttöoikeudet mukaan lukien valvotun VPN-yhteyden käyttö annettaisiin vain valikoiduille ihmisille, kuten viranomaisille ja tutkijoille (Stone, 2023).

Iran pyrkii myös estämään salattujen viestisovellusten kuten Signalin käyttöä. Politiikka on kuitenkin vaihdellut, ja toisinaan esimerkiksi WhatsApp ja Telegram ovat toimineet. Iran on myös estänyt pääsyn lukuisiin ulkomaisiin verkkopalveluihin ja esimerkiksi hakukoneisiin.

Kotimaisten hakukoneiden tuloksia Iran suodattaa voimakkaasti, samoin ulkomaisten, jos käytössä ei ole SSL-salausta (Center for Human Rights in Iran, 2018, s. 42, 63).

Iran on yleensä tiukentanut internet-sensuuria silloin, kun maassa on ollut mielenosoituksia tai levottomuuksia. Esimerkiksi syksyllä 2022 Iran sulki koko internetin osissa Teherania ja Kurdistania, kun meneillään oli kurditaustaisen opiskelijanaisen Mahsa Aminin kuolemasta seuranneita suuria mielenosoituksia. Tuolloin Iran myös esti pääsyn Instagramiin ja WhatsAppiin. (Strzyżyńska, 2022.)

Iranin on myös väitetty hankaloittaneen joidenkin länsimaalaisten sosiaalisten medioiden ja viestipalvelujen käyttöä estämällä näiden palvelujen kaksivaiheisessa tunnistautumisessa käytettävien tekstiviestien saapuminen Iranin mobiiliverkoissa oleviin puhelimiin. Teleoperaattorien on väitetty suodattavan tekstiviestejä avainsanojen perusteella. Kiellettyjä avainsanoja olisivat esimerkiksi ”code”, ”Telegram”, ”WhatsApp” ja ”Instagram”. (Sinaee, 2022.)

3.4.6 Venäjä

Venäjän viranomaiset ovat väittäneet, että Venäjällä on Iranin tapaan kyky irrottaa maa kansainvälisestä internetistä siten, että maan sisäinen internet kuitenkin toimii. Venäjä väitti joulukuussa 2019 tehneensä testejä, jotka osoittivat tämän olevan mahdollista. Venäjä on pyrkinyt tiivistämään internet-arkkitehtuuriaan niin, että verkkoliikenne ulkomaille kulkee verrattain harvojen strategisten kuristuskohtien (engl. choke points) kautta. Venäjä perustelee tätä järjestelyä ”kansallisella turvallisuudella”. (Balašova ym., 2023; Cimpanu, 2019a, 2019b.)

Venäjä on vain muutamien vuosien kuluessa rakentanut sensuurijärjestelmän, josta käytetään nimitystä TSPU. Lyhenne on venäjäksi ТСПУ, ja se tulee sanoista Технические средства противодействия угрозам eli ”uhkien vastustamisen tekniset keinot” (Švets & Frenkel, 2023). TSPU on verkkoliikenteen analysointiin perustuva järjestelmä, jonka käyttöä vaatii Venäjän vuonna 2019 hyväksymä niin sanottu suvereeni RuNet -laki (Xue, Mixon-Baca, ym., 2022, s. 179). RuNet on nimitys, jota käytetään lähinnä geopoliittisessa mielessä siitä

Venäjän hallitsemasta internetin osasta, joka sijaitsee Venäjän ja osin myös muiden entisen Neuvostoliiton maiden alueella (Douzet ym., 2020, s. 159).

Vuonna 2022 tehdyn tutkimuksen perusteella Venäjä sensuroi verkostaan tuohon aikaan lähinnä uhkapeleihin, huumeisiin ja rahoitukseen liittyviä sisältöjä sekä informaatiomediaa, joka tarkoitti muun muassa uutismediaa, blogeja, sosiaalista mediaa ja multimedia-alustoja (Xue, Mixon-Baca, ym., 2022, s. 186–187). Venäjän helmikuussa 2022 aloittama täysimittainen sota Ukrainassa on johtanut siihen, että Venäjällä sensuroidaan internetiä yhä voimakkaammin. Hyökkäyssodan alettua Venäjä esti vuoden 2022 aikana pääsyn yli 5 000 verkkosivustolle, joiden joukossa oli muun muassa riippumattomia uutissivustoja, jotka raportoivat sodasta (Freedom House, 2022f).

Keväällä 2022 Venäjän viestintäviranomainen Roskomnadzor ilmoitti estävänsä pääsyn Instagramiin, Facebookiin ja Twitteriin ja kieltävänsä uusien julkaisujen tekemisen TikTokiin. Venäjän viranomaiset ovat rajoittaneet pääsyä myös moniin länsimaisiin uutis- ja mediapalveluihin kuten BBC:hin, Deutsche Welleen, Radio Free Europe/Radio Libertyyn ja Voice of Americaan. (Feldstein, 2022.)

3.4.7 Muut maat

Myös lukuisat muut maat sensuroivat internetiä tavalla tai toisella, joko ajoittain tai pysyvästi. Esimerkiksi itsevaltainen monarkia Saudi-Arabia on estänyt pääsyn kymmenille tuhansille internet-sivustoille, joiden joukossa on esimerkiksi ulkomaisia uutissivustoja. Sensuurilla pyritään tukahduttamaan kansalaisoikeusaktivismia, pitämään yllä uskonnollista ja poliittista kontrollia sekä ehkäisemään sellaisia ulkomaisia vaikutteita, joita maata johtava suku pitää uhkana. Kiellettyä on esimerkiksi islaminuskon arvostelu ja radikaalin islamin edistäminen. Lisäksi hallinto pyrkii verkkosensuurilla estämään poliittista oppositiota ilmaisemasta mielipiteitään ja koordinoimasta toimintaansa esimerkiksi viestisovellusten avulla. (Porutiu, 2021.)

Kaakkois-Aasiassa sijaitseva Myanmar eli entinen Burma puolestaan on sensuroinut internetiä etenkin vuoden 2021 sotilasvallankaappauksen jälkeen. Ennen sotilasvallankaappausta Myanmar oli hiljalleen siirtymässä kohti demokraattista hallintoa,

mutta armeija päätti lopettaa demokratiaohjelman ottamalla vallan käsiinsä. Armeija hallinnoi Myanmarissa toimivia neljää mobiili-internet-palveluntarjoajaa. Useimmat internet-käyttäjät pääsevät Myanmarista vain 1 200:lle hallinnon hyväksymälle internet-sivustolle. Myanmarissa on vuodesta 2021 alkaen toisinaan suljettu koko internet alueellisesti tai paikallisesti, kun armeija on suorittanut operaatioita opposition joukkoja vastaan. (Freedom House, 2022d.)

3.5 Internet-sensuurin syyt

Internetin käyttöä rajoittavat valtiot ovat usein melko niukkasanaisia rajoituksista ja niiden syistä. Osa valtioista on kuitenkin julkisesti perustellut rajoituksiaan. Julki lausutut perustelut liittyvät yleensä valtiolliseen itsemääräämisoikeuteen sekä kansalliseen turvallisuuteen ja kyberturvallisuuteen.

Ääneen lausuttujen syiden lisäksi tai sijasta sensuurille on myös muita syitä, jotka liittyvät autoritaaristen valtioiden hallintojen haluun pitää kiinni vallasta. Sensuuria voi pitkälti selittää demokratian puute.

3.5.1 Julki lausutut perustelut

Yksi maailman merkittävimmistä internetin rajoittajista, Kiina, ei ole tavannut puhua internet-sensuurista suoraan, mutta Kiinan johdon puheista saa kuitenkin käsityksen siitä, kuinka rajoituksia pyritään perustelemaan yleisölle kotimaassa ja ulkomailla. Kiinaa hallitsevan kommunistisen puolueen pääsihteeri Xi Jinping on toistuvasti vuodesta 2015 alkaen pitänyt esillä niin sanottua kybersuvereniteetin käsitettä (Mai, 2017).

Kybersuvereniteetilla Kiina tarkoittaa kunkin valtion oikeutta hallinnoida internetiä omalla alueellaan parhaaksi katsomallaan tavalla. Kiina käytännössä rinnastaa käsitteen alueelliseen suvereniteettiin eli maiden itsemääräämisoikeuteen tietyillä maantieteellisillä alueilla. Kiina on selittänyt näkemyksiään internetin hallinnoinnista esimerkiksi Kiinan valtioneuvoston tiedotustoimiston marraskuussa 2022 julkaisemassa virallisessa lausunnossa (State Council Information Office of of China, 2022). Lausunnossa Kiina korostaa ”kybersuvereniteetin” lisäksi myös turvallisuusnäkökohtia. Lausunnossa perustellaan internetin kontrollointia muun

muassa tietomurtojen, petosten, piratismin ja misinformaation eli virheellisen tiedon ehkäisyllä sekä yritysten vapaan kilpailun edistämisellä. Lausunnossa ei mainita internetin sensuuritoimia, joita Kiinalla on erittäin kattavasti käytössä.

Myös Venäjä on perustellut internetinsä rajoittamista kansallisella turvallisuudella ja itsemääräämisoikeudella. Venäjän vuonna 2019 käyttöön ottama asiaa koskeva lakihanke on ulkomailla saanut nimityksen ”Suvereeni internet -laki”. Lakikokonaisuuden yhtenä tarkoituksena on virallisten linjausten mukaan suojella Venäjää ulkoisilta uhkilta. Keinoina tavoitteiden saavuttamiseen Venäjällä on ennen kaikkea valvonta ja kontrolli: Valtio haluaa olla keskeinen internetiä valvova ja hallinnoiva elin, ja Venäjä haluaa edistää myös kansainvälisesti mallia, jossa valtiot ovat internetin tärkeimpiä hallinnoijia ja sääntöjen asettajia (Epifanova, 2020).

Venäjän pyrkimykset internetin suhteen ovat linjassa presidentti Vladimir Putinin hallinnon yleisen pyrkimyksen kanssa, jossa valtaa yhteiskunnan eri osa-alueilla talous mukaan lukien keskitetään valtiolle ja erityisesti presidentille. Turvallisuuspalvelutaustaisen Putinin ajattelussa myös valtion turvallisuuden ja turvallisuusviranomaisten roolin korostaminen on ollut erittäin keskeistä (Gessen, 2012, Luku 4).

Lukuisat muutkin maat ovat perustelleet internetin rajoituksia kansallisella turvallisuudella, yleisen järjestyksen ylläpitämisellä ja misinformaation levittämisen estämisellä. Lisäksi eräät maat ovat perustelleet rajoituksia esimerkiksi oppilaitosten koevilpin estämisellä ja vihapuheen ehkäisemisellä. Tällaiset rajoitukset voivat olla lyhytaikaisia ja alueellisesti rajattuja esimerkiksi yhteen maakuntaan, kaupunginosaan tai kylään. Niissä voidaan toisinaan sulkea pääsy internetiin kokonaan, tai internetiä saatetaan hidastaa lähes käyttökelvottomaksi esimerkiksi poistamalla käytöstä mobiiliverkon 4G- ja 3G-ominaisuudet. (Access Now, 2021.)

3.5.2 Todelliset syyt

Vaikka valtiot julkisuudessa perustelevat internetin rajoituksia turvallisuudella ja itsenäisyydellä, rajoituksilla näyttäisi olevan myös muita syitä, jotka liittyvät lähinnä autoritaaristen valtioiden kontrollipyrkimyksiin. Usein ensisijaisena tavoitteena on estää

väestöltä tiedonsaantia sekä tietojen ja mielipiteiden ilmaisemista. Tilapäisiä rajoituksia otetaan usein käyttöön mielenosoitusten tai vaalien yhteydessä (Access Now, 2021).

Valtiot pyrkivät kontrolloimaan ja sensuroimaan internetiä samoista syistä kuin ne kontrolloivat esimerkiksi tiedotusvälineiden toimintaa: ne haluavat hallita informaatiotilaa. Tällaista kontrollia tehdään lähinnä autoritaarisissa maissa. Samat valtiot, jotka ovat jo pitkään kontrolloineet esimerkiksi lehdistöä, televisiota ja radiota, haluavat nyt kontrolloida internetiä, koska monille ihmisille internet ja sen eri palvelut ovat korvanneet tiedonlähteinä perinteiset joukkoviestimet. Kris Ruijgrokin (2017, s. 509) mukaan internetin käytön lisääntyminen lisää mielenilmausten määrää merkittävästi etenkin autoritaarisesti hallituissa maissa merkittävästi, koska internet parantaa kansalaisten mahdollisuuksia saada tietoa. Vaikka internetin käyttö lisää mielenilmauksia, se ei kuitenkaan välttämättä johda demokratisoitumiseen (Ruijgrok, 2017, s. 514).

Tiedon kontrollointi on etenkin autoritaarisille hallinnoille äärimmäisen tärkeää, koska hallitsemalla tietoa voi hallita ihmisiä. Tieto ja tiedonvälitys ovat kautta historian olleet aivan perustavanlaatuisia vallan lähteitä. Se, miten ihmiset ajattelevat ja myös mitä he tietävät tai eivät tiedä, määrittää niitä normeja ja arvoja, joille yhteiskunnat rakentuvat. Ihmisiä on mahdollista hallita myös esimerkiksi pakottamalla tai uhkailemalla, mutta ne eivät ole tehokkaimpia ja kestävimpiä tapoja hallita. Jos enemmistö ihmisistä on sisäistänyt arvot ja normit, jotka ovat vastoin hallinnon virallisia ja institutionalisoituja normeja, hallinnon järjestelmällä on taipumus ennemmin tai myöhemmin muuttua. Siksi kaikkein tehokkain, pitkäkestoisin ja usein myös taloudellisin tapa hallita ihmisiä on pyrkiä vaikuttamaan ihmisten mieleen ja mielipiteisiin eli siihen tietoon, jonka pohjalta ihmiset muodostavat mielipiteitä, asenteita, arvoja ja normeja. (Castells, 2007, s. 238–239.)

Tunnettu ranskalainen filosofi ja aatehistorioitsija Michel Foucault on kuvannut keskustelun hallitsemisen suurta merkitystä vallanpitäjille diskurssin käsitteen avulla. Diskurssi tarkoittaa tässä yhteydessä puhetapaa, jolla tuotetaan sosiaalista todellisuutta. Foucault'n mukaan diskurssi ei ole ainoastaan vallan tai hallintajärjestelmien välittäjä, vaan diskurssi on peräti yhtä kuin valta (Foucault, 1981, s. 52–53).

3.6 Sensuurilla on yhteys demokratian puutteeseen

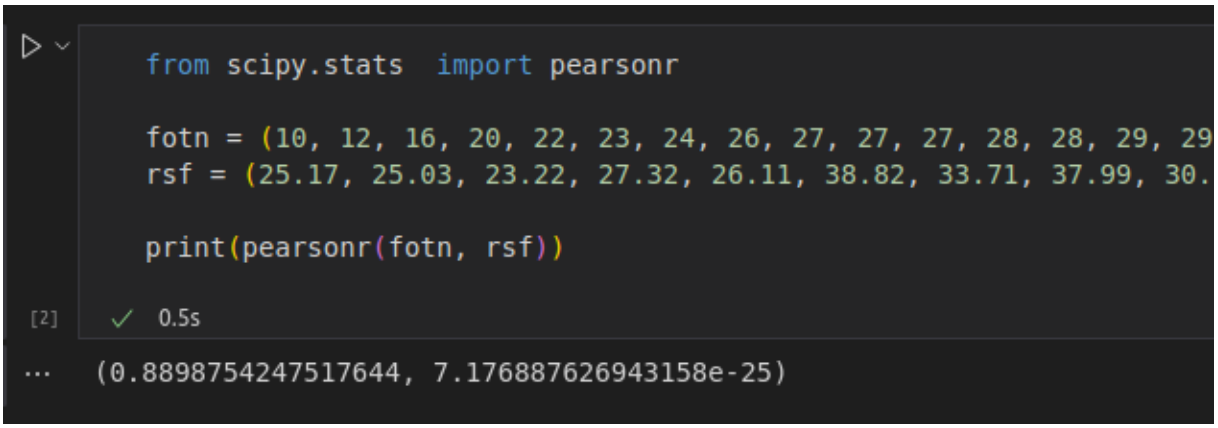
Internetin rajoittamisella on erittäin vahva yhteys muuhun sananvapauden rajoittamiseen. Internetiä rajoittavat maat ovat pitkälti samoja maita, jotka rajoittavat sananvapautta muutenkin. Se voidaan todentaa esimerkiksi vertaamalla toisiinsa Toimittajat ilman rajoja -järjestön koostamaa, lehdistönvapautta kuvaavaa Press Freedom Index -indeksiä (RSF, 2022b) ja Freedom Housen määrittelemää internetin vapautta kuvaavaa Freedom on the Net -indeksiä (Freedom House, 2022i).

Vuoden 2022 Press Freedom Indexissä on mukana 180 maata tai aluetta, joille on laskettu lehdistönvapautta kuvaava indeksi. Indeksin laskenta perustuu asiantuntijoille suunnatulla kyselylomakkeella hankittuun laadulliseen arvioon lehdistönvapaustilanteesta kussakin maassa sekä tietoon siitä, paljonko maissa on dokumentoitu journalistien vainoamistapauksia (RSF, 2022a). Freedom on the Net -indeksissä puolestaan on mukana 70 maata, joissa Freedom Housen mukaan elää 89 prosenttia maailman internet-käyttäjistä. Indeksi lasketaan asiantuntijoille suunnatusta kyselyaineistosta (Freedom House, 2022b). Indeksiä laadittaessa on mitattu kolmea asiakokonaisuutta: pääsyn esteitä (obstacles to access), sisältörajoituksia (limits on content) ja käyttäjien oikeuksien loukkauksia (violations of user rights). Näistä kahden ensimmäisen voidaan ajatella kuvaavan internet-sensuuria. Varsinaiset tekniset pääsyn estot kuuluvat luokkaan sisältörajoitukset.

Kumpikin indeksi saa arvoja välillä 0–100, jossa sata kuvaa parasta mahdollista vapautta ja nolla huonointa mahdollista. Indeksejä voidaan pitää välimatka-asteikollisina muuttujina, joten niiden välille voidaan laskea Pearsonin korrelaatiokerroin. Lasketaan korrelaatio Pythonin scipy.stats-modulin pearsonr-funktiolla siten, että funktiolle syötetään kaksi tuplea, joiden arvoina ovat vuoden 2022 indeksien arvot niistä 70 maasta, joille on saatavissa Freedom on the Net -indeksi. Press Freedom Index on saatavilla yli kaksinkertaisesta määrästä maita, mutta mukaan on turha ottaa sellaisia maita, joille ei ole vertailukohtaa Freedom on the Net -indeksissä. Laskennan tulokseksi saadaan erittäin voimakas positiivinen

korrelaatio (0,89), eli lehdistönvapauden ja internetin vapauden välillä on erittäin selkeä riippuvuus (Kuva 2).

Kuva 2: Verkon vapauden ja median vapauden korrelaation laskeminen



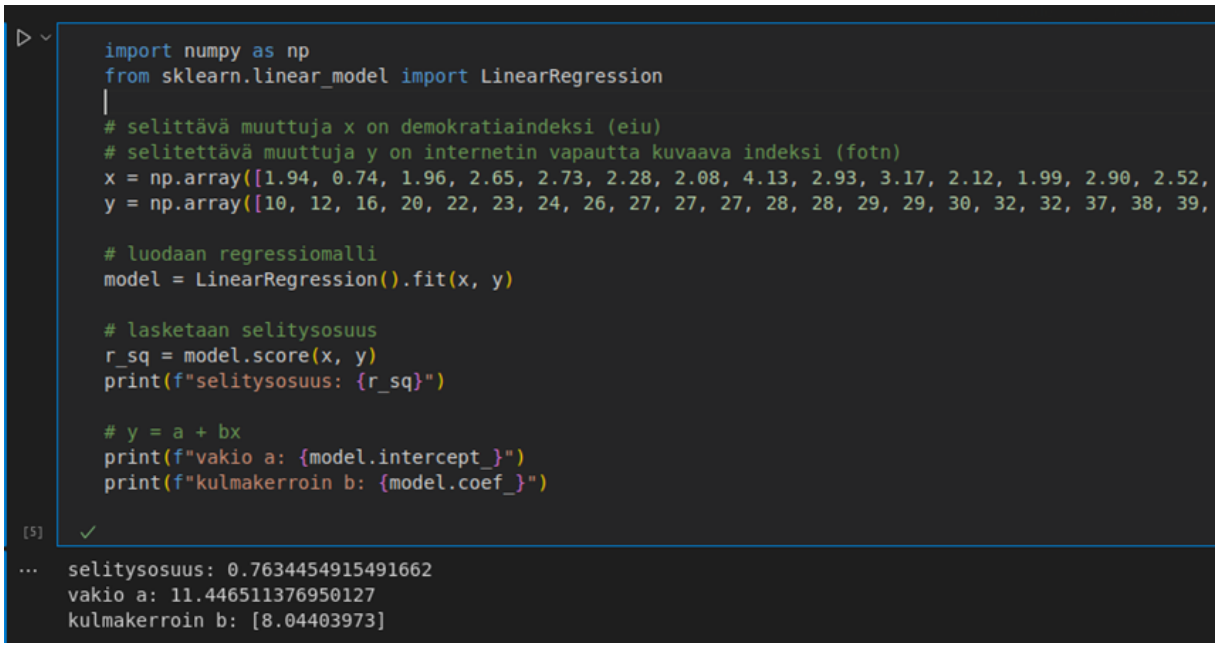
Korrelaatio on näin vahva mahdollisesti ainakin osittain siitä syystä, että kumpikin muuttuja mittaa periaatteessa samaa asiaa. Ne voidaan molemmat nähdä yhteiskunnan demokratian tason operationalisointeina. Freedom on the Net -indeksissä on huomioitu se, että tiettyjä haitallisia sisältöjä voidaan demokraattisissakin maissa rajoittaa internetistä hyväksyttävästä syystä, jolloin rajoittaminen ei riko esimerkiksi kansainvälisiä ihmisoikeusnormeja (Freedom House, 2022b).

Sensuurin ja demokratian suhdetta voidaan tutkia vielä lisää tarkastelemalla Freedom on the Net -indeksin ja jonkin demokratiaa kuvaavan indeksin yhteisvaihtelua. Valitaan demokratiaa kuvaamaan Economist Intelligence Unitin uusin, vuoden 2022 tilannetta kuvaava Democracy Index (EIU, 2023). Indeksi kuvaa demokratian tilaa 165 maassa tai alueella. Indeksi on laadittu viittä eri demokratian aspektia kuvaavien indikaattorien pohjalta. Indikaattorit kuvaavat vaalijärjestelmää ja pluralismia, hallinnon toimintaa, poliittista osallistumista, poliittista kulttuuria ja kansalaisvapauksia. Kutakin näistä on mitattu useilla eri mittareilla. Indeksi saa arvoja väliltä 0–10 siten, että jos maa saa indeksin arvoksi yli kahdeksan, sitä pidetään demokratiana. Alle neljän indeksi tarkoittaa autoritaarista maata.

Maan demokraattisuuden vaikutusta internet-sensuuriin voidaan tarkastella tekemällä yksinkertainen lineaarinen regressioanalyysi, jossa selittävänä muuttujana on Economist Intelligence Unitin Democracy Index ja selitettävänä eli muuttujana Freedom Housen

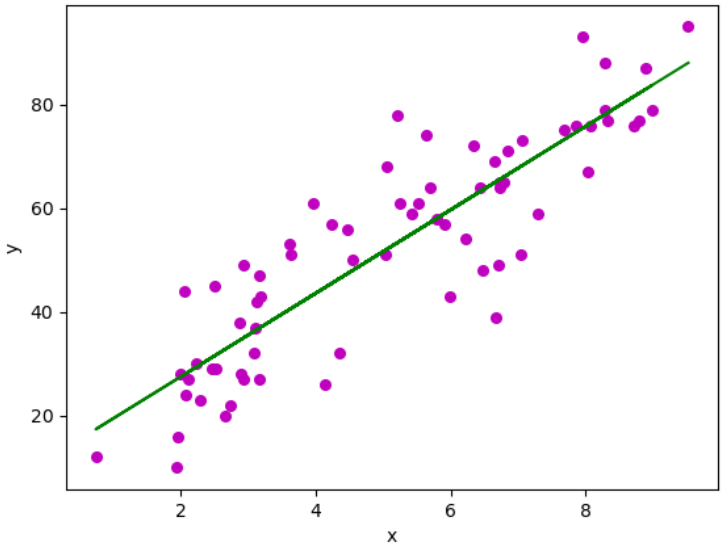
Freedom on the Net -indeksi. Indeksejä voi pitää vähintään välimatka-asteikollisina muuttujina, joten ne soveltuvat regressioanalyysiin. Mukaan valitaan ne 70 maata, joille on saatavissa Freedom on the Net -indeksi. Tuloksena saadaan regressiosuoran ominaisuudet (Kuva 3).

Kuva 3: Regressiomallin Python-koodi ja regressiosuoran ominaisuudet



Jakaumien hajontakuviosta (Kuva 4) näkyy, että internetin vapaus (muuttuja y) korreloi positiivisesti demokratian määrän (muuttuja x) kanssa. Regressiomallin selitysosuus on noin 76 prosenttia, eli valtaosa internetin vapaudesta kussakin maassa selittyy demokratian määrällä. On hyvä muistaa, että tässä internetin vapauden käsite sisältää muutakin kuin sensuurin tai sen puutteen (ks. kohta 2.6). Freedom on the Net -indeksi koostuu kuitenkin pääosin pääsyn estoista ja sisältöjen rajoittamisesta, jotka voidaan luokitella sensuuriksi (Freedom House, 2022b).

Kuva 4: Hajontakuvio demokratian ja internetin vapauden suhteesta



Pikaisen regressioanalyysin perusteella siis internetin vapaus jossakin maassa riippuu siitä, kuinka demokraattinen maa on. Mitä demokraattisempi järjestelmä, sitä vapaampi on internet, eli sitä vähemmän on internetin käytön rajoituksia, kuten sensuuria.

3.7 Sananvapauden merkitys

Aiemmin mainittu vallanpitäjien tarve kontrolloida informaatiotilaa koskee siis käytännössä vain autoritaarisia, ei-demokraattisia maita. Avoimissa demokratioissa ei ole tarvetta samalla tavoin kontrolloida tietoa. Demokratiassa pidetään vapaata tiedonvälitystä jopa edellytyksenä koko yhteiskuntajärjestelmän eli avoimen demokratian olemassaololle, joten voimakas sensuuri voisi rapauttaa koko järjestelmän perustaa. Kun demokratiassa ihmiset valitsevat omat vallanpitäjänsä, ihmisillä on oltava vapaasti saatavilla neutraalia ja avointa tietoa yhteiskunnasta ja vallanpitäjien toiminnasta yhteiskunnassa. (esim. United Nations ym., 2023)

Internetissä olevan tiedon, sosiaalisten medioiden tai viestipalveluiden käytön rajoittamisessa on kyse sananvapauden rajoittamisesta. Sananvapaudelle on eri aikoina ja eri yhteyksissä esitetty erilaisia määritelmiä. Suomalaisessa ja eurooppalaisessa kontekstissa ehkäpä relevantein sananvapauden määritelmä on Euroopan ihmisoikeussopimuksen 10 artiklassa (Euroopan ihmisoikeussopimus, 1984). Sopimuksen ovat hyväksyneet Euroopan neuvoston jäsenmaat Suomi mukaan lukien. Käytännössä se on näissä maissa – myös

Suomessa – voimassa olevaa lainsäädäntöä, jonka soveltamisesta päättää viime kädessä Euroopan ihmisoikeustuomioistuin.

Sananvapaus on myös Suomen perustuslaissa määritelty perusoikeus. Perustuslain (731/1999) mukaan sananvapauteen sisältyy oikeus ilmaista, julkistaa ja vastaanottaa tietoja, mielipiteitä ja muita viestejä kenenkään ennakolta estämättä. Määritelmä on lähellä Euroopan ihmisoikeussopimuksen määritelmää, mutta perustuslain sanamuodossa korostuu ennakkosensuurin kielto. Sananvapautta voidaan siis rajoittaa jälkeenpäin, esimerkiksi rankaisemalla kunnianloukkauksista tai salassapitorikoksista.

Myös Euroopan ihmisoikeussopimuksessa todetaan, ettei kaikki sananvapauden rajoittaminen ole kiellettyä. Sananvapauden käyttöön liittyy sopimustekstin mukaan myös velvollisuuksia ja vastuuta, joten sananvapaudelle voidaan asettaa rajoituksia, kunhan ne ovat ”välttämättömiä demokraattisessa yhteiskunnassa” esimerkiksi kansallisen turvallisuuden, yleisen turvallisuuden, maineen, terveyden tai moraalin suojelemiseksi. Sekä Suomen perustuslain että Euroopan ihmisoikeussopimuksen mukaan rajoitusten on myös perustuttava lakiin, eli niitä voi ottaa käyttöön vain lainsäädännöllä, mikä demokraattisissa maissa tarkoittaa myös, että ne pitää perustella.

Myös internet-sensuurin kohdalla voidaan tiettyjä rajoituksia pitää perusteltuina ja sallittuina. Monissa Euroopan maissa Suomi mukaan lukien on esimerkiksi rajoitettu pääsyä internetin lapsipornoaineistoihin ja eräisiin tekijänoikeuksia loukkaaviin aineistoihin (TTVK, 2012). Venäjän aloitettua laittoman hyökkäyssodan Ukrainassa helmikuussa 2022 Euroopan unioni kielsi pääsyn Venäjän sotapropagandaa levittäviin Sputnik- ja RT-yhtiöiden jakelemiin sisältöihin (Euroopan unionin neuvosto, 2022). EU:n neuvosto perusteli päätöstä muun muassa unionin ja sen jäsenvaltioiden turvallisuudella sekä sillä, että Venäjän hyökkäyssota rikkoo kansainvälistä oikeutta.

4 Kuinka internet toimii

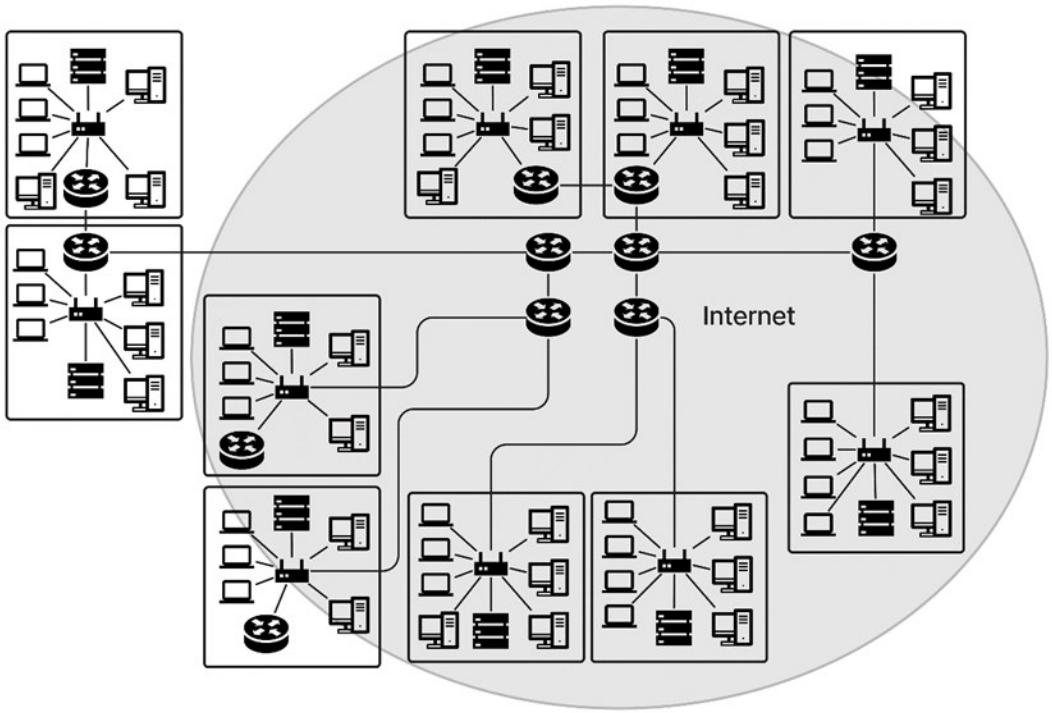
Jotta internet-liikenteen estomenetelmiä olisi mahdollista ymmärtää, on selvitettävä, miten internet toimii. Tässä luvussa käydään läpi muutamia peruskäsitteitä tasolla, joka on melko pintapuolinen, mutta antaa pohjatietoa, jota tarvitaan, ennen kuin mennään internet-sensuurin teknisiin menetelmiin.

4.1 Verkkojen verkko

Internet eräänlainen verkkojen verkko (Kuva 5). Se on maailmanlaajuinen joukko verkkoja, jotka ovat yhteydessä toisiinsa erilaisten verkkolaitteiden kuten reitittimien ja kytkimien sekä kaapelien välityksellä. Tätä verkkojen muodostamaa verkkoa ei kukaan omista tai hallinnoi kokonaisuudessaan. Verkon osaverkkoja omistavat ja hallinnoivat esimerkiksi yritykset, järjestöt, valtiolliset virastot ja muut tahot. Osa niistä toimii samaan aikaan eri maissa, ja niillä voi olla useissa eri maissa myös verkkoon kuuluvia fyysisiä laitteita, kuten palvelimia tai reitittimiä. (Nye, 2016.)

Verkkojen välillä siirtyy tietoa tavoilla, jotka perustuvat yhteisiin, sovittuihin tekniikoihin ja standardeihin. Näitä sovittuja liikenteen hoitamisen tapoja sanotaan protokolliksi. Verkot liittyvät toisiinsa reitittimien avulla. Kunkin verkon sisällä laitteet liitetään verkkoon kytkimillä. Verkkojen topologia eli se, missä järjestyksessä ja kuinka paljon erilaisia kytkimiä, reitittimiä ja muita laitteita on verkkoon kytketty, voi vaihdella. (Cisco Press, 2013, Luku 1.3.1, 1.3.3.)

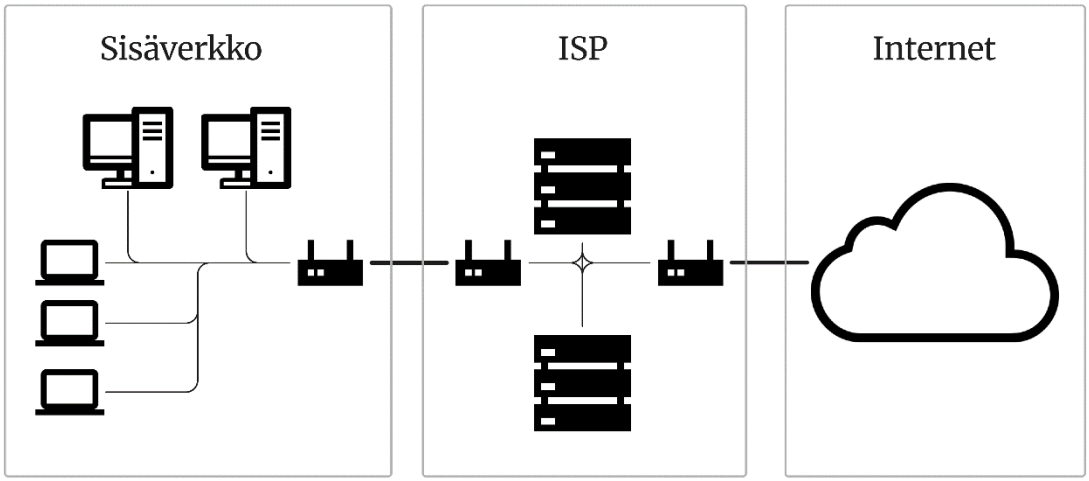
Kuva 5: Internet on verkko, joka koostuu verkoista (Cisco Press, 2013, Luku 1.3.3)



Internet voidaan ajatella myös järjestelmäksi, johon on kytkeytynyt palveluntarjoajia (ISP, Internet Service Provider) tai vastaavia organisaatioita. Palveluntarjoaja on periaatteessa mikä tahansa taho, joka myy tai antaa yhteyden internetiin ja siirtelee dataa joko omassa verkossaan tai verkkojen välillä. Palveluntarjoaja voi olla esimerkiksi julkishallinnon virasto, yritys tai oppilaitos. (Kabelová & Dostálek, 2006, Luku 6.2.2.)

Yleensä loppukäyttäjät liittyvät internetiin palveluntarjoajan eli ISP:n välityksellä (Kuva 6). Yhteys loppukäyttäjän ja palveluntarjoajan välillä voidaan järjestää useilla vaihtoehtoisilla tekniikoilla, kuten valokaapelilla, puhelin- tai kaapelitelevisioverkon kautta, matkapuhelinverkossa tai satelliitin kautta. (Cisco Press, 2013, kpl. 1.3.4.)

Kuva 6: Yhteys internetiin palveluntarjoajan eli ISP:n kautta



Internetin eräänlaisen ytimen muodostaa niin sanottu runkoverkko (backbone). Se muodostuu kaikkein laajimmista ja nopeimmista verkoista, jotka on kytketty toisiinsa nopeiden valokaapelien välityksellä ja tehokkailla reitittimillä. Myös runkoverkko on internetin tapaan hajautettu järjestelmä, jota hallinnoivat erilaiset tahot. Näitä verkkoja omistavat ja ylläpitävät lähinnä suuret yhtiöt, oppilaitokset, asevoimien yksiköt ja muut merkittävät organisaatiot. Yhdessä tällaiset verkot muodostavat perustan palveluntarjoajien toiminnalle. (Arelion, ei pvm.; Burke, 2023.)

Suurilla yrityksillä, oppilaitoksilla tai muilla organisaatioilla on usein omia WAN- ja LAN-verkkojaan. LAN (local area network) on yleensä verkko, joka yhdistää melko nopeilla yhteyksillä laitteita, jotka ovat fyysisesti verrattain lähellä toisiaan, esimerkiksi samassa rakennuksessa. WAN (wide area network) puolestaan yhdistää LAN-verkkoja. Samassa WAN-verkossa olevat verkot voivat sijaita maantieteellisesti hyvinkin kaukana toisistaan, jopa eri maissa. (Scarpati, 2023.)

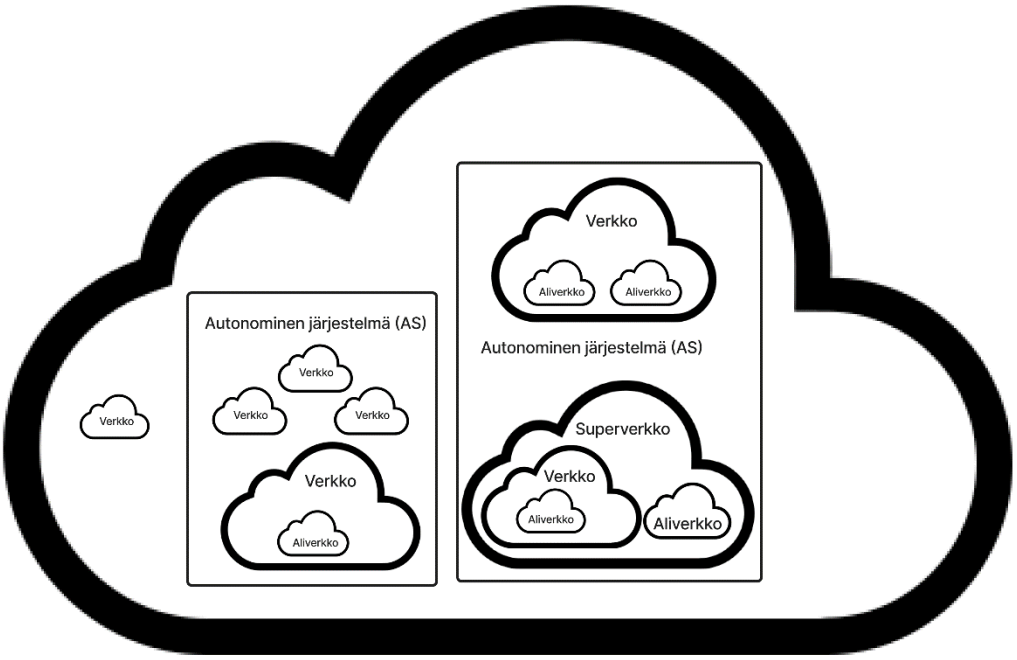
4.2 Autonomiset järjestelmät

Dataliikenteen reitityksen ja IP-osoitteiston näkökulmasta internet ei jakaudu palveluntarjoajiin, vaan autonomisiin järjestelmiin (AS, Autonomous System). Kun sanotaan, että internet on verkoista koostuva verkko, jokainen verkko on autonominen järjestelmä.

Autonomiset järjestelmät ovat itsenäisiä hallinnollisia kokonaisuuksia, joita voi hallinnoida esimerkiksi internet-palveluntarjoaja, suuri yritys, oppilaitos, yrityksen osa tai ryhmä yrityksiä. Kun internet on verkoista koostuva verkko, autonominen järjestelmä on joukko keskenään tietoja vaihtavista reitittimistä ja muista laitteista koostuvia verkkoja, joita ylläpidetään keskitetysti ja joille ylläpitäjä on asettanut tietyn IP-osoiteavaruuden. Autonominen järjestelmä on siis periaatteessa joukko reitittimiä, joita hallinnoi sama taho. (Krzyzanowski, 2016; Salamatian ym., 2021.)

Jokaisella verkkoon kytketyllä tietokoneella on IP-osoite. Autonominen järjestelmä on ryhmä toisiinsa liitettyjä IP-osoiteryhmiä, jotka on annettu järjestelmää hallinnoivalle organisaatiolle. Eri IP-osoiteavaruuksissa toimivia verkkoja voidaan koota yhtenäisiksi kokonaisuuksiksi, niin sanotuiksi superverkoiksi (Kuva 7). (Kabelová & Dostálek, 2006, Luku 6.2.2; Krzyzanowski, 2016.)

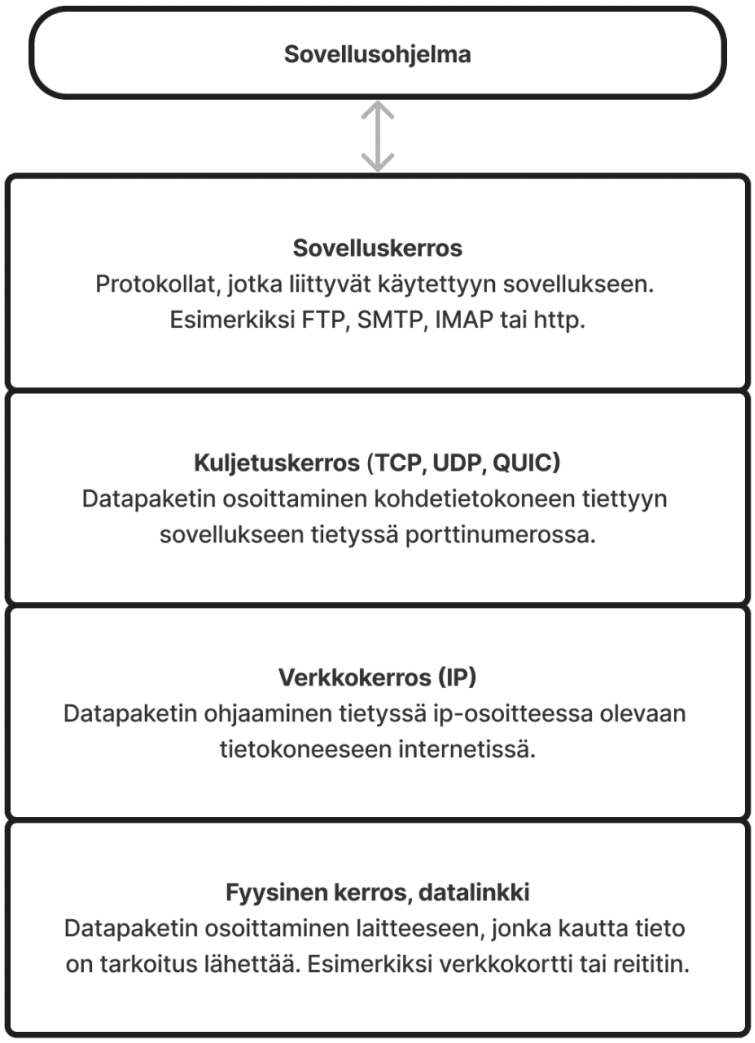
Kuva 7: Autonomiset järjestelmät ja superverkko (Kabelová & Dostálek, 2006)



4.3 TCP/IP-protokollaperhe

Tietoverkoissa liikenne on jaettu useisiin erilaisiin ja eri tasoilla toimiviin protokolliin. Yleensä puhutaan virtuaalisista tietojenvaihdon kerroksista. Sensuuritoimia voidaan kohdistaa periaatteessa mihin tahansa kerrokseen tai protokollaan, sillä toimiakseen internet-yhteys yleensä tarvitsee kaikki kerrokset. Valtaosa liikenteestä käyttää standardoitua TCP/IP-nimistä protokollaperhettä, joka on alun perin kehitetty jo 1970-luvulla. Protokollaperheestä voidaan käyttää myös nimitystä protokollapino, sillä eri protokollat toimivat päällekkäin siten, että ylemmän tason protokolla hyödyntää alemman tason protokollaa. Liikenne kahden internetiin liitetyn tietokoneen välillä voidaan ajatella eräänlaiseksi pinoksi, jossa jokaisella kerroksella on oma tehtävänsä tiedonsiirrossa (Kuva 8). Jokaista pinon kerrosta tarvitaan, jotta tieto liikkuisi. (Kabelová & Dostálek, 2006, Luku 1.2.1-1.2.2; Niemi, 2012.)

Kuva 8: TCP/IP-protokollapino (Kabelová & Dostálek, 2006; Schuler, 2002)



TCP/IP:ssä TCP on lyhenne sanoista Transmission Control Protocol ja IP sanoista Internet Protocol. Näistä IP on internetin perusprotokolla, jonka päällä toimivat kaikki muut protokollat. TCP-protokolla on niin sanottu siirtokerroksen protokolla, joka pääasiassa hoitelee liikennettä keskenään yhteydessä olevissa kahdessa tietokoneessa pyörivien sovellusohjelmien välillä. Liikenne voidaan TCP:n sijasta hoitaa myös UDP-protokollalla, joka toimii teknisesti hieman eri tavalla. Myös UDP kuuluu TCP/IP-protokollaperheeseen, vaikka sitä ei protokollaperheen nimessä mainita. TCP ja UDP eroavat toisistaan yhteystavaltaan. TCP on yhteyspohjainen (englanniksi connection-oriented) palvelu, jossa lähettäjän ja kohdepalvelimen välille on luotava yhteys, jotta tietoliikenne toimii. Siinä kohdepalvelin kuittaa datan vastaanotetuksi tai vaatii uudelleen lähetystä, jos data ei ole tullut perille. UDP sen sijaan on yhteydetön (connectionless), eli datan lähettämiseksi ei tarvitse ensin luoda yhteyttä, vaan protokollalle on periaatteessa yhdentekevää, mitä datalle tapahtuu, kun se on lähetetty. UDP-protokollaa ei kiinnosta, kuitataanko data vastaanotetuksi. (Kabelová & Dostálek, 2006, Luku 1.2.2; Niemi, 2012; Zoltan, 2023.)

TCP ja UDP siirtelevät tietoa porttinumeroiden perusteella. Tietoliikenteessä portti on numeroitu, virtuaalinen viestintäkanava, joka ei ole fyysinen laite, vaan eräänlainen IP-osoitteen laajennus. Eri protokollat käyttävät eri portteja. Porttinumerot 1–1024 on varattu tiettyihin tarkoituksiin, esimerkiksi porttia 80 käytetään www-liikenteeseen. Yleisesti käytetyn vertauksen mukaan koneen IP-osoite on kuin talon katuosoite, ja porttinumero on kuin asunnon numero talossa. (Kabelová & Dostálek, 2006, Luku 1.2.2; Niemi, 2012; Zoltan, 2023.)

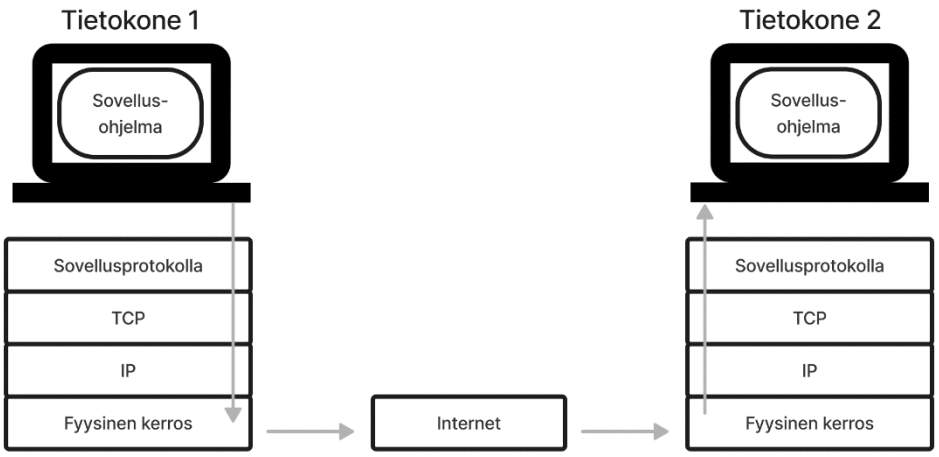
Siirtokerroksen yläpuolella on niin sanottu sovelluskerros, jossa toimivat kunkin sovelluksen tarvitsemat protokollat. Sovelluskerroksen protokollia ovat esimerkiksi Telnet, FTP, SMTP, IMAP ja HTTP. Siirtokerroksen alapuolella puolestaan on niin sanottu verkkokerros, jossa IP-protokollan avulla siirrellään tietoa tietokoneiden välillä IP-osoitteesta toiseen. Verkkokerroksen alapuolella on vielä fyysinen kerros, joka aktivoi verkkolaitteet. (Kabelová & Dostálek, 2006, kpl. 1.1 –1.2.)

Viime vuosina on alkanut verkkoselainten käyttämässä http-liikenteessä yleistyä myös UDP:hen perustuva, Googlen kehittämä protokolla nimeltä QUIC. Sen nimi tulee sanoista Quick UDP Internet Connections. Kyseessä on siirtokerroksen protokolla, jota käytetään

sovelluskerrokseen kuuluvan HTTP/3-protokollan kanssa. QUIC-protokollassa on salaus valmiina, jolloin erillistä salausprotokollaa ei tarvita. Sen on yhdessä HTTP/3:n kanssa tarkoitus korvata protokollien TCP, TLS ja HTTP/2 yhdistelmä. (Chromium.org, ei pvm.)

Protokollapino voidaan ajatella niin, että tieto kulkee sovellusohjelmasta pinon läpi internetin kautta toiselle tietokoneelle, jossa se kulkee samanlaisen pinon läpi toiseen suuntaan (Kuva 9) (Schuler, 2002).

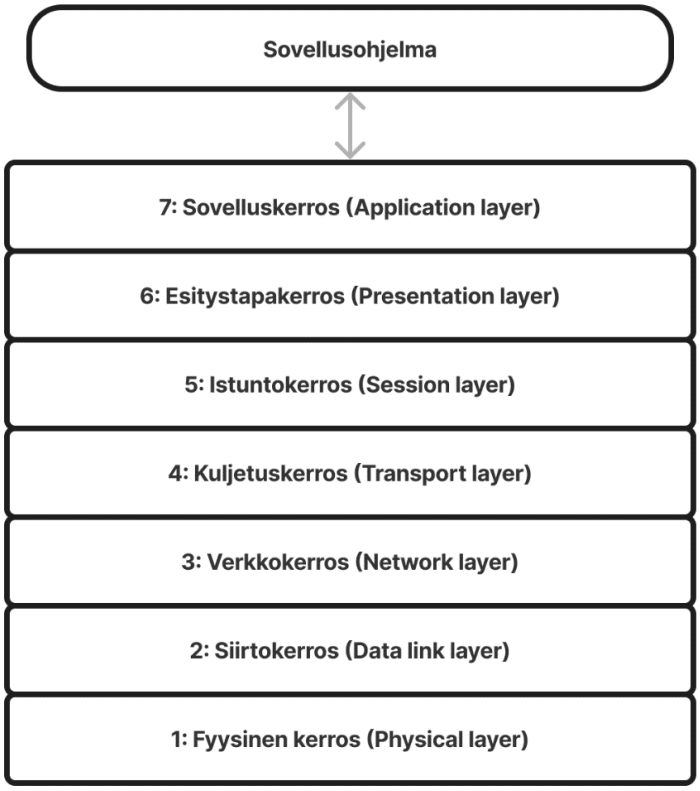
Kuva 9: Protokollapinojen rooli tietokoneiden välisessä yhteydessä (Schuler, 2002)



4.4 OSI-malli

TCP/IP-mallin ohella internet-liikennettä voidaan kuvata myös ISO-standardointijärjestön standardoimalla OSI-mallilla (Open Systems Interconnection) (Kuva 10). Siinä liikennettä kuvataan seitsenportaisella protokollapinolla, jossa kerrokset likimain vastaavat TCP/IP-protokollapinon kerroksia, mutta on jaoteltu useampaan osaan. OSI-mallissa fyysinen kerros ja siirtokerros vastaavat TCP/IP-mallin fyysistä kerrosta. Verkko- ja siirtokerros vastaavat kummassakin mallissa toisiaan. OSI-mallin istunto-, esitys- ja sovelluskerros puolestaan vastaavat TCP/IP-mallin sovelluskerrosta (Kabelová & Dostálek, 2006).

Kuva 10: OSI-malli (Kabelová & Dostálek, 2006)



4.5 BGP-protokolla

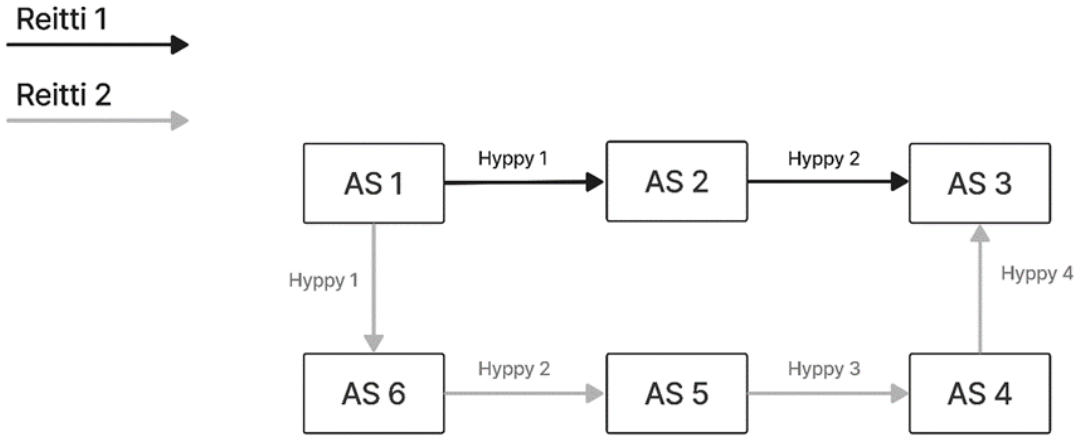
Autonomisen järjestelmän sisäisessä kommunikaatiossa reitittimet käyttävät protokollia, jotka ovat niin sanottuja IGP-protokollia (Interior Gateway Protocol). Niitä on useita erilaisia. Sen sijaan autonomisten järjestelmien välisessä kommunikaatiossa käytetään EGP-protokollaa (Exterior Gateway Protocol). Tähän tarkoitukseen käytössä on yksi standardiprotokolla, nimeltään BGP (Border Gateway Protocol). Nykyisin käytössä on BGP:n versio 4. (Krzyzanowski, 2016.)

BGP on reititysprotokolla, jonka ansiosta internet ylipäätään toimii (Pepelnjak, 2019). Se vastaa internetin maailmanlaajuisesta reitityksestä, kun tieto liikkuu eri verkkojen eli autonomisten järjestelmien kautta lopulliseen kohteeseensa. BGP perustuu TCP/IP-malliin, ja se toimii OSI-järjestelmän verkko- ja kuljetuskerroksissa (kerrokset 3 ja 4) (Burke, 2023).

BGP:n tehtävänä on reitittää datapaketit sopivinta mahdollista reittiä pitkin eri IP-osoitteiden välillä. Esimerkiksi lyhin reitti autonomisesta järjestelmästä 1 autonomiseen

järjestelmään 3 on reitti 1, koska siinä on vain kaksi autonomisten järjestelmien välistä hyppyä (Kuva 11). Todellisuudessa internet koostuu kymmenistä tuhansista autonomisista järjestelmistä. (Cloudflare, ei pvm.-b)

Kuva 11: BGP-reititys autonomisten järjestelmien välillä (Cloudflare, ei pvm.-b)



Jotta liikenne päätyisi autonomisten järjestelmien kautta oikeaan paikkaan, autonomisten järjestelmien välistä liikennettä ohjaavien reitittimien pitää tietää, mitä kautta liikenne tulee ohjata. Ajatellaan esimerkiksi tilanne, jossa kaksi autonomista järjestelmää, AS x ja AS y on kytketty reitittimillä toisiinsa. AS x tietää reitin johonkin verkkoon nimeltä Verkko 1, jolla on käytössään jokin IP-osoiteavaruus. AS y puolestaan tietää reitin toiseen verkkoon nimeltä Verkko 2. Jotta tietoliikenne voisi kulkea Verkko 1:stä Verkko 2:een, sen tulisi kulkea AS x:n ja AS y:n kautta. Tällöin AS x:n pitää tiedottaa AS y:lle, että se tietää reitin Verkko 1:een. AS y:n puolestaan pitää kertoa AS x:lle, että se tietää reitin Verkko 2:een. Tähän tiedottamiseen käytetään BGP-protokollaa. Saatuaan tiedon reitistä, AS x ja AS y voivat päättää, käyttävätkö ne tätä tietoa vai jättävätkö käyttämättä, jos niillä on esimerkiksi tieto paremmasta reitistä. (Krzyzanowski, 2016.)

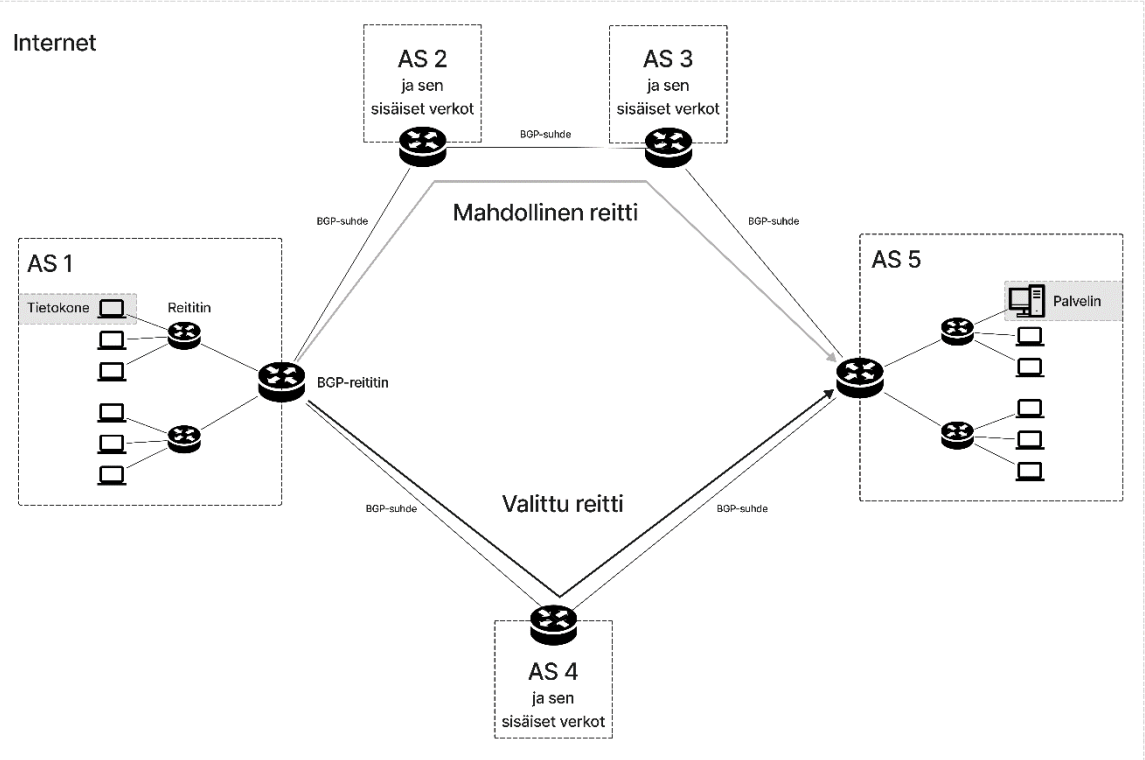
Autonomisten järjestelmien BGP-protokollaa käyttävät reitittimet jakavat keskenään säännöllisesti tietoa siitä, mitä IP-osoitteita ne kattavat ja mitä reittiä pitkin pääsee mihinkin IP-osoitteisiin. Koska internet on jatkuvasti kasvava ja muuttuva verkkojen verkko, näitä tietoja on päivitettävä säännöllisesti, jotta ne pysyvät ajan tasalla. BGP mahdollistaa verkon vakauden, vaikka verkkoihin tulisi vikoja, sillä protokolla löytää nopeasti vaihtoehtoisen reitin, jos jokin reitti lakkaa toimimasta. (Burke, 2023; Cloudflare, ei pvm.-b.)

Paras reitti asiakaskoneelta jollekin palvelimelle jossakin IP-osoitteessa joidenkin autonomisten järjestelmien kautta ei kuitenkaan välttämättä ole lyhin reitti, ja joskus esimerkiksi paluuliikenne saattaa kulkea eri reittiä kuin ulos menevä liikenne. Nämä erikoisuudet johtuvat siitä, että BGP-protokolla huomioi internet-palveluntarjoajien keskenään tekemät niin sanotut peering-sopimukset (peering agreements), joissa määritellään liikenteen välittämisen ehdot ja edellytykset. BGP huomioi sopimuksissa määritellyt ehdot attribuutteina, jotka on liitetty kuhunkin kyseisen reitittimen tuntemaan IP-osoiteavaruuteen. Attribuutit otetaan huomioon tietyn, protokollaan kuuluvan algoritmin perusteella. (Pepelnjak, 2019.)

BGP-protokollan monimutkaisuuden takia internet-palveluntarjoajat eli autonomisten järjestelmien omistajat yleensä käyttävät pienintä mahdollista määrää BGP-reitittimiä. Näitä reitittimiä on vain siellä, missä niitä tarvitaan, eli esimerkiksi kohdissa, joista oma verkko eli autonominen järjestelmä on yhteydessä ulkoiseen verkkoon. Oman verkon sisäinen liikenne hoidetaan reitittimillä, jotka käyttävät IGP-protokollia. (Krzyzanowski, 2016; Pepelnjak, 2019.)

Internet voidaan siis ajatella rakennelmaksi, jonka runko koostuu autonomisista järjestelmistä, jotka on liitetty toisiinsa BGP-suhteilla eli peering-sopimuksilla (Limonier ym., 2021). Esimerkiksi tietoliikennereitti tietokoneelta palvelimelle valikoituu BGP-suhteiden ja BGP:n mukaan algoritmin perusteella (Kuva 12).

Kuva 12: Laajempi esitys BGP-protokollan toiminnasta (Limonier ym., 2021)



4.6 Paketinvaihtoverkosto

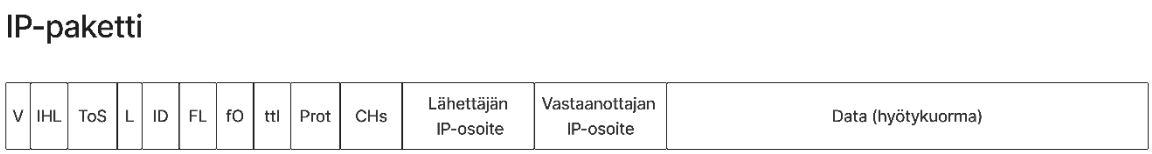
Internet voidaan ajatella myös paketinvaihtoverkostoksi, sillä internetissä tieto kulkee jaettuna osiin, joita sanotaan paketeiksi. Lähetettäessä data eli esimerkiksi teksti, valokuva tai muu tiedosto, pilkotaan datapaketeiksi, ja vastaanottavassa päässä paketit kootaan taas kokonaisuudeksi. Jakamalla tieto paketteihin mahdollisestaan se, ettei tiedonsiirtoväylää tarvitse varata pitkäksi aikaa vain yhdelle yhteydelle, jossa siirretään suuri määrä dataa. Saman datan eri paketit voivat kulkea määränpäähänsä myös eri reittejä, ja määränpäässä ne kootaan yhtenäiseksi datakokonaisuudeksi, joka voi olla esimerkiksi teksti, valokuva tai jokin muu tiedosto (Cloudflare, ei pvm.-a).

IP-paketti koostuu kahdesta osasta: otsikkotiedoista (header) ja hyötykuormasta (payload). Otsikkotiedot sisältävät tietoa paketista, esimerkiksi paketin lähettäneen tietokoneen ja kohdetietokoneen IP-osoitteet sekä tietoa paketin sisällöstä. Hyötykuorma on varsinainen tietosisältö eli data. Käytännössä yhdellä paketilla on yleensä useita otsikkotietokenttiä, koska verkon toimintaprosessin eri vaiheet käyttävät eri otsikkotietokenttiä. Otsikkotietojen

liittämisestä paketteihin vastaavat eri protokollat. Paketteja voidaan määritellä sen mukaan, mitä protokollaa ne käyttävät. Esimerkiksi pakettia, jossa on IP-protokollan asettamat otsikkotiedot, voidaan nimittää IP-paketiksi. (Cloudflare, ei pvm.-a)

IP-paketissa (Kuva 13) otsikkotieto-osa eli header sisältää lähettäjän ja vastaanottajan IP-osoitteiden lisäksi muun muassa tietoja käytettävästä protokollasta ja sen versiosta, paketin pituudesta, header-osan pituudesta, palvelun tyypistä, paketille määrätystä eliniästä (RFC 791, 1981).

Kuva 13: Kaavio IP-paketista (Bendrath & Mueller, 2011; RFC 791, 1981)



Vastaavanlaisia paketteja on myös muissa protokollissa. Esimerkiksi TCP-paketeissa on samankaltaisia tietoja, mutta niissä osoitetietoina ovat IP-osoitteiden sijasta porttien numerot. TCP-pakettien otsikkotiedot sisältävät yksittäisiä bittejä, jotka toimivat kytkiminä (flag). Esimerkiksi TCP:n reset -kytkimellä (TCP RST) voi määrätä yhteyden nollattavaksi. (RFC 793, 1981.)

5 Rajoitusten tekniset ratkaisut

Internetin sisältöjen ja palvelujen sensurointiin on käytettävissä lukuisia erilaisia tekniikoita. Kaikkein tehokkaimmin sensuuri toimii, jos käytetään niistä useita tai jopa kaikkia samanaikaisesti. Tässä luvussa esitellään yleisimmät käytössä olevat sensuroinnin tekniset menetelmät.

5.1 IP-osoitteiden ja porttien estot

Liikenne tietylle verkkosivustolle tai verkkopalveluun voidaan estää yksinkertaisesti estämällä liikenne IP-osoitteeseen, josta kyseinen sivusto tai palvelu on saatavissa. Tällaisia estoja varten useat valtiot, Suomi mukaan lukien, ovat laatineet kieltolistoja, joilla olevat

osoitteet määrätään estettäviksi (Opetus- ja kulttuuriministeriö, 2013; Terman, 2021b). Estäminen voidaan määrätä esimerkiksi palveluntarjoajana eli ISP:nä toimivan teleyrityksen tehtäväksi, kuten Suomessa tehtiin vuonna 2007 lapsipornosivustojen kohdalla (ks. kohta 3.4.1), tai valtio voi määrä ohjaamaan maan rajan ylittävän verkkoliikenteen viranomaisten hallinnoiman reitittimen kautta.

5.1.1 TCP-protokollan IP-estot

Yksinkertaisimmillaan IP-osoite voidaan estää hylkäämällä kaikki liikenne kyseiseen osoitteeseen eli pudottamalla kaikki datapaketit, jotka liikkuvat osoiteessa olevalle palvelimelle tai sieltä asiakaskoneelle. Tällainen varsin karkea esto on helppo ja halpa toteuttaa, sillä datapakettien pudottamismahdollisuus TCP-protokollan drop-komennolla kuuluu palomuurien ja reitittimien standarditoimintoihin (Clayton ym., 2006). Pakettien pudottaminen kuuluu palomuurien niin sanottuihin IDS (Intrusion Detection System) - ja IPS (Intrusion Prevention System) -toimintoihin, joita yleisesti käytetään esimerkiksi yrityksissä, kun pyritään estämään luvatonta tunkeutumista järjestelmiin (Juniper Networks, ei pvm.).

Hieman vähemmän karkea tapa estää liikenne IP-osoitteeseen on nollata yhteys TCP-protokollan reset-komennolla, joka saa päätelaitteen hylkäämään kyseisen yhteyden. Esimerkiksi Kiinassa yksi tapa estää internet-liikennettä ovat väärennetyt reset-komennot, joita Kiinan ja ulkomaailman välistä liikennettä välittävät reitittimet injektoivat verkkoliikenteen joukkoon. Pelkällä reset-menetelmällä toteutettu liikenteen esto on kuitenkin mahdollista ohittaa käyttämällä sekä lähettävässä että vastaanottavassa päässä ei-standardinmukaista laitteistoa, joka yksinkertaisesti jättää reset-komennon huomiotta. (Clayton et al., 2006.)

TCP reset -menetelmää käyttää esimerkiksi Kiinan palomuuri, joka teknisesti voidaan ajatella eräänlaiseksi suureksi IPS-järjestelmäksi. Kiinan palomuuri lisää liikenteeseen TCP reset -komennon sisältäviä paketteja, kun se huomaa jonkin kieltolistalla olevan avainsanan tai muita sellaisia liikenteen ominaisuuksia, joita Kiina ei hyväksy (Anderson, 2012, s. 3).

Liikenne voidaan estää koko IP-osoitteen sijasta myös tiettyyn porttiin tai joukkoon portteja. Esto voidaan määritellä toimimaan myös tietyn IP-osoite–portti-yhdistelmän perusteella (Fifield ym., 2019). Porttien estäminen kuuluu palomuurien normaaleihin perustoimintoihin.

5.1.2 UDP-liikenteen estäminen

Yhteydetöntä UDP-protokollaa käyttävän dataliikenteen sensurointi on tehtävä osin eri tavoin kuin TCP-protokollaa käyttävän liikenteen. Esimerkiksi Kiinan palomuuri estää UDP-liikennettä antamalla väärennetyn DNS-vastauksen (ks. jäljempänä kohta 5.2.1), kun taas TCP-protokollan liikennettä se estää yllä mainitulla reset-menetelmällä (Z. Wang ym., 2017). Sekä UDP- että TCP-liikennettä voi estää myös estämällä liikenteen siitä palvelimen portista, josta liikenne kulkee (esim. Zoltan, 2023).

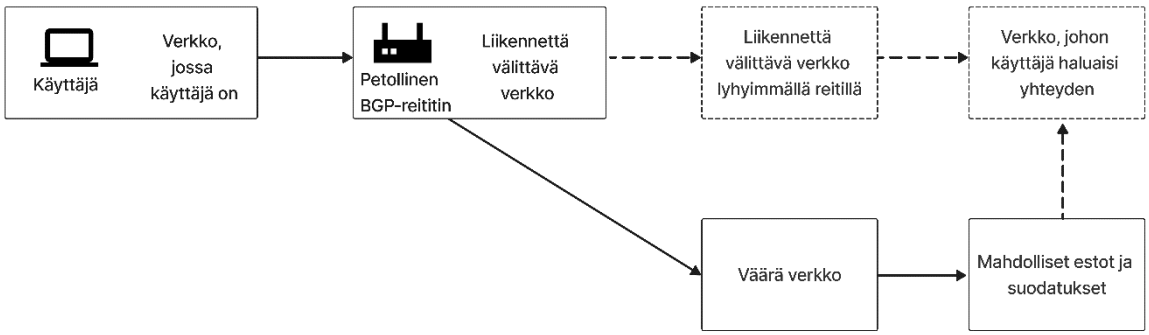
Sensuuritekniikat mahdollisesti tulevaisuudessa estävät yhä enemmän UDP-liikennettä, koska web-selainliikenteen uusin, HTTP/3-liikenteen käyttämä ja vuonna 2021 julkaistu QUIC-protokolla käyttää UDP-protokollaa. Aiemmat HTTP-versiot käyttivät TCP-protokollaa. QUIC on kuitenkin verrattain tehokkaasti salattu ja sensuuriresistentti protokolla (Elmenhorst, 2022), jonka estäminen vaatii myös kehittyneitä toimia, kuten datapakettien syväanalyysiä (ks. jäljempänä kohta 5.3.2).

5.1.3 BGP-protokollan IP-estot

Usein IP-osoitteita estetään myös BGP-protokollaa hyödyntämällä. Autonomisen järjestelmän on mahdollista kaapata BGP-liikennettä kulkemaan kauttaan jakamalla virheellistä tietoa siitä, mitä IP-osoitteita järjestelmä kattaa. Järjestelmä voi väittää kontrolloivansa sellaisia IP-osoitteita, joita se ei todellisuudessa kontrolloi, jolloin muut järjestelmät tietyissä tilanteissa reitittävät liikennettä kulkemaan virheellisesti tämän petollisen autonomisen järjestelmän kautta. Jotta tällainen BGP-kaappaus onnistuisi, virheelliset reititystietojen jakajan on oltava autonomista järjestelmää hallinnoiva operaattori tai hyökkääjä, joka on kaapannut autonomiseen järjestelmään kuuluvan BGP-reitittimen. Näistä tapauksista yleisempi on sellainen, jossa operaattori itse antaa harhaanjohtavaa tietoa. Kaapattuaan liikenteen omaan verkkoonsa operaattori voi panna

toimeen liikenteen estoja, suodatuksia tai tarkkailua (Kuva 14). (Cloudflare, n.d.-b; Kruse, 2018.)

Kuva 14: BGP-kaappaus (Cloudflare, ei pvm.-c; Kruse, 2018)



Yleinen tapa estää liikennettä BGP-protokollan avulla on kaapatun liikenteen reitittäminen ei-mihinkään. Tästä käytetään usein nimitystä nollareititys (null routing) tai reititys ”mustaan aukkoon” (black hole routing). Esimerkiksi Kiinan palomuuri käyttää nollareititystä yhtenä keinona IP-osoitteiden estämiseen. Kiinan palomuuri antaa reititystietoja BGP:n kautta kaikille kiinalaisille internet-palveluntarjoajille ja kaappaa sellaisen liikenteen, joka on tarkoitettu kieltolistalla oleviin osoitteisiin. Liikenne nollareititetään eli yksinkertaisesti jätetään välittämättä eteenpäin. (Anderson, 2012, s. 1.)

Koko IP-osoitteen estäminen vaatii, että ylläpidetään listaa niistä IP-osoitteista, joihin liikenne halutaan estää. Tällaisten listojen ylläpitäminen on työlästä ja vaatii jatkuvaa laitteistojen päivittämistä. Resursseja tällaiseen on vain harvalla maalla tai organisaatiolla, ja operaation toteuttaminen voi olla ongelmallista, kuten Suomessakin havaittiin lapsipornosivustojen estoyritysten yhteydessä 2000-luvulla (ks. kohta 3.4.1).

Kokonaisten IP-osoitteiden tukkimisella on myös sivuvaikutus, että tullaan estäneeksi sellaisia sivustoja, joita ei ollut tarkoitus estää. Menetelmä estää liikenteen kaikkiin sivustoihin, jotka toimivat samalla palvelimella jakaen saman IP-osoitteen. IP-osoitteen jakaminen on varsin yleistä, sillä verkkosivujen pitäminen jaetussa IP-osoitteessa on halvempaa kuin oman IP-osoitteen varaaminen. (Clayton et al., 2006.)

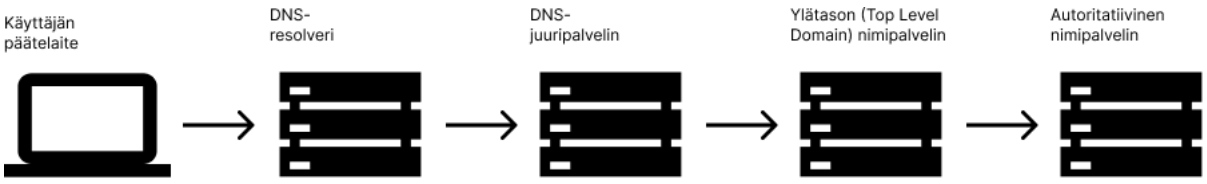
5.2 URL-osoitteiden estot

Usein ihmiset käyttävät verkossa olevia resursseja niiden selkokielisen URL-osoitteen perusteella (uniforme resource locator). URL-osoite on se osoite, joka yleensä kirjoitetaan esimerkiksi verkkoselaimen osoitekenttään. Esimerkiksi https://www.hamk.fi/vuosikertomus/ on URL-osoite. URL sisältää verkkotunnuksen (engl. domain name), joka äskeisessä esimerkissä on hamk.fi. Tietokone kuitenkin löytää kyseisen palvelimen sen IP-osoitteen perusteella, joka tässä tapauksessa on 95.217.104.240. Ihmisen on huomattavasti helpompi muistaa URL-osoitteita tai verkkotunnuksia kuin IP-osoitteita, joten verkkotunnusten ja IP-osoitteiden yhdistämistä varten on olemassa DNS- eli Domain Name System -niminen protokolla, jonka toiminnallisuutta voi verrata vaikkapa perinteiseen puhelinluetteloon. DNS muuntaa ihmisten ymmärtämän verkkotunnuksen koneiden ymmärtämäksi IP-osoitteeksi. DNS-järjestelmä toteutetaan DNS- eli nimipalvelimien avulla (Cloudflare, ei pvm.-d; Terman, 2021a).

5.2.1 DNS-manipulointi

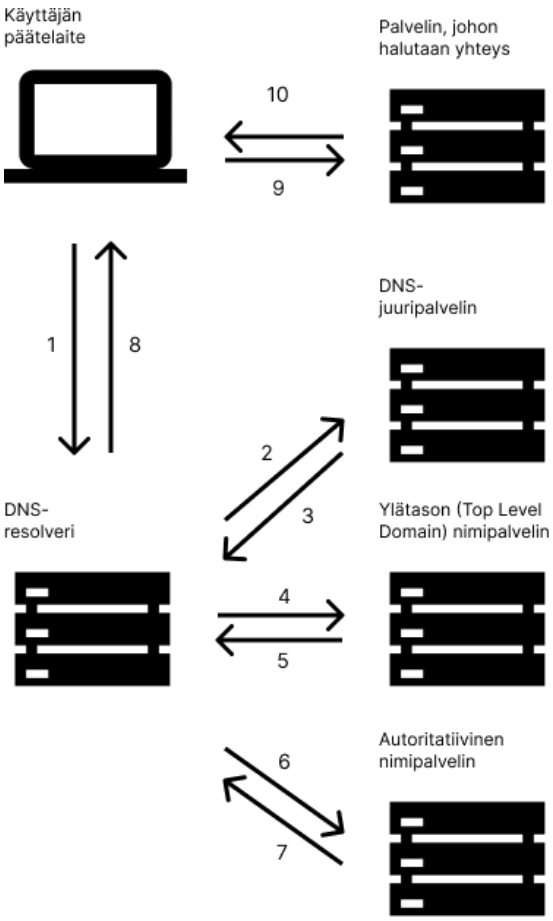
DNS-pyyntö vaatii yleensä useita eri tasoisia DNS-palvelimia eli nimipalvelimia. Yleensä asiakas ottaa ensin yhteyden niin sanottuun DNS-resolveriin. Sen tehtävänä on lähinnä vastaanottaa DNS-tiedusteluja asiakkaiden päätelaitteiden sovelluksista kuten verkkoselaimista. Resolveri tekee puolestaan jatkokyselyjä eri tasoisille DNS-palvelimille. DNS-juuripalvelin ja ylätason nimipalvelin ohjaavat tiedustelun yhä yksityiskohtaisemmalle tasolle, kunnes viimeinen eli autoritatiivinen nimipalvelin palauttaa lopullisen IP-osoitteen. Saatuaan IP-osoitteen asiakkaan päätelaite hankkii kaivatun sisällön tai palvelun kyseisestä IP-osoiteesta (Kuva 15).

Kuva 15: DNS-järjestelmän perusperiaate (Cloudflare, ei pvm.-d)



Hieman yksityiskohtaisemmin kuvattuna asiakkaan päätelaite ottaa ensin yhteyden resolverille, joka ottaa yhteyden seuraavaan palvelimeen ja saa siltä vastauksen, jonka perusteella resolveri ottaa yhteyden seuraavaan palvelimeen, kunnes se saa lopullisen IP-osoitteen autoritatiiviselta nimipalvelimelta. Lopuksi asiakkaan päätelaite ottaa yhteyden saatuun IP-osoitteeseen ja saa sieltä vastauksen (Kuva 16).

Kuva 16: DNS-palvelimien yhteydet ja niiden järjestys (Cloudflare, ei pvm.-d)



DNS-järjestelmällä on merkitystä internet-sensuurin kannalta, koska järjestelmä käytännössä ohjaa liikennettä. Jos pääsy jonkin internetissä toimivan sivuston tai palvelun IP-osoitteeseen on estetty, palvelun voi siirtää toiseen IP-osoitteeseen ja ohjata DNS-palvelimen viittaamaan tähän uuteen osoitteeseen. Vanhan IP-osoitteen estolla ei ole vaikutusta uuteen IP-osoitteeseen, joten esto on tällöin ohitettu ja sivusto tai palvelu toimii, kunnes myös uusi IP-osoite estetään.

Siksi tehokkaassa internet-sensuurissa on asetettava estoja myös DNS-palvelimille. Liikenne tiettyyn IP-osoitteeseen voidaan estää niin sanotulla DNS-myrkyttämisellä, jossa DNS-palvelin asetetaan joko olemaan palauttamatta mitään tai palauttamaan väärä IP-osoite. Jos DNS-palvelin ei palauta oikeaa osoitetta, kohdesivusto tai palvelu on käytännössä näkymätön asiakkaan selaimelle (Terman, 2021b). DNS-palvelinten palauttamassa väärässä IP-osoitteessa puolestaan voi olla esimerkiksi ilmoitus, että haettu sisältö tai palvelu on kielletty (Clayton ym., 2006).

Manipuloinnin ei tarvitse kohdistua itse DNS-palvelimiin, vaan niin sanotun DNS-injektion tapauksessa sen voi hoitaa laite, joka on matkan varrella ennen DNS-palvelinta. Esimerkiksi Kiinan palomuuri käyttää järjestelmää, jossa DNS-resolverin ja muiden DNS-palvelimien väliin on asetettu DNS-injektoreja, joka palauttavat väärän IP-osoitteen (Anonymous, 2012).

Pelkkä DNS-järjestelmään perustuva sensuuri ei kuitenkaan riitä estämään pääsyä sivustolle tai palveluun. Jos palveluntarjoaja ei ole estänyt pääsyä IP-osoitteeseen, sinne pääsee helposti pelkällä IP-osoitteella (Terman, 2021a).

DNS-manipulointia käyttää sensuurijärjestelmiensä osana Kiinan (Anderson, 2012, s. 3) lisäksi ainakin Iran (Isfahani, 2022). Venäjä puolestaan on viime vuosina kehitellyt täysin kansallista DNS-järjestelmää, jonka tavoitteena on mahdollistaa tarvittaessa koko Venäjän internetin irrottaminen maailmanlaajuisesta internetistä (Epifanova, 2020).

5.2.2 HTTP- ja TLS-liikenteen suodatus

Verkkoselainten käyttämässä HTTP-protokollassa yhteyspyynnön otsikkotiedoissa kerrotaan paljon sensuroijia kiinnostavaa tietoa, kuten haettu verkkotunnus. Sensuroiva taho voi estää liikenteen kiellettyihin verkkotunnuksiin tämän tiedon perusteella (Hall ym., 2023, Luku 4.2.1-4.2.2).

Salaamaton HTTP-protokolla käy kuitenkin yhä harvinaisemmaksi, ja valtaosa web-liikenteestä käyttää nykyisin salattua HTTPS-protokollaa. Tässä protokollassa tieto verkkotunnuksesta ei enää kulje liikenteen mukana salaamattomana, joten sensuroijan on vaikea poimia otsikkotietoa (Hall ym., 2023, Luku 4.2.2). Myös DNS-manipulointia voidaan hankaloittaa huomattavasti käyttämällä salattua yhteyttä (Jin ym., 2021, s. 485).

Salatun HTTPS-yhteyden tapauksessa voidaan kuitenkin palvelimen nimi poimia hyödyntämällä TLS-protokollan laajennusta SNI:tä (Server Name Identificcation). TLS (Transport Layer Security) -salausprotokollaa hyödynnetään HTTPS-liikenteessä. Vaikka TLS:ää käyttävässä liikenteessä datapaketin hyötykuorma on salattu, asiakaskoneen on kuitenkin mahdollista kertoa kättelyvaiheessa SNI:n avulla, minkä nimiselle isäntäkoneelle paketti on tarkoitettu. SNI:n käyttö mahdollistaa sen, että samassa IP-osoitteessa voi toimia useita eri nimisiä palvelimia, mikä on melko yleistä. (Claburn, 2018.)

Koska palvelimen nimi tällä tavoin kerrotaan, liikenne kielletyn nimisiin palvelimiin on luonnollisesti mahdollista estää tarkkailemalla liikennettä ja poimimalla sieltä verkkotunnustietoja. Estoja voidaan tehdä esimerkiksi palomuurin kaltaisilla ratkaisuilla, kuten Etelä-Koreassa (Gatlan, 2019).

Datapakettien tarkempaan analysointiin perustuvia sensuurimenetelmiä käsitellään jäljempänä alaluvussa 5.3.

5.3 Liikenteen analysointi

Tietyissä IP-osoitteissa olevien palvelimien estäminen tai DNS-manipulointi koskevat kokonaisia osoitteita, ja URL-suodatus voi koskea jopa yksittäisiä verkkosivuja. Kaikki nämä menetelmät edellyttävät päätöstä siitä, mitä osoitteita halutaan estää. Siksi menetelmät ovat melko karkeita ja vaativat kieltolistojen jatkuvaa ja työlästä päivittämistä. Se ei ole suuressa mittakaavassa ja pitkällä aikavälillä toimiva tapa. Tehokkaan ja toimivan internet-sensuurin olisi toimittava reaaliaikaisesti niin, että se tarkkailee verkkoliikennettä etsien sieltä tiettyjä avainsanoja tai -virkkeitä tai tietyn tyyppistä liikennettä, kuten VPN-liikennettä (Bendrath & Mueller, 2011, 1145).

Nykyaikaiset valtiolliset sensuurijärjestelmät, kuten Kiinan niin sanottu suuri palomuuri, pystyvät tarkkailemaan ja analysoimaan terabiteittäin dataliikennettä reaaliajassa. Etenkin salaamattomat protokollat, esimerkiksi HTTP, DNS ja IMAP, ovat suoraan alttiita tarkkailulle ja jopa manipuloinnille. Useiden maiden on havaittu esimerkiksi suodattavan HTTP-liikennettä siten, että ne etsivät kiellettyjä avainsanoja ulos menevistä URL-pyynnöistä ja sisään tulevista HTTP-vastauksista. Salatut protokollat kuten SSH, TLS/SSL ja PPTP/MPPE sekä

Tor-verkon liikenne puolestaan on mahdollista tunnistaa niiden ominaispiirteiden perusteella, jolloin voidaan estää liikenne siihen IP-osoitteeseen, johon tällaista liikennettä huomataan kulkevan. (Clayton ym., 2006; Z. Wang ym., 2017; Xue, Mixon-Baca, ym., 2022, s. 180.)

5.3.1 Matalan tason pakettianalyysi

Kaikkein yleisin ja yksinkertaisin niin sanottu matalan tason analyysimenetelmä dataliikenteen urkkimiseksi on pakettien otsikkotietojen analyysi. Tutkimalla datapakettien otsikko- eli header-tietoja saadaan esimerkiksi IP-osoite- ja porttitietoja, joiden perusteella voidaan estää liikennettä kiellettyihin IP-osoitteisiin tai sallia tiettyjen sovellusten käyttämiä portteja. Yhdistämällä IP- ja porttitietoihin vielä tieto protokollasta, joka sekin usein on saatavissa otiskkotiedoista, voidaan tunnistaa ja estää liikenne tiettyihin TCP- tai UDP-päätepisteisiin (Hall ym., 2023, Luku 4.3.1).

Liikenteen estäminen otsikkotietojen perusteella tiettyihin IP- ja porttiosoitteisiin on teknisesti helppoa, mutta ei täysin ongelmatonta. Se on hankala toteuttaa laajassa mittakaavassa runkoverkon tasolla. IP- ja porttiosoitteiden estäminen johtaa helposti ylisensurointiin eli sellaisenkin liikenteen estämiseen, jota ei ole tarkoitus estää. Porttien estäminen on ongelmallista myös, koska samoja portteja saattavat käyttää monet erilaiset sovellukset. Näistä syistä matalan tason pakettianalyysiä käytetään usein yhdessä pakettien syväanalyysin kanssa, joka merkittävästi vähentää summittaista massasensurointia (Hall ym., 2023, s. 4.3.1).

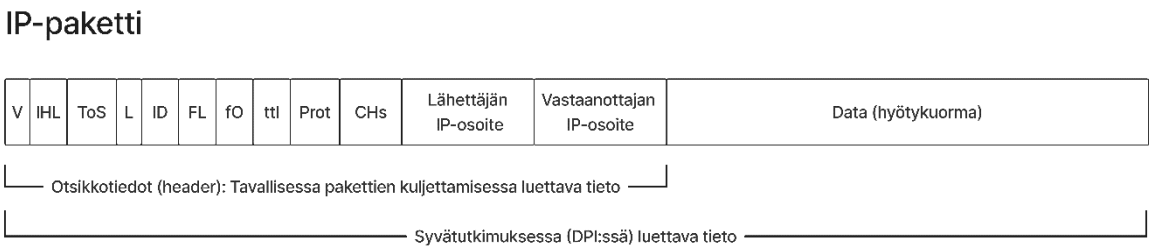
5.3.2 Datapakettien syväanalyysi (DPI)

Perinteiset tietoliikenteen suodatusmenetelmät analysoivat liikenteen joukosta vain datapakettien otsikkotietoja, mutta nykyaikaiset tarkkailu- ja sensuurijärjestelmät käyttävät tekniikkaa nimeltä pakettien syvätutkimus (Deep Packet Inspection, DPI), jota usein käytetään esimerkiksi palomuureissa (Brook, 2023). DPI:llä tarkoitetaan sellaista pakettien anaysointia, joka tutkii liikenteestä muutakin kuin otsikkotietoja. Alun perin internetin protokollat olettivat, ettei internet-palveluntarjoajan kuulu tietää datapaketista varsinaisen datan sisältöä, vaan ainoastaan otsikkotiedot eli header-osa, jossa on riittävät tiedot paketin

kuljettamiseksi oikeaan kohteeseen, mutta syvätutkimuksessa tarkastellaan myös datapakettien hyötykuormia eli varsinaista dataa (Kuva 17). (Hall ym., 2023, Luku 4.2.5.)

DPI-järjestelmiä käytetään myös muutoin kuin sensurointitarkoituksessa. Tällainen järjestelmä voidaan ohjelmoida etsimään datapaketeista esimerkiksi haittaohjelmakoodeja tai muuta haitallista sisältöä ja reagoimaan niihin. DPI-tekniikkaa käytetään esimerkiksi yrityksissä tietoverkkojen IDS-järjestelmissä ja tietojen varastamisen ilmaisujärjestelmissä (exfiltration detection). Sitä voidaan käyttää myös kuluttajille tarkoitetuissa niin sanotuissa parental control -palveluissa, joilla pyritään suodattamaan pois lapsille sopimatonta verkkosisältöä. (Bendrath & Mueller, 2011, s. 1144; Sherry ym., 2015, s. 213.)

Kuva 17: IP-paketista DPI:ssä luettava tieto (Bendrath & Mueller, 2011, s. 1144)



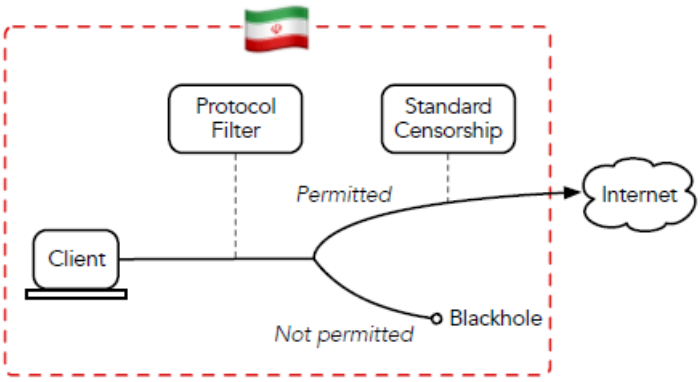
Koska DPI on tarkoitettu tunnistamaan ja luokittelemaan liikennettä, se antaa internet-palveluntarjoajille mahdollisuuden tarkkailla liikennettä reaaliajassa ja tehdä päätöksiä siitä, mitä paketeille tehdään. Siksi se soveltuu erinomaisesti internetin sensurointiin. Palveluntarjoajat voivat esimerkiksi nopeuttaa, hidastaa, estää tai suodattaa liikennettä sen perusteella, millaista tietoa ollaan kuljettamassa. (Bendrath & Mueller, 2011, 1143.)

DPI-järjestelmiä voi käyttää vaikkapa VPN-liikenteen estämiseen, koska tällaisilla järjestelmillä voidaan tunnistaa liikenteen ominaispiirteitä. Ainakin osalle VPN-protokollista on mahdollista määritellä eräänlainen sormenjälki, joka kertoo, että kyse on VPN-liikenteestä. Esimerkiksi erittäin yleisesti käytetylle OpenVPN-protokollalle tällainen sormenjälki on mahdollista määritellä tutkimalla datapakettien rakennetta ja kokoa sekä kohdepalvelimen käyttäytymistä (Xue, Ramesh, ym., 2022).

Sensuroivista maista esimerkiksi Kiinan palomuuri pyrkii estämään monien ulkomaalaisten VPN-järjestelmien käytön, mutta se kuitenkin sallii tietyt Kiinan viranomaisten hyväksymät

paikalliset VPN:t, joiden liikennettä Kiinan oletetaan pystyvän valvomaan (Hornby & Yang, 2018). Myös Iran käyttää järjestelmää, jossa se pyrkii suodattamaan tiettyjä protokollia määrittämällä protokollien ominaispiirteitä. Iran otti vuonna 2020 käyttöön protokollasuodattimen, joka päästää läpi vain DNS-, HTTP- ja HTTPS-protokollat. Näitä protokollia käyttävä liikenne ohjataan muihin sensuurijärjestelmiin lisäanalyyseihin, ja muu liikenne ohjataan niin sanottuun mustaan aukkoon eli ei mihinkään (Kuva 18). Suodatusjärjestelmä toimii niin, että se pudottaa pois kaiken liikenteen asiakaskoneen suunnasta, jos protokolla vaikuttaa kielletyltä (Bock ym., 2020).

Kuva 18: Iranin protokollasuodatin (Bock ym., 2020)



Teknisesti VPN-yhteyksiä voidaan estää esimerkiksi estämällä liikenne niistä palvelimen porteista, joista VPN-liikenne tulee tai estämällä liikenne palvelimen kaikista porteista eli koko IP-osoitteesta. Yleisimmille VPN-protokollille on määritelty portit, joita ne käyttävät (esim. Zoltan, 2023). Sensuroijan kannalta saattaa olla helpointa estää liikenne palvelimen koko IP-osoitteesta, koska usein VPN-palvelimet on tarkoitettu vain sensuurin kiertämiseen, jolloin niitä estäessä ei sivuvaikutuksena esty muita toimintoja (Alice ym., 2020, Luku 6).

Koska liikennettä voidaan analysoida, DPI-järjestelmiä voidaan käyttää myös tarkkailuun ja vakoiluun. Jos käytetään usein käytettyä vertausta, jossa datapaketin ajatellaan olevan kuin postissa lähetettävä kirje, syvätutkimus eli DPI on ikään kuin postitoimistossa avattaisiin ja luettaisiin jokainen sen kautta kulkeva kirje (Geere, 2012). Verkkosensuuriin sovellettuna mallin voisi ajatella vielä niin, että avattuaan ja luettuaan kirjeet postitoimiston virkailijat tuhoavat sellaiset kirjeet, jotka sisältävät kiellettyä sisältöä, ja mahdollisesti lähettävät poliisiviranomaisille kopion epäilyttävistä sisällöistä (Bendrath & Mueller, 2011, 1148).

5.3.3 Kiinan käyttämä suodatusjärjestelmä

Kehittyneet suodatusjärjestelmät yhdistävät eri tekniikoita. Esimerkkinä tällaisesta järjestelmästä voidaan tarkastella Kiinan sensuurijärjestelmää. Kiina ei ole kertonut suuren palomuurinsa toimintaperiaatteita, mutta ainakin yhdestä järjestelmän versiosta on testien perusteella tehnyt päätelmiä joukko britannialaisen Cambridgen yliopiston tutkijoita vuonna 2006 (Clayton ym., 2006). Heidän mukaansa järjestelmä käyttää eräänlaista IDS-järjestelmää (Intrusion Detection System), joka tarkkailee verkkoliikennettä ja tarvittaessa estää tietyt tunnusmerkit täyttävää liikennettä.

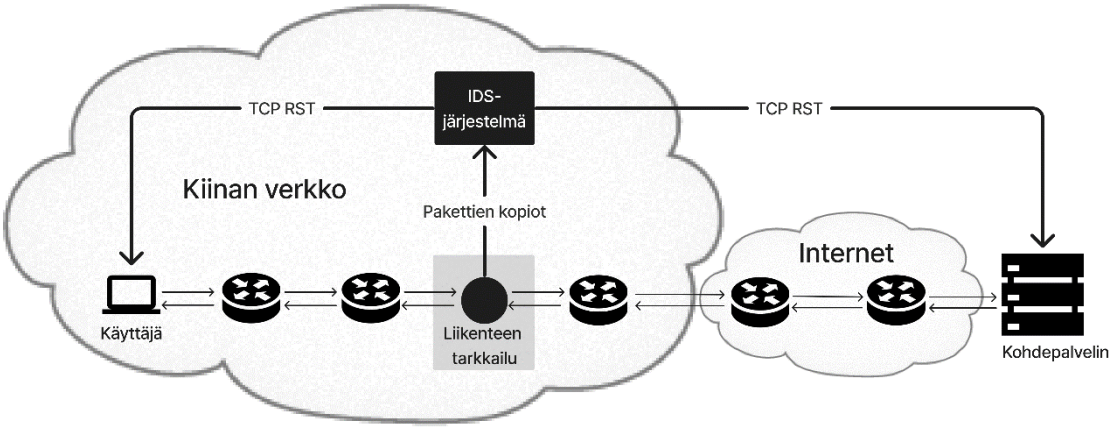
Perinteisesti liikenteen tarkkailujärjestelmät ovat ohjanneet kaiken verkkoliikenteen kulkemaan välipalvelimen kautta, joka kieltäytyy toimittamasta perille sellaista sisältöä, joka on määrätty kiellettäväksi. Tällaisten järjestelmien rakentaminen ja ylläpitäminen niin, että ne kykenevät käsittelemään valtavia tietomääriä, esimerkiksi kokonaisen maan verkkoliikenteen, on kuitenkin erittäin kallista, eivätkä nämä järjestelmät siksi ole levinneet kovin laajaan käyttöön. (Clayton et al., 2006.)

Vaihtoehtoinen tapa on liikenteen tarkkailun hoitaminen IDS-järjestelmällä. Se tarkkailee liikennettä reaaliajassa ja tutkii, onko liikenne hyväksyttävää. Kielletyt paketit järjestelmä voi lähettää esimerkiksi palomuurille hylättäviksi, tai se voi panna liikenteeseen TCP reset -paketteja, jolloin yhteys katkeaa. Kiina käyttää Cambridgen tutkijoiden (Clayton ym., 2006) mukaan TCP reset -menetelmää.

Kiinalaisessa järjestelmässä, kun paketti saapuu reitittimelle, se asetetaan suoraan jonoon paketin eteenpäin toimittamista varten, eli paketit jatkavat matkaansa ilman estoja. Samalla paketista kuitenkin lähetetään kopio ulkopuoliselle IDS-laitteelle, joka tarkastaa sen sisällön. Jos IDS havaitsee tarkastuksessa kiellettyjä ominaisuuksia, jotka voivat olla esimerkiksi IP-osoitteita tai avainsanoja, järjestelmä siirtää reitittimen kautta datavirran joukkoon väärennettyjä paketteja, joissa TCP RST -kytkin on asetettu päälle (Kuva 19), jolloin sekä lähettäjä että vastaanottaja hylkäävät yhteyden. Lisäksi järjestelmä säilyttää tiedon lähettäjän ja vastaanottaja IP-osoitteista, protokollasta ja porttinumeroista ja estää mahdolliset uudet yhteydenottoyritykset näiden laitteiden välillä. Koska järjestelmä ei estä ensimmäisiä paketteja päätymästä kohteeseen, on mahdollista, että kohdepalvelimelta ehtii

saapua vastaus käyttäjän koneelle ennen kuin TCP RST -paketti ehtii perille. Järjestelmä lähettää useita erilaisia TCP RST -paketteja, jotta yhteyden katkeaminen varmistuu tällaisessakin tapauksessa. (Clayton et al., 2006; Verkamp & Gupta, 2012; Xu, 2016.)

Kuva 19: Päätelmä Kiinan sensuurijärjestelmästä (Clayton ym., 2006; Xu, 2016)



Perinteisellä IDS-järjestelmällä toteutettu liikenteen tarkkailu kykenee estämään vain salaamattoman liikenteen (Clayton ym., 2006). Sensuurin kiertomenetelmien kehittyessä Kiina on kuitenkin jatkuvasti kehittänyt palomuuriaan, ja nykyisin se pysyy tunnistamaan ja estämään jopa täysin salatun verkkoliikenteen, eli sellaisen liikenteen, joka on yritetty tehdä tunnistamattomaksi salaamalla sen jokainen bitti, otsikkotiedot mukaan lukien. Tässä Kiina käyttää niin sanottua aktiivista luotausta (active probing), joka vaatii työläämpiä ja kalliimpia keinoja kuin perinteinen deep packet inspection -tyyppinen datapakettien lukeminen. (Wu et al., 2023.)

Perinteiset protokollat kuten TLS aloittavat liikenteen niin sanotulla kättelyllä, jossa on salaamattomia bittejä. Sen sijaan täysin salatut protokollat kuten VMess, Shadowsocks ja Obfs4 ovat kokonaan salattuja. Tällöin liikenne näyttää täysin satunnaiselta, jolloin siitä on vaikea löytää tunnusmerkkejä, joiden perusteella sen voisi määrätä estettäväksi. Aktiivisessa luotauksessa sensuroiva palomuuri lähettää epäilyttävinä pitämilleen palvelimille tarkoin muotoiltuja paketteja ja katsoo, miten palvelimet vastaavat. Jos palvelin vastaa tunnistettavalla tavalla eli osoittaa olevansa proxy- eli välityspalvelin, sensori voi estää yhteydet kyseiselle palvelimelle. (Wu et al., 2023, 2.)

Tällainen täysin salatun liikenteen tunnistaminen muun liikenteen joukosta aktiivisin toimin vaatii lisäpakettien lähettämistä liikenteeseen, ja suuressa mittakaavassa sellainen on luonnollisesti kallista. Kiina on kuitenkin käyttänyt tätä menetelmää ainakin vuodesta 2011 asti (M. Wu ym., 2023). Marraskuussa 2021 Kiina näyttää harpanneen vielä askeleen eteenpäin ottamalla käyttöön järjestelmän, jolla se kykenee tunnistamaan ja estämään täysin salattua liikennettä myös passiivisesti. Kyseessä oli Wun ja muiden (2023) mukaan ensimmäinen kerta, kun Kiina pystyi estämään täysin salattuja proxy-palvelimia joukoittain perustuen täysin passiiviseen liikenteen analysointiin.

Kiinan palomuuri toteutti tämän analysoimalla liikennettä poimiakseen sieltä liikenteen, joka todennäköisesti ei ole täysin salattua liikennettä – sen sijaan, että se olisi pyrkinyt etsimään täysin salattua liikennettä. Palomuuri päästi läpi kaiken sellaisen liikenteen, joka analyysin mukaan todennäköisesti ei ole täysin salattua liikennettä, ja muun liikenteen palomuuri esti. Analyysi tehtiin ainakin viiden erilaisen heuristisen mallin avulla. Ainakin tutkimusaikana vuoden 2021 lopulta vuoteen 2022 Kiina käytti uutta passiivista analyysityökaluaan rinnakkain aktiivisen luotaamisen kanssa. Uusi passiivinen menetelmä näyttää kohdentuvan täysin salattuun liikenteeseen melko hyvin, mutta ei täydellisesti. Tutkijoiden arvion mukaan menetelmä voisi laajasti käytettynä estää noin 0,6 prosenttia liikenteestä sivuvaikutuksena eli tarkoittamatta estää juuri kyseistä liikennettä. (Wu et al., 2023.)

5.4 Hajautetun verkon sensuroiminen

Useimmissa valtioissa internet kehittyi alun perin hajautetusti niin, että useat tahot osallistuivat verkon kehittämiseen siinä järjestyksessä kuin se kullekin sopi. Tämän verkoista koostuvan verkon kehittämisessä Yhdysvallat oli keskeisessä roolissa, ja se antoi tehtävän paljolti yksityiselle sektorille. Aluksi vain harvassa valtiossa kehitettiin internetiä turvallisuus- ja kontrollinäkökulma edellä, joten valtaosa maailmanlaajuisesta internetistä on verrattain hajautettu, jolloin sen liikennettä on hyvin vaikea kontrolloida yhdestä tai muutamasta reitittimestä. (Salamatian ym., 2021, s. 2.)

Osassa maita internet-liikenne maan ja ulkomaiden välillä ohjataan rajan yli solmukohdista, joita on melko rajallinen määrä. Tällaisia maita ovat esimerkiksi Kiina ja Iran (Ramesh ym., 2020). Kiinassa nähtiin internetin strateginen ulottuvuus hyvin varhain, ja Kiinan internet-

arkkitehtuuri on rakennettu paljolti valtion kontrolli etusijalla niin, että liikennettä voidaan tiukasti kontrolloida Kiinan rajoilla (Salamatian ym., 2021, s. 2). Vaikka Kiina on väkiluvultaan maailman suurin maa, sen rajojen yli kulkevasta internet-liikenteestä valtaosa kulkee vain kolmen kansainvälisen solmukohdan kautta (Demchak & Shavitt, 2018, s. 7). Solmukohdat sijaitsevat Pekingissä, Shanghaissa ja Hongkongissa. Tällaisessa maassa internet-sensuuri on verrattain helppo toteuttaa tarkkailemalla ja rajoittamalla liikennettä solmukohdissa, ja Kiina onkin tehnyt niin jo vuosikymmeniä. Sen sijaan sellaisen verkon sensuroiminen on vaikeampaa, joka reitittyy ulkomaille hajautetusti hyvin monesta kohtaa (Ramesh ym., 2020).

Ratkaisuna hajautetun verkon sensurointiongelmiin eri maat ovat käyttäneet sensuurin ulkoistamista palveluntarjoajille ja verkkoarkkitehtuurin muokkaamista sekä liikenteen ohjaamista sensuuria helpottavaan muotoon. Liikenteen ohjaamisessa on tärkeässä roolissa BGP-protokolla.

5.4.1 Sensuurin ulkoistaminen palveluntarjoajille

Verrattain hajanainen verkko on pitkään ollut esimerkiksi Venäjällä. Siellä valtio ei itse sensuroi verkkoliikennettä, vaan velvoittaa palveluntarjoajat hoitamaan asian lainsäädännön nojalla. Venäjän viestintää, tietoverkkoja ja mediaa valvova viranomainen Roskomnadzor ylläpitää listoja kielletyistä sivustoista, joihin pääsy palveluntarjoajien on Venäjällä estettävä. Lisäksi Venäjän valtio jakaa tekniikoita, joilla liikennettä voi estää. Venäjällä palveluntarjoajat ovat velvollisia käyttämään palvelinkeskuksissaan esimerkiksi verkkoliikennettä analysoivaa SORM-järjestelmää (System of Operative Search Measures), jota käytetään sekä liikenteen tarkkailuun että suodattamiseen. (Ramesh ym., 2020.)

Kun sensurointi tehdään palveluntarjoajakohtaisesti erikseen eri puolilla maata, myös tulokset voivat vaihdella. Jokin verkkoresurssi, joka on jossain päin maata sensuroitu, voikin olla saatavissa naapuritalossa, joka käyttää eri palveluntarjoajaa. Myös hajautetusti sensuroiduissa maissa sensuuri on kuitenkin yhtenäistymässä ja tehostumassa, kun SORM:n kaltaiset tarkkailujärjestelmät leviävät. Lisäksi hajautettu sensuuri vaikeuttaa sensuurin kiertämistä. Kun esimerkiksi VPN-palveluja estetään, on löydettävä harvinaisempia tapoja kiertää sensuuria, ja toimivat menetelmät voivat vaihdella palveluntarjoajittain. Tällöin on

hyvin vaikea löytää valtakunnallisesti toimivaa kiertomenetelmää, jota voisi jakaa tai suositella ihmisille, joiden on tarpeen kiertää sensuuria. (Ramesh et al., 2020, 13.)

Sensuuria on ulkoistanut palveluntarjoajille myös muiden muassa Iran, vaikka sen verkkoliikenne ulkomaille kulkeekin melko keskitetysti (Salamatian ym., 2021, s. 12).

5.4.2 Verkkoliikenteen ohjaaminen

Vaihtoehto sille, että palveluntarjoajat pakotetaan sensuroimaan liikennettä datakeskuksissaan, on tiivistää koko verkon arkkitehtuuria niin, että verkkoliikenne ulkomaille keskitetään kulkemaan vain muutamien strategisten kuristuskohtien kautta. Tällöin liikennettä on helpompi tarkkailla ja suodattaa, koska sen vaatimia järjestelmiä ei tarvitse asentaa kovin moneen paikkaan. Vaikka kyseessä ei ole suoraan sisällön estämisen tekninen menetelmä, ilmiö kuitenkin liittyy verkkosensuurin menetelmiin, koska sillä pyritään helpottamaan sisältöjen kontrollia ja sensuuria ja se näyttää olevan maailmalla yleistyvä trendi. Venäjä, jonka autoritaarinen kehitys alkoi kiihtyä vuosituhannen vaihteessa Vladimir Putinin noustua valtaan (esim. Gessen, 2012), on jo noin vuosikymmenen ajan pyrkinyt muokkaamaan verkkoaan tähän suuntaan (Cimpanu, 2019a, 2019b; Xue, Mixon-Baca, ym., 2022, s. 2). Venäjällä on kehitteillä niin sanottu Runet-verkko, jonka voisi irrottaa ulkomaailman verkosta. Venäjä on testannut Venäjän verkon irrottamista ulkomaailmasta Roskomnadzor-viranomaisen väittämän mukaan onnistuneesti, viimeksi vuonna 2023 (Balašova ym., 2023). Myös Iran on pyrkinyt 2010-luvulta asti kehittämään verkkoarkkitehtuuriaan siten, että etusijalla on valtion kontrollimahdollisuuksien varmistaminen (Salamatian ym., 2021, s. 3).

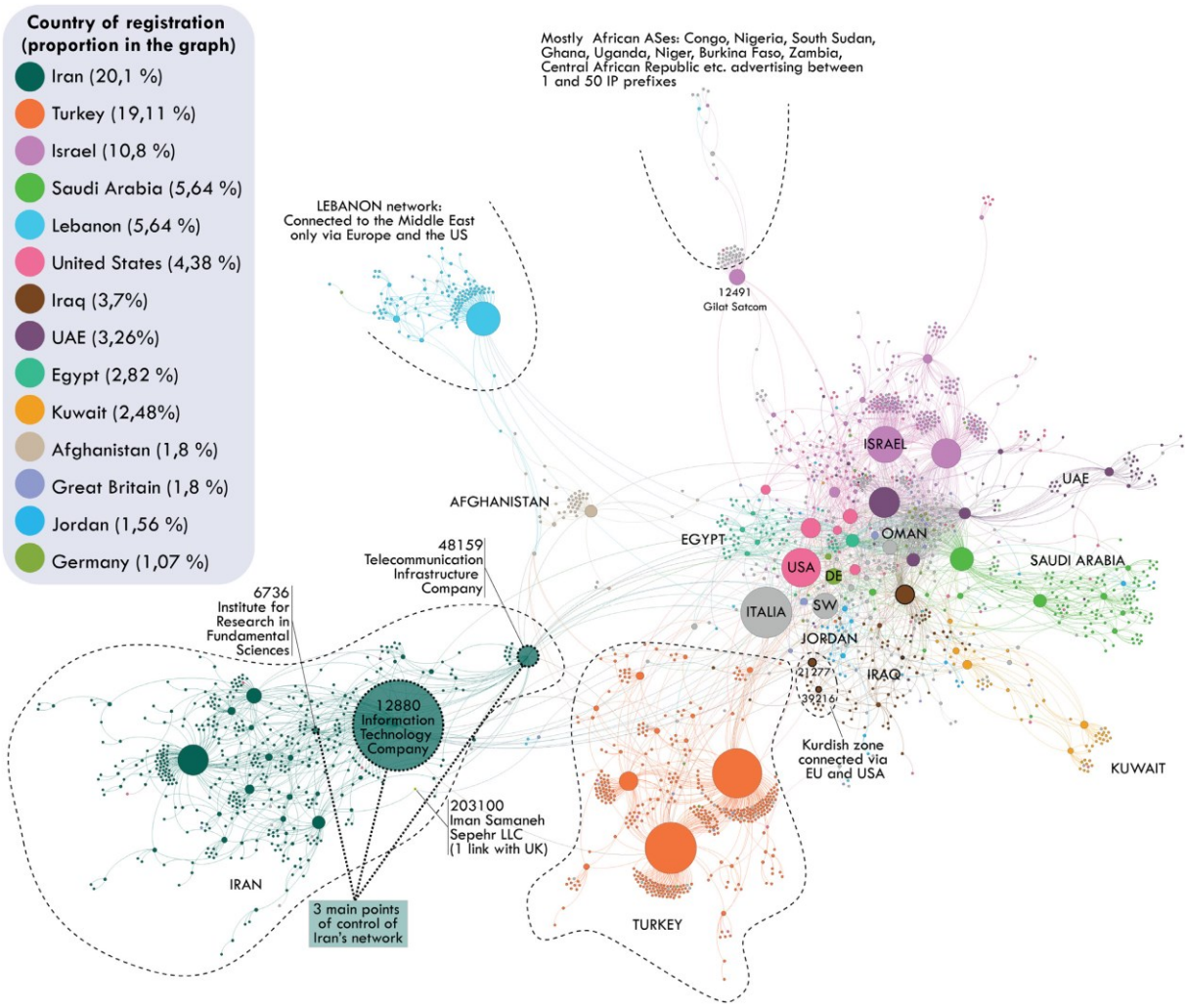
Verkkoliikenteen reititystä määrittää verkon fyysinen arkkitehtuuri, johon kuuluvat esimerkiksi kaapelit, reitittimet, palvelimet ja muut fyysiset laitteet. Suuri merkitys on kuitenkin myös BGP-protokollalla ja sillä, miten eri autonomisten järjestelmien väliset BGP-suhteet on järjestetty. Tässä yhteydessä kyse ei ole alaluvussa 5.1.3 mainitusta BGP-kaappauksesta vaan siitä, kuinka autonomisten verkkojen välistä liikennettä ohjaillaan BGP-protokollan avulla. BGP on siten protokolla, jolla on merkittävä geopoliittinen ulottuvuus. (Douzet ym., 2020, s. 159–160; Limonier ym., 2021; Salamatian ym., 2021.)

Douzetin ja muiden (2020) tutkimuksen mukaan Venäjän otettua hallintaansa Krimin niemimaan ja Donbassin Ukrainalta vuonna 2014 se otti muutaman vuoden kuluessa hallintaansa myös näiden alueiden verkkoliikenteen. Tässä Venäjä hyödynsi BGP-protokollan reititysominaisuuksia sen lisäksi, että se muutti fyysistä infrastruktuuria muun muassa katkaisemalla kaapeleita erikoisjoukkojensa avulla ja hankkimalla paikallisia verkkoja ja kaapeleita venäläiseen omistukseen (Douzet ym., 2020). Donbassissa niin sanottujen venäläismielisten separatistien hallitsemilla Donetskin ja Luhanskin alueilla alkoi verkkoliikenne kulkea Venäjän kautta elokuussa 2018, kun se aiemmin oli kulkenut Ukrainan kautta (Limonier ym., 2021).

Venäjä on myös jo vuosia pyrkinyt eristämään maan rajojen sisällä olevaa verkkoa ulkomaailmasta rakentamalla omaa, maan sisäistä DNS-järjestelmää. Vuonna 2019 hyväksytty laki mahdollistaa Venäjän rajojen sisällä toimivan DNS-järjestelmän käyttöönoton ja velvoittaa testaamaan vuosittain Venäjän internetin eli niin sanotun Runetin irrottamista kansainvälisestä internetistä (Page, 2023). Venäjä on väittänyt testanneensa onnistuneesti verkon irrottamista ulkomaailmasta kesällä 2023 (Balašova ym., 2023). Vuonna 2022 kaikki valtiolliset verkkopalvelut määrättiin käyttämään vain Venäjällä sijaitsevia DNS-palvelimia ja siirtymään venäläisen .ru-verkkotunnuksen alle (Tišina ym., 2022).

Esimerkkinä verkon kontrollimahdollisuuksien lisäämisestä internet-arkkitehtuurin avulla toimii myös Iran. Vaikka Iranin verkkoa ei alusta asti rakennettu kontrolli johtoajatuksena, Salamatian ja muut (2021) havaitsivat, että Iranin verkon nykyinen arkkitehtuuri mahdollistaa erittäin tehokkaan kontrollin. Iranissa toimivilla autonomisilla järjestelmillä on tätä nykyä verrattain vähän suoria yhteyksiä useimpien naapurimaiden järjestelmiin. Lisäksi suurin osa Iranin ulkomaan liikenteestä kulkee vain kolmen autonomisen järjestelmän kautta, ja nämä ovat valtion kontrollissa olevia järjestelmiä (Kuva 20).

Kuva 20: Lähi-idän järjestelmien väliset yhteydet (Salamatian ym., 2021, s. 6)



Iranissa verkkoliikenteen keskittäminen toimii eräänlaisena hätäkatkaisimena, jonka avulla valtio voi katkaista verkkoyhteyksiä ulkomaille, jos se ei kykene muilla menetelmillä sensuroimaan tietoa riittävän nopeasti ja tehokkaasti, esimerkiksi opposition liikehdinnän aikana. Iran käyttää verkon sensuroimiseen ainakin DNS-manipulointia, välityspalvelinten liikenteen suodattamista ja pakettien syvätutkimusta eli DPI:tä, mutta kansainvälisten pakotteiden ja Kiinan vientikieltojen takia sen on ollut vaikea hankkia tekniikkaa, jolla suodatusta voisi tehdä nopeasti ja keskitetysti suuressa mittakaavassa. Tästä syystä Iran on pyrkinyt ulkoistamaan sensuuria internet-palveluntarjoajille, mutta siinä on ongelmana, että uusien sensuurimääräysten jakeleminen ja käyttöönotto kaikilla palveluntarjoajilla vie aikaa. Niinpä Iranilla on ollut strategisena tavoitteena keskittää verkkoarkkitehtuuria sellaiseksi, että valtiolla olisi tarpeen tullen mahdollisuus katkaista verkkoyhteydet maan ulkopuolelle. (Salamatian ym., 2021, s. 12.)

5.5 Karkeat menetelmät

Internetiä voi sensuroida myös varsin suoraviivaisilla menetelmillä, jotka eivät vaadi erityisen kehittynyttä ja kallista tekniikkaa. Niistä käytetään niiden yksinkertaisen luonteen takia tässä nimitystä karkeat menetelmät. Näistä ehkäpä yksinkertaisin on niin sanottu töpselin irrottaminen eli internet-yhteyksien katkaiseminen kokonaan. Hieman hienovaraisempi tapa on hidastaa verkkoliikennettä niin, että verkko on käytännössä lähes käyttökelvoton. Nämä karkeat menetelmät ovat tulevaisuudessa todennäköisesti vähenemässä, ja sen sijaan hallinnot käyttävät yhä enemmän kehittyneempiä kohdennettuja menetelmiä, joilla estetään pääsy vain tiettyihin kohteisiin internetissä (Feldstein, 2022).

5.5.1 Verkon sulkeminen

Monissa maissa hallitukset ovat määränneet internet-palveluntarjoat tietyissä tilanteissa sulkemaan internetin kokonaan tietyillä maantieteellisillä alueilla. Hallinnot eri puolilla maailmaa ovat sulkeneet ja häirinneet internet- yhteyksiä tukahduttaakseen mielenosoituksia, estääkseen häviöitä vaaleissa, vahvistaakseen sotilasvallankaappauksia ja eristääkseen konfliktialueita muusta maailmasta (Feldstein, 2022).

Esimerkiksi niin sanotun arabikevään aikana vuonna 2011 ainakin Bahrainin, Egyptin, Libyan ja Syyrian hallitukset pyrkivät estämään joukkomielenosoitusten organisointia määräämällä internet-operaattorit sulkemaan verkkonsa (Fatafta, 2020). Poikkeuksellisen pitkä, jopa vuosia kestänyt internet- ja myös puhelinyhteyksien katkaisu on ollut meneillään Etiopian pohjoisosassa Tigrayn alueella, jossa paikalliset kapinalliset ovat sotineet Etiopian hallituksen joukkoja vastaan marraskuusta 2020 lähtien (Zelalem, 2022).

Digitaalisia oikeuksia ajavan Access Now -kansalaisjärjeston vuonna 2023 julkaiseman raportin mukaan internetin sulkemiset ovat varsin yleisiä. Vuoden 2022 aikana näin oli raportin mukaan tehty 187 kertaa 35 eri maassa. Sulkemisten kimmokkeina ovat toimineet yleisimmin mielenosoitukset, aseelliset konfliktit, vaalit ja joskus myös kouluissa pidetyt tärkeät valtakunnalliset kokeet. Vauraissa länsimaissa sulkemiset ovat harvinaisia. (Rosson ym., 2023)

5.5.2 Verkon hidastaminen

Johtojen katkaisemista hienovaraisempi tapa sensuroida internetiä on rajoittaa verkon tiedonsiirtonopeutta. Tällaisesta toiminnasta käytetään usein englanninkielistä termiä throttling.

Verkkoa voidaan hidastaa niin paljon, että se on lähes käyttökelvoton, tai hidastaminen voidaan kohdentaa jonkin tietyn tyyppiseen liikenteeseen. Esimerkiksi Venäjä hidasti jo ennen Ukrainan täysimittaista sotaa keväällä 2021 liikennettä Twitteriin, kun Twitter ei ollut suostunut Venäjän Roskomnadzor-viestintäviranomaisen pyyntöihin tiettyjen verkkosisältöjen poistamisesta saatavilta. Venäläiset autonomiset järjestelmät käyttivät liikenteen tarkkailua suodattaakseen liikenteen joukosta sellaisen, joka suuntautui Twitterin palvelimille. Myös Iran on käyttänyt liikenteen hidastamista ainakin vaalien alla vuosina 2009 ja 2013 sekä poliittisten levottomuuksien aikana. (Master, 2023, 91.)

Verkon hidastamisessa on sensuroijan kannalta etuna tietyn asteinen kiistettävyys. Tässä se eroaa monista muista sensuurimenetelmistä, jotka huomataan siitä, että tietyt yhteydet eivät toimi lainkaan. Hidastuksen kohdalla on vaikea näyttää toteen, että kyse on sensuurista eikä esimerkiksi ruuhkasta, kun yhteys on kuitenkin olemassa, vaikkakin hitaana (Master, 2023, 91).

5.6 Muita sensuurimenetelmiä

Internetin sensurointiin on käytetty myös muita menetelmiä, jotka ovat enemmän tai vähemmän teknisiä. Esimerkiksi perinteisellä palvelunestohyökkäyksellä (Denial of Service Attack, DoS attack) voi toisinaan olla sensurointitarkoitus. Ihmiset ja yritykset voidaan houkutella myös sensuroimaan itse itseään, jos niillä on esimerkiksi taloudellisia intressejä toimia jossain tietyssä maassa.

5.6.1 Palvelunestohyökkäys

Palvelunestohyökkäystä on käytetty sensuuritarkoituksiin ainakin Kiinassa ja Venezuelassa. Palvelunestohyökkäys eli DoS-hyökkäys (denial of service attack) on hyökkäys, jossa pyritään

estämään verkkoresurssin käyttö häiritsemällä sen toimintaa, yleensä kuormittamalla kohdetta niin, että sen toiminta vaikeutuu tai lakkaa. Palvelunestohyökkäys tehdään yleensä joko kuormittamalla kohdetta erittäin suurella liikennemäärällä tai lähettämällä kohteeseen sellaista liikennettä, joka saa kohdelaitteen käyttämään tavallista enemmän muistia ja laskentatehoa. (Traficom, 2022, s. 2.)

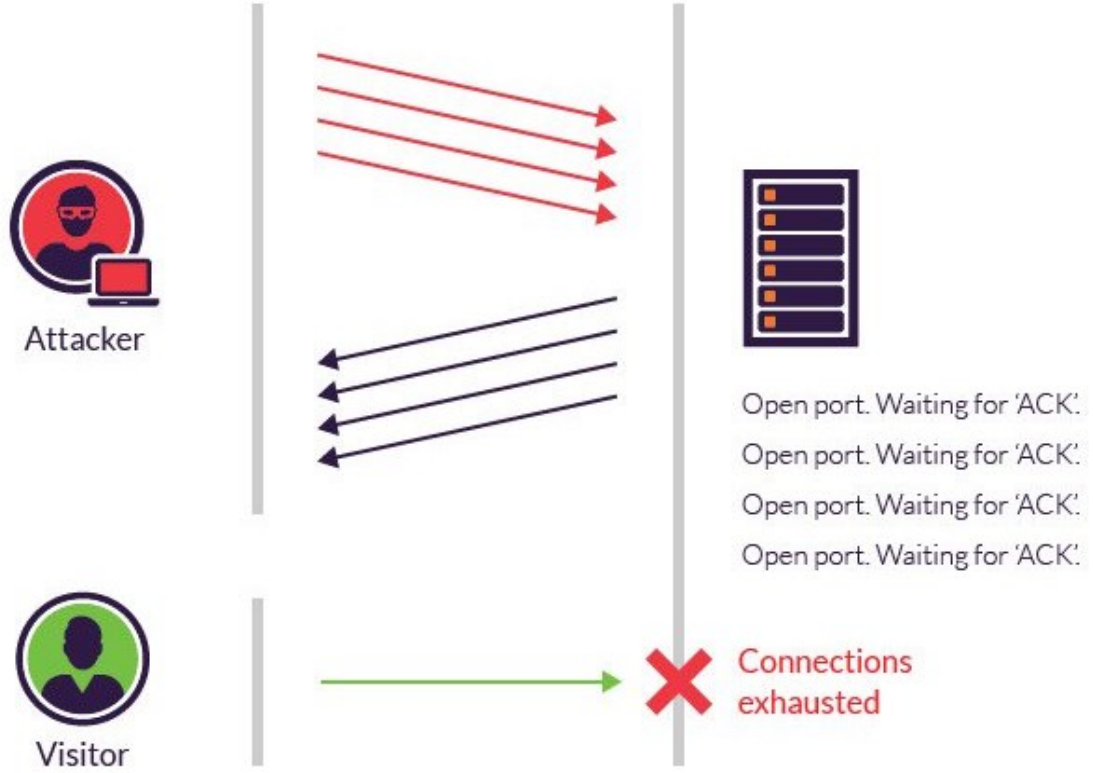
Valtaosa palvelunestohyökkäyksistä on hajautettuja eli sellaisia, joissa liikenne lähetetään kohteeseen useasta lähteestä samanaikaisesti. Palvelunestohyökkäyksen voi toteuttaa monilla eri tavoilla, joissa kaikissa lopputuloksena on palvelun ruuhkautuminen. Yleinen toteutus on esimerkiksi niin sanottu SYN -tulvahyökkäys. (Traficom, 2022, s. 2.)

SYN -tulvahyökkäys perustuu TCP-yhteysprotokollan yhteydenmuodostamisessa käytettävään niin sanottuun kättelyyn. Normaalisti kättelyprosessi tapahtuu kolmessa vaiheessa:

1. Asiakas lähettää kohdepalvelimelle SYN-viestin (synchronize)
2. Palvelin vastaa lähettämällä takaisin SYN-ACK-viestin (synchronize-acknowledge)
3. Asiakas vastaa lähettämällä ACK-viestin (acknowledge), ja yhteys muodostetaan.

SYN-tulvahyökkäyksessä bottiverkko lähettää kohdepalvelimen kaikkiin portteihin SYN-paketteja (Kuva 21). Kohdepalvelin vastaa kuhunkin normaalisti SYN-ACK-paketilla, mutta hyökkäystilanteessa asiakkaat eivät enää lähetäkään takaisin ACK-viestiä, jolloin hyökkäyksen kohteena oleva palvelin jää odottamaan vastauksia. Ennen kuin puoliksi syntynyt yhteys aikakatkaistaan, hyökkääjä ehtii lähettää palvelimelle uuden SYN-paketin. Näin palvelimelle kasautuu suuri määrä puoliksi tehtyjä yhteyksiä, jolloin lopulta tavallisten käyttäjien yhteydet estyvät, ja pahimmassa tapauksessa palvelin voi vikaantua tai kaatua. (Imperva, ei pvm.)

Kuva 21: SYN-tulvahyökkäys (Imperva, ei pvm.)



Palvelunestohyökkäystä käyttää ainakin Kiina. Marczak ja muut (2015) ovat analysoineet Kiinan käyttämää järjestelmää, jota tutkijat nimittävät ”suureksi kanuunaksi” (Great Cannon). Kyseessä on Kiinan palomuurista erillinen järjestelmä, jolla voi muun muassa kaapata liikennettä tiettyyn IP-osoitteeseen. Tutkijoiden mukaan järjestelmä kykenee kaappaamaan Kiinan ulkopuolella olevien järjestelmien verkkoselaimia ja luomaan niiden avulla suuria hajautettuja palvelunestohyökkäyksiä. Järjestelmää käytettiin tutkijoiden mukaan ainakin keväällä 2015 estämään Greatfire.org-sivuston ja kahden siihen liittyvän Github-sivuston toiminta (Marczak ym., 2015). Greatfire.org on sivusto, joka seuraa Kiinan sensuroimien verkkopalvelujen toimintaa.

Lutscher (2023) puolestaan löysi tutkimuksessaan positiivisen korrelaation tiettyjen uutistapahtumien ja venezuelalaisille uutissivustoille tehtyjen DoS-hyökkäysten välillä. Palvelunestohyökkäysten todennäköisyys kasvoi, kun sivustolla julkaistiin esimerkiksi Venezuelan hallinnon legitimiteettiä kyseenalaistavia tai mielenosoituksista ja niiden tukahduttamisesta kertovia uutisia (Lutscher, 2023, s. 708–709).

5.6.2 Itsesensuuri

Verkon sensurointiin ei aina tarvita teknisiä menetelmiä, sillä verkkopalveluja ja -sisältöjä tarjoavat ihmiset ja yritykset pyrkivät usein itse pitämään huolen siitä, että niiden tarjoamat sisällöt noudattavat valtioiden toiveita. Tähän niillä voi olla esimerkiksi liiketaloudellisia intressejä: jos vaihtoehtona on merkittävän markkina-alueen menettäminen kokonaan, valtion todellisiin tai oletettuihin sensuuritoiveisiin taipuminen saattaa olla yritykselle pienempi paha kuin joutuminen poistetuksi maasta.

Esimerkiksi Kiina vaatii Kiinassa toimivilta yrityksiltä Kiinan viranomaisten asettamien sensuurivaatimusten noudattamista. Monet länsimaalaiset palvelut kuten Facebook tai Twitter eivät noudata Kiinan sensuuritoiveita, ja niihin pääsy on Kiinasta estetty (Knockel & Ruan, 2022b). Microsoft puolestaan tarjoaa palveluitaan myös Kiinassa, ja niinpä esimerkiksi sen Bing-hakukone sensuroi hakutuloksia. Kanadalaisen Citizen Labin tutkijat huomasivat vuonna 2023, että Bingin poliittisia sisältöjä koskevat sensuurisäännöt ovat jopa laajempia ja vaikuttavat suurempaan määrään hakutuloksia kuin Bingin kiinalaisen pääkilpailijan Baidu-hakukoneen säännöt (Knockel ym., 2023).

Suurista yhdysvaltalaisista teknologiayhtiöistä myös Apple toimii Kiinan markkinoilla. Applelle Kiina on vieläpä hyvin merkittävä alue, sillä Apple kokoaa valtaosan tuotteistaan Kiinassa, ja vuonna 2021 noin viidennes Applen liikevaihdosta tuli Kiinasta. Vaikka Applen toimitusjohtaja Jim Cook on länsimaissa korostanut kansalaisoikeuksia ja yksityisyyttä, Kiinassa yhtiö kuitenkin noudattelee Kiinan viranomaisten vaatimuksia. Apple esimerkiksi sensuroi sovelluskauppansa kiinalaisen version sisältöä. Applen kiinalaisasiakkaille tarkoitetusta sovelluskaupasta puuttuu esimerkiksi VPN-sovelluksia, joita länsimaiden Apple-sovelluskaupoissa on tarjolla. (Nicas ym., 2021.)

Citizen Labin mukaan Apple on Kiinassa sensuroinut poliittista sisältöä myös kaiverruksista, joita asiakkaat voivat tilata joihinkin Apple-tuotteisiinsa (Knockel & Ruan, 2022a). Vuonna 2022 Apple julkaisi iOS-käyttöjärjestelmänsä versiossa 16.1.1 vain manner-Kiinassa myytyjä laitteita koskevan päivityksen, joka rajoitti Airdrop-tiedostonjakotoiminnon ”kaikille”-asetuksen päällä olon kymmeneen minuuttiin (Gilchrist, 2022). Aiemmin samana vuonna ihmisten kerrottiin jakaneen kuvia Kiinan hallintoa arvostelleista viesteistä Pekingissä

esimerkiksi metrovaunuissa pitämällä päällä Airdrop-tiedostonjakoa niin, että kuka tahansa saattoi vastaanottaa kuvan (Yuan, 2022). Hongkongissa vuoden 2019 suurmielenosoitusten aikaan samaa toiminnallisuutta käytettiin tiedon levittämiseen mielenosoitustapahtumista (Feng, 2022). Vuoden 2022 lopulla Apple otti Kiinassa testatun Airdrop-rajoituksen käyttöön maailmanlaajuisesti iOS-versiossa 16.2 (Apple, 2023).

Yritysten itsesensuuria voi aiheuttaa muukin valtio kuin se, jossa yritys toimii. Esimerkiksi Iranissa yhä useammat ulkomaiset yritykset rajoittavat pääsyä omiin sisältöihinsä ja palveluihinsa, koska pelkäävät muuten joutuvansa epäillyiksi Yhdysvaltojen asettamien talouspakotteiden rikkomisesta (Salamatian ym., 2021, s. 12).

6 Miten rajoituksia voi kiertää

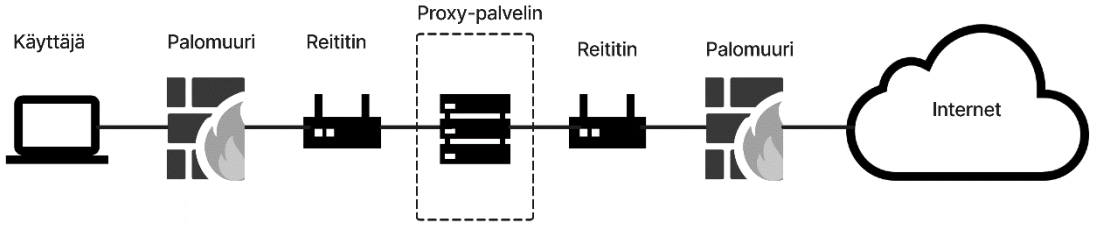
Kuten yllä on huomattu, verkkosisältöjen ja -palvelujen sensuroimiseen on käytettävissä monia toimivia ja kehittyneitä tekniikoita. On kuitenkin myös monia tekniikoita, joilla näitä rajoituksia voi kiertää.

6.1 Proxy- ja VPN-palvelimet

Yksinkertainen tapa kiertää verkkosensuuria on käyttää proxy-palvelinta. Etenkin IP-osoitteiden estoja on melko helppo kiertää proxy-palvelimilla. (Anderson, 2012, s. 2).

Proxy-palvelin on välityspalvelin, joka sijaitsee käyttäjän tietokoneen ja käytettävän internet-sivuston tai -palvelun välissä (Kuva 22). Kun käyttäjä esimerkiksi selailee verkkosivuja, normaalisti hänen selaimensa ottaa yhteyden suoraan siihen palvelimeen, jossa hänen haluamansa verkkosivu on. Jos hän käyttää proxy-palvelinta, selain ottaa ensin yhteyden proxy-palvelimelle, joka puolestaan ottaa yhteyden halutulle palvelimelle. Sensuurin kiertäminen proxyn avulla perustuu siihen yksinkertaiseen ajatukseen, että sensuurijärjestelmän näkemä liikenne käyttäjän päätelaitteelta ei kulje sensuroituun kohteeseen vaan proxy-palvelimelle. (Anderson, 2012; Microsoft, 2022; Oracle, 2010; Patil ym., 2019.)

Kuva 22: Proxy-palvelimen sijainti verkossa (Oracle, 2010)



Proxy-palvelimia on erilaisia ja eri protokollilla toimivia. Esimerkiksi OSI-mallin seitsemännessä kerroksessa eli sovelluskerroksessa toimiva HTTP-proxy toimii niin, että ainoastaan verkkoselaimen käyttämä liikenne kulkee proxy-palvelimen kautta. Kerroksessa 5 eli istuntokerroksessa toimiva SOCKS-proxy sen sijaan pystyy käsittelemään viitostason ja sitä ylempiä protokollia, kuten HTTP, HTTPS, POP3, SMTP ja FTP (Patil ym., 2019). SOCKS on

nimenomaan proxy-palvelimien avulla tapahtuvaan verkkoestojen kiertämiseen tarkoitettu verkkoprotokolla. Siitä on kaksi versiota: SOCKS4 ja SOCKs5. SOCKS4:stä poiketen SOCKs5 tukee myös käyttäjän tunnistautumista ja kykenee välittämään myös UDP-liikennettä. Yleisimmin käytetty versio SOCKS-protokollasta on SOCKs5 (Patil ym., 2019).

Proxy-palvelimen kanssa samankaltainen järjestely on VPN-palvelin, mutta erona on se, että liikenne VPN-palvelimen ja asiakaskoneen välillä on täysin salattu. VPN on lyhenne sanoista virtual private network eli virtuaalinen yksityinen verkko. VPN-järjestelmät, kuten OpenVPN ja OpenConnect, toimivat OSI-mallin tasolla 3 eli verkkokerroksessa. VPN-järjestelmät yleensä myös hoitavat asiakaskoneen kaiken liikenteen, kun tavallisesti proxy-palvelimen kautta ohjautuu vain tiettyä protokollaa käyttävä tietyn sovelluksen tai palvelun liikenne. VPN on siis eräänlainen salattu virtuaalinen putki, jonka kautta liikenne kulkee julkisen internetin yli. Salaus on yleensä vähimmäisedellytys sille, että sensuurin kiertäminen toimii, sillä nykyaikaiset sensuurimenetelmät kykenevät helposti suodattamaan salaamatonta liikennettä. (Microsoft, 2022; Xue, Ramesh, ym., 2022, s. 484.)

VPN-palvelimen voi perustaa itse, tai vaihtoehtoisesti voi käyttää kaupallisia VPN-palveluja. Monissa kaupallisissa palveluissa asiakkaalle on tarjolla monia eri VPN-palvelimia, joilla on omat julkiset IP-osoitteensa ja joita on useissa eri maissa. Tällöin käyttäjä voi valita, mitä palvelinta hän käyttää. Käytännössä käyttäjä voi siis valita, mistä maasta käsin hän haluaa olla yhteydessä internetiin. Käyttäjä voi kiertää oman sijaintimaansa internet-sensuuria valitsemalla VPN-palvelimen sellaisesta maasta, joka ei suodata tai sensuroi internetiä. (Theodorou ym., 2023.)

VPN-liikenteen eräänlainen selkäranka on VPN-liikenteessä käytetty protokolla. Valittu protokolla määrittää sen, millä tavalla VPN-yhteys muodostetaan. Käytettävissä on useita vaihtoehtoisia VPN-protokollia, joista yleisimpiä ovat OpenVPN, WireGuard, IPSec, IKEv2, L2TP ja PPTP. Lisäksi monilla suurilla kaupallisilla VPN-palvelujen tarjoajilla on omat protokollansa, jotka on joko muokattu yleisesti käytetyistä protokollista tai kehitetty alusta asti. Protokollissa on eroja esimerkiksi sen suhteen, kuinka tehokasta salausta käytetään ja kuinka nopeasti data liikkuu. (Cruz & Turner, 2023; Xue, Ramesh, ym., 2022.)

VPN-palvelujen ongelmana on, että VPN-liikenne pystytään nykyisin yhä paremmin ja tehokkaammin tunnistamaan, jolloin se voidaan myös estää. Koska VPN:t toimivat verkkokerroksessa, ne voidaan estää estämällä VPN-palvelimen IP-osoite. Esimerkiksi Kiina on viime vuosina panostanut paljon VPN-liikenteen tunnistamiseen ja estämiseen (H. Wu ym., 2022; M. Wu ym., 2023). Eri VPN-palvelujen toiminta tai toimimattomuus Kiinassa on yleinen keskustelun aihe verkkokeskusteluissa, jotka käsittelevät Kiinassa asumista tai sinne matkustamista. Keskusteluista käy ilmi, että kaupallisista VPN-palveluista valtaosa on käyttökelvottomia Kiinassa, mutta aina jokunen niistä kuitenkin toimii (esim. King_Jian, 2023; paul1rickly, 2022; Sly, 2023).

Osa VPN-palvelujen tarjoajista kehittää palvelujaan jatkuvasti, jotta ne kykenisivät läpäisemään myös sensuurimaiden palomuurit. Samaan aikaan myös palomuureja kehitetään, jotta ne onnistuisivat estämään parannellut VPN-palvelut. Kyseessä on eräänlainen kilpajuoksu, jossa toisinaan palomuuri on voitolla eli VPN:t on onnistuttu estämään ja toisinaan VPN:t ovat voitolla eli ne toimivat esimerkiksi Kiinassa (Oyaro, 2022). Osa VPN-palvelujen tarjoajista vaikuttaa myös tietoisesti päättäneet olla osallistumatta kilpajuoksuun sensuurimaiden kanssa. Esimerkiksi suomalainen F-Secure on tyytynyt toteamaan, että sen Freedome VPN -palvelu ei toimi Kiinassa (F-Secure, ei pvm.).

Kiina sallii kuitenkin tietyt VPN-palvelut. Saadakseen valtion hyväksynnän palveluntarjoajalla on oltava Kiinan teollisuus- ja informaatioteknologiaministeriön myöntämä toimilupa, ja luvan saadakseen yrityksen on täytettävä tietyt vaatimukset. Yksi tärkeimmistä vaatimuksista on, että palveluntarjoajan on oltava ainakin osittain kiinalainen. Vuonna 2023 Kiina alkoi sallia 50 prosentin ulkomaalaisen omistusosuuden VPN-palvelujen tarjoajille. (Shen, 2023.)

Kun tiedetään, että minkä tahansa VPN-palvelimen haltijalla on pääsy kaikkeen dataan, joka kulkee palvelimen kautta (esim. Migliano, 2018), on kyseenalaista, kannattaako Kiinan tai jonkin muun internetiä sensuroivan valtion sallimaa VPN-palvelua käyttää ainakaan arkaluontoiseen tai yrityssalaisuuksia sisältävään viestintään. Esimerkiksi Kiinan tiedetään harjoittavan aktiivista yritysvakoilua länsimaissa Kiinan oman teollisuuden kehittämiseksi (esim. Yong, 2023), joten olisi riskialtista käyttää VPN-palvelinta, jota hallinnoi kiinalainen tai kiinalaisenemmistöinen yritys. Kiinan on havaittu olevan taustalla myös monissa länsimaissa

tarjolla olevissa maksuttomissa VPN-palveluissa, joiden on epäilty olevan käytännössä lähinnä datankeruuoperaatioita (Migliano, 2018).

6.2 Tor

Yksi vaihtoehto sensuurin kiertämiseen on Tor-verkon käyttö. Tor (The Onion Router) on reititysjärjestelmä joka alun perin kehitettiin estämään verkkoliikenteen tarkkailua. Tor salaa web-liikenteen useaan kertaan ja ohjaa sen kohdepalvelimelle useiden proxy-palvelimien kautta, jolloin kohdepalvelin ei voi tunnistaa liikenteen alkulähdettä. Torin palvelimia nimitetään solmuiksi. Järjestelmässä on sisääntulosolmu, useita välisolmuja ja ulosmenosolmu. Välisolmuista mikään ei tiedä, mistä data on alun perin tullut ja mihin se on menossa. Välisolmut tietävät vain edellisen ja seuraavan solmun identiteetit. Jokainen solmu matkan varrella poistaa datasta yhden salauskerroksen, kunnes data saavuttaa kohdepalvelimen salaus purettuna. Keskeinen ero Torin ja VPN:n välillä on, että VPN:ssä data kulkee yhden palvelimen kautta, jota ylläpitää yksittäinen palveluntarjoaja, kun taas Tor-verkko on useista palvelimista koostuva hajautettu, vapaaehtoisten ylläpitämä järjestelmä. (Ghimiray, 2022.)

Tor-verkkoa voi periaatteessa käyttää sensuurin kiertämiseen, koska se ohjaa liikenteen välipalvelimien kautta. Käytännössä se ei kuitenkaan sovellu tähän tarkoitukseen kovin hyvin, koska useat maat, kuten Iran, Venäjä ja Kiina (Ghimiray, 2022; Quintin, 2022) ovat estäneet suorat yhteydet Tor-verkkoon. Tor-verkon estäminen on valtiolliselle sensuroijalle periaatteessa helppoa, sillä Tor-järjestelmä julkaisee tunneittain niin sanotun konsensuksen, jossa on tiedot solmuista. Tällöin sensuroijan ei teoriassa tarvitse kuin tallentaa konsensus joka tunti ja saatujen tietojen avulla estää solmujen IP-osoite–TCP-porttiparit (Ensafi ym., 2015, s. 65).

Käytännössä pelkkä solmujen estäminen ei kuitenkaan riitä. Esimerkiksi Kiinan palomuurin ja Tor-verkon ylläpitäjien välillä on ollut oma kilpajuoksunsa, jossa Toriin on kehitetty Kiinan palomuuria läpäiseviä ominaisuuksia sitä mukaa, kun Kiinan palomuuriin on kehitetty näiden läpäisyominaisuuksien estotoimia. Tor vastasi solmujen estämiseen ottamalla käyttöön yksityisiä solmuja, joiden tietoja ei julkaistu. Tällöin Kiinan palomuuri alkoi pakettien syvätutkimuksella eli DPI:llä tunnistaa Torin käyttämää TLS-kättelyä ja estää sitä, jonka

jälkeen Tor otti käyttöön menetelmiä, joilla kättelyä peiteltiin, jonka jälkeen Kiinan palomuuriin kehitettiin menetelmiä, joilla kättely pyrittiin peittelystä huolimatta tunnistamaan. (Xue, Ramesh, ym., 2022, s. 485.)

6.3 Yhteyden peittely (obfuscation)

Koska DPI-tekniikalla voidaan tunnistaa tietoliikenneprotokollia, sensuroijien on mahdollista estää esimerkiksi VPN-liikenne ja Tor-liikenne. Tätä vastaan on kehitetty erilaisia menetelmiä, joilla kielletty liikenne pyritään naamioimaan (engl. obfuscate) niin, ettei sitä tunnisteta kielletyksi liikenteeksi. Peittelyprotokollia voidaan käyttää esimerkiksi niin, että tavallinen VPN-yhteys, vaikkapa OpenVPN-protokollaa käyttävä, kääritään salatun peittelyprotokollan sisään, jotta liikennettä ei tunnistettaisi VPN-liikenteeksi (Xue, Ramesh, ym., 2022, s. 485).

Naamiointimenetelmät voidaan L. Wangin ja muiden (2015) mukaan karkeasti luokitella kolmen pääasiallisen menetelmän perusteella:

- Jokaisen lähetetyn tavun salaaminen, jotta liikenne näyttäisi täysin satunnaiselta
- Kielletyn protokollan naamioiminen näyttämään sallitulta protokollalta
- Liikenteen tunneloiminen jonkin sallitun protokollan läpi

Kaikkia kolmea naamiointitapaa on käytetty esimerkiksi Tor-järjestelmän niin sanotuissa pluggable transport -tekniikoissa, joilla on pyritty kiertämään Tor-verkon estämistä. Menetelmiä on sittemmin sovellettu myös muuhun verkkoliikenteeseen. (L. Wang ym., 2015.)

Jokainen näistä sensuuritavoista on ollut vielä 2010-luvun puolessavälissä toimiva, mutta nykyisin mikään niistä ei välttämättä toimi kaikkein nykyaikaisimpia ja tehokkaimpia sensuroijia vastaan. Sensuroivat valtiot kehittävät menetelmiään jatkuvasti, sitä mukaa kun sensuurin kiertämiseen erikoistuneet kehittäjät saavat aikaan parempia kiertomenetelmiä (esim. L. Wang ym., 2015; M. Wu ym., 2023). Sensorit ovat yleensä valtioita, ja voidaan olettaa, että ainakin Kiinan kaltaisilla suurilla valtiollisilla toimijoilla on riittävästi resursseja

periaatteessa minkä tahansa sensuurinkiertomenetelmän avaamiseen tai estämiseen, jos ne niin haluavat tehdä (LEAP, 2022).

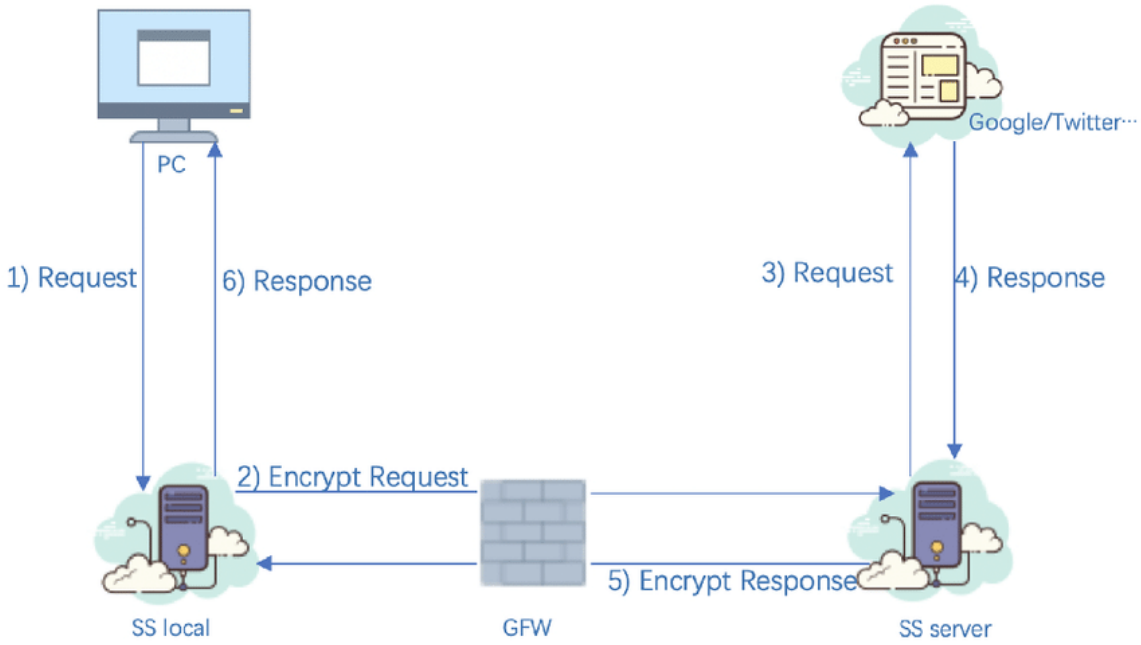
6.3.1 Liikenteen naamiointi näyttämään ei miltään

Satunnaistamalla verkkoliikenteen jokainen tavu pyritään siihen, että liikenne näyttäisi täysin satunnaiselta, eli ei miltään. Tällöin ajatuksena on, että liikenteestä ei ole tunnistettavissa minkään protokollan sormenjälkeä, jonka perusteella liikenteen voisi tunnistaa kielletyksi ja estää. Satunnaistavat naamiointijärjestelmät pyrkivät peittämään kaikki sovelluskerroksen staattiset sormenjäljet. Yleensä ne toteuttavat tämän naamiointikerroksella, joka tuottaa satunnaiselta näyttäviä bittejä. (L. Wang ym., 2015, Luku 2.)

Satunnaistamiseen perustuvia protokollia ovat esimerkiksi obfs2, obfs3, obfs4, joita käytetään alun perin Tor-liikenteen naamiointiin kehitetyssä Obfsproxyssa (Tor Project, 2012). Tähän samaan luokkaan kuuluu myös Shadowsocks, joka on etenkin Kiinassa oli erittäin suosittu sensuurienkiertoprotokolla, ennen kuin Kiinan palomuuri vuonna 2019 alkoi kyetä estämään sen käyttöä (Alice ym., 2020).

Shadowsocks-järjestelmään kuuluu käyttäjän laitteessa oleva paikallinen asiakasohjelma ja sensuroivan palomuurin ulkopuolella sijaitseva palvelin. Käyttäjän päätelaiteesta kulkee salattu yhteys Shadowsocks-asiakasohjelman kautta palomuurin läpi Shadowsocks-palvelimelle, joka hoitaa liikenteen varsinaiseen, sensuroituun kohteeseen (Kuva 23: Shadowsocksin toimintaperiaate (Cheng ym., 2020)Kuva 23). Kyseessä on siis eräänlainen VPN:n kaltainen salattu proxy-palvelin (Xue, Ramesh, ym., 2022). Samaa toimintaperiaatetta käyttää myös kehittyneempi naamiointijärjestelmä V2Ray (Project V, ei pvm.).

Kuva 23: Shadowsocksin toimintaperiaate (Cheng ym., 2020)



Liikenteen satunnaistaminen ei välttämättä ole toimiva menetelmä kaikkia sensoreita vastaan. Esimerkiksi Obfsproxy-protokollan versioita on kyetty tunnistamaan yhdistämällä entropiaan eli epäjärjestyksen määrään perustuvia testejä yksinkertaiseen heuristiseen analyysiin eli lähinnä pakettien kokojen vertailuun. Yksinkertaistettuna tämä tarkoittaa, että protokollan tunnistamiseen kelpaavan niin sanotun sormenjäljen puute on sormenjälki sekin (L. Wang ym., 2015, Luku 1).

Siihenkin on kehitetty torjuntakeinoja. Esimerkiksi Googlen Jigsaw-yksikkö on kehittänyt Shadowsocksia hyödyntävän sovelluksen nimeltä Outline, jonka käyttäjät voivat perustaa omia salattuja välityspalvelimiaan. Outlinen yhtenä ideana on, että kun ihmiset perustavat hajautetusti yksityisiä palvelimia, niitä on työläämpi estää kuin kaupallisten VPN-palveluntarjoajien samankaltaisia palveluja. Jigsaw on pyrkinyt tekemään Outlinesta verrattain helppokäyttöisen siihen kuuluvien sovellusohjelmien avulla, jotta mahdollisimman monella olisi mahdollisuus perustaa palvelimia. (Williams, 2023.)

6.3.2 Sallitun protokollan matkiminen

Matkiva naamiointijärjestelmä pyrkii tuottamaan liikennettä, joka sensuroijien DPI-järjestelmässä näyttää jonkin sallitun protokollan liikenteeltä. Tätä sallittua protokollaa

nimitetään peiteprotokollaksi. Naamiointiin voidaan käyttää esimerkiksi FTE-salausta (Format Transforming Encryption), joka muuttaa liikenteen sisällön toiseen muotoon. Jotta lopputulos näyttäisi joltain halutulta protokollalta, salatun tekstin tulee sisältää merkkijonoja tai ilmauksia, joiden perusteella DPI-järjestelmät tunnistavat sen halutulla tavalla. (L. Wang ym., 2015, Luku 2.)

Tällä menetelmällä on muokattu verkkoliikennettä muistuttamaan esimerkiksi HTTPS- tai SSH-protokollien liikennettä. Niiden kaltaisten hyvin yleisten protokollien liikennettä valtioiden on hankala estää, koska näitä protokollia tarvitaan esimerkiksi liike-elämän pyörittämiseen (LEAP, 2022). FTE-salauksella on onnistuttu kiertämään myös Kiinan sensuuria, ennen kuin Kiinan palomuuri alkoi kyetä estämään sitä (Dyer ym., 2013, Luku 6).

Matkimismenetelmässäkin on kuitenkin puutteensa. Esimerkiksi Houmansadr ja muut (2013) ovat katsoneet, että tällaisessa ”papukaijamenetelmässä” koko lähestymistapa on perustavanlaatuisesti virheellinen, koska nykyaikaisten, monimutkaisten järjestelmien matkiminen vakuuttavasti on käytännössä ylipääsemätön haaste. Yksi järjestelmistä, joiden liikennettä näissä järjestelmissä on pyritty matkimaan, on esimerkiksi Skype, joka hyödyntää useita, toisistaan riippuvia aliprotokollia ja niiden välisiä suhteita. Tällaisen kokonaisuuden matkimiseksi on täytettävä erittäin pitkä lista vaatimuksia, kun taas sensuroivat tahon tarvitsee löytää vain melko pieni epäsuhta, jonka perusteella se voi paljastaa huijauksen. Lisäksi menestyksekäs imitointi yleensä vaatii, ettei imitoida vain protokollaa yleisellä tasolla, vaan imitoidaan jotakin tiettyä protokollan sovellusta, jolloin se olisi tehtävä hyvin pieniä yksityiskohtia myöten oikein (Houmansadr ym., 2013, s. 65–66).

6.3.3 Liikenteen tunnelointi sallitulla protokollalla

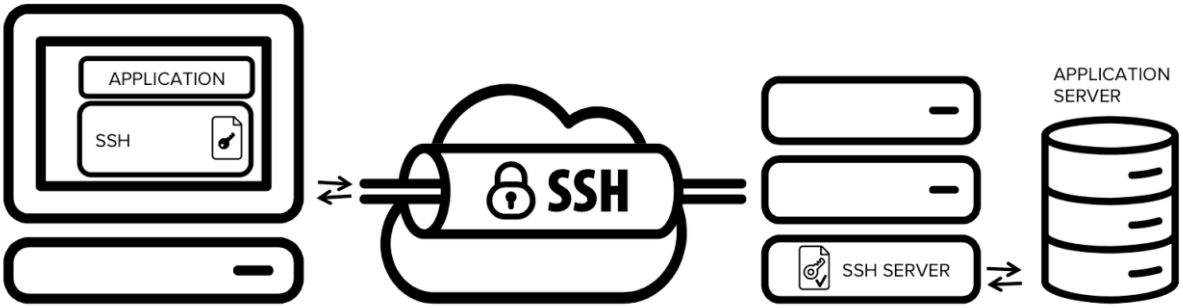
Matkimisen tilalle on kuitenkin tarjolla tehokkaampi menetelmä. Eräänlainen äärimmäinen tapa matkia jotakin toista protokollaa on tunneloida liikenne tämän protokollan läpi. Tällöin peiteprotokollana on yleensä jokin salattu protokolla (L. Wang ym., 2015, Luku 2).

Melko yksinkertainen tapa kiertää sensuuria on tunneloida verkkoliikenne vaikkapa SSH:n läpi. Lähes 30 vuotta vanha SSH eli Secure Shell on salattu tietoliikenneprotokolla, jota käytetään hyvin paljon palvelinten ylläpitoon etäyhteydellä. Ensimmäisen version siitä

julkaisi suomalainen Tatu Ylönen vuonna 1995, ja jopa 95 prosentissa internetiin kytketyistä palvelimista on SSH asennettuna. Koska SSH on niin yleinen ja tärkeä protokolla palvelimien ylläpitäjille, sensuurivaltiot eivät välttämättä pidä kaiken SSH-liikenteen estämistä järkevänä suurten sivuvaikutusten takia. (Gonano, 2023; SSH, ei pvm.; University College London, 2018.)

SHH:ta voi käyttää paitsi palvelimien etäkäyttöön myös datan siirtämiseen, joten sillä voi kiertää sensuuria tunneloimalla (englanniksi tunneling tai port forwarding). Tunnelointi tarkoittaa, että dataliikenne ohjataan salatun SSH-yhteyden läpi (Kuva 24). Periaatteessa mistä tahansa TCP/IP-portista voidaan ohjata jonkin sovelluksen käyttämä liikenne SSH-asiakasohjelman kautta salatulla SSH-yhteydellä SSH-palvelimelle, joka ohjaa liikenteen edelleen sovelluksen käyttämälle palvelimelle (SSH, 2019).

Kuva 24: SSH-tunnelointi sovellukselta palvelimelle (SSH, 2019)



Ratkaisu muistuttaa hieman VPN-yhteyttä, koska kyseessä on eräänlaisen putken muodostaminen salatulla yhteydellä verkon yli palvelimelle. Kyseessä on kuitenkin sikäli eri asia, että SSH-tunneliin ohjataan data vain tietystä sovelluksesta (SSH, 2019), kun taas VPN-yhteyden kautta ohjataan tavallisesti kaikki data kaikista sovelluksista (Microsoft, ei pvm.).

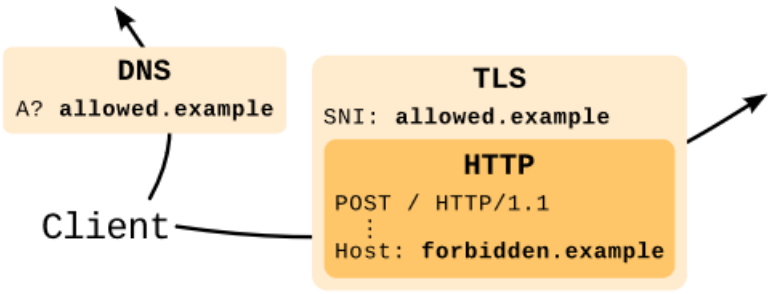
Myöskään tunnelointi toisen protokollan sisään ei aina onnistu kiertämään sensuuria, vaikka siihen perustuvia menetelmiä usein pidetään kaikkein varmimpina naamiointimenetelminä. Näitä menetelmiä sensorin on mahdollista tunnistaa koneoppimiseen perustuvalla luokittelijalla, joka analysoi verkkoliikenteestä muun muassa entropiaa. Tällaisen luokittelijan käyttö on realistista lähinnä edistyneille sensuurimaille, kuten Kiinalle. Järjestelmä on teknisesti sikäli vaativa, että DPI-järjestelmän on säilytettävä tila eli muistettava tiettyjä

muuttujien arvoja jonkin aikaa, mikä vaatii paljon resursseja, jos halutaan analysoida kaikkea verkkoliikennettä (L. Wang ym., 2015, Luku 6).

6.3.4 Domain fronting

Tunnelointiin yhdistetään usein niin sanottua domain fronting -tekniikkaa, etenkin uusimmissa sensuurinkiertojärjestelmissä. Siinä on ideana, että sovelluskerroksen HTTPS-yhteyden kohteen tiedot piilotetaan antamalla eri viestintäkerroksissa eri palvelintiedot (Kuva 25). Liikenteen uloimmissa kerroksissa eli DNS-palvelupyynnössä ja TLS-protokollan SNI (Server Name Indication) -tiedoissa näytetään jonkin sallitun palvelimen verkkotunnus, kun taas todellisen kohteen verkkotunnus on sensorilta näkymättömissä TLS-salauksen alle jäävässä HTTP-protokollan otsikkotiedon Host-kohdassa (Fifield ym., 2015).

Kuva 25: Otsikkotiedot domain frontingissa (Fifield ym., 2015, s. 47)



Domain fronting toimii myös muilla protokollilla kuin HTTPS:llä. Sitä voi käyttää myös verkkotunnuksen peittämismenetelmänä laajemmissa sensuurinkiertämisjärjestelmissä, jolloin se voi toimia HTTPS-tunnelina proxy-palvelimelle. Näkyvänä osoitteena on yleensä jokin sisällönjakeluverkko eli CDN (content delivery network). Sisällönjakeluverkot ovat maantieteellisesti hajautettuja palvelinkokonaisuuksia, jossa suuret palveluntarjoajat pyrkivät varastoimaan sisältöjä välimuisteihin lähelle loppukäyttäjiä. Nykyisin erittäin merkittävä osa kaikista internet-sisällöistä välitetään CDN-järjestelmien avulla. Tyypillinen CDN varastoi asiakkaidensa eli internet-sisällöntarjoajien sisältöjä välimuisteihin useille eri palvelimille, jotka sijaitsevat maantieteellisesti hajallaan, usein eri puolilla maailmaa. Järjestelmä ohjaa tallennettua sisältöä etsivän käyttäjän sille palvelimelle, jossa kyseinen sisältö on tallennettuna ja josta se helpoiten saadaan toimitettua juuri kyseiselle käyttäjälle. (Holowczak & Houmansadr, 2015.)

Tyypillisesti CDN-järjestelmien keskeisimpiä komponentteja ovat reunapalvelimet (edge servers) ja osoitusjärjestelmä (mapping system). Reunapalvelimia on yleensä hyvin paljon, ja niiden tehtävänä on toimittaa sisältö käyttäjälle, joko paikallisesta välimuistista tai pyytämällä sisältö sisällöntarjoajalta. Osoitusjärjestelmä puolestaan huolehtii siitä, että käyttäjä ohjataan hakemaan sisältöä siltä reunapalvelimelta, joka parhaiten pystyy toimittamaan kyseisen sisällön. Palvelimen valinta on monimutkainen prosessi, jossa osoitusjärjestelmä huomioi käyttäjän maantieteellisen sijainnin lisäksi muun muassa verkon tilan ja palvelinten kuormituksen. (Holowczak & Houmansadr, 2015.)

Sisällönjakeluverkot toimivat niin, että saadessaan pyynnön johonkin järjestelmän verkkotunnukseen reunapalvelin avaa salauksen ja välittää pyynnön siihen osoitteeseen, joka on HTTP-protokollan Host-kohdassa. Kun ollaan kiertämässä sensuuria, tässä osoitteessa toimii proxy-palvelin. Koska kyseessä on proxy-palvelin, sensuurijärjestelmä todennäköisesti estäisi pääsyn siihen, jos siihen yritettäisiin yhteyttä suoraan, mutta domain frontingin avulla yhteys onnistuu, koska palomuurin läpäisyvaiheessa palvelimen todellinen osoite on piilotettu. Koska CDN-järjestelmät eivät yleensä välitä palvelupyyntöjä muihin kuin asiakkaidensa verkkotunnuksiin, tällaisen proxy-palvelimen on oltava kyseisen CDN-palvelun asiakas. (Fifield ym., 2015, s. 47.)

Yksi variaatio domain frontingista on niin sanottu domainless fronting. Siinä jätetään verkkotunnus kokonaan pois DNS-pyynnöstä ja TLS-protokollan SNI-kohdasta. Tällöin sensorin näkökulmasta näyttää siltä, että käyttäjä joko selaa HTTPS-sivua sen IP-osoitteen perusteella tai käyttää selainta, joka ei tue SNI:tä. Tätä tapaa voidaan käyttää esimerkiksi silloin, kun ei ole käytettävissä sopivaa näkyvää verkko-osoitetta. Sopiva verkko-osoite olisi yleensä sellainen, jonka estämisestä koituisi sensorille niin suuret kielteiset sivuvaikutukset, että se kannattaisi jättää sensuroimatta. Domainless frontingia käytettäessä sensorille jää keinoiksi estää koko IP-osoite tai estää kaikki sellainen liikenne, jossa ei ole SNI:tä käytössä. (Fifield ym., 2015, s. 47.)

Verkkoa sensuroivien valtioiden on varsin hankala estää domain frontingilla toteutettuja sensuurinkiertomenetelmiä, sillä se vaatisi ensimmäisen eli sallitun verkkotunnuksen kieltämisen kokonaisuudessaan, mikä johtaisi merkittäviin sivuvaikutuksiin etenkin silloin, kun näkyvänä verkkotunnuksena on jonkin suuren pilvipalveluntarjoajan, kuten Googlen,

Amazonin tai Microsoftin verkko-osoite. Tällaisten verkko-osoitteiden estäminen ei välttämättä olisi sensuroivan valtion kannalta järkevää, koska niitä tarvitaan esimerkiksi liike-elämän pyörittämiseen (Fifield ym., 2015; Milin-Ashmore, 2023).

Myöskään domain fronting -tekniikka ei kuitenkaan aina ole toimiva tai käyttökelpoinen ratkaisu. Kasvavana ongelmana sensuurin kiertämisen kannalta on se, että suuret pilvipalveluntarjoajat kuten Microsoftin Azure (Microsoft, 2021) pyrkivät tietoturvasyistä estämään järjestelmiensä käytön domain frontingiin. Tätä perustellaan sillä, että Domain frontingia voi käyttää myös pahantahtoisiin tarkoituksiin, esimerkiksi tietomurroissa hyökkäyksen peittelyyn (Milin-Ashmore, 2023).

6.4 Yrityksen verkon ulottaminen sensuroivaan maahan

Eräänlaisena sensuurin kiertämisenä tai ainakin ohittamisena voidaan pitää myös ulkomaalaisen yrityksen oman tietoverkon ulottamista sensuroivaan maahan. Tällaisen verkon toteuttamismahdollisuudet riippuvat sensuroivan maan lainsäädännöstä ja viranomaiskäytännöistä. Tässä kyse ei varsinaisesti ole sensuurin kiertämistekniikoista vaan yrityksen verkon toteuttamisesta, mutta koska nämäkin tekniikat voivat käytännössä jossain määrin mahdollistaa myös sensuurin kiertämisen, nekin on syytä huomioida.

Kansainvälisiä verkkoinfrastruktuuripalveluja tarjoavan alankomaalaisen Expereo-yhtiön mukaan sensuuri ei välttämättä merkittävästi vaikeuta yrityksen oman tietoverkon ulottamista esimerkiksi rankasti sensuroivaan Kiinaan, sillä Kiinan palomuurin estot on suunnattu lähinnä tavallisille Kiinan kansalaisille, kun taas yritykset voivat perustaa SD-WAN-verkkoja (Expereo, 2021).

Yrityksellä on käytännössä käytettävissä kolme tekniikkaa oman verkkonsa ulottamiseksi sensuroiviin maihin: oma verkkoyhteys, MPLS ja SD-WAN (Microsoft, 2023). Se, mitä näistä voi käyttää, riippuu yrityksen tarpeiden, maan verkkoarkkitehtuurin ja kustannusten lisäksi siitä, mitä tekniikoita maa tai sen internet-operaattorit sallivat. Usein eri tekniikoita kannattaa yhdistää toisiinsa. Mainittujen tekniikoiden käytön sallii esimerkiksi Kiina, kunhan yhteydet ostetaan joltain Kiinan kolmesta suuresta valtiollisesta internet-palveluntarjoajasta (Musthaler, 2019; Weber.digital, ei pvm.).

6.4.1 Oma verkkoyhteys

Oma verkkoyhteys eli DIA (dedicated internet access) tarkoittaa vain yhteyden ostaneen yrityksen käytössä olevaa suoraa yhteyttä julkiseen internetiin. Tällaisia yhteyksiä voi ostaa internet-operaattoreilta. Niiden nopeus ja muut ominaisuudet määritellään palvelun myyjän kanssa tehtävällä sopimuksella. (Woolridge, 2021.)

Ainakin osa internetiä sensuroivista maista sallii yrityksille omia internet-yhteyksiä, kunhan yrityksen sitoutuvat noudattamaan tiettyjä viranomaisten vaatimia sääntöjä. Esimerkiksi Kiinasta on mahdollista saada hongkongilaisilta operaattoreilta PCCW:ltä tai Hong Kong Telecomilta oma verkkoyhteys Hongkongiin, joka on huomattavasti kevyemmin sensuroitu kuin Manner-Kiina (Microsoft, 2023). Myös Myanmarissa on vuoden 2021 sotilasvallankaappauksen jälkeen ainakin oletettu, että suurille yrityksille tullaan sallimaan DIA-yhteyksiä ulkomaailmaan, kunhan yrityksen lupaavat olla arvostelematta sotilasjunttaa (International Crisis Group, 2021).

Omien internet-yhteyksien käytössä yrityksen on syytä huomioida, että niitä yleensä saa vain valtion hyväksymiltä internet-palveluntarjoajilta, jotka usein ovat myös valtion omistamia tai vähintäänkin valtion kontrolloimia. Tällöin yrityksen on pohdittava, missä määrin voi luottaa siihen, ettei verkkoja esimerkiksi vakoilla.

6.4.2 MPLS

Yksi tapa järjestää yrityksen verkko sensuroivaan maahan on MPLS (Multiprotocol Label Switching). Kyseessä on tekniikka, jossa data liikkuu haluttuun kohteeseen lipukkeiden (labels) perusteella, sen sijaan, että se liikkuisi IP-osoitteiden perusteella kuten yleensä. MPLS-tekniikkaa käytetään usein WAN-verkkoihin esimerkiksi yrityksen toimipisteiden ja pääkonttorin tai datakeskusten välillä. (Palo Alto Networks, ei pvm.-a.)

MPLS on yleensä nopeampi kuin perinteinen IP-reititys. Lisäksi sitä pidetään tietoturvallisena ja luotettavana yhteytenä, mutta se on myös kalliimpi ja vähemmän joustava, etenkin pitkillä etäisyyksillä. Se ei myöskään ole palveluntarjoajariippumaton kuten IP-reititys. Lisäksi MPLS soveltuu huonosti nykyaikaisten pilvipalvelujen käyttöön. (Palo Alto Networks, ei pvm.-a, ei pvm.-b; Weber.digital, ei pvm.)

Ongelmaksi sensuurimaissa voi MPLS:n kohdalla muodostua se, että vaikka järjestelmä on teknisesti turvallinen, tietoturva ei kuitenkaan käytännössä välttämättä ole taattu, koska joudutaan luottamaan paikallisiin palveluntarjoajiin, jotka ovat riippuvaisia paikallisista viranomaisista. Esimerkiksi Kiinassa Hongkongin ja Macaon erityishallintoalueita lukuun ottamatta MPLS-yhteyksiä tarjoavat vain Kiinan kolme suurta teleoperaattoria China Telecom, China Unicom ja China Mobile, jotka ovat kaikki Kiinan valtion enemmistöomistamia yhtiöitä (Weber.digital, ei pvm.).

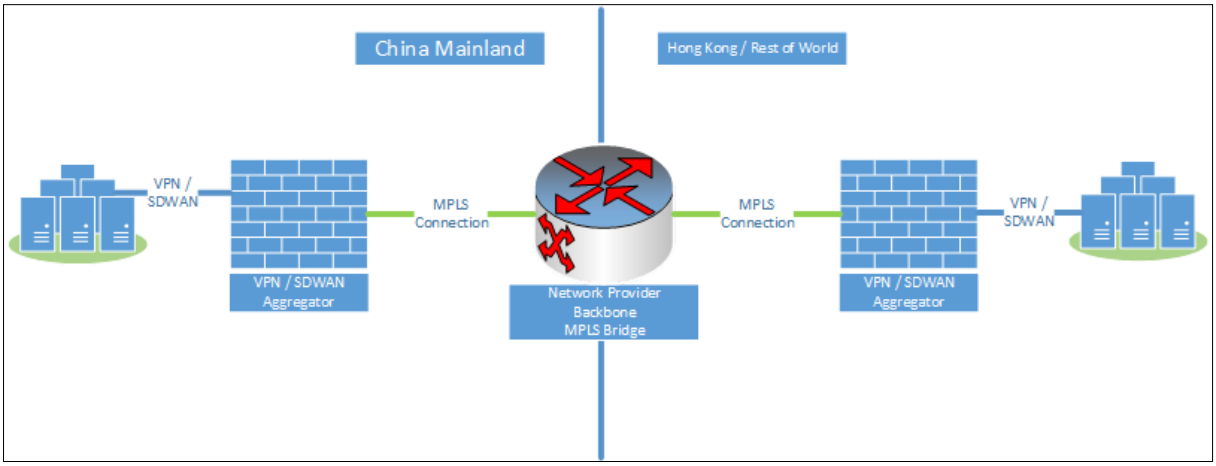
Kiinaa johtavalla kommunistisella puolueella on erittäin paljon valtaa kaikkiin kiinalaisiin yrityksiin, ja varsinkin valtionyhtiöihin (Kawase, 2022). Siksi on mahdollista, että antamalla verkkonsa suuren kiinalaisen teleoperaattorin hallinnoitavaksi ulkomainen yritys käytännössä antaa verkkonsa Kiinan viranomaisten hallinnoitavaksi. Tämä ei välttämättä sovi yrityksille, joiden verkossa liikkuu luottamuksellista tietoa, kuten salassa pidettäviä teknisiä yksityiskohtia yrityksen tuotteista. Sensuroivista maista esimerkiksi Kiinan tiedetään harjoittavan varsin laajaa ja systemaattista teollisuusvakoilua (esim. Bhattacharjee, 2023). MPLS-yhteys voidaan rakentaa VPN-yhteydeksi, joka on salattu, mutta tällöinkin VPN on lisensoitava teleyhteyksiä tarjoavien valtionyhtiöiden kautta, joten se ei ratkaise vakoiluriskiin liittyviä ongelmia (Weber.digital, ei pvm.).

6.4.3 SD-WAN ja yhdistelmäratkaisut

SD-WAN (software defined WAN) on ohjelmallisesti rakennettu WAN-verkko, joka ei perustu fyysisiin verkkolaitteisiin ja kaapelointeihin samalla tavoin kuin perinteinen WAN-verkko. SD-WAN-tekniikalla voidaan yhdistää yrityksen eri paikoissa sijaitsevia datakeskuksia, toimistoja ja pilviresursseja eräänlaiseksi virtuaaliseksi WAN-verkoksi salatuilla yhteyksillä julkisen internetin yli. Yhdysvaltalaisen IT-konsulttiyhtiö Gartnerin määritelmän mukaan SD-WAN-verkot on tarkoitettu lähinnä yrityksen eri paikoissa sijaitsevien toimipisteiden yhdistämiseen yrityksen muihin sijainteihin ja pilvipalveluihin. SD-WAN-tekniikan käyttö yrityksissä on viime vuosina yleistynyt, samalla kun pilvipalvelujen käyttö on yleistynyt, koska SD-WAN soveltuu pilvipalvelujen käyttöön paremmin kuin esimerkiksi MPLS (Cooney & Shaw, 2022; Gartner, 2023.)

Jotta SD-WAN toimisi myös sensuurin ulkopuolella, se on kytkettävä kansainväliseen internetiin. Tähän tarvitaan yleensä joko DIA- tai MPLS-yhteyttä (Kuva 26). Esimerkiksi Kiinan tapauksessa SD-WAN-verkot voi yhdistää Kiinan palomuurin ulkopuoliseen maailmaan käytännössä DIA- tai MPLS-ratkaisuilla joko Hongkongin, Singaporen, Etelä-Korean tai Japanin kautta (Microsoft, 2023; Musthaler, 2019).

Kuva 26: SD-WAN Manner-Kiinasta Hongkongin kautta (Microsoft, 2023)



Kuten todettu, yrityksille tarkoitettujen verkkoratkaisujen toimivuus sensuroivassa maassa riippuu kyseisen maan viranomaisten asettamista rajoista. Säännöt voivat myös yllättäen muuttua. Esimerkiksi Kiina ilmoitti vuonna 2018 estävänsä ”kaupallisilta käyttäjiltä” eli yrituksiltä SD-WAN-liikenteen, kunnes ne hankkivat lisenssin, jollaista siihen asti oli vaadittu vain internet-palveluntarjoajilta (Garson, 2018).

6.5 Roaming-palvelut ja satelliittiyhteydet

Sensuurin kiertämiseen voi käyttää myös muita ratkaisuja kuin varsinaisia sensuroivan palomuurin läpäisytekniikoita. Osa sensuroivista maista sallii palomuurin ohittamisen esimerkiksi mobiililaitteilla tietyissä tapauksissa ulkomaalaisille.

6.5.1 Roaming

Osassa sensuroivia maita sensuurin voi ohittaa mobiiliverkossa käyttämällä ulkomaista liittymää roaming- eli verkkovierailutilassa, jossa ulkomaisen teleoperaattorin liittymä toimii

toisen operaattorin verkossa. Osassa sensuroivista maista ainakin osa ulkomaisista mobiililiittymistä on rajattu sensuurin ulkopuolelle. Maat ja mobiilioperaattorit eivät yleensä aktiivisesti mainosta tätä ominaisuutta eivätkä kerro, millä teknisillä keinoilla liikenne reititetään sensuurin ohi.

Yhdysvalloissa asuville on tarjolla esimerkiksi erityisesti roaming-käyttäjille suunnattu Google Fi -liittymä, jolla on voinut roaming-tilassa ohittaa ainakin Kiinan palomuurin (Benetti, 2021; Imel, 2018). Myös muilla, lähinnä matkailijoille suunnatuilla, pelkästään roaming-käyttöön tarkoitetuilla mobiililiittymillä on raportoitu olevan mahdollista ohittaa Kiinan palomuuri. Esimerkiksi Nomad-nimistä liittymää myyvä yhtiö mainitsee tällaisen mahdollisuuden omassa markkinointimateriaalissaan (Nomad, 2023).

6.5.2 Satelliitti

Koko sensuurijärjestelmän voi ohittaa kytkeytymällä suoraan jonkin demokraattisessa maassa toimivan palveluntarjoajan satelliittiverkkoon. Internetiä sensuroivissa maissa satelliittiyhteyksien käyttö on kuitenkin usein kielletty ilman viranomaisten lupaa, samaan tapaan kuin VPN-yhteyksien käyttö tietyissä maissa. Esimerkiksi Iran on vaatinut satelliittidataoperaattoreita hankkimaan Iranin viranomaisilta luvat järjestelmiensä käytölle (Iran International, 2023).

Satelliittien kautta kulkevat datayhteydet kuitenkin toimivat periaatteessa missä tahansa, jos satelliitteja on riittävästi. Esimerkiksi SpaceX-yhtiö lupaa, että sen Starlink-järjestelmä toimii ”lähes kaikkialla maailmassa”. Maat, joissa Starlink-yhteyksiä on myynnissä, ovat kuitenkin lähinnä demokraattisia länsimaita, joissa internetiä ei kovin merkittävästi sensuroida. Alalla pitkään toiminut satellittidatayhteyksien tarjoaja Inmarsat puolestaan lupaa, että sen järjestelmä toimii ”missä tahansa päin maailmaa” (”anywhere in the world”) (Inmarsat, ei pvm.; Starlink, ei pvm.).

Myöskään satelliittiyhteydet eivät välttämättä ole kaikissa olosuhteissa luotettavia. Esimerkiksi sota-alueilla tai niiden läheisyydessä sotivat osapuolet saattavat tahallaan häiritä satelliittien käyttämiä tietoliikenneyhteyksiä (esim. Wilkenfeld, 2023).

7 Käytännön esimerkki tietoturvallisesta sensuurin kiertämisestä

Jotta ymmärrettäisiin, mitä sensuurin kiertäminen käytännössä vaatii, on hyvä perustaa testi- ja demonstrointimielessä oma sensuurin kiertämisjärjestelmä. Järjestelmän tulee täyttää joitakin perusvaatimuksia. Sen on oltava:

- Tietoturvallinen
- Melko nopea
- Luotettava
- Toimiva myös maissa, joissa on kehittynyt sensuurijärjestelmä
- Helppo käyttää

Tietoturvallinen merkitsee käytännössä salattua yhteyttä ja sitä, että koko järjestelmä on luotettavan tahon hallinnoima. Kaikkein luotettavin taho on todennäköisesti käyttäjä itse. Esimerkiksi kaupalliset VPN-yhteydet, kuten Astrill, Express VPN, Surfshark tai muut vastaavat palvelut, käyttävät salattua yhteyttä, mutta niitä hallinnoivat kyseisiä palveluja tarjoavat yritykset, jolloin myös palvelujen läpi kulkeva data on niiden käsissä. Siksi tässä yhteydessä kannattaa perustaa oma, salattua yhteyttä käyttävä välityspalvelin. Tietoturvaa lisää se, jos järjestelmän lähdekoodi on avoin eli kenen tahansa tarkastettavissa esimerkiksi mahdollisten takaporttien varalta.

Nopeus ja luotettavuus riippuvat paljon niiden yksityisten tai julkisten verkkoyhteyksien laadusta ja ominaisuuksista, joita yhteyden muodostamiseksi aiotaan käyttää. Ne riippuvat kuitenkin merkittävästi myös protokollasta, jolla yhteys aiotaan muodostaa. Protokollasta riippuu myös se, kuinka hyvin järjestelmä toimii kehittyneiden sensuurijärjestelmien maissa. Monet maat kykenevät tunnistamaan ja estämään esimerkiksi hyvin yleisesti käytetyn OpenVPN-protokollan. Käytetyn järjestelmän yleisyys kuitenkin vaikuttaa helppokäyttöisyyteen, sillä harvinaisiin järjestelmiin on usein vaikea löytää ohjeita ja tukea, ja niissä voi olla myös ohjelmistovirheitä, jotka aiheuttavat yllättäviä vikatilanteita.

Helppokäyttöisyys on osin ristiriidassa myös sensuurinläpäisykyvyn kanssa, sillä kehittyneetkään sensuurijärjestelmät eivät usein kykene estämään esimerkiksi kaikkein uusimpia ja harvinaisimpia protokollia, koska niiden tunnistamisjärjestelmiä ei ole vielä

ehditty kehittää. Siksi käytetyn järjestelmän tulisi olla jonkinlainen kompromissi kaikkein uusimman tekniikan ja jo jonkin aikaa käytössä olleen, mutta paljon käytetyn ja testatun tekniikan välillä. Käytettävissä olevista nykyaikaisista järjestelmistä kyseeseen voisi tässä yhteydessä tulla joko Shadowsocks tai samankaltaiseen tekniikkaan perustuva NaiveProxy.

7.1 Shadowsocks

Shadowsocks on erityisesti Kiinan palomuurin kiertämiseen tarkoitettu järjestelmä, joka jakaa proxy-palvelimen kahteen osaan: paikalliseen palvelimeen ja etäpalvelimeen. Näin liikenne maasta ulos mahdollisten sensuurijärjestelmien läpi voidaan salata kokonaan, jolloin se voidaan myös yrittää tehdä tunnistamattomaksi. Kuten kohdassa 6.3.1 todettiin, Shadowsocks pyrkii satunnaistamaan verkkoliikenteen niin, että se näyttää ”ei miltään”.

Alun perin Shadowsocksin kehitti vuonna 2012 kiinalainen ohjelmoija, joka käytti GitHub-palvelussa käyttäjänimeä Clowwindy (Clowwindy, 2012). Noin kolme vuotta myöhemmin hän ilmoitti, että poliisi oli ottanut häneen yhteyttä ja kehottanut keskeyttämään työskentelyn projektin parissa ja poistamaan GitHubissa jaetun ohjelmakoodin (Clowwindy, 2015). Avoin lähdekoodi on kuitenkin mahdollistanut järjestelmän jatkokehityksen, ja Shadowsocksista tuli pitkäksi aikaa yksi suosituimmista sensuurin kiertämisjärjestelmistä Kiinassa (Alice ym., 2020).

Shadowsocks olisi yksi mahdollinen järjestelmä sensuurin kiertämiseen, mutta Kiinan palomuurin on raportoitu kykenevän estämään sen käytön. Kiinan erittäin tehokkaan palomuurinkin voisi mahdollisesti kiertää yhdistämällä Shadowsocksin johonkin domain fronting-ratkaisuun, mutta koska nyt ollaan hakemassa mahdollisimman yksinkertaista ratkaisua, se ei ole ensisijainen vaihtoehto.

7.2 NaiveProxy

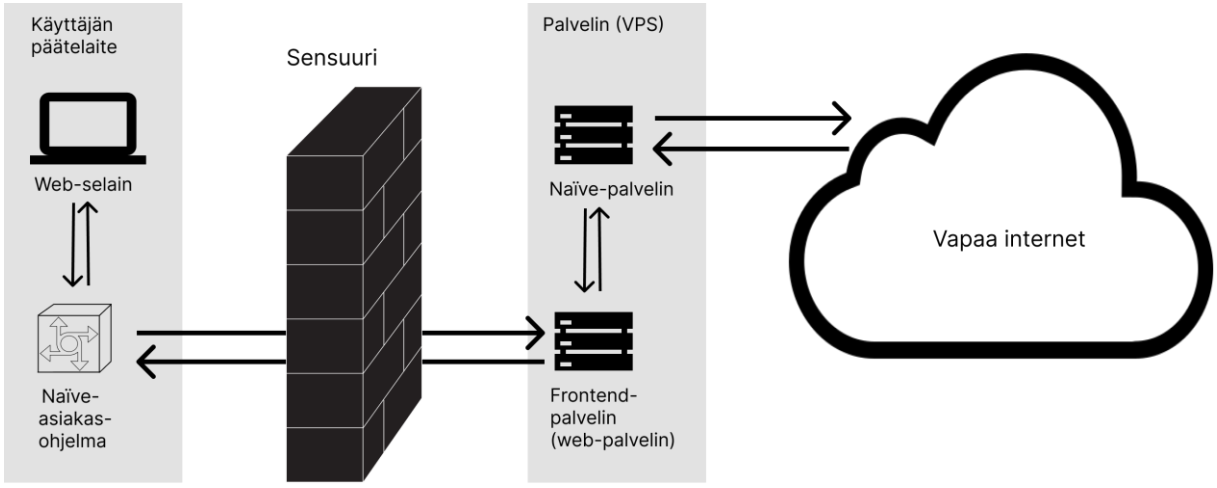
Kun Kiina lokakuussa 2022 onnistui estämään useiden TLS-protokollaa käyttävien sensuurinkiertoratkaisujen kuten Xrayn ja V2Rayn käytön, Kiinan verkkosensuuria seuraavan GFW Report -projektin mukaan eston ei havaittu koskeneen NaiveProxy-nimistä järjestelmää (GFW-report, 2022). Siksi NaiveProxy vaikuttaa paremmalta tavalta sensuurin kiertämiseen

kuin Shadowsocks. Kuten aiemmin on todettu, sekä sensuurijärjestelmät että niiden kiertämisjärjestelmät kehittyvät jatkuvasti, joten tilanne voi muuttua nopeastikin.

Naiveproxy on huonoon havaittavuuteen ja hyvään läpäisykykyyn pyrkivä sensuurinkiertämisjärjestelmä, jonka kehittämiseen osallistuu joukko anonyymeja, mahdollisesti kiinalaistaustaisia kehittäjiä (klzgrad, 2023a). Järjestelmä käyttää vapaan ja avoimen Chromium-selaimen protokollapinoa eli kirjastoa, joka määrittelee, kuinka verkkoliikenne hoidetaan. Chromium-protokollapinon käytöllä pyritään kehittäjien mukaan siihen, ettei liikenteen ominaispiirteitä voisi tunnistaa.

NaiveProxy-järjestelmä koostuu Shadowsocksin tapaan asiakasohjelmasta ja palvelimesta, mutta palvelin on jaettu frontend-palvelimeen ja Naïve palvelimeen (Kuva 27). Liikenne palomuurin läpi kulkee asiakasohjelman ja frontend-palvelimen välillä, ja Naïve-palvelin välittää liikennettä Frontend-palvelimen ja sensuroimattoman internetin välillä. Nämä palvelimet voi asentaa vaikkapa virtuaalipalvelimelle (VPS, virtual private server), joka sijaitsee jonkin demokraattisen länsimaan sensuurisäännösten piirissä. Frontend-palvelimena käytetään web-palvelinta. Sen tehtävänä on piilottaa varsinainen proxy-palvelin eli Naïve-palvelin yleisesti käytetyn, sovelluskerrosta käyttävän reitityksen taakse (klzgrad, 2023a). Sovelluskerrosta käyttävä reititys on tässä tapauksessa HTTPS-liikennettä. Kyseessä on siis käytännössä liikenteen tunnelointi sallitulla protokollalla, jota sensuroijat eivät pyri estämään. Tällaisen tekniikan perusajatus esiteltiin kohdassa 6.3.3.

Kuva 27: NaiveProxy -järjestelmän arkkitehtuuri (klzgrad, 2023a)



7.3 Palvelimen perustaminen vaiheittain esiteltynä

Koska NaiveProxy vaikuttaa kriteerit täyttävältä ja nykyaikaisia sensuurinkiertoratkaisuja melko hyvin edustavalta ratkaisulta, rakennetaan siihen perustuva järjestelmä. Näin on tarkoitus lähinnä demonstroida, mitä järjestelmän perustaminen ja käyttäminen vaatii. Nyt pystytettävä järjestelmä on tarkoitettu vain lyhytaikaiseen esittely- ja testauskäyttöön, eikä sitä ole tarkoitus ottaa varsinaiseen tuotantokäyttöön. Järjestelmä pyritään rakentamaan mahdollisimman halvalla. Tässä yhteydessä ei pohdita esimerkiksi palvelimen resurssien tarvetta, vaan järjestelmä perustetaan minimiresursseilla.

7.3.1 Resurssien hankkiminen

Jotta järjestelmä saadaan rakennettua, tarvitaan toimialuenimi (domain-nimi) ja palvelin. Toimialuenimi toimii tässä yhteydessä web-osoitteena.

Toimialuenimeksi valitaan sopiva nimi, ja se rekisteröidään halpoja domaineja myyvässä rekisteröintipalvelussa. Tällaisia palveluja on maailmalla useita. Osa niistä rekisteröi toimialuenimiä jopa maksutta. Tätä projektia varten rekisteröitiin toimialuenimi, mutta tietosuojasyistä toimialueen ja rekisteröintipalvelun nimi jätetään tässä mainitsematta. Toimialuenimi on muotoa [jotain.jotain]. Se rekisteröitiin vuodeksi ja se maksoi noin kaksi euroa. Kuten hinnasta voi päätellä, kyseessä ei ole erityisen kysytty verkko-osoite.

Sillä aikaa, kun juuri hankittu toimialuenimi odottaa tallentumistaan rekisterinpitäjän tietokantaan, hankitaan palvelin. Tähän tarkoitukseen kelpaa virtuaalipalvelin, joka sijaitsee jossakin sensuroimattomassa maassa, josta on pääsy vapaaseen internetiin.

Koska Digital Ocean -palvelussa on tarjolla maksuton 60 päivän kokeilujakso, perustetaan virtuaalipalvelin Digital Oceanin pilveen. Perustetaan siellä niin sanottu droplet eli Linux-virtuaalipalvelin, joka sijaitsee Frankfurtissa Saksassa ja jossa on Ubuntu 22.04 (LTS) -käyttöjärjestelmä.

Virtuaalipalvelimen hallinnointiin tarvitaan SSH-asiakasohjelma. Sellaiseksi valitaan vapaa, avoimen lähdekoodin ohjelma PuTTY. Kun on kirjauduttu uudelle palvelimelle root-käyttäjänä SSH-yhteydellä, päivitetään palvelimen käyttöjärjestelmä. Lisäksi vaihdetaan

palvelimen root-käyttäjälle saman tien uusi, vahva salasana ja päivitetään palvelimen ohjelmistot (Komento 1).

Komento 1: Palvelimen päivitys

```
apt update && apt upgrade.
```

Toimialuenimen välittäjän web-käyttöliittymän avulla käydään luomassa DNS-osoitus (DNS record), jossa pannaan toimialuenimi osoittamaan äsken luodun virtuaalipalvelimen IP-osoitteeseen. DNS-osoitus on tässä tapauksessa tyyppiä A (address) ja osoituksen isäntäkone eli host on tyyppiä www.

Kun jonkin ajan kuluttua kirjaudutaan palvelimelle SSH-yhteydellä käyttäen osoitteena toimialuenimeä, joka on muotoa www.jotain.jotain, palvelin löytyy, mikä tarkoittaa, että toimialuenimi on rekisteröitynyt DNS-tietokantaan ja DNS-osoitus toimii.

7.3.2 Palvelimen valmistelu

Asetetaan palvelimen nimeksi oma toimialuenimi ja lisätään nimi tiedostoon /etc/hosts. Käynnistetään palvelin uudelleen komennolla reboot. Tarkistetaan komennoilla hostname, että äsken tehty koneen nimen muutos on voimassa uudelleenkäynnistyksen jälkeenkin.

Tehdään palvelimen palomuuriin tarpeelliset asetukset. Ohjeena palomuuriasetusten tekemiseen käytetään Technical Blog -nimisessä blogissa vuonna 2019 julkaistua NaiveProxyn asennusohjetta, joka on muilta osin pääosin vanhentunut (Technical Blog, 2019).

Palomuuriasetusten määrittämisessä hyödynnetään Linuxin ytimeen kuuluvaa nftables-ohjelmaa, joka käyttää Linuxin netfilter-järjestelmää. Nftables on Linuxissa korvannut aiemmin paljon käytetyn iptablesin, ja se on nyt käytetyssä käyttöjärjestelmäversiossa valmiiksi asennettuna. Palomuuri on kuitenkin vielä otettava käyttöön (Komento 2).

Komento 2: Palomuurin aktivoiminen

```
systemctl enable nftables
```

```
systemctl start nftables
nft list ruleset
```

Viimeisellä komennolla varmistetaan, että järjestelmässä on palomuurisääntötaulukko. Seuraavaksi annetaan sarja komentoja, joilla luodaan joukko sääntöjä kyseiseen taulukkoon (Komento 3).

Komento 3: Palomuurisääntöjen luominen

```
nft add rule inet filter input ct state related,established counter
accept && nft add rule inet filter input iif lo counter accept && nft
add rule inet filter input tcp dport 22 ip saddr [OMA IP-OSOITE]/32
counter accept && nft add rule inet filter input tcp dport {80, 443}
counter accept && nft add rule inet filter input counter drop && nft
list ruleset > /etc/nftables.conf
```

Komentojen välissä olevat merkit `&&` kehottavat järjestelmää suorittamaan seuraavan komennon vain siinä tapauksessa, että edeltävän komennon suorittaminen onnistuu. Ensimmäinen komento lisää palomuuriin säännön, joka sallii palvelimelle kaiken luotujen yhteyksien liikenteen (established) ja niihin liittyvän (related) liikenteen. Toinen sääntö sallii palautuvan liikenteen eli loopback-liikenteen. Kolmas sääntö sallii SSH-liikenteen porttiin 22 oman päätelaitteen julkisesta IP-osoitteesta, jotta palvelinta voidaan hallinnoida SSH-yhteydellä. Tietosuojasyistä IP-osoite ei ole näkyvissä. Neljäs sääntö sallii liikenteen portteihin 80 ja 443 eli HTTP- ja HTTPS-liikenteen. Viides sääntö kieltää kaiken odottamattoman liikenteen. Lopuksi kuudennella komennolla säännöt tallennetaan nftablesin asetustiedostoon, jotta ne tulevat voimaan myös palvelimen seuraavan käynnistyksen yhteydessä.

Nft-komennoissa inet tarkoittaa osoiteperhettä, joka kattaa sekä IPv4- että IPv6-liikenteen. Kirjainyhdistelmä ct viittaa netfilter-järjestelmän yhteyksienseurantajärjestelmään (Connection Tracking System), joka hallitsee datapakettien ja palvelimen muodostamien yhteyksien välisisä suhteita. State viittaa yhteyden tilaan. Counter-komennolla käynnistetään pakettilaskuri.

7.3.3 Web-palvelimen asentaminen palvelimelle

Seuraavaksi palvelimelle asennetaan web-palvelin. Maailmalla yleisimpiä web-palvelimia ovat Nginx ja Apache (W3Techs, 2023), mutta NaiveProxyn kehittäjät kehottavat käyttämään

harvinaista Caddy-web-palvelinohjelmistoa (klzgrad, 2023a). Sen asentaminen vaati Go-ohjelmointikielen (Go, ei pvm.). Gon asentamisessa sovelletaan TinrLin-nimisen kiinalaisen GitHub-käyttäjän laatimaa ohjetta (TinrLin, 2023).

Asennetaan palvelimelle tarpeelliset ohjelmat wget, socat ja curl, haetaan Go-tiedosto, puretaan se /usr/local/-hakemistoon, viedään tieto Go-ohjelman sijainnista PATH-ympäristömuuttujaa varten /etc/profile-tiedostoon, ajetaan kyseinen profiilitiedosto ja lopuksi listataan asennetun Go-ohjelman versio (Komento 4).

Komento 4: Go-kielen ja sen riippuvuuksien asennus

```
apt -y install wget socat curl && wget -c
https://go.dev/dl/go1.21.1.linux-amd64.tar.gz -O - | tar -xz -C
/usr/local && echo 'export PATH=$PATH:/usr/local/go/bin' >
/etc/profile && source /etc/profile && go version
```

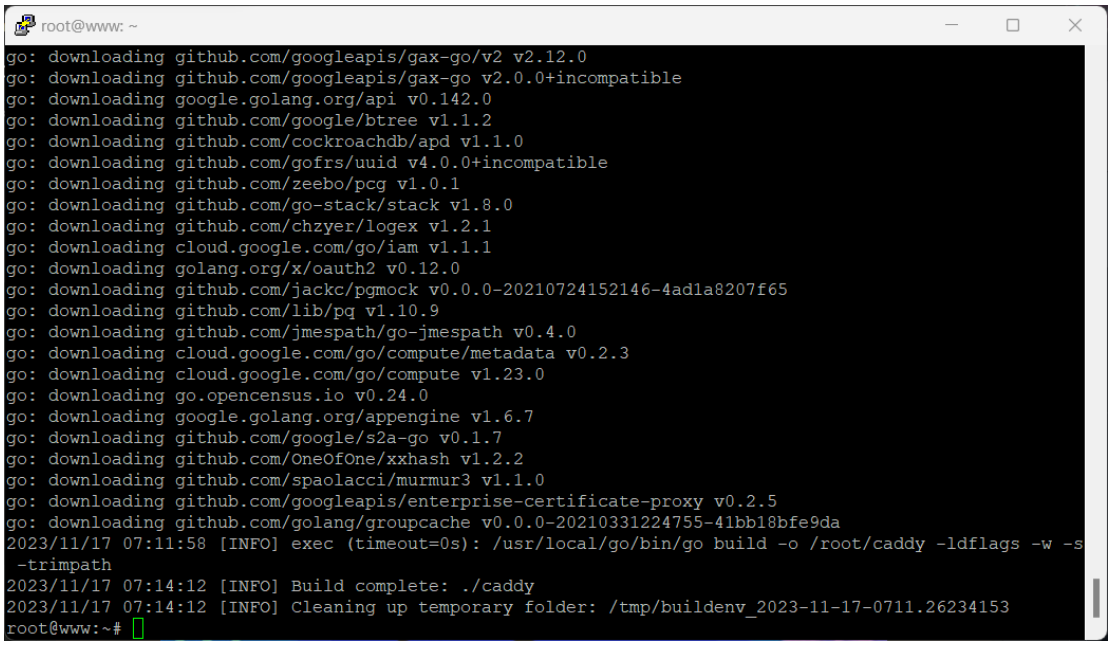
Komentosarjan viimeisen komennon tuloksena Go-ohjelman versionumero tulostuu, mikä tarkoittaa, että Go on asennettu ja lisäksi tallentunut PATH-muuttujaan oikein. Nyt voidaan asentaa Caddy. Tehdään se Go-ohjelmalla hyödyntäen GitHub-käyttäjä TinrLinin ohjetta (TinrLin, 2023) (Komento 5).

Komento 5: Caddyn ja lisäosien asennus Gon avulla

```
go install github.com/caddyserver/xcaddy/cmd/xcaddy@latest &&
~/go/bin/xcaddy build --output caddy --with github.com/mholt/caddy-l4
--with github.com/caddy-dns/cloudflare --with github.com/caddy-
dns/duckdns --with github.com/mholt/caddy-dynamicdns --with
github.com/mholt/caddy-events-exec --with github.com/WeidiDeng/caddy-
cloudflare-ip --with github.com/mholt/caddy-webdav --with
github.com/caddyserver/forwardproxy@caddy2=github.com/klzgrad/forwardp
roxy@naive && setcap cap_net_bind_service=+ep ./caddy && chmod +x
caddy && mv caddy /usr/bin/
```

Komento asentaa Xcaddy-työkalun, joka asentaa Caddyn ja siihen kuuluvan Forwardproxy-lisäosan sekä joukon muita lisäosia. Caddy-palvelin tarvitsee Forwardproxy-lisäosan voidakseen toimia aiotulla tavalla frontend-palvelimena. Komentosarjan viimeiset komennot antavat Caddy-prosessille oikeuden käyttää tiettyjä portteja ilman root-oikeuksia, tekevät siitä ajettavan ja siirtävät ohjelmatiedoston /usr/bin-hakemistoon. Asentaminen kestää jonkin aikaa, ja lopuksi tulee ilmoitus, että asennus on valmis (Kuva 28).

Kuva 28: Palvelimen konsolinäkymä, kun Caddy on asennettu



Toimiakseen Caddy tarvitsee myös system unit -tiedoston systemd-järjestelmää varten. Sellaisena käytetään GitHub-käyttäjä TinrLinin tiedostoa nimeltä caddy.service (TinrLin, 2023), joka tallennetaan hakemistoon /etc/systemd/system/ (Komento 6).

Komento 6: Systemd-asetustiedoston haku

```
wget -P /etc/systemd/system
https://raw.githubusercontent.com/TinrLin/NaiveProxy-
installation/main/caddy.service
```

Caddy tarvitsee lisäksi asetukset sisältävän tiedoston. Tämä voidaan toteuttaa joko niin sanotulla caddyfile-tiedostolla tai json-muotoisella tiedostolla (Caddy Documentation, ei pvm.). Käytetään json-tiedostoa, jonka pohja saadaan TinrLin-käyttäjän GitHub-tililtä (TinrLin, 2023) (Komento 7).

Komento 7: Caddyn asetustiedoston haku

```
wget -O /usr/local/etc/caddy.json
https://raw.githubusercontent.com/TinrLin/NaiveProxy-
installation/main/caddy_443.json
```

Komento tallentaa tiedon hakemistoon /usr/local/etc/. Tiedosto sisältää suuren joukon Caddy-palvelimen asetuksia (Ohjelmakoodi 1).

Ohjelmakoodi 1: Caddy-palvelimen asetukset (TinrLin, 2023)

```
{
 "storage": {
  "module": "file_system",
  "root": "/etc/ssl"
 },
 "apps": {
  "http": {
   "servers": {
    "srvh2c": {
     "listen": [":443"],
     "routes": [
      {
       "handle": [
        {
         "handler": "forward_proxy",
         "auth_user_deprecated": "oma_käyttäjätunnus",
         "auth_pass_deprecated": "oma_salasana",
         "hide_ip": true,
         "hide_via": true,
         "probe_resistance": {}
        }
       ]
      },
      {
       "handle": [
        {
         "handler": "headers",
         "response": {
          "set": {
           "Strict-Transport-Security": ["max-age=31536000; includeSubDomains;
preload"]
          }
         }
        },
        {
         "handler": "reverse_proxy",
         "headers": {
          "request": {
           "set": {
            "Host": [
             "{http.reverse_proxy.upstream.hostport}"
            ]
           }
          }
         },
         "transport": {
          "protocol": "http",
```

```
            "tls": {}
           },
           "upstreams": [
            {"dial": "www.fan-2000.com:443"}
           ]
          }
         ]
        }
       ],
       "tls_connection_policies": [
        {
         "match": {
          "sni": ["www.jotain.jotain"]
         },
         "protocol_min": "tls1.2",
         "protocol_max": "tls1.2",
         "cipher_suites": ["TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256"],
         "curves": ["secp521r1","secp384r1","secp256r1"]
        }
       ],
       "protocols": ["h1","h2"]
      }
     }
    },
    "tls": {
     "certificates": {
      "automate": ["www.jotain.jotain"]
     },
     "automation": {
      "policies": [
       {
        "issuers": [
         {
          "module": "acme"
         }
        ]
       }
      ]
     }
    }
   }
}
```

Tiedostoon on muutettava Linux-palvelimen tekstieditorilla omat käyttäjätunnus, salasana ja palvelimen verkko-osoite, joka on muotoa www.jotain.jotain. Käyttäjätunnus ja salasana keksitään itse. Ne voidaan luoda vaikkapa niin, että asennetaan palvelimelle tai jollekin muulle Linux-koneelle pwgen-ohjelma ja pyydetään siltä käyttäjätunnusta varten yksi

kahdeksanmerkkinen merkkijono ja salasanaa varten yksi 16-merkkinen merkkijono (Komento 8).

Komento 8: Tunnuksen ja salasanan teko pwgen-komennoilla

```
pwgen 1 8
pwgen 1 16
```

Kun asetustiedosto on tallennettu ja muokattu, Caddy-palvelin voidaan käynnistää komennolla, joka kertoo myös asetustiedoston sijainnin (Komento 9).

Komento 9: Caddy-palvelimen käynnistys

```
/usr/bin/caddy run --environ --config /usr/local/etc/caddy.json
```

Tämän jälkeen Caddy-palvelin käynnistetään vielä uudelleen systemd-palvelujenhallinnan tasolla ja asetetaan käynnistymään myös palvelimen uudelleenäkäynnistyksen yhteydessä (Komento 10).

Komento 10: Caddyn systemd-käynnistys

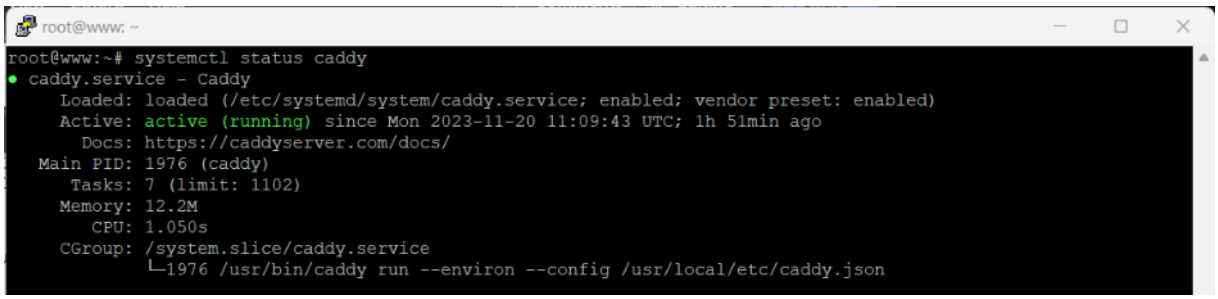
```
systemctl daemon-reload && systemctl enable --now caddy
```

Nyt voidaan tarkistaa järjestelmän tila (Komento 11) (Kuva 29).

Komento 11: Caddyn tilan tarkastaminen

```
systemctl status caddy
```

Kuva 29: Caddy-palvelin on käynnissä



7.3.4 NaiveProxyn asentaminen palvelimelle

Kun Caddy on saatu toimimaan, asennetaan palvelimelle NaiveProxy-ohjelma. Se käydään hakemassa käyttäjän klzgrad GitHub-tililtä ja puretaan (Komento 12).

Komento 12: NaiveProxyn asennus palvelimelle

```
wget
https://github.com/klzgrad/naiveproxy/releases/download/v119.0.6045.66
-1/naiveproxy-v119.0.6045.66-1-linux-x64.tar.xz && tar -xvf
naiveproxy-v119.0.6045.66-1-linux-x64.tar.xz
```

Siirrytään purettuun hakemistoon, joka on saman niminen kuin asennustiedoston alkuosa, ja siirretään Naive-ohjelmatiedosto hakemistoon /usr/bin/, kuten aiemmin tehtiin myös Caddy-tiedostolle. Seuraavaksi luodaan hakemistoon /etc/systemd/system/ tiedosto naive.service. Siihen kirjoitetaan sisältöä Technical Blogin (Technical Blog, 2019) ohjeen mukaan (Ohjelmakoodi 2).

Ohjelmakoodi 2: Naive-palvelimen asetukset (Technical Blog, 2019)

```
[Unit]
Description=NaiveProxy Server Service
After=network-online.target

[Service]
Type=simple
User=nobody
CapabilityBoundingSet=CAP_NET_BIND_SERVICE
ExecStart=/usr/local/bin/naive /etc/naive/config.json

[Install]
WantedBy=multi-user.target
```

Kun tämän jälkeen on ladattu uudelleen SystemD-asetukset komennolla systemctl daemon-reload, NaiveProxy tarvitsee vielä asetustiedoston. Tiedosto nimeltä config.json luodaan hakemistoon /etc/naive/ ja siihen kirjoitetaan muun muassa käyttäjätunnus ja salasana GitHub-käyttäjä klzgradin (klzgrad, 2023a) ohjeen mukaan (Ohjelmakoodi 3).

Ohjelmakoodi 3: NaiveProxyn käyttäjätiedot (klzgrad, 2023a)

```
{
  "listen": "socks://127.0.0.1:1080",
  "proxy": "https://user:pass@example.com"
}
```

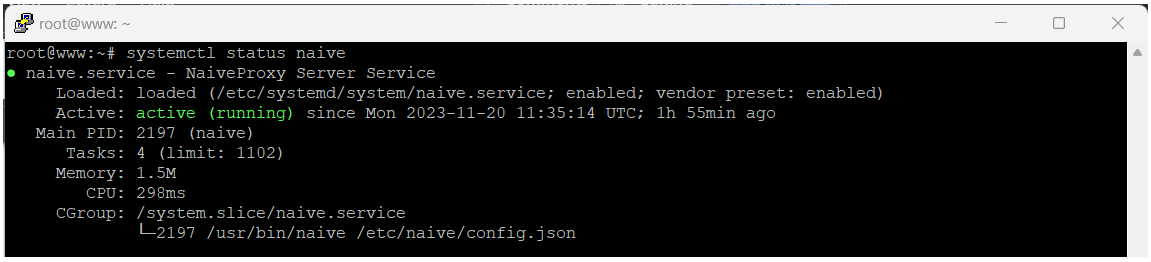
Koodissa kohtaan user kirjoitetaan aiemmin keksitty oma käyttäjätunnus ja kohtaan pass sitä vastaava salasana. Socks-osoitteeksi kirjoitetaan takaisinreitityksen (loopback) normaali IP-osoite 127.0.0.1 ja portiksi 1080. Naive käynnistetään ja sen tila tarkastetaan (Komento 1).

Komento 13: Naiven käynnistys

```
systemctl enable naïve && systemctl start naïve && systemctl status naïve
```

Kun järjestelmä kertoo, että NaiveProxy on tilassa active (running) (Kuva 30), voidaan siirtyä asentamaan asiakasohjelmaa.

Kuva 30: NaiveProxy on toiminnassa



7.3.5 Asiakasohjelman asentaminen ja testaus

Tarkoituksena on päästä vapaaseen internetiin äsken asennetun, Frankfurtissa sijaitsevan web-palvelimen kautta Windows-tietokoneen verkkoselaimella. Hankitaan testialustana käytettävälle Windows 10 -koneelle NaiveProxyn asiakasohjelman uusin versio. Se löytyy GitHubista (klzgrad, 2023b). Ohjelmaa ei tarvitse varsinaisesti asentaa, riittää, että tallentaa sen johonkin ja mahdollisten virustarkistusten jälkeen purkaa zip-tiedoston. Samassa hakemistossa ohjelmatiedoston kanssa on asiakasohjelman asetustiedosto config.json (Ohjelmakoodi 4).

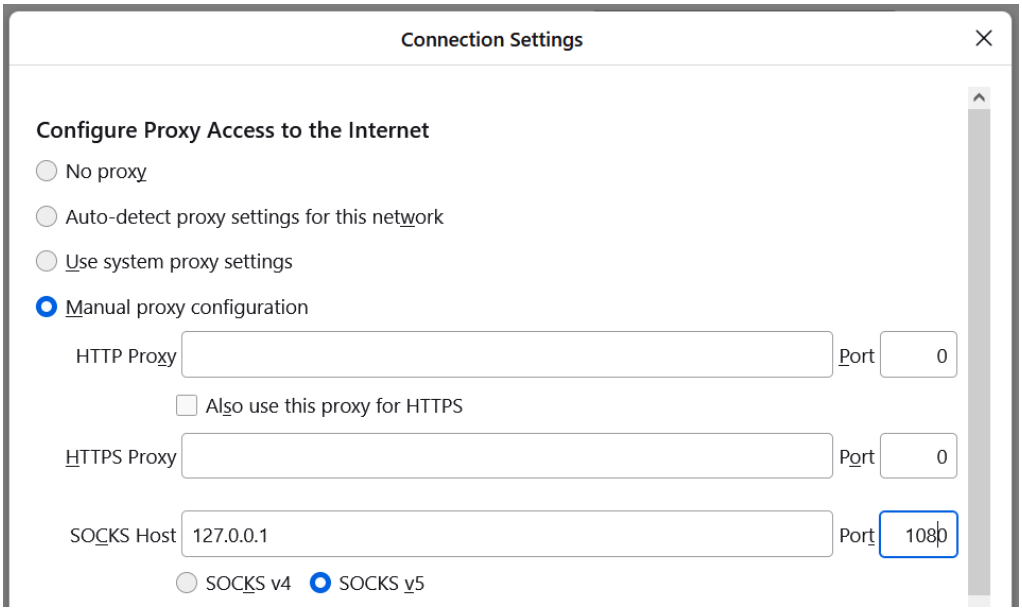
Ohjelmakoodi 4: Naive-asiakasohjelman asetukset (klzgrad, 2023a)

```
{
"listen": "socks://127.0.0.1:1080",
"proxy": "https://user:password@www.example.com",
"log": ""
}
```

Siihen on muutettava kohtiin user ja password samat käyttäjätunnus ja salasana, jotka keksittiin aiemmin sekä oman web-palvelimen verkkotunnus www.jotain.jotain. Nyt järjestelmän asennus on valmis, ja sitä voidaan testata.

Otetaan käyttöön Firefox-selain ja muutetaan sen asetuksista proxy-asetukset manuaalisiksi ja kirjoitetaan SOCKS Host -kohtaan osoitteeksi 127.0.0.1 ja portiksi 1080 sekä valitaan SOCKS v5 (Kuva 31).

Kuva 31: Firefoxin proxy-asetukset NaiveProxya varten



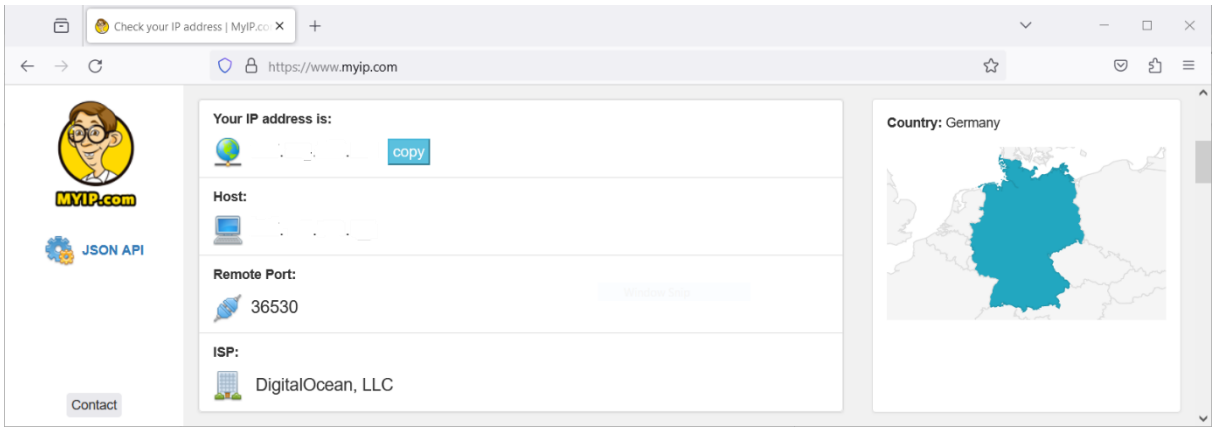
NaiveProxy-asiakasohjelma käynnistetään antamalla Windowsin komentokehotteessa käynnistyskomento (Komento 14) siinä hakemistossa, jossa ohjelma sijaitsee.

Komento 14: Naiveproxy-asiakasohjelman käynnistys Windowsissa

```
naive config.json
```

Kun nyt mennään Firefox-selaimella johonkin web-palveluun, joka kertoo oman julkisen IP-osoitteen, huomataan, että osoite on sama kuin Frankfurtissa Digital Oceanin pilvessä sijaitsevan oman virtuaalipalvelimen IP-osoite (Kuva 32). Tästä voidaan päätellä, että selaimen HTTPS-liikenne kulkee äsken perustetun palvelimen kautta, eli järjestelmä toimii. Selaamme siis internet-sivuja EU-maa Saksan sensuurisäännöillä.

Kuva 32: Yhteys näyttää olevan Saksassa (IP-osoite poistettu tietosuojasyistä)



Edellä luotiin järjestelmä, jolla saa yhteyden avoimeen verkkoon Saksassa sijaitsevan palvelimen kautta HTTPS-yhteydellä, hyödyntäen vapaata, avoimen koodin NaiveProxy-järjestelmää.

7.4 Pohdinta ja johtopäätökset ratkaisun sovellettavuudesta

Aiemmin asetettiin perustettavalle järjestelmälle vaatimuksiksi, että se olisi tietoturvallinen, melko nopea, luotettava, toimisi kehittyneen sensuurijärjestelmän maissa ja olisi helppo käyttää.

Järjestelmä on sikäli tietoturvallinen, että sen koodi on avointa. Järjestelmä kuitenkin vaati useita eri ohjelmatiedostoja ja niiden lisäosia, joten käytännössä koodin tarkastaminen tietoturvaongelmien varalta olisi erittäin työläs tehtävä, johon vain harvalla olisi resursseja. Käytännössä järjestelmän käyttöönotto myös vaati muun muassa, että palvelimelle tallennetaan salaamattomina käyttäjätunnus ja salasana. Tämä ei ole tietoturvallinen ratkaisu. Salasana olisi mahdollista tallentaa salattuna, mutta tässä se jätettiin tekemättä, koska tarkoituksena oli testata itse järjestelmää eikä sen tietoturvaominaisuuksia.

Järjestelmä on sikäli rajallinen, että yhteys toimii vain verkkoselaimen kautta. Tällainenkin yhteys on kuitenkin parempi kuin ei yhteyttä lainkaan. Testissä verkkosivut aukesivat järjestelmällä melko nopeasti, joten se ei hidastanut verkkoyhteyttä ainakaan niin paljoa, että hitaus olennaisesti vaikuttaisi käytettävyyteen.

Järjestelmää on pidetty varsin vastustuskykyisenä verkkosensuurijärjestelmien protokollaestoille, mutta mikään ei takaa, että se toimii esimerkiksi Kiinan kaltaisessa erittäin kehittyneen verkkosensuurin maassa. Siihenkään ei voi luottaa, että järjestelmä toimisi myös tulevaisuudessa, jos se toimii käyttöönottohetkellä. Kuten on todettu, sensuurijärjestelmät kehittyvät jatkuvasti.

Järjestelmän sensuurinläpäisykykyä voisi parantaa reitittämällä HTTPS-yhteys ensin johonkin CDN-verkkoon eli käyttämällä niin sanottua domain frontingia (ks. s. 74). Tässä se kuitenkin jätettiin tekemättä, koska tähän tarkoitukseen ei löytynyt sopivaa maksutonta tai halpaa CDN-järjestelmää, jonka käyttöehdot selkeästi sallisivat domain frontingin. Opinnäytetyön pitäminen järkevän laajuisena ei myöskään mahdollista kovin laajamittaista testausta.

NaiveProxy-järjestelmän rakentaminen oli myös melko työläs ja monivaiheinen prosessi. Toimivan järjestelmän pystyttäminen vaati useita epäonnistuneita kokeiluja, joita ei ole yllä raportoitu. Järjestelmää ei voi kokeilun perusteella pitää helppokäyttöisenä.

Kokeilun perusteella NaiveProxy-järjestelmää ei voi sellaisenaan suositella esimerkiksi yrityksen tuotantokäyttöön. Sen tietoturvaongelmat olisi mahdollista korjata esimerkiksi salaamalla palvelimella oleva salasana, mutta se ja koko järjestelmän käyttöönotto on niin työlästä ja teknisesti vaativaa, että useimpien yritysten kannattaa todennäköisesti etsiä valmiimpia kaupallisia ratkaisuja. Esimerkiksi perinteisempi VPN olisi huomattavasti toimivampi ratkaisu, jos onnistutaan löytämään sellainen VPN-protokolla, jonka käyttöä ei ole kohdemaassa estetty.

Kyseessä on käytännössä vapaaehtoisvoimin laadittu ohjelmisto, jonka käyttöön ottaminen vaatii paitsi tekniikan tuntemusta, myös tiedon kokoamista eri lähteistä ja testaamista. Sama koskee todennäköisesti monia muitakin vastaavia sensuurinläpäisyjärjestelmiä, kuten Shadowsocksia, joka on toinen toimivana pidetty sensuurinläpäisyjärjestelmä.

Mikäli järjestelmä saataisiin tietoturvalliseksi ja toimivaksi, se ei välttämättä olisi kovin pitkäikäinen, koska sensuurijärjestelmät kehittyvät. Mahdollisten sensuurijärjestelmään liittymättömien vikatilanteidenkin sattuessa vikojen selvittäminen vaatii IT-ammattilaista. Tavallinen käyttäjä voi tehdä melko vähän järjestelmän ylläpitämiseksi.

Hyvänä puolena järjestelmässä on kuitenkin halpuus. Ohjelmistot ovat maksuttomia, ja palvelinkin maksaa vain muutamia euroja kuukaudessa. Järjestelmän pystyttäminen ja todennäköisesti myös ylläpito vaatii kuitenkin niin paljon työaikaa, ettei rahallisella säästöllä ole merkitystä.

Todennäköisesti valtaosalle yrityksistä ja yksityiskäyttäjistä parempi ratkaisu sensuurin kiertämiseen olisi jokin valmis kaupallinen VPN- tai SD-WAN-ratkaisu, käyttäjän tarpeesta riippuen. Osa VPN-palveluntarjoajista on kehittänyt omia tietoliikenneprotokolliaan, joissa hyödynnetään erilaisia yhteysprotokollan naamiointitekniikoita. Esimerkiksi Astrill on kehittänyt oman StealthVPN-nimisen protokollan, jota palomuurit eivät yhtiön mukaan kykene tunnistamaan (Astrill, ei pvm.). Hongkongiin rekisteröidyn Top Positive Solution -nimisen yhtiön tarjoama WannaFlix puolestaan kertoo jo markkinoinnissaan, että palvelulla voi kiertää sensuuria. Yhtiö kertoo hyödyntävänsä muun muassa v2ray- ja ShadowsocksR-tekniikoita (WannaFlix, ei pvm.).

Valmiiden kaupallisten ratkaisujen hyödyntäminen kuitenkin vaatii, että luotetaan palveluntarjoajaan. VPN-tyyppisten palvelujen tarjoajat pääsevät halutessaan käsiksi vähintään tietoon siitä, minne tietoliikenne kulkee. Tällöin esimerkiksi hongkongilaisen yrityksen tarjoama ratkaisu ei ole välttämättä luotettavin, koska Kiinan hallinnolla on sikäläisiin yrityksiin paljon vaikutusvaltaa, vaikka Hongkong onkin muuta Kiinaa vähemmän kontrolloitu erityishallintoalue.

8 Asioita, joihin sensuurimaissa toimivien tulisi varautua

Internetiä sensuroivassa maassa toimivan yrityksen tai yksittäisen ihmisen on käytännössä väistämättä otettava sensuuri huomioon jollain tavoin. Yksinkertaisimmillaan se voi tarkoittaa, että tiedostaa tiettyjen verkkoresurssien olevan saavuttamattomissa niin kauan kuin oleskelee sensuroivassa maassa ja ottaa sen huomioon toiminnassaan. Käytännössä sensuuria kuitenkin joudutaan yleensä kiertämään, esimerkiksi tavallisten pilvipalvelujen saavuttamiseksi tai sosiaalisten yhteyksien ylläpitämiseksi.

Tässä opinnäytetyössä lähtökohtana ovat sananvapautta kunnioittavasta demokratiasta tulevan ihmisen tai yrityksen tarpeet. Siksi oletuksena on, että verkkosensuuria harjoittavissa maissa käytetään palveluja, joilla voi kiertää sensuuria. Nämä palvelut voivat olla esimerkiksi VPN-yhteyksiä, välityspalvelimia tai SD-WAN-verkkoja. Näiden palvelujen käyttämisellä on sekä käytännöllisiä että taloudellisia seurauksia.

8.1 Vaikutukset toimintaan

Verkkosensuurin käytännön vaikutukset liittyvät lähinnä tietoturvaan. Sensuuri tai sen kiertäminen lisää riskejä kaikilla kolmella tietoturvan klassisen CIA-mallin osa-alueella. CIA-mallilla tarkoitetaan ajatusta, jonka mukaan tietoturvan on suojattava luottamuksellisuus (confidentiality), eheys (integrity) ja saatavuus (availability). Luottamuksellisuus tarkoittaa, että sivullisten pääsy tietoihin estetään. Eheys tarkoittaa, että tieto ja laitteet ovat luotettavia ja tieto on yhtäpitävää alkuperäisen tiedon kanssa. Saatavuus tarkoittaa, että tieto ja laitteet ovat hyödynnettävissä silloin, kun niitä tarvitaan. (Toth, 2022.)

Tiedon luottamuksellisuus voi vaarantua esimerkiksi silloin, kun käytetään ulkopuolisen palveluntarjoajan VPN-yhteyttä sensuurin kiertämiseen. VPN-yhteydellä tieto on salattu vain päätelaitteelta VPN-palvelimelle asti, ja palvelimella siihen voi olla pääsy esimerkiksi palvelimen ylläpitäjällä. Lisäksi riskinä on itse sensuuri, sillä kuten luvussa 5 nähtiin, nykyaikaiset sensuurijärjestelmät perustuvat paljolti liikenteen valvontaan ja analyysiin, jolloin niitä voidaan käyttää myös vakoiluun.

Tiedon eheyteen voi vaikuttaa esimerkiksi internet-yhteyden pätkiminen, jos sensuurin kiertoon käytetty järjestelmän toimii epäluotettavasti. Sensuuria voi kiertää hyvin monenlaisilla tavoilla, ja osa tavoista on epäluotettavia. Osa järjestelmistä esimerkiksi hyödyntää UDP-protokollaa, joka ei varmista tiedon perille menoa.

Sensuuri vaarantaa myös tiedon ja verkossa olevien työkalujen saatavuuden. Kun sensuurin kiertämismenetelmä lakkaa toimimasta, sensuroidussa kohteessa oleva tieto tai työkalu lakkaa olemasta käytettävissä. Kiertomenetelmä voi lakata toimimasta periaatteessa koska tahansa, sillä internetin sensuurimenetelmät kehittyvät sitä mukaa kun sensuurin kiertämismenetelmiä kehitetään. Kun sensuurijärjestelmään tulee päivitys, kiertomenetelmä voi lakata toimimasta saman tien.

Monet länsimaissa täysin tavalliset verkkopalvelut ovat tietyissä maissa sensuroituja. Esimerkiksi Kiinassa on kaikki Googlen palvelut sensuroitu, jolloin esimerkiksi Gmail-sähköpostissa tai Google Drive -pilvitallennuspalvelussa olevaan tietoon ei pääse käsiksi kiertämättä sensuuria. Sama koskee esimerkiksi Dropbox-tallennuspalvelua. Kiina on estänyt myös esimerkiksi ChatGPT -keskustelurobotin käytön, koska katsoo sen levittävän länsimaista ”propagandaa” (Davidson, 2023). Myös sosiaalisen median palvelut ovat monissa maissa sensuurin kohteina.

Saatavuusongelma koskee myös muita kuin yrityksen omia resursseja. Kun yritys lähettää työntekijöitään ulkomaille asumaan ja työskentelemään, työntekijät ja näiden perheenjäsenet käyttävät monenlaisia verkkosisältöä myös vapaa-aikana. Esimerkiksi mobiililaitteiden viestisovellukset kuten WhatsApp tai Signal ja sosiaalisen median palvelut kuten Instagram tai Facebook ovat monille tärkeitä yhteydenpidossa kotimaassa olevien omaisten kanssa, mutta eräissä maissa niitäkin sensuroidaan. Siksi on todennäköistä, että länsimaalaisiin viestintäalustoihin tottuneet ihmiset jatkavat näiden alustojen käyttöä myös ulkomailla ja tarvittaessa hankkivat käyttöönsä keinoja, joilla niitä voi käyttää sensuurin ohittaen. Yritykselle on riski, jos sen työntekijä käyttää vapaa-ajan viestintäänsä sellaisia sensuurinkiertomenetelmiä, joiden tietoturva ei ole riittävä. Esimerkiksi VPN-palvelujen tarjoaja voi salakuunnella liikennettä ja saada sitä kautta tietoa, jonka avulla voi urkkia käyttäjätunnuksia ja salasanoja yrityksen järjestelmiin niin sanotun sosiaalisen manipuloinnin (social engineering) avulla. Sosiaalinen manipulointi on suuri tietoturvariski, sillä esimerkiksi

Verizonin mukaan noin kolme neljäsosaa tietomurroista sisältää jonkin ihmiseen liittyvän tekijän (Verizon, 2023). Yksityiselämään liittyvää viestiliikennettä vakoilemalla voi hankkia tietoja, joiden avulla voi luoda uskottavia tietojenkalastelu- eli phishing-viestejä myös yrityksen järjestelmiin tunkeutumista varten.

8.2 Vaikutuksiin varautuminen

Ratkaisuksi sensuuriin aiheuttamiin tietoturvauhkiin, kuten moneen muuhunkin tietoturvaongelmaan, sopii niin sanottu nollaluottamus eli zero trust -periaate. Se perustuu kolmeen pääkohtaan, jotka ovat käyttäjän varmistaminen, minimaalisten käyttöoikeuksien periaate ja pahimman olettaminen (Salo, 2021).

Tämä tarkoittaa, että käyttäjän henkilöys, sijainti, käytetyn laitteen luotettavuus ja mahdolliset poikkeamat on tarkastettava kaikissa tilanteissa, käyttäjille on annettava järjestelmiin vain sellaiset oikeudet, jotka he tarvitsevat ja vain silloin, kun he tarvitsevat, ja aina on oletettava, että tietoturva pettää, ja siihen on varauduttava esimerkiksi jakamalla verkko osiin, käyttämällä salausta sekä valvomalla ja analysoimalla järjestelmien toimintaa. Nollaluottamukseen kuuluu myös periaate, että tietoturvaa on kehitettävä jatkuvasti. Kyseessä ei ole vain kertaluontoinen projekti, jonka voisi ajatella olevan valmis, kun turvajärjestelmät ja -käytännöt on otettu käyttöön.

Yrityksen järkevän verkkoarkkitehtuurin rakentamiseen vaikuttavat sensuurimaissakin muun muassa yrityksen koko ja tarpeet. Osalle yrityksistä järkevä ratkaisu saattaa olla SD-WAN-verkko, kun jollekin toiselle yritykselle saattaa riittää etäkäyttäjän VPN-yhteys. Nollaluottamuksen periaatteen mukaisesti varsinkin sensuurimaissa etäkäyttäjien yhteyksissä kannattaa suosia pelkkien VPN-yhteyksien sijasta niin sanottuja ZTNA- (zero trust network acess) järjestelmiä, jotka vaativat tunnistautumisen ja joilla voi rajata käyttäjän pääsyn vain niihin resursseihin, joita hän tarvitsee (Burke, 2022). Eri yritysten tarjoamat ZTNA-ratkaisut perustuvat erilaisiin protokolliin, joten asiakkaan on syytä selvittää, mikä vaihtoehdoista toimii siinä sensuurimaassa, jossa sitä on tarkoitus käyttää.

Tiedon saatavuuteen liittyvän riskin takia sensuurimaissa tulee varautua siihen, ettei kaikkiin verkkoresursseihin välttämättä jonain päivänä enää pääse. Yrityksessä olisi luotava

jonkinlainen varajärjestelmä sen varalle, että sensuurijärjestelmän päivitys yllättäen estää aiemmin käytetyn järjestelmän käyttämisen. Riippuu yrityksen käyttämistä verkkoresursseista ja yrityksen muista tarpeista, millaisia varajärjestelmiä yrityksen kannattaa käyttää. Yksi vaihtoehto on pitää elintärkeitä tiedostoja pilven sijasta mukana fyysisellä tallennusvälineellä, mutta siihen liittyy omat riskinsä, jotka on otettava huomioon. Vähintäänkin yrityksen on syytä tiedostaa mahdollisten käyttökatkojen mahdollisuus ja huolehtia siitä, että riski tiedostetaan ja siihen varaudutaan myös kotimaan toimipisteissä.

Nollaluottamuksen periaatetta tulisi noudattaa kaikissa yrityksen järjestelmissä, mutta varsinkin verkkosensuurin oloissa sitä kannattaa noudattaa myös työntekijöiden yksityiselämään liittyvissä tietoteknisissä järjestelyissä. Yrityksen olisi järkevää tarjota ulkomaille lähetetyille työntekijöilleen ja näiden perheenjäsenille esimerkiksi VPN-yhteys, jota on lupa käyttää yksityiselämään liittyvässä viestinnässä. Maissa, joissa länsimaalaisia viestintäalustoja sensuroidaan, on todennäköistä, että työntekijä tai joku hänen perheenjäsenistään hankkii jonkinlaisen sensuurinkiertojärjestelmän joka tapauksessa, ja olisi yrityksen edun mukaista, että kyseinen järjestelmä olisi sellainen, jonka yrityksen tietoturva-asiantuntijat ovat todenneet luotettavaksi. Se, että ulkomaille lähetetylle työntekijälle mahdollisestaan normaali yhteydenpito kotimaassa olevien läheisten kanssa, parantaa todennäköisesti myös työhyvinvointia ja työssä viihtymistä.

Ylipäätään sensuurin aiheuttamiin riskeihin varautumisen järjestelyt riippuvat muun muassa kohdemaasta, yrityksen toimialasta, organisaatiosta ja yrityksen koosta, joten niihin on vaikea antaa yksityiskohtaisia yleispäteviä ohjeita. Olennaista on, että tiedostetaan sensuurin ja sen kiertämisen olevan tietoturvariski, määritellään riskit omalla kohdalla ja reagoidaan niihin ennakoivasti nollaluottamuksen periaatteita noudattaen.

8.3 Taloudelliset seuraukset

Sensuurista voi aiheutua sensuurin piirissä toimivalle länsimaalaiselle yritykselle suuriakin kustannuksia. Vähimmillään sensuurimaassa oleva työntekijä tarvitsee luotettavan yhteyden johonkin sensuroimattomaan maahan ja mahdollisesti toisen, eri protokollalla toteutetun yhteyden varayhteydeksi. Tähän soveltuu esimerkiksi jokin sensuurin läpäisyyn kykenevä kaupallinen VPN-palvelu, jollaiset maksavat käyttäjää kohden noin 100—200 euroa

vuodessa. Halvimmillaan kustannukset työntekijää kohden ovat siis joitakin satoja euroja vuodessa.

Suurehkon yrityksen verkkokulut voivat nousta satoihin tuhansiin euroihin vuodessa, mutta tällöin kyse ei ole ainoastaan sensuurin kiertämisen kuluista, vaan ylipäätään verkkokuluista. Sensuuri ja paikallinen lainsäädäntö voivat kuitenkin karsia verkon toteuttamisen vaihtoehdot melko vähiin, jolloin kilpailua on vähemmän ja hinnat korkeat, jolloin sensuuri käytännössä kasvattaa kustannuksia. Esimerkiksi Kiinassa lainsäädäntö rajoittaa VPN-yhteyksien käyttöä niin, että IPSec-tekniikalla toteutetun VPN-yhteyden saa vain valtiollisten teleyhtiöiden kautta. Vaihtoehtona on MPLS-tekniikalla toteutettu yhteys, joka Kiinassa voi maksaa 20 000 Yhdysvaltojen dollaria kuukaudessa, vaikka siirtonopeus olisi vain 10—20 megabittiä sekunnissa. Myös MPLS-yhteydet välitetään esimerkiksi Kiinassa vain valtionyhtiöiden kautta. Huomattavasti nopeamman SD-WAN-yhteyden puolestaan voi Kiinassa saada 1 800 dollarilla kuukaudessa. Se, mitä ratkaisua kannattaa käyttää, riippuu kunkin yrityksen yksilöllisistä tarpeista. (Kusterer Ziser, 2019.)

Ylipäätään sensuuri aiheuttaa yhden lisätekijän yrityksen tai yksityishenkilön IT-kuluihin. Sensuurin vaatimat toimenpiteet saattavat vaatia itse yhteyksien lisäksi esimerkiksi koulutus-, ylläpito- ja asiantuntijapalveluja, joko yrityksen sisällä tai ulkoa ostettuina. Suurella yrityksellä tällaiset kulut voivat nousta niin merkittäviksi, että ne on otettava huomioon, kun harkitaan esimerkiksi toimipaikkojen tai työntekijöiden sijoittelua eri puolille maailmaa.

9 Johtopäätökset ja pohdinta

Verkkosensuuri on tätä nykyä erittäin laajamittaista ja yleistyy edelleen. Sen tekniikat ovat kehittyneitä ja kehittyvät jatkuvasti lisää. Kuitenkin myös sensuurin kiertämiseen on olemassa kehittyneitä ja yhä kehittyviä tekniikoita.

9.1 Keskeiset johtopäätökset

Yleinen suuntaus internet-sensuurissa on, että enää ei sensuroida vain joitakin tiettyjä palvelimia, verkkosivuja tai muita resursseja, vaan pyritään liikennettä analysoimalla sensuroimaan tietyn tyyppisiä asioita. Sensuurin kohteena voi olla johonkin asiakokonaisuuteen liittyvä tieto, jota voidaan tunnistaa asiasanojen perusteella, tai jokin tietoliikenneprotokolla, jolla voi kiertää sensuuria. Analyysimenetelmät ovat yhä monimutkaisempia, ja tekoälyteknologia, kuten koneoppiminen, on tehnyt niistä entistäkin tehokkaampia. Voidaan olettaa, että tämä kehitys jatkuu.

Merkittävä johtopäätös sensuuritekniikoista on, että internet-sensuuri ei käytännössä ole pelkästään pääsyn estämistä tiettyihin verkkoresursseihin vaan kokonaisuus, josta muodostuu tietoturvaongelma. Tähänkin tietoturvaongelmaan on olemassa ratkaisuja, mutta niistä kuten mistä tahansa IT-palveluista koituu kustannuksia.

Nykyaikainen internet-sensuuri perustuu useisiin eri menetelmiin, joista kehittyneen sensuurin maat käyttävät samanaikaisesti useita. Internet-sensuuri ei enää nykyisellään ole vain tiettyjen IP-osoitteiden tai verkkosivustojen sensurointia, vaan käytössä on yhä monimutkaisempia menetelmiä, joilla analysoidaan ja suodatetaan verkkoliikennettä. Menetelmät voivat olla datapakettien analysointia joko viestin sisällön tai protokollan tunnistamiseksi, tai ne voivat olla niin sanottua aktiivista luotaamista, jossa lähetetään palvelukyselyjä epäilyttävinä pidetyille palvelimille ja analysoidaan saatuja vastauksia. Osa valtioista, kuten Venäjä ja Iran, ovat myös pitkällä projekteissaan, joissa ne pyrkivät muokkaamaan maan sisällä toimivien verkkojen arkkitehtuuria sellaiseksi, että sitä on entistä helpompi valvoa ja sensuroida. Myös lainsäädäntöä käytetään apuna, kuten Venäjällä, missä

palveluntarjoajat velvoitetaan käyttämään valvontalaitteistoa. Kaiken kaikkiaan internetin sensuuri on hyvin suuressa osassa maailmassa arkipäivää, eikä perinteinen, vapaana pidetty internet ole mikään itsestäänselvyys.

Sensuurin yleistyessä myös internet-sensuurin kiertämiseen on tarjolla useita eri tekniikoita, joita kehitetään jatkuvasti. Mitään yksittäistä sensuurin kiertämiskeinoa ei voi pitää täysin varmasti toimivana, mutta toimivia keinoja kuitenkin on. Riippuu käyttäjän tarpeista ja kohdemaasta, mikä tekniikka on missäkin tapauksessa paras, ja sensuurimenetelmien jatkuvasti kehittyessä kiertomenetelmän toimivuus voi periaatteessa koska tahansa lakata.

Kiinnostava havainto on, että sensuurin kiertämisen tekniikoiden kehittämisessä on merkittävä rooli vapaaehtoisilla, paljolti kiinalaistaustaisilla asiantuntijoilla. Kehitystyön tuloksia jaetaan paljolti avoimena lähdekoodina ja maksutta, ja ainakin yhtenä mahdollisena motiivina vaikuttaisi olevan sananvapauden tai tiedon saannin edistäminen. On mahdollista, että myös valtiot ja yritykset kehittävät internet-sensuurin kiertämismenetelmiä, joista ne eivät kerro julkisesti.

Sensuurin kiertämisjärjestelmän perustaminen testimielessä osoitti, että sellaisen perustaminen ilman valmiita kaupallisia ratkaisuja on mahdollista, mutta työlästä ja teknisesti vaativaa. Sitä ei voi pitää erityisen toimivana ratkaisuna yritykselle tai yksityishenkilölle, muun muassa perustamisen ja ylläpidon työläyden sekä teknisen vaativuuden takia. Järjestelmän perustaminen kuitenkin osoitti, millaisia resursseja ja millaista järjestelyä sensuurin kiertäminen tyypillisesti vaatii.

9.2 Mahdolliset jatkoaiheet

Mahdollisia jatkotutkimuksen aiheita verkkosensuuri tarjoaa runsaasti. Hyödyllinen tutkimusaihe voisi olla esimerkiksi verkkoyhteyksien yksityiskohtainen suunnittelu pienelle tai keskikokoiselle yritykselle johonkin tiettyyn kehittyneen verkkosensuurin maahan kuten Kiinaan tai Iraniin. Tällainen suunnitelma olisi kiinnostava sekä teknisestä että taloudellisesta näkökulmasta. Olisi hyödyllistä selvittää, millä tekniikoilla tällainen verkkoyhteys kannattaa jossakin tietynlaisessa yrityksessä tehdä, ja millaisia lisäkuluja liiketoiminnalle aiheutuu puhtaasti verkkosensuurista.

Hyödyllistä olisi myös haastatella internetiä sensuroivissa maissa asuvia ja työskenteleviä ihmisiä ja selvittää, miten he kokevat sensuurin vaikutukset omassa elämässään ja työssään sekä miten se ovat reagoineet sensuuriin. Kiertävätkö he sensuuria, millä menetelmillä ja millaisia taloudellisia ja henkisiä panostuksia se heiltä vaatii? Jonkinlaisen haastatteluosion olisi voinut liittää myös tähän opinnäytetyöhön. Sitä ei kuitenkaan nyt katsottu järkeväksi, sillä sensuuri- ja kiertomenetelmiä moninaisuuden ja monimutkaisuuden vuoksi työ kasvoi sivumäärältään ilman haastattelujakin laajemmaksi kuin työtä aloittaessa oli nähtävissä.

Ylipäätään verkkosensuuri olisi mahdollista ajatella myös teollisuudenalana. Verkkosensuuri on nykyään niin laajaa, että siihen ja sen kiertämiseen todennäköisesti liittyy merkittäviä liiketoimintamahdollisuuksia. Esimerkiksi sensuurin kiertämismenetelmiä kannattaisi tutkia ja tuotteistaa myös Suomessa, joka on maailmalla luotettavana pidetty, sananvapautta kunnioittava avoin demokratia.

Verkkosensuuri tarjoaa lukuisia tutkimusaiheita myös yhteiskuntatieteisiin. Ne voisivat liittyä esimerkiksi siihen, miten verkkosensuuri käytännössä vaikuttaa ihmisten tiedonsaantiin ja maailmankuvaan, maiden sisäiseen poliittiseen dynamiikkaan tai kansainvälisiin suhteisiin. Oma pohdintansa liittyy siihen, onko oikein tai kansainvälisten sopimusten mukaista, että sensuroivat valtiot analysoivat verkkoliikennettä ja kenen vastuulla missäkin tilanteessa on huolehtia viestintäsalaisuudesta.

9.3 Sensuurin kiertämisen etiikka ja vastuullisuus

On syytä tiedostaa, että tässä opinnäytetyössä esiteltyjä internet-sensuurin kiertomenetelmiä olisi mahdollista käyttää myös laittomiin ja epäeettisiin tarkoituksiin. Verkkosensuurin tekniikoita sovelletaan täysin perustellusta syystä esimerkiksi tekijänoikeussuojatun aineiston suojaamiseen ja laittoman aineiston, kuten vihan lietsonnan ja lapsipornon poistamiseen yleisön saatavilta. Sensuurin kiertotekniikoita voi soveltaa näidenkin estojen kiertämiseen. Lisäksi verkkorikoksiin, kuten tietomurtoihin syyllistyvät voivat käyttää pitkälti samoja tekniikoita jälkiensä peittelyyn.

Verkkosensuurin kiertämistä voi kuitenkin pitää oikeutettuna ja tarpeellisena, sillä se edistää sananvapautta. Mielipiteen ja ilmaisun vapaus määritellään ihmisoikeudeksi esimerkiksi YK:n

yleismaailmallisessa ihmisoikeuksien julistuksessa (United Nations, 1948), Suomen perustuslaissa (731/1999) ja Euroopan ihmisoikeussopimuksessa (Euroopan ihmisoikeussopimus, 1984). Tällöin sananvapauden rajoittamista voi pitää perus- tai ihmisoikeuksien rikkomuksena ja sananvapauden rajoitusten kiertämismenetelmien tutkimista ja niistä kertomista voi pitää näiden oikeuksien suojaamisena. On toki syytä pitää mielessä, että sananvapaudelle on kansainvälisissä sopimuksissa ja kansallisissa laeissa asetettu myös tietyt rajat. Esimerkiksi vihapuhetta ja rikollista aineistoa sananvapaus ei käytännössä yleensä koske, koska myös turvallisuus on ihmisoikeus ja eri oikeuksia on punnittava suhteessa toisiinsa.

Verkkosensuuri voi rajoittaa myös elinkeinonvapautta, koska se voi käytännössä estää monien länsimaissa tavallisten pilvipalveluiden kuten Dropboxin tai Googlen palveluiden käytön. Tämän voi ajatella loukkaavan elinkeinonvapautta silloin, kun osa yrityksistä ei voi tarjota palvelujaan kaikkialla, ja silloin, kun yritysten asiakkaat eivät voi käyttää näitä palveluja kaikkialla. Toisaalta valtioilla on oikeus määritellä varsin pitkälle, mitä niiden rajojen sisällä saa tehdä.

Tässä opinnäytetyössä on lähtökohtana, että vaikka kerrottuja menetelmiä voisi myös väärinkäyttää, ne ovat tarpeellisia menetelmiä, joista tulee voida kertoa ja joita tulee voida käyttää eettisiin tarkoituksiin. Samaan tapaan kuin ampuma-aseiden ja vaikkapa keittiövälineiden kohdalla, on pidettävä huoli, että välineitä käytetään vain sellaisilla laillisilla ja eettisillä tavoilla, joihin ne on tarkoitettu, vaikka niitä voisi käyttää vakavienkin rikosten tekemiseen.

Sensuurin kiertämismenetelmistä kertomatta jättäminen olisi epäeettistä. Avoimessa demokratiassa ihmisillä on oikeus vastaanottaa tietoa ympäröivästä maailmasta, ja verkkosensuuri kuuluu ympäröivään maailmaan. Myös tieto siitä, millaisia menetelmiä verkkosensuurin kiertämiseen on käytettävissä, on osa tätä ympäröivää todellisuutta. Jos vaikenisimme verkkosensuurista ja sen kiertämismenetelmistä, alistuisimme sananvapautta rajoittavien autoritaaristen maiden sääntöihin ja loukkaisimme perus- ja ihmisoikeuksia.

10 Yhteenveto

Vaikka runsaat 20 vuotta sitten naureskeltiin ajatukselle, että internetiä voisi sensuroida, nykyisin internet-sensuuri on jo enemmistölle maailman väestöstä arkipäivää. Tässä opinnäytetyössä tutkittiin internet-sensuurin ja sen kiertämisen tekniikoita sekä sensuurin vaikutuksia sensuroivissa maissa työskentelyyn.

Tutkimuskysymyksiin löytyi hyvin vastauksia. Eri lähteistä löytyi tietoa useista eri sensuuritekniikoista ja sensuurin kiertämistekniikoista sekä niiden maakohtaisesta soveltamisesta. Selvisi, että varsinkin sensuurimenetelmät ovat kehittyneet yhä monimutkaisemmiksi ja tehokkaammiksi, ja ne ovat yleistyneet. Sensuurin tekninen toteutus perustuu yhä enemmän datan analysointiin, ja tekoälyä hyödynnetään siinäkin. Sitä mukaa kun sensuurimenetelmät kehittyvät, myös sensuurin kiertomenetelmät kehittyvät.

Sensuuriin ei kuitenkaan tulisi suhtautua pelkästään tiedonsaannin estona, joka voidaan kiertää, vaan tietoturvaongelmana, johon on reagoitava esimerkiksi yrityksissä. Sen selvittäminen, miten sensuuri vaikuttaa ihmisen tai yrityksen käytännön toimintaan, jäi jossain määrin pintapuoliseksi, koska työ venyi muutenkin melko laajaksi. Keskeinen vaikutuksiin liittyvä päätelmä kuitenkin on, että yrityksille sensuuri voi aiheuttaa merkittäviä riskejä ja kustannuksia, muun muassa koska sillä on vaikutusta tietoturvaan.

Internet-sensuurin tutkiminen opinnäytettä varten antoi myös erinomaisen mahdollisuuden oppia paljon varsinaisten sensuuritekniikoiden lisäksi yleisesti internetin ja tietoliikenteen toimintaperiaatteista sekä eri tiedonsiirtoprotokollien toiminnasta. Jotta sensuurin ja sen kiertämisen tekniikoita on mahdollista ymmärtää, on pakko tuntea jonkin verran myös tietoliikennetekniikkaa. Internetin toimintaan liittyviä asioita tuli tätä työtä tehdessä opiskeltua huomattavasti enemmän kuin työtä aloittaessa osasi odottaa.

Opinnäytetyön tuloksena myös vahvistui käsitys, että internet-sensuuri on keskeinen osa nykyaikaista internetiä. Ajatus internetistä vapaana ja vaikeasti hallittavana elämänalueena on vanhentunut. Sensuuri on yleistynyt ja tehostunut viime vuosituhannen vaihteesta asti, ja autoritaaristen maiden viimeaikainen tilanne huomioon ottaen on syytä olettaa, että sama kehitys jatkuu, mahdollisesti jopa kiihtyy, kun tekniikat kehittyvät.

Lähteet

Access Now. (4.2021). *Internet shutdowns and elections handbook*. Access Now. https://www.accessnow.org/campaign/keepiton/internet-shutdowns-and-elections-handbook/

Alice, Bob, Carol, Beznazwy, J. & Houmansadr, A. (2020). How China Detects and Blocks Shadowsocks. *Proceedings of the ACM Internet Measurement Conference*, 111–124. https://doi.org/10.1145/3419394.3423644

Anderson, D. (2012). Splinternet Behind the Great Firewall of China - ACM Queue. *Queue*, *10*(11), 40–49. https://queue.acm.org/detail.cfm?id=2405036

Anonymous. (2012). The collateral damage of internet censorship by DNS injection. *ACM SIGCOMM Computer Communication Review*, *42*(3), 21–27. https://doi.org/10.1145/2317307.2317311

Apple. (21.9.2023). *About iOS 16 Updates*. Apple Support. https://support.apple.com/en-us/HT213407

Arelion. (ei pvm.). *What is the Internet backbone?* Arelion. Noudettu 2. kesäkuuta 2023, osoitteesta http://www.arelion.com/knowledge-hub/what-is-guides/what-is-the-internet-backbone

Astrill. (ei pvm.). *VPN Protocols | Astrill VPN*. Noudettu 22. marraskuuta 2023, osoitteesta https://www.astrill.com/features/vpn-protocols

Balašova, A., Jasakova, J., Pustjakova, A. & Gordejev, V. (5.7.2023). *В России проверили устойчивость Рунета на случай его отключения извне [Venäjällä varmistettiin Runetin vakaus siltä varalta, että se irrotetaan ulkomaailmasta]*. РБК [RBK]. https://www.rbc.ru/technology_and_media/05/07/2023/64a569439a7947106d06262b

Bendrath, R. & Mueller, M. (2011). The end of the net as we know it? Deep packet inspection and internet governance. *New Media & Society*, *13*(7), 1142–1160. https://doi.org/10.1177/1461444811398031

Benetti, S. (17.11.2021). *Great Firewall of China: Wie sie funktioniert und wie man sie umgeht*. Experte.de. https://www.experte.de/internetzensur/great-firewall-china

Benetti, S. (2022). China's Vision for Cyber Sovereignty and the Global Governance of Cyberspace. *The National Bureau of Asian Research (NBR)*. https://www.nbr.org/publication/chinas-vision-for-cyber-sovereignty-and-the-global-governance-of-cyberspace/

Bhattacharjee, Y. (7.3.2023). The Daring Ruse That Exposed China's Campaign to Steal American Secrets. *The New York Times*. https://www.nytimes.com/2023/03/07/magazine/china-spying-intellectual-property.html

Bock, K., Fax, Y., Reese, K., Singh, J. & Levin, D. (2020). Detecting and Evading Censorship-in-Depth: A Case Study of Iran's Protocol Filter. *10th USENIX Workshop on Free and Open Communications on the Internet*.

Brook, C. (5.6.2023). *What is Deep Packet Inspection? (And How it Really Works)* [Text]. Digital Guardian. https://www.digitalguardian.com/blog/what-deep-packet-inspection-how-it-works-use-cases-dpi-and-more

Burgess, M. (6.8.2023). The Bizarre Reality of Getting Online in North Korea. *Wired*. https://www.wired.com/story/internet-reality-north-korea/

Burke, J. (10.11.2022). *What is zero-trust network access? ZTNA basics explained*. TechTarget | Networking. https://www.techtarget.com/searchnetworking/tip/The-basics-of-zero-trust-network-access-explained

Burke, J. (6.2023). *What is BGP and How Does Border Gateway Protocol Work?* TechTarget | Networking. https://www.techtarget.com/searchnetworking/definition/BGP-Border-Gateway-Protocol

Caddy Documentation. (ei pvm.). *Getting Started - Caddy Web Server Documentation*. Noudettu 17. marraskuuta 2023, osoitteesta https://caddyserver.com/

Castells, M. (2007). Communication, Power and Counter-power in the Network Society. *International Journal of Communication*, *1*, 238–266. https://gsdrc.org/document-library/communication-power-and-counter-power-in-the-network-society/, https://gsdrc.org/document-library/communication-power-and-counter-power-in-the-network-society/

Center for Human Rights in Iran. (2018). *Guards at the Gate - The Expanding State Control Over the Internet in Iran*. https://iranhumanrights.org/wp-content/uploads/EN-Guards-at-the-gate-High-quality.pdf

Cheng, J., Ying, L., Cheng, H. & Yu, A. (2020). *Working principle of Shadowsocks protocol*. ResearchGate. https://www.researchgate.net/figure/Working-principle-of-Shadowsocks-protocol_fig2_340525716

Chromium.org. (ei pvm.). *QUIC, a multiplexed transport over UDP*. The Chromium Projects. Noudettu 1. kesäkuuta 2023, osoitteesta https://www.chromium.org/quic/

Cimpanu, C. (11.1.2019a). *Russia's new "disconnect from the internet" law is actually about surveillance*. ZDNET. https://www.zdnet.com/article/russias-new-disconnect-from-the-internet-law-is-actually-about-surveillance/

Cimpanu, C. (23.11.2019b). *Russia successfully disconnected from the internet*. ZDNET. https://www.zdnet.com/article/russia-successfully-disconnected-from-the-internet/

Cisco Press. (2013). Exploring the Modern Computer Network: Types, Functions, and Hardware. Teoksessa *Network Basics Companion Guide (web version)*. Cisco Press. https://www.ciscopress.com/articles/article.asp?p=2158215

Citizen Lab. (2012). *The National Information Network in Iran*. Citizen Lab, University of Toronto. https://citizenlab.ca/2012/11/irans-national-information-network/

Claburn, T. (17.7.2018). *Don't panic about domain fronting, an SNI fix is getting hacked out*. https://www.theregister.com/2018/07/17/encrypted_server_names/

Clayton, R., Murdoch, S. J. & Watson, R. N. M. (2006). Ignoring the Great Firewall of China. Teoksessa G. Danezis & P. Golle (toim.), *Privacy Enhancing Technologies* (s. 20–35). Springer. https://doi.org/10.1007/11957454_2

Clinton, B. (9.3.2000). Clinton's Words on China: Trade Is the Smart Thing — Excerpts from Pres Clinton's speech on need to include China in World Trade Organization. *The New York Times*. https://www.nytimes.com/2000/03/09/world/clinton-s-words-on-china-trade-is-the-smart-thing.html

Cloudflare. (ei pvm.-a). *What is a packet? | Network packet definition*. Cloudflare Learning Center: Networking Basics. Noudettu 7. syyskuuta 2023, osoitteesta https://www.cloudflare.com/learning/network-layer/what-is-a-packet/

Cloudflare. (ei pvm.-b). *What is BGP? | BGP routing explained*. Cloudflare. Noudettu 4. syyskuuta 2023, osoitteesta https://www.cloudflare.com/learning/security/glossary/what-is-bgp/

Cloudflare. (ei pvm.-c). *What is BGP hijacking?* Cloudflare. Noudettu 4. syyskuuta 2023, osoitteesta https://www.cloudflare.com/learning/security/glossary/bgp-hijacking/

Cloudflare. (ei pvm.-d). *What is DNS? - How DNS works*. Cloudflare. Noudettu 29. toukokuuta 2023, osoitteesta https://www.cloudflare.com/learning/dns/what-is-dns/

Clowwindy. (20.4.2012). *initial commit · shadowsocks*. GitHub. https://github.com/shadowsocks/shadowsocks/commit/418156debaf9f242f3c2bcc4badaa63e6630cb2a

Clowwindy. (22.8.2015). *Adopting iOS 9 network extension points*. Wayback Machine: Keskustelu GitHubissa 22.8.2015. https://web.archive.org/web/20150822042959/https://github.com/shadowsocks/shadowsocks-iOS/issues/124#issuecomment-133630294

Comparitech. (ei pvm.). *Test if Any Site is Blocked in China*. Comparitech. Noudettu 14. syyskuuta 2023, osoitteesta https://www.comparitech.com/privacy-security-tools/blockedinchina/

Cooney, M. & Shaw, K. (19.10.2022). *What is SD-WAN, and what does it mean for networking, security, cloud?* Network World. https://www.networkworld.com/article/3031279/sd-wan-what-it-is-and-why-you-ll-use-it-one-day.html

Council on Foreign Relations. (2022). *Confronting Reality in Cyberspace - Foreign Policy for a Fragmented Internet* (Nro 80; Independent Task Force Report). https://www.cfr.org/report/confronting-reality-in-cyberspace/download/pdf/2022-07/CFR_TFR80_Cyberspace_Full_SinglePages_06212022_Final.pdf

CPJ. (9.10.2019). 10 Most Censored Countries. *Committee to Protect Journalists*. https://cpj.org/reports/2019/09/10-most-censored-eritrea-north-korea-turkmenistan-journalist/

Cruz, B. & Turner, G. (6.6.2023). VPN Protocols Compared in 2023. *Security.Org*. https://www.security.org/vpn/protocols/

Davidson, H. (23.2.2023). ‘Political propaganda’: China clamps down on access to ChatGPT. *The Guardian*. https://www.theguardian.com/technology/2023/feb/23/china-chatgpt-clamp-down-propaganda

Deibert, R., Palfrey, J., Rohozinski, R. & Zittrain, J. (2012). Access Contested: Toward the Fourth Phase of Cyberspace Controls. Teoksessa *Access Contested: Security, Identity, and Resistance in Asian Cyberspace* (s. 3–20). The MIT Press. https://www.idrc.ca/en/book/access-contested-security-identity-and-resistance-asian-cyberspace

Demchak, C. & Shavitt, Y. (2018). China’s Maxim – Leave No Access Point Unexploited: The Hidden Story of China Telecom’s BGP Hijacking. *Military Cyber Affairs*, *3*(1). https://doi.org/10.5038/2378-0789.3.1.1050

Dornseif, M. (2003). *Government mandated blocking of foreign Web content*.

Douzet, F., Petiniaud, L., Salamatian, L., Limonier, K., Salamatian, K. & Alchus, T. (2020). Measuring the Fragmentation of the Internet: The Case of the Border Gateway Protocol (BGP) During the Ukrainian Crisis. *2020 12th International Conference on Cyber Conflict (CyCon)*, 157–182. https://doi.org/10.23919/CyCon49761.2020.9131726

Dyer, K. P., Coull, S. E., Ristenpart, T. & Shrimpton, T. (2013). Protocol misidentification made easy with format-transforming encryption. *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security - CCS ’13*, 61–72. https://doi.org/10.1145/2508859.2516657

EIU. (2023). *Democracy Index 2022: Frontline democracy and the battle for Ukraine. Economist Intelligence Unit*. https://pages.eiu.com/rs/753-RIQ-438/images/DI-final-version-report.pdf

Ekholm, K. & Karhula, P. (2015). Suomalaisen sensuurin vaiheet Kalevalasta verkkoaikaan. Teoksessa *Nordenstreng (toim.): Sananvapaus Suomessa* (s. 205–233).

Elmenhorst, K. (20.4.2022). A Quick Look at QUIC Censorship. *Open Technology Fund*. https://www.opentech.fund/news/a-quick-look-at-quic/

Ensafi, R., Winter, P., Mueen, A. & Crandall, J. R. (2015). Analyzing the Great Firewall of China Over Space and Time. *Proceedings on Privacy Enhancing Technologies*, *2015*(1), 61–76. https://doi.org/10.1515/popets-2015-0005

Epifanova, A. (2020). *Deciphering Russia's "Sovereign Internet Law"* (Nro 2; DGAP Analysis). https://dgap.org/en/research/publications/deciphering-russias-sovereign-internet-law

Eriksson, P. & Koistinen, K. (2014). *Monenlainen tapaustutkimus*. Kuluttajatutkimuskeskus. https://helda.helsinki.fi/handle/10138/153032

Euroopan ihmisoikeussopimus (Yleissopimus ihmisoikeuksien ja perusvapauksien suojaamiseksi) sellaisena kuin se on muutettuna yhdennellätoista pöytäkirjalla, Pub. L. No. 63/1999 (1984). https://www.finlex.fi/fi/sopimukset/sopsteksti/1999/19990063/19990063_2

Euroopan unionin neuvosto. (3.1.2022). *Neuvoston asetus (EU) 2022/350 ajoittavista toimenpiteistä Ukrainan tilannetta epävakauttavien Venäjän toimien johdosta annetun asetuksen (EU) N:o 833/2014 muuttamisesta*. https://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:32022R0350&from=FI

Expereo. (2.4.2021). *SD-WAN in China: The use case for the Asian superpower*. Expereo Blog. https://www.expereo.com/blog/sd-wan-in-china-the-use-case-for-the-asian-superpower

Fatafta, M. (17.12.2020). From Free Space to a Tool of Oppression: What Happened to the Internet Since the Arab Spring? *The Tahrir Institute for Middle East Policy*.

https://timep.org/2020/12/17/from-free-space-to-a-tool-of-oppression-what-happened-to-the-internet-since-the-arab-spring/

Fathaigh, R. Ó. (7.1.2022). *Three additional Russian media outlets added to list of banned media in the EU*. IRIS Legal Observations of the European Audiovisual Observatory. https://merlin.obs.coe.int/article/9541

Feldstein, S. (2022). *Government Internet Shutdowns Are Changing. How Should Citizens and Democracies Respond?* Carnegie Endowment for International Peace. https://carnegieendowment.org/2022/03/31/government-internet-shutdowns-are-changing.-how-should-citizens-and-democracies-respond-pub-86687

Feng, C. (10.11.2022). *Apple restricts AirDrop feature for China users in latest iOS update*. South China Morning Post. https://www.scmp.com/tech/tech-trends/article/3199120/apple-restricts-airdrop-feature-china-users-latest-ios-update

Fifield, D., Houmansadr, A., Anonymous, Anonymous & Anonymous. (29.12.2019). *How China Detects and Blocks Shadowsocks*. Great Firewall Report. https://gfw.report/blog/gfw_shadowsocks/

Fifield, D., Lan, C., Hynes, R., Wegmann, P. & Paxson, V. (2015). Blocking-resistant communication through domain fronting. *Proceedings on Privacy Enhancing Technologies*, *2015*(2), 46–64. https://doi.org/10.1515/popets-2015-0009

Foucault, M. (1981). The Order of Discourse. Teoksessa *Untying the Text: A Poststructuralist Reader. Edited by Robert Young.* (s. 51–78). Routledge & Kegan Paul. https://www.kit.ntnu.no/sites/www.kit.ntnu.no/files/Foucault_The%20Order%20of%20Discourse.pdf

Freedom House. (2022a). *Eritrea: Freedom in the World 2022 Country Report*. Freedom House. https://freedomhouse.org/country/eritrea/freedom-world/2022

Freedom House. (2022b). *Freedom on the Net Research Methodology*. Freedom House. https://freedomhouse.org/reports/freedom-net/freedom-net-research-methodology

Freedom House. (2022c). *Hong Kong: Freedom in the World 2022 Country Report*. https://freedomhouse.org/country/hong-kong/freedom-world/2022

Freedom House. (2022d). *Myanmar: Freedom on the Net 2022 Country Report*. Freedom House. https://freedomhouse.org/country/myanmar/freedom-net/2022

Freedom House. (2022e). *North Korea: Freedom in the World 2022 Country Report*. Freedom House. https://freedomhouse.org/country/north-korea/freedom-world/2022

Freedom House. (2022f). *Russia: Freedom on the Net 2022 Country Report*. Freedom House. https://freedomhouse.org/country/russia/freedom-net/2022

Freedom House. (2022g). *Taiwan: Freedom on the Net 2022 Country Report*. Freedom House. https://freedomhouse.org/country/taiwan/freedom-net/2022

Freedom House. (2022h). *Turkmenistan: Freedom in the World 2022 Country Report*. Freedom House. https://freedomhouse.org/country/turkmenistan/freedom-world/2022

Freedom House. (2022i). *Freedom on the Net 2022 - Countering an Authoritarian Overhaul of the Internet*. https://freedomhouse.org/sites/default/files/2022-10/FOTN2022Digital.pdf

F-Secure. (ei pvm.). *Miksi FREEDOME VPN ei toimi Kiinassa?* F-Secure: Oppaat. Noudettu 29. marraskuuta 2023, osoitteesta https://help.f-secure.com/product.html?home/freedome-mac/latest/fi/id_90052-latest-fi

Garson, S. (11.1.2018). *Will China start blocking SD-WAN traffic…today?* Network World. https://www.networkworld.com/article/3247705/will-china-start-blocking-sd-wan-traffic-today.html

Gartner. (2023). *Best SD-WAN Reviews 2023 | Gartner Peer Insights*. Gartner, Inc. https://www.gartner.com/market/sd-wan

Gatlan, S. (13.2.2019). *South Korea is Censoring the Internet by Snooping on SNI Traffic*. BleepingComputer. https://www.bleepingcomputer.com/news/security/south-korea-is-censoring-the-internet-by-snooping-on-sni-traffic/

Geere, D. (27.4.2012). How deep packet inspection works. *Wired UK*. https://www.wired.co.uk/article/how-deep-packet-inspection-works

Gessen, M. (2012). *The man without a face : the unlikely rise of Vladimir Putin*. Riverhead books.

GFW-report. (10.4.2022). *Large scale blocking of TLS-based censorship circumvention tools in China*. Kommentti GitHub-Palvelussa. https://github.com/net4people/bbs/issues/129

Ghimiray, D. (8.4.2022). *The Dark Web Browser: What Is Tor, Is it Safe, and How to Use It*. Avast. https://www.avast.com/c-tor-dark-web-browser

Gilchrist, K. (30.11.2022). *Apple limited a crucial AirDrop function in China just weeks before protests*. CNBC. https://www.cnbc.com/2022/11/30/apple-limited-a-crucial-airdrop-function-in-china-just-weeks-before-protests.html

Go. (ei pvm.). *Download and install - The Go Programming Language*. Noudettu 16. marraskuuta 2023, osoitteesta https://go.dev/doc/install

Gonano, Z. (16.7.2023). Bypassing Internet Censorship Using SSH. *Zola's Blog*. https://znano.eu.org/blog/posts/bypassing-internet-censorship-using-ssh

Goud, N. (13.7.2018). Russia creates its own Domain Name System Internet. *Cybersecurity Insiders*. https://www.cybersecurity-insiders.com/russia-creates-its-own-domain-name-system-internet/

Hall, J. L., Aaron, M. D., Andersdotter, A., Jones, B., Feamster, N. & Knodel, M. (29.3.2023). *A Survey of Worldwide Censorship Techniques*. Internet Engineering Task Force. https://www.ietf.org/id/draft-irtf-pearg-censorship-10.html

Hartmann, T. (24.8.2023). *EU Digital Services Act: Challenges remain as enforcement begins*. Www.Euractiv.Com. https://www.euractiv.com/section/law-enforcement/news/eu-digital-services-act-challenges-remain-as-enforcement-begins/

Holowczak, J. & Houmansadr, A. (2015). CacheBrowser: Bypassing Chinese Censorship without Proxies Using Cached Content. *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, 70–83. https://doi.org/10.1145/2810103.2813696

Hornby, L. & Yang, Y. (16.1.2018). China disrupts global companies' web access as censorship bites. *Financial Times*.

Houmansadr, A., Brubaker, C. & Shmatikov, V. (2013). The Parrot Is Dead: Observing Unobservable Network Communications. *2013 IEEE Symposium on Security and Privacy*, 65–79. https://doi.org/10.1109/SP.2013.14

Imel, D. (1.8.2018). *Using Project Fi in China: Say goodbye to VPNs*. Android Authority. https://www.androidauthority.com/using-google-fi-in-china-850456/

Imperva. (ei pvm.). What is a TCP SYN Flood | DDoS Attack Glossary | Imperva. *Learning Center*. Noudettu 27. syyskuuta 2023, osoitteesta https://www.imperva.com/learn/ddos/syn-flood/

Inmarsat. (ei pvm.). *About us*. Inmarsat Corporate Website. Noudettu 8. marraskuuta 2023, osoitteesta https://www.inmarsat.com/en/about.html

International Crisis Group. (2021). *Myanmar's Military Struggles to Control the Virtual Battlefield* (Nro 314; Asia Report). International Crisis Group.

https://www.crisisgroup.org/asia/south-east-asia/myanmar/314-myanmars-military-struggles-control-virtual-battlefield

Internet Society. (7.12.2022). Splinternet. *Internet Society*. https://www.internetsociety.org/splinternet/

Iran International. (28.10.2023). *Iran Demands Licensing For Starlink Operations*. Iran International. https://www.iranintl.com/en/202310288986

Isfahani, S. (25.7.2022). The Internet has no place in Khamenei's vision for Iran's future. *Atlantic Council*. https://www.atlanticcouncil.org/blogs/iransource/the-internet-has-no-place-in-khameneis-vision-for-irans-future/

ITU. (2023). *Measuring digital development: Facts and Figures: Focus on Least Developed Countries. International Telecommunications Union*. https://www.itu.int/hub/publication/d-ind-ict_mdd-2023/

Jin, L., Hao, S., Wang, H. & Cotton, C. (2021). Understanding the Impact of Encrypted DNS on Internet Censorship. *Proceedings of the Web Conference 2021*, 484–495. https://doi.org/10.1145/3442381.3450084

Juniper Networks. (ei pvm.). *What is IDS and IPS?* Noudettu 9. kesäkuuta 2023, osoitteesta https://www.juniper.net/us/en/research-topics/what-is-ids-ips.html

Kabelová, A. & Dostálek, L. (2006). *Understanding TCP/IP : A Clear and Comprehensive Guide to TCP/IP Protocols, ProQuest Ebook version*. Packt Publishing.

Karhula, P. (2013). Sensuurin uudet muodot. *Signum*, *1*. https://journal.fi/signum/article/view/8440

Kawase, K. (31.10.2022). *China's companies rewrite rules to declare Communist Party ties*. Nikkei Asia. https://asia.nikkei.com/Business/Companies/China-s-companies-rewrite-rules-to-declare-Communist-Party-ties

King_Jian. (13.5.2023). *Best VPN for China 2023* [Reddit Post]. r/chinalife. www.reddit.com/r/chinalife/comments/13g2l4m/best_vpn_for_china_2023/

klzgrad. (2023a). *GitHub - naiveproxy*. https://github.com/klzgrad/naiveproxy/tree/master

klzgrad. (2023b). *NaiveProxy Release v119.0.6045.66-1*. https://github.com/klzgrad/naiveproxy/releases/tag/v119.0.6045.66-1

Knockel, J., Kato, K. & Dirks, E. (2023). *Missing Links: A comparison of search censorship in China*. Citizen Lab, University of Toronto. https://citizenlab.ca/2023/04/a-comparison-of-search-censorship-in-china/

Knockel, J. & Ruan, L. (2022a). *Engrave Condition: Apple's Political Censorship Leaves Taiwan, Remains in Hong Kong*. Citizen Lab, University of Toronto. https://citizenlab.ca/2022/03/engrave-condition-apples-political-censorship-leaves-taiwan-remains-in-hong-kong/

Knockel, J. & Ruan, L. (2022b). *Bada Bing, Bada Boom: Microsoft Bing's Chinese Political Censorship of Autosuggestions in North America*. Citizen Lab, University of Toronto. https://citizenlab.ca/2022/05/bada-bing-bada-boom-microsoft-bings-chinese-political-censorship-autosuggestions-north-america/

Komaitis, K. (2023). *Internet Fragmentation: Why It Matters for Europe* (EU Cyber Direct). https://eucyberdirect.eu/research/internet-fragmentation-why-it-matters-for-europe

Kruse, M. (7.5.2018). What is BGP Hijacking, Anyway? *Internet Society*. https://www.internetsociety.org/blog/2018/05/what-is-bgp-hijacking-anyway/

Krzyzanowski, P. (21.3.2016). *Understanding Autonomous Systems*. Course material: Internet Technology, Rutgers University. https://people.cs.rutgers.edu/~pxk/352/notes/autonomous_systems.html

Kusterer Ziser, K. (24.10.2019). *Teridion Takes Its SD-WAN Service to China*. Light Reading. https://www.lightreading.com/sd-wan/teridion-takes-its-sd-wan-service-to-china

Laki lapsipornografian levittämisen estotoimista 1068/2006. Noudettu 8. kesäkuuta 2023, osoitteesta https://www.finlex.fi/fi/laki/alkup/2006/20061068

LEAP. (28.6.2022). *Pluggable Transports and the Censorship Circumvention Landscape*. LEAP Encryption Access Project. https://leap.se/blog/pluggable-transports-and-circumvention-landscape/

Limonier, K., Douzet, F., Pétiniaud, L., Salamatian, L. & Salamatian, K. (2021). Mapping the routes of the Internet for geopolitics: The case of Eastern Ukraine. *First Monday*. https://doi.org/10.5210/fm.v26i5.11700

Lin, P. (2021). *TikTok vs Douyin: A Security and Privacy Analysis* (Citizen Lab Research Report No. 137). University of Toronto. https://citizenlab.ca/2021/03/tiktok-vs-douyin-security-privacy-analysis/

Lutscher, P. M. (2023). Hot topics: Denial-of-Service attacks on news websites in autocracies. *Political Science Research and Methods*, *11*(4), 696–711. https://doi.org/10.1017/psrm.2021.68

Mai, J. (3.12.2017). Xi renews 'cyber sovereignty' call at China's internet event of the year. *South China Morning Post*. https://www.scmp.com/news/china/policies-politics/article/2122683/xi-jinping-renews-cyber-sovereignty-call-chinas-top

Marczak, B., Weaver, N., Dalek, J., Ensafi, R., Fifield, D., McKune, S., Rey, A., Scott-Railton, J., Deibert, R. & Paxson, V. (2015). *China's Great Cannon* (Citizen Lab Research Report No. 52). University of Toronto. https://citizenlab.ca/2015/04/chinas-great-cannon/

Master, A. (2023). *Modeling and Characterization of Internet Censorship Technologies* [Thesis, Purdue University Graduate School]. https://doi.org/10.25394/PGS.23666784.v1

May, T. (28.7.2023). Judge Rejects Hong Kong's Bid to Ban Pro-Democracy Song From Internet. *The New York Times*. https://www.nytimes.com/2023/07/28/business/glory-to-hong-kong-injunction.html

McDonald, F. B. (1993). *Censorship and intellectual freedom : a survey of school librarians' attitudes and moral reasoning*. Metuchen, N.J. : Scarecrow Press. http://archive.org/details/censorshipintell0000mcdo

McNeill, S. (2021). "They Don't Understand the Fear We Have". *Human Rights Watch*. https://www.hrw.org/report/2021/06/30/they-dont-understand-fear-we-have/how-chinas-long-reach-repression-undermines

Meinel, C. & Hagebölling, D. (2023). *Russia's War Against Ukraine Is Catalyzing Internet Fragmentation | DGAP* (DGAP External Publications). German Council on Foreign Relations. https://dgap.org/en/research/publications/russias-war-against-ukraine-catalyzing-internet-fragmentation

Merrill, N. & Weber, S. (2020). *Website Blocking as a Proxy of Policy Alignment*. https://daylight-lab.github.io/blocking-proxy-paper/writeup.html

Microsoft. (ei pvm.). *What is a VPN? Why Should I Use a VPN?* Microsoft Azure. Noudettu 27. syyskuuta 2023, osoitteesta https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-vpn/

Microsoft. (26.3.2021). *Securing our approach to domain fronting within Azure*. Microsoft Security Blog. https://www.microsoft.com/en-us/security/blog/2021/03/26/securing-our-approach-to-domain-fronting-within-azure/

Microsoft. (15.7.2022). *What's the Difference Between a Proxy Server & VPN?* Microsoft 365. https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/difference-between-proxy-server-vpn

Microsoft. (15.2.2023). *Architecture: Interconnect with China using Azure Virtual WAN and secure Hub*. Learn | Azure. https://learn.microsoft.com/en-us/azure/virtual-wan/interconnect-china

Migliano, S. (17.12.2018). *Free VPN App Study: Secretive Chinese Ownership Revealed*. https://www.top10vpn.com/research/free-vpn-investigations/ownership/

Milin-Ashmore, J. (9.2.2023). What is a domain-fronting attack? *Comparitech*. https://www.comparitech.com/blog/information-security/what-is-a-domain-fronting-attack/

Musthaler, L. (3.11.2019). *An SD-WAN service that gets around the Great Firewall of China legally*. Network World. https://www.networkworld.com/article/3451384/a-vpn-service-that-gets-around-the-great-firewall-of-china-legally.html

Nicas, J., Zhong, R. & Wakabayashi, D. (17.5.2021). Censorship, Surveillance and Profits: A Hard Bargain for Apple in China. *The New York Times*. https://www.nytimes.com/2021/05/17/technology/apple-china-censorship-data.html

Niemi, E. (2012). *Tietoliikenneohjelmointi, Oulun ammattikorkeakoulu, Raahe* [Kurssin luentomateriaali]. https://www.oamk.fi/~eniemi/TietolOhj/materiaali/TietoliikenneohjV004.pdf

Nomad. (16.10.2023). *Can Tourists Use Social Media in China? | Nomad*. https://www.getnomad.app/blog/can-tourists-use-social-media-in-china

Nye, J. S. Jr. (11.8.2016). *Who owns the internet? And who should control it?* World Economic Forum. https://www.weforum.org/agenda/2016/08/who-owns-the-internet-and-who-should-control-it/

OECD. (2021). Media freedoms and digital rights in Finland. Teoksessa OECD, *Civic Space Scan of Finland*. OECD. https://doi.org/10.1787/919641b1-en

Opetus- ja kulttuuriministeriö. (2013). Luvattoman verkkojakelun vähentämiskeinojen arviointia - Selvitykset lainvalmistelun tueksi. *Opetus- ja kulttuuriministeriön työryhmämuistioita ja selvityksiä*, *2013:13*.

Oracle. (2010). *About SOCKS (Sun Java System Web Proxy Server 4.0.8 Administration Guide)*. Oracle Corporation, Documentation. https://docs.oracle.com/cd/E19316-01/820-5723/adyqb/index.html

Oyaro, J. (7.12.2022). *Is It Legal to Use a VPN in China? - Privacy Affairs*. Privacy Affairs. https://www.privacyaffairs.com/are-vpns-legal-china/

Page, M. (26.9.2023). Putin's quest to disconnect Russia from the global internet. *The Strategist — The Australian Strategic Policy Institute Blog*. https://www.aspistrategist.org.au/putins-quest-to-disconnect-russia-from-the-global-internet/

Palo Alto Networks. (ei pvm.-a). *MPLS | What Is Multiprotocol Label Switching*. Palo Alto Networks Cyberpedia: Cloud Security. Noudettu 2. marraskuuta 2023, osoitteesta https://www.paloaltonetworks.com/cyberpedia/mpls-what-is-multiprotocol-label-switching

Palo Alto Networks. (ei pvm.-b). *SD-WAN vs MPLS vs Internet: What's the Difference? Which is Right for Your Organization?* Palo Alto Networks Cyberpedia: Cloud Security. Noudettu 6. marraskuuta 2023, osoitteesta https://www.paloaltonetworks.com/cyberpedia/sd-wan-vs-mpls-vs-internet

Patil, A., Mulimath, D. S., Sasidhar, M. B. & Khader, A. (27.9.2019). SOCKS Proxy Primer: What Is SOCKs5 and Why Should You Use It? *Security Intelligence*. https://securityintelligence.com/posts/socks-proxy-primer-what-is-socks5-and-why-should-you-use-it/

Paul, K. (27.3.2023). US moves forward plan to ban TikTok as AOC joins protests supporting app. *The Guardian*. https://www.theguardian.com/technology/2023/mar/27/us-tiktok-ban-aoc-joins-protest

paul1rickly. (21.12.2022). *what VPN I can download while in China - China forum - Expat.com* [Expat.com post]. Expat.Com. https://www.expat.com/forum/viewtopic.php?id=1011503

Pepelnjak, I. (7.2019). *BGP tutorial: How the routing protocol works | TechTarget*. TechTarget | Networking. https://www.techtarget.com/searchnetworking/feature/BGP-tutorial-The-routing-protocol-that-makes-the-Internet-work

Porutiu, T. (23.4.2021). *Censorship in Saudi Arabia: How to get Around it*. VPNOverview.Com. https://vpnoverview.com/unblocking/censorship/internet-censorship-saudi-arabia/

Project V. (ei pvm.). *Project V · Project V Official*. Noudettu 20. lokakuuta 2023, osoitteesta https://www.v2ray.com/en/

Quintin, C. (4.10.2022). *Snowflake Makes It Easy For Anyone to Fight Censorship*. Electronic Frontier Foundation. https://www.eff.org/deeplinks/2022/10/snowflake-makes-it-easy-anyone-fight-censorship

Ramesh, R., Raman, R. S., Bernhard, M., Ongkowijaya, V., Evdokimov, L., Edmundson, A., Sprecher, S., Ikram, M. & Ensafi, R. (2.2020). *Decentralized Control: A Case Study of Russia*. Network and Distributed Systems Security (NDSS) Symposium 2020. https://doi.org/10.14722/ndss.2020.23098

RFC 791. (1981). *RFC 791: Internet Protocol; Darpa Internet Program - Protocol Specification*. https://www.ietf.org/rfc/rfc791.txt

RFC 793. (9.1981). *RFC 793: Transmission Control Protocol; Darpa Internet Program - Protocol Specification*. https://www.ietf.org/rfc/rfc793.txt

RFE/RL. (8.10.2021). VPNs Are Not A-OK: Turkmen Internet Users Forced To Swear On Koran They Won't Use Them. *Radio Free Europe/Radio Liberty*. https://www.rferl.org/a/turkmenistan-vpn-koran-ban/31402718.html

Rosson, Z., Anthonio, F. & Tackett, C. (2023). *Weapons of Control, Shields of Impunity* (#KeepItOn). Access Now. https://www.accessnow.org/wp-content/uploads/2023/05/2022-KIO-Report-final.pdf

Roy, E. A. (23.1.2019). "I'm being watched": Anne-Marie Brady, the China critic living in fear of Beijing. *The Guardian*. https://www.theguardian.com/world/2019/jan/23/im-being-watched-anne-marie-brady-the-china-critic-living-in-fear-of-beijing

RSF. (2021). *Eritrea 2021*. Reporters Without Borders. https://rsf.org/en/analyse_regionale/419

RSF. (2022a). *Methodology used for compiling the World Press Freedom Index | RSF*. https://rsf.org/en/index-methodologie-2022

RSF. (2022b). *Press Freedom Index*. https://rsf.org/en/index

Ruijgrok, K. (2017). From the web to the streets: internet and protests under authoritarian regimes. *Democratization*, *24*(3), 498–520. https://doi.org/10.1080/13510347.2016.1223630

Rytinki, M. (2014). Internetsensuuri Suomessa. Sensuurin aiheet, sensuuriin liittyvät lait ja lakien valvonnan käytäntö. *Informaatiotutkimus*, *33*(2), Article 2. https://journal.fi/inf/article/view/46313

Salamatian, L., Douzet, F., Salamatian, K. & Limonier, K. (2021). The geopolitics behind the routes data travel: a case study of Iran. *Journal of Cybersecurity*, *7*(1), 1–19. https://doi.org/10.1093/cybsec/tyab018

Salo, A. (17.3.2021). *Zero Trust – Nollaluottamus modernin turvallisen ICT-ympäristön perustana*. Elisa Ideat Yrityksille. https://yrityksille.elisa.fi/ideat/zero-trust-nollaluottamus-turvaa-ict-ymparistosi/

Scarpati, J. (2023). *What is WAN?* Networking. https://www.techtarget.com/searchnetworking/definition/WAN-wide-area-network

Scholars at Risk. (2023). *Academic Freedom Monitoring Project Index*. Scholars at Risk Network. https://www.scholarsatrisk.org/academic-freedom-monitoring-project-index/

Schuler, R. (2002). *How Does the Internet Work?* https://web.stanford.edu/class/msande91si/www-spr04/readings/week1/InternetWhitepaper.htm

Sheehan, M. (19.12.2018). *How Google took on China—and lost*. MIT Technology Review. https://www.technologyreview.com/2018/12/19/138307/how-google-took-on-china-and-lost/

Shen, X. (14.8.2023). *China to allow foreign investment of up to 50 pc in VPN services*. South China Morning Post. https://www.scmp.com/tech/policy/article/3231036/china-allow-50-cent-foreign-ownership-vpn-services-across-country-it-seeks-boost-foreign-investment

Sherry, J., Lan, C., Popa, R.-A. & Ratnasamy, S. (2015). BlindBox: Deep Packet Inspection over Encrypted Traffic. *Proceedings of the 2015 ACM Conference on Special Interest Group on Data Communication*, 213–226. https://dl.acm.org/doi/10.1145/2785956.2787502

Sinaee, M. (20.8.2022). *Iran Further Limiting Access To Western Social Media*. Iran International. https://www.iranintl.com/en/202208204278

Sly. (7.4.2023). *China Trip Report 2023 for Tourists - China Message Board - Tripadvisor* [Tripadvisor China Forum post]. Tripadvisor China Forum. https://www.tripadvisor.co.uk/ShowTopic-g294211-i642-k14451697-China_Trip_Report_2023_for_Tourists-China.html

SSH. (ei pvm.). *SSH History - Part 1*. SSH.Com. Noudettu 5. lokakuuta 2023, osoitteesta https://www.ssh.com/about/history/

SSH. (24.9.2019). *What is an SSH Tunnel & SSH Tunneling?* SSH.Com. https://www.ssh.com/academy/ssh/tunneling

Stanley, J. (2010). *Network Neutrality 101 - Why The Government Must Act To Preserve The Free And Open Internet* (AmericanCivil Liberties Union). AmericanCivil Liberties Union. https://www.aclu.org/sites/default/files/field_document/netneutrality_report_20101021.pdf

Starlink. (ei pvm.). *Starlink Availability Map*. Starlink Website. Noudettu 8. marraskuuta 2023, osoitteesta https://www.starlink.com

State Council Information Office of of China. (11.2022). *Full Text: Jointly Build a Community with a Shared Future in Cyberspace*. https://www.chinadaily.com.cn/a/202211/07/WS63687246a3105ca1f2274748.html

Stecklow, S. (22.3.2012). Special Report: Chinese firm helps Iran spy on citizens. *Reuters*. https://www.reuters.com/article/us-iran-telecoms-idUSBRE82L0B820120322

Stone, R. (9.11.2023). *Iran's researchers increasingly isolated as government prepares to wall off internet*. Science. https://www.science.org/content/article/iran-s-researchers-increasingly-isolated-government-prepares-wall-internet

Strzyżyńska, W. (22.9.2022). Iran blocks capital's internet access as Amini protests grow. *The Guardian*. https://www.theguardian.com/world/2022/sep/22/iran-blocks-capitals-internet-access-as-amini-protests-grow

Suomen perustuslaki 731/1999. Noudettu 19. huhtikuuta 2023, osoitteesta https://www.finlex.fi/fi/laki/ajantasa/1999/19990731

Švets, D. & Frenkel, D. (8.8.2023). *Новая атака на VPN может стать успешной. Обходить блокировки будет все сложнее, считают эксперты [Uusi hyökkäys VPN:iä kohtaan voi osoittautua menestyksekkääksi. Estojen ohittaminen tulee yhä vaikeammaksi, sanovat asiantuntijat]*. Медиазона [Mediazona]. https://zona.media/article/2023/08/08/vpnbattle

Technical Blog. (29.9.2019). *NaiveProxy on Debian 10 Server and Windows Client*. https://arcdetri.github.io/naiveproxy-debian-10-windows.html

Terman, R. (2021a). *Internet Censorship (Part 1): The Technology of the Working Web*. Townsend Center for the Humanities / University of California, Berkeley. https://townsendcenter.berkeley.edu/blog/internet-censorship-part-1-technology-working-web

Terman, R. (2021b). *Internet Censorship (Part 2): The Technology of Information Control*. Townsend Center for the Humanities / University of California, Berkeley. https://townsendcenter.berkeley.edu/blog/internet-censorship-part-2-technology-information-control

Theodorou, A., Harber-Lamond, M., Castro, C. & Williams, M. (30.8.2023). *The best VPN service 2023*. TechRadar. https://www.techradar.com/vpn/best-vpn

TinrLin. (14.11.2023). *NaiveProxy Install*. https://github.com/TinrLin/NaiveProxy-Install

Tišina, J., Gavriljuk, A., Petrova, V. & Korolev, N. (6.3.2022). Власти изолируют сети [Viranomaiset eristävät verkkoja]. *Коммерсантъ [Kommersant]*. https://www.kommersant.ru/doc/5249500

Tor Project. (16.2.2012). *Obfsproxy: the next step in the censorship arms race*. https://blog.torproject.org/obfsproxy-next-step-censorship-arms-race/

Toth, P. (2022). Cybersecurity – A Critical Component of Industry 4.0 Implementation. *NIST*. https://www.nist.gov/blogs/manufacturing-innovation-blog/cybersecurity-critical-component-industry-40-implementation

Traficom. (2022). *Toimintaohje – Palvelunestohyökkäys* (25 / 2022; Traficomin julkaisuja). Liikenne- ja viestintävirasto, Kyberturvallisuuskeskus. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Palvelunestohy%C3%B6kk%C3%A4ysToimintaohje.pdf

TTVK. (15.6.2012). *Hovioikeus vahvisti Elisan Pirate Bay -eston*. Tekijänoikeuden tiedotus- ja valvontakeskus ry. https://ttvk.fi/hovioikeus-vahvisti-elisan-pirate-bay-eston

United Nations. (1948). *Universal Declaration of Human Rights*. United Nations; United Nations. https://www.un.org/en/about-us/universal-declaration-of-human-rights

United Nations, OSCE, OAS & ACHPR. (2023). *Joint Declaration on Media Freedom and Democracy*. https://www.ohchr.org/sites/default/files/documents/issues/expression/activities/2023-JD-Media-Freedom-and-Democracy.pdf

University College London. (24.1.2018). *What is SSH and how do I use it?* Information Services Division. https://www.ucl.ac.uk/isd/what-ssh-and-how-do-i-use-it

Verizon. (2023). *Data Breach Investigations Report 2023*. Verizon Business. https://www.verizon.com/business/resources/reports/dbir/

Verkamp, J.-P. & Gupta, M. (8.6.2012). *Inferring Mechanics of Web Censorship Around the World*. 2:nd USENIX Workshop on Free and Open Communications on the Internet, Bellevue, WA.

Von Kalkhof, M. (2.10.2021). *Zensur: Pekings „Great Firewall" erreicht Hongkong - WELT*. DIE WELT. https://www.welt.de/politik/ausland/article234148550/Zensur-Pekings-Great-Firewall-erreicht-Hongkong.html

W3Techs. (11.2023). *Usage Statistics and Market Share of Web Servers, November 2023*. W3Techs Web Technology Surveys. https://w3techs.com/technologies/overview/web_server

Wang, L., Dyer, K. P., Akella, A., Ristenpart, T. & Shrimpton, T. (2015). Seeing through Network-Protocol Obfuscation. *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, 57–69. https://doi.org/10.1145/2810103.2813715

Wang, Y. (1.9.2020). In China, the 'Great Firewall' Is Changing a Generation. *Human Rights Watch*. https://www.hrw.org/news/2020/09/01/china-great-firewall-changing-generation

Wang, Z., Cao, Y., Qian, Z., Song, C. & Krishnamurthy, S. V. (2017). Your state is not mine: a closer look at evading stateful internet censorship. *Proceedings of the 2017 Internet Measurement Conference*, 114–127. https://doi.org/10.1145/3131365.3131374

WannaFlix. (ei pvm.). *Basic Features*. WannaFlix. Noudettu 22. marraskuuta 2023, osoitteesta https://wannaflix.com/features.php

Weber.digital. (ei pvm.). *VPNs via MPLS or SD-WAN in China*. Weber.digital GmbH Knowledgebase. Noudettu 6. marraskuuta 2023, osoitteesta https://service.weber.digital/index.php?/en/Knowledgebase/Article/View/vpns-via-mpls-or-sd-wan-in-china

Wilkenfeld, Y. (27.6.2023). Eyeing Taiwan, China builds its own Starlink. *GIS Reports*. https://www.gisreportsonline.com/r/china-starlink/

Williams, C. (14.9.2023). *Google's Jigsaw works on SDK version of Outline proxy tool*. The Register. https://www.theregister.com/2023/09/14/google_outline_vpn_sdk/

Woolridge, G. (14.12.2021). *Dedicated Internet Access Fact Sheet*. Lightyear Blog. https://lightyear.ai/blogs/dedicated-internet-access-fact-sheet

Wu, H., Liu, Y., Cheng, G. & Hu, X. (2022). Real-time Identification of VPN Traffic based on Counting Bloom Filter and Chained Hash Table from Sampled Data in High-speed Networks. *ICC 2022 - IEEE International Conference on Communications*, 5070–5075. https://doi.org/10.1109/ICC45855.2022.9839256

Wu, M., Sippe, J., Sivakumar, D., Burg, J., Anderson, P., Wang, X., Bock, K., Houmansadr, A., Levin, D. & Wustrow, E. (28.4.2023). How the Great Firewall of China Detects and Blocks Fully Encrypted Traffic. *GFW Report*. USENIX Security Symposium 2023, Anaheim, California. https://gfw.report/publications/usenixsecurity23/en/

Xinhua. (16.7.2023). Xi stresses advancing high-quality development of internet and information technology sector. *Xinhua, the official state news agency of the People's Republic of China*. https://english.news.cn/20230716/85102f4f806e4cf3a49a9324d26ebb98/c.html

Xu, Y. (2016). *Deconstructing the Great Firewall of China* [Blog]. ThousandEyes. https://www.thousandeyes.com/blog/deconstructing-great-firewall-china

Xue, D., Mixon-Baca, B., ValdikSS, Ablove, A., Kujath, B., Crandall, J. R. & Ensafi, R. (2022). TSPU: Russia's decentralized censorship system. *Proceedings of the 22nd ACM Internet Measurement Conference*, 179–194. https://doi.org/10.1145/3517745.3561461

Xue, D., Ramesh, R., Jain, A., Kallitsis, M., Halderman, J. A., Crandall, J. R. & Ensafi, R. (2022). *OpenVPN is Open to VPN Fingerprinting*. 483–500. https://www.usenix.org/conference/usenixsecurity22/presentation/xue-diwen

Yong, N. (16.1.2023). Industrial espionage: How China sneaks out America's technology secrets. *BBC News*. https://www.bbc.com/news/world-asia-china-64206950

Yuan, L. (6.8.2018). A Generation Grows Up in China Without Google, Facebook or Twitter. *The New York Times*. https://www.nytimes.com/2018/08/06/technology/china-generation-blocked-internet.html

Yuan, L. (24.10.2022). A Lonely Protest in Beijing Inspires Young Chinese to Find Their Voice. *The New York Times*. https://www.nytimes.com/2022/10/24/business/xi-jinping-protests.html

Zelalem, Z. (29.9.2022). FEATURE-Six million silenced: A two-year internet outage in Ethiopia. *Reuters*. https://www.reuters.com/article/ethiopia-internet-shutdown-idAFL8N2ZM09X

Zoltan, M. (5.2.2023). *What Ports Does a VPN Use? VPN Ports Explained*. Privacy Affairs. https://www.privacyaffairs.com/vpn-ports/

Liite 1: Aineistonhallintasuunnitelma

Opinnäytetyötä varten kerätään julkisista kirjallisista lähteistä aineisto, joka koostuu päiväkirjamaisista muistiinpanoista. Aineisto ei sisällä henkilötietoja, yrityssalaisuuksia tai muuta arkaluontoista tai salassa pidettävää tietoa.

Aineisto säilytetään kannettavan tietokoneen kiintolevyllä ja Onedrive-levyllä. Aineistosta tehdään varmuuskopio ulkoiselle kiintolevylle kerran viikossa. Tekeillä oleva opinnäytetyö tallennetaan samalla tavoin.

Mikäli aineiston joukkoon sattuisi vastoin odotuksia päätymään henkilötietoja tai muuta arkaluontoista tai salassa pidettävää tietoa, niitä ei tallenneta Onedriveen.

Aineistoa säilytetään vähintään vuosi opinnäytetyön hyväksymisestä.