Mereta Helin

Kohti EU:n omaa turvallista kybermaailmaa

Tietotekniikan kandidaatintutkielma

25. huhtikuuta 2021

Jyväskylän yliopisto

Informaatioteknologian tiedekunta

Tekijä: Mereta Helin

Yhteystiedot: mehelin@student.jyu.fi

Ohjaaja: Timo Tiihonen

Työn nimi: Kohti EU:n omaa turvallista kybermaailmaa

Title in English: Towards the EU's own secure cyber world

Työ: Kandidaatintutkielma

Opintosuunta: Koulutusteknologia

Sivumäärä: 35+0

Tiivistelmä: Kyberrikollisuus kasvaa yhä kiihtyvään tahtiin. USA hallitsee globaalia internetiä teknologioillaan ja niin Venäjä kuin Kiinakin ovat jo rakentaneet oman kybermaailman omia tarkoitusperiä varten, joten voisiko Eurooppa ratkaista kyberrikollisuuden rakentamalla oman kybermaailman globaalin internetin rinnalle. Tässä kandidaattitutkielmassa tutkitaan olisiko mahdollista toteuttaa Euroopalle oma turvallinen kybermaailma ja voisiko se olla ratkaisu kasvavaan kyberrikollisuuteen. Kaikista lainsäädännöistä ja kyberrikollisuuden ehkäisevistä toimenpiteistä huolimatta, uutisista saa jatkuvasti lukea uusista tietoturvahyökkäyksistä, tietovuodoista, lunnasvaatimuksista ja yhä kehittyneimmistä haittaohjelmista sekä viruksista, joita yritetään epätoivoisesti korjata, paikata ja tukahduttaa. Nykyisellä linjalla ei voida enää jatkaa, vaan globaalin internetin rinnalle tarvitaan uusi turvallinen kybermaailma. Globaali internet pirstaloituu ja EU:n onkin syytä varautua maailmanlaajuisten tietoverkkojen hajoamiseen ja pohtia eurooppalaisille sopivia ratkaisuja tulevaisuutta varten.

Avainsanat: kyber, kyberuhka, kybermaailma, infrastruktuuri, kybertoimintaympäristö, EU, RuNet, GFW

Abstract: Cybercrime is growing at an ever-increasing rate. The US controls the global internet with its technologies and both Russia and China have already built their own cyber world for their own purposes, so could Europe solve cybercrime by building its own cyber world alongside the global internet. This bachelor's thesis examines whether it would be

possible to create a secure cyber world for Europe and whether it could be a solution to the growing cybercrime. Despite all legislation and measures to prevent cybercrime, the news keeps reading about new security attacks, data leaks, ransom claims and increasingly sophisticated malware, as well as viruses that are desperately trying to fix, patch and suppress. The current line can no longer be continued, but a new secure cyber world is needed alongside the global Internet. The global internet is fragmented and the EU needs to prepare for the disintegration of global information networks and consider solutions for the future for Europeans.

Keywords: cyber, cyber threat, cyber world, infrastructure, cyber environment, European Union, RuNet, GFW

Jyväskylässä 25. huhtikuuta 2021

Tutkielman tekijä Mereta Helin

Termiluettelo

BGP	Border Gateway Protocol on polkuvektoreihin perustuva reititysprotokolla, joka vastaa Internetin runkoverkossa tehtävistä reitityspäätöksistä.
Big Data	Big data tai massadata on erittäin suurten, järjestelemättömien, jatkuvasti lisääntyvien tietomassojen keräämistä, säilyttämistä, jakamista, etsimistä, analysointia sekä esittämistä tilastotiedettä ja tietotekniikkaa hyödyntäen.
BYOD- filosofia	Bring Your Own Device -ilmiö eli BYOD tarkoittaa omien laitteiden käyttämistä työtehtävien hoidossa.
DNS- injektio	DNS-injektio (DNS injection) on strategisesti sijoitettu verkon sisään DNS-pyyntöjen sieppaamiseksi. Aina kun injektio näkee estetyn verkkotunnuksen vastaavan DNS-pyynnön, se lähettää väärennetyn DNS-vastauksen, joka sisältää virheellisiä tietoja.
DNS- kaappaus	DNS-kaappaus tarkoittaa, että joku on muokannut reitittimesi asetuksia tahallaan ilman lupaasi. Tällaisen hyökkäyksen tekevä hyökkääjä voi seurata internet- liikennettäsi ja ohjata sitä uudelleen. Jos reitittimesi DNS on kaapattu, sinut saatetaan esimerkiksi ohjata tekaistuun versioon verkkopankkisivustostasi missä tahansa kyseiseen reitittimeen yhteyden muodostaneessa laitteessa. Hyökkääjä voi sitten saada verkkopankkiistuntosi haltuunsa ja käyttää sitä rahan siirtämiseen tietämättäsi. Kodin reitittimiä voidaan hakkeroida, jos ne sisältävät haavoittuvuuksia, tai jos ne on määritetty väärin.
Esineiden internet eli IoT	IoT on englanninkielinen lyhenne esineiden internetille. Esineiden internetillä tarkoitetaan internet- verkon laajentumista laitteisiin ja koneisiin, joita voidaan ohjata, mitata ja sensoroida internet- verkon yli.
IP-esto	IP-osoitteen esto (IP address blocking) on verkkopalvelun ko-

	koonpano, joka estää pyynnöt isänniltä, joilla on tietty IP-osoite. IP-osoitteen estoa käytetään yleisesti suojaamaan raakoja voimahyökkäyksiä vastaan ja estämään häiritsevän osoitteen pääsy. IP-osoitteen estoa voidaan käyttää rajoittamaan pääsyä tietylle maantieteelliselle alueelle tai alueelta, esimerkiksi sisällön jakelua tietylle alueelle.
Hajautettu palvelunestohyökkäys	Useista lähteistä tapahtuvaa hyökkäystä kutsutaan nimellä hajautettu palvelunestohyökkäys (Distributed Denial of Service, DDoS).
Mobiliteetti	Mobiliteetti on matkaviestinjärjestelmän ominaisuus, joka antaa matkaviestimen käyttäjälle mahdollisuuden telepalvelujen käyttöön samalla telepäätelaitteella oltaessa liikkeellä ja ennalta määräämättömissä paikoissa.
Pakettien väärinkäsittely	Pakettien väärinkäsittelyssä (Packet “mistreating” attacks) pääreititin käsittelee paketteja väärin, mikä johtaa ruuhkautumiseen, palvelunestoon ja niin edelleen. Tämän tyyppisiä hyökkäyksiä on vaikea havaita.
Palvelunestohyökkäys	Palvelunestohyökkäys (Denial of Service, DoS) tarkoittaa verkkohyökkäystä, jossa pyritään estämään verkkosivuston tarkoitettu käyttö. Tavallisimmin tämä toteutetaan kohdistamalla verkkosivustolle niin paljon liikennettä, että tämä ei käytännössä kykene palvelemaan asiakkaitaan.
Pilvipalvelu	Pilvipalvelu tarkoittaa tietoteknisten palveluiden toimittamista tarvittaessa tyypillisesti internetin välityksellä ja käytön mukaan maksamalla. Ydinkäsite tarkoittaa tietoteknisen infrastruktuurin tai datakeskuksien omistamisen sijaan vuokraamista pilvipalvelun tarjoajalta.
Reititystaulukon myrkytyshyökkäys	Reititystaulukon myrkytyshyökkäykset (Routing table attacks) viittaavat reititystaulukoiden haitalliseen muokkaamiseen tai

	"myrkyttämiseen". Tämä voidaan saavuttaa muuttamalla reititysprotokollien edellyttämiä reititystietopäivityspaketteja vahingollisesti. Tämä hyökkäys voi johtaa virheellisiin merkintöihin reititystaulukossa ja voi johtaa yhden tai useamman internet- toimialueen hajoamiseen.
SCADA	SCADA:lla (Supervisory Control and Data Acquisition) tarkoitetaan erilaisia teollisuusjärjestelmien ohjausjärjestelmiä, joita käytetään usein kriittisessä infrastruktuurissa. SCADA- järjestelmät koostuvat: fyysisistä ja ohjelmistollisista komponenteista eli osista kuten sensoreista ja antureista, tiedonsiirtoverkoista, ohjaimista, viestintälaitteista, käyttöliittymistä ja ohjelmistoista.
Syvä pakettien tarkastus	Syvä pakettien tarkastus (Deep packet inspection eli DPI) perustuu protokollien analyysiin ja tilastollisiin tietueisiin. IP-protokollan, jonka tarkoituksena on mahdollistaa tietojen siirtäminen Internetissä, on lisäksi olemassa lisäprotokollia, jotka koodaavat lähetettävää tietoa sovitulla tavalla (kuljetus, istunto, esitys ja sovellus jne.). Näiden protokollien tarkoituksena on varmistaa, että viestinnässä mukana olevat osapuolet ymmärtävät toisiaan.
TCP-nollaushyökkäys	TCP-nollaushyökkäys (TCP RST), on tapa manipuloida ja lopettaa internet- yhteys lähettämällä väärennetty TCP- palautuspaketti. Palomuuri voi käyttää tätä väärentämistekniikkaa keskeyttääkseen internet- yhteydet.

Kuviot

Taulukot

Sisällys

1 Johdanto

Internetiä ei ollut alun perin suunniteltu globaaliksi ja sen tietoturva on hyvin heikko ja kyberrikollisuus kasvaa yhä kiihtyvään tahtiin. Venäjä ja Kiina ovat jo rakentaneet oman kybermaailmaansa omiin tarkoitusperiinsä USA:n rinnalle, joka hallitsee globaalia internetiä teknologioillaan. Tämän työn taustakysymyksenä on, olisiko mahdollista rakentaa Euroopalle oma turvallinen kybermaailma ja voisiko se olla ratkaisu lisääntyneeseen kyberrikollisuuteen. Aihe on liian laaja tähän työhön, joten kirjallisuuskatsauksessa tarkastellaan vastauksia seuraaviin kahteen kyberturvallisuutta koskevaan kysymykseen:

- Mitkä ovat kybermaailman uhkat ja riskit?

- Onko yhteiskunnallisia ja teknisiä haasteita rakentaa Euroopalle oma kybermaailma?

Aluksi tarkastellaan kybermaailman rakennetta sekä sen suurimpia uhkia ja kustannuksia, jonka jälkeen käydään läpi yhteiskunnan haasteita hallita globaalia internetiä, siirtyen tarkastelemaan Kiinan suurta palomuuria ja Venäjän RuNet- verkkoa sekä internetin pirstaloitumisen vaikutuksia. Lopuksi pohditaan EU:n oman kybermaailman toteutumisen tarvetta ja päätetään työ johtopäätöksiin.

2 Kybermaailma

Lehto (2020a) kuvailee kybermaailman muodostuvan kaikista niistä erilaisista digitaalisessa muodoissa olevista tietojen käsittelyyn tarkoitetuista tietoverkoista ja -laitteista, tietojärjestelmistä sekä niiden käyttäjistä, ympäristöistä jossa niitä käytetään ja toimintaprosesseista. Kuitenkin hän toteaa kybermaailman eri aktiviteettien olevan hankalaa, sillä niiden rajat ovat epäselviä ja päällekkäisiä.

Jo kaksikymmentä vuotta sitten kansallisen turvallisuusneuvoston tietoverkkoturvallisuuden erityisneuvonantaja Richard Clarken totesi CNN:n haastattelussa:(2001) "Elintapamme riippuu kyberavaruudesta riippuvien kriittisten järjestelmien turvasta ja luotettavasta toiminnasta" CNN.com (2001). (suomennos minun)

Kybermaailmasta ja kyberturvallisuudesta on tullut osa arkipäiväämme ja bittien toimivuudesta on riippuvaisia niin maailmantalous, yhteiskuntien turvallisuus, yritysten toiminta kuin elämäntapammekin. On yhä upeampia mahdollisuuksia nauttia maantieteellisesti ja ajallisesti rajatonta digitaalista maailmaa, mutta samalla haittapuolena on haavoittuvuuden lisääntyminen. Kybermaailmaa ei voi sijoittaa vain bittien maailmaan, sillä selkeää jakoa ei voi tehdä fyysiseen ja bittien maailmaan, sillä kyberulottuvuuden tapahtumilla on selkeitä seurauksia myös fyysiseen maailmaan (Limnéll, Majewwski ja Salminen 2014).

Limnell (2014) mukaan kyberturvallisuus ja erilaiset kyberkäsitteet on ymmärrettävä monitahoisena ja voimistuvana ilmiönä, joten ei ole yhdentekevää kuinka niistä keskustelemme suomalaisessa yhteiskunnassa. Tästä syystä käsitteet ovat välttämättömiä, sillä ne auttavat meitä hahmottamaan ja jäsentämään maailmaa, tai sitä kuinka haluamme sitä hahmotettavan. Tärkeää on saada määriteltyä selkeästi mitä tarkoitetaan kyber- alkuisilla käsitteillä ja vaikka Suomen Kyberturvallisuusstrategiassa on jo tehty näitä määritelmiä, määrittelytyö tulee jatkumaan vaikka kyber- käsitteiden voi nähdä jo tulleen suomalaiseen turvallisuusajatteluun.

Seuraavaksi esitellään tämän työn kannalta keskeisimmät kybermaailman käsitteet: kyber, kybertoimintaympäristö, kriittinen infrastruktuuri, kyberuhka ja kyberturvallisuus. Lisäksi liitteenä on termiluettelo tarvittavista teknisistä termeistä, sekä hahmottellemani kuva kyber-

maailmasta, joka pohjautuu Sanastokeskus (2018) määrittelyyn siitä, mistä osista kybermaailma koostuu.

2.1 Kyber

Sana kyber on peräisin kreikankielen sanasta “kybereo” eli ohjata, opastaa, hallita ja sitä käytetään lähes aina yhdyssanan määriteosana. Sanan merkityssisältö liittyy yleensä sähköisessä muodossa olevan informaation käsittelyyn, kuten tietotekniikkaan, sähköiseen viestintään, tieto- ja tietokonejärjestelmiin. Vasta koko yhdyssanan määriteosalla ja perusosalla saadaan sille oma merkityksensä (Turvallisuuskomitea 2013).

Myös Sanastokeskus (2018) määrittelee kyber- sanan merkityssisällön liittyvän yleensä digitaalisessa muodossa olevan informaation käsittelyyn, kuten tietotekniikkaan, digitaaliseen viestintään, tietojärjestelmiin tai tietokonejärjestelmiin.

2.2 Kybertoimintaympäristö

Limnell (2014) mukaan kybertoimintaympäristö on yhdestä tai useammasta tietojärjestelmästä muodostuva toimintaympäristö, jossa käsitellään sähköisessä muodossa olevaa informaatiota. Sanastokeskuksen (2018) mukaan myös datan ja informaation käsittelyyn liittyvät fyysiset rakenteet kuuluvat kybertoimintaympäristöön. Esimerkiksi tietojärjestelmiin perustuvat ydinvoimalan ohjausjärjestelmä ja elintarvikkeiden kuljetus- ja logistiikkajärjestelmä ovat kybertoimintaympäristöjä, samoin kuin liikenteen ohjausmääritelmät sekä pankki- ja maksujärjestelmät.

Kyberavaruuden teknologiat muuttuvat jatkuvasti ja uusia verkkoon kytkettäviä kodinkoneita, sosiaalisia verkostoja, pilvipalveluja sekä mobiilisovelluksia tulee jatkuvasti lisää, jolloin ympäristön toimijoiden on muutettava tai mukautettava tekniikoitaan (Kriz 2011).

2.3 Kriittinen infrastruktuuri

Kriittinen infrastruktuuri koostuu rakenteista ja toiminnoista, jotka ovat välttämättömiä yhteiskunnan elintärkeille toiminnoille, sisältäen niin fyysisiä laitoksia ja rakenteita kuin sähköisiä toimintoja ja palvelujakin (Turvallisuuskomitea 2013). Sanastokeskus (2018) mukaan esimerkiksi energian tuotanto-, siirto- ja jakelujärjestelmät, liikenne ja logistiikka, tieto- ja viestintäjärjestelmät sekä vesi- ja jätehuolto ovat osa kriittistä infrastruktuuria.

2.4 Kyberuhka

Sanastokeskus (2018) kuvaa kyberuhkan olevan kybertoimintaympäristössä mahdollisesti tapahtuva teko tai tapahtuma, joka vaarantaa toteutuessaan jonkin siitä riippuvaisen toiminnon. Kyberuhkat voivat aiheutua tietoturvauhkista, jotka ovat jo toteutuneet, mutta myös digitaalisessa viestintäympäristössä toteutettavista teoista, jotka vaarantavat yhteiskunnan turvallisuutta. Kyberuhkat voivat olla peräisin maan rajojen sisältä tai niiden ulkopuolelta ja kohdistua yhteiskunnan elintärkeisiin toimintoihin, kansalliseen kriittiseen infrastruktuuriin tai kansalaisiin joko suoraan tai välillisesti.

Valtioneuvoston kanslia (2012) toteaa kybertilan häiriöiden olevan kriittinen uhkatekijä. Kyberuhkaa voivat aiheuttaa niin tietoverkkojen sisäiset heikkoudet kuin ulkoiset toimijatkin, jotka joko aiheuttavat vahinkoa tai hankkivat laittomasti tietoa. Lisäksi myös laajat tietoverkot ovat alttiita tahattomillekin toimintahäiriöille. Onkin haastavaa erottaa, onko kyseessä vahinkoa aiheuttanut valtiollinen vai ei-valtiollinen toimija sekä uhkien alkuperä.

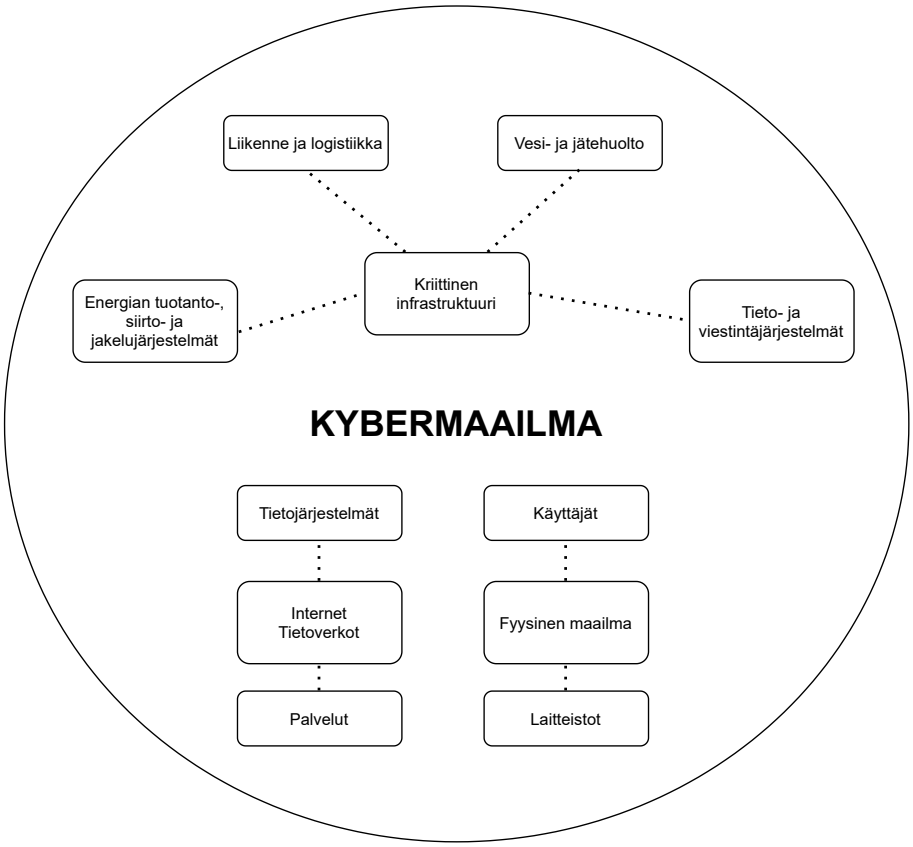
Suurin osa toteutuneista kyberuhkista ei ole tarkoituksellisesti aiheutettuja, vaan esimerkiksi syysmyrskyt, ohjelmistovirheet ja erilaiset tekniset viat ovat kybermaailman toimimattomuuden taustalla (Limnéll, Majewwski ja Salminen 2014). Valtioneuvoston kanslian (2012) mukaan kyberuhkat ovatkin laaja-alainen ja merkittävä haaste kokonaisturvallisuudelle ja kybertoimintaympäristöön kohdistuvat uhkat ovat koko yhteiskunnan kannalta muuttuneet vaikutuksiltaan yhä vaarallisemmiksi.

2.5 Kyberturvallisuus

Kyberturvallisuus on tavoitetila, jossa kybertoimintaympäristöön luotetaan ja sen toiminta on turvattu (Sanastokeskus 2018). Tavoitetilassa kybertoimintaympäristö ei aiheuta haittaa eikä häiriötä sähköisen informaation käsittelystä riippuvaiselle toiminnalle eikä sen toimivuudelle, ja luottamus kybertoimintaympäristössä perustuu toimijoiden tarkoituksenomaisiin ja riittäviin tietoturvallisuusmenettelyihin (Turvallisuuskomitea 2013). Häiriöt kybertoimintaympäristön toiminnassa aiheutuvat usein toteutuneesta tietoturvauhkasta, joten tietoturva on keskeinen tekijä kun pyritään kyberturvallisuuteen (Sanastokeskus 2018).

Kyberturvallisuuteen pyritään tietoturvan lisäksi myös toimenpiteillä, joiden tarkoituksena on turvata häiriytyneestä kybertoimintaympäristöstä riippuvaiset fyysisen maailman toiminnot (Sanastokeskus 2018). Kyberturvallisuus sisältää yhteiskunnan elintärkeisiin toimintoihin ja kriittiseen infrastruktuuriin kohdistuvat toimenpiteet, joilla pyritään ennakoivasti hallitsemaan ja tarvittaessa jopa sietämään kyberuhkia ja niiden vaikutuksia, jotka voivat aiheuttaa merkittävää haittaa tai vaaraa valtiolle tai väestölle (Turvallisuuskomitea 2013). Kyberturvallisuus on digitaalisen ja verkottuneen yhteiskunnan tai organisaation turvallisuutta ja sen vaikutusta niiden toimintoihin (Sanastokeskus 2018).

Tästä voi päätellä, että kybermaailmaa tarvitaan päivittäisiin toimiin, mutta kybermaailmassa on runsaasti heikkouksia ja erilaisia uhkia joita vastaan on kehitettävä alati uusia keinoja varautua ja puolustautua. Koko yhteiskunta toimii kybermaailmassa, joten kyberuhkat ovat merkittävä vaaratekijä.



Kuvio 1. Kybermaailma (Kuva oma, piirretty Sanastokeskus (2018) lähteitä mukaillen

3 Kyberuhkat ja niiden kustannukset

Minchev (2016) toteaa nykyaikaisten verkkotekniikoiden olevan välttämätön osa arkipäiväämme, joka on muodostanut uuden, päällekkäisen teknisen ja sosiaalisen todellisuuden. Se on kuitenkin tuonut kybermahdollisuuksien lisäksi myös runsaasti uhkia, jotka syntyvät ihmisen ollessa koneella ja tietokoneelta tietokoneelle välisen vuorovaikutuksen seurauksena.

Limnéll, Majewwski ja Salminen (2014) korostavat että kyberturvallisuuden näkökulma täytyy huomioida alusta alkaen, sillä toimivin kyberturvallisuus luodaan, kun se rakennetaan sisään järjestelmiin, tuotteisiin ja ratkaisuihin. Kyberuhkat ovat todellisia ja ovat pahimmillaan vaikutuksiltaan hyvin vakavia ja voivat tulla hyvin kalliiksi niin yhteiskunnissa kuin yrityksissäkin, jos asiaan suhtautuu välinpitämättömästi. Heidän mielestänsä on tärkeää on muistaa kuitenkin myös toinen puoli, eli kyberturvallisuuden tuomat mahdollisuudet. Vaikka uhkat ovat vakavia, täytyy muistaa kybermaailman mahdollisuudet, joista voidaan nauttia päivittäisessä työelämässä kuin vapaa-ajallakin. Onkin etsittävä tasapaino mahdollisuuksien ja uhkien välille, ottaen huomioon kunkin organisaation erityispiirteet ja tilanne.

3.1 Kyberuhkat ja kybermaailman haavoittuvuudet

Limnéll, Majewwski ja Salminen (2014) toteaa maailmassa käytävän kahta kilpajuoksua kybermaailman osalta, kun yhteiskunnat, yritykset, asevoimat ja tietoturvat yrittävät luoda mahdollisimman tehokkaita puolustusmekanismeja suojatakseen tietojärjestelmät ja kybermaailman, kun taas toisella puolella kyberrikolliset, toiset valtiot ja haktivistit tekevät jatkuvalla syötöllä hyökkäyksiä puolustajan järjestelmiä vastaan ja pyrkivät löytämään sieltä haavoittuvuuksia ja aukkoja. Hyökkääjien keinojen käydessä yhä monimutkaisemmiksi ja ovelimmiksi, puolustajat pyrkii estämään hyökkääjien onnistumisen ja tätä hyökkäyksen ja puolustuksen välistä taistelua käydään joka hetki. Kyberympäristössä ongelmien aiheuttajat toimivat usein ammattimaisesti, jolloin tulee uusia haasteita uhkien torjumiseen. Rikolliset onkin siirtyneet sinne missä rahaa on, eli bittien maailmaan. Symantecin kyberrikollisuudesta kertovan raportin (2012) mukaan joka sekunti 18 ihmistä joutuu kyberrikollisuuden

kohteeksi, eli 1,5 miljoonaa uhria päivässä.

Lehto ym. (2017) ovat käyneet läpi johtavien kyberturvallisuustoimijoiden ennusteita läpi ja tietoturvayhtiö McAfee (2016) mukaan kyberturvallisuutta eniten muokkaavat tekijät ovat yhä enemmän laajeneva kyberhyökkäysala, hakkeroinnin teollistuminen, IT- tietoturvamarkkinoiden monimutkaisuus sekä hajautuneisuus. McAfee ennakoi tulevaisuudessa nähtävän: laajempia kyberhyökkäyksiä, hyökkääjät kehittyvät entisestään, tietovuotojen kustannukset kasvavat, yhteensopivista tietoturvateknologioista ja taitavista tietoturva-ammattilaisista on puutetta. AT&T (2015) mainitsee suurimmat alueet, joihin se arvioi syntyvän uusia, vaarallisia mahdollisuuksia kyberhyökkääjille tulevina vuosina: Esineiden internet, pilvipalvelut, Big Data, Mobiliteetti ja BYOD -filosofia, eli Bring Your Own Device.

Kybertoimintaympäristö on perinteisten virusten, haittaohjelmien ja identiteettivarkauksien lisäksi jatkuvasti alttiina myös esimerkiksi luonnonkatastrofeille, fyysisen maailman ongelmille ja kyberrikollisten hyökkäyksille. Tiedustelutoiminta ja kybervakoilu on valtioilla yleistä ja monet maat suunnittelevat vastaiskuja niitä vastaan kohdistettuihin kyberhyökkäyksiin, eikä kybersotakaan ole mahdoton (Jansson ja Sihvonen 2018).

3.2 Kyberhyökkäykset

Internetin infrastruktuuriin hyökkääminen voi johtaa valtavaan tuhoon, sillä internetin eri komponentit ovat implisiittisessä luottamussuhteessa toisiinsa (Chakrabarti ja Manimaran 2002). Border Gateway Protocol (BGP) yhdistää reitittimiä, joiden määrä kasvaa jatkuvasti ympäri maailmaa. Se on laadittu ensimmäisen kerran vuonna 1989, eikä sitä ole yritetty tänä aikana turvata jonka vuoksi tämä jättää tilaa suurelle määrälle virheitä, joita onkin hyödynnetty useita kertoja historian aikana (Sauer 2020).

Hyökkäykset ovat toimia, joiden tarkoitus on vahingoittaa järjestelmää tai häiritä sen normaalia toimintaa hyödyntäen haavoittuvuuksia erilaisilla tekniikoilla ja työkaluilla (Abomhara ja Køien 2015). Tämä onkin mahdollistanut sen, että pahantahtoiset käyttäjät ovat hyödyntäneet haavoittuvuuksia niin kauan kuin globaali tietokoneverkko on ollut olemassa (Hutchins, Cloppert, Amin ym. 2011, s. 13–15). Chakrabarti ja Manimaran (2002) mukaan internetin infrastruktuurin turvallisuuden perimmäinen tavoite on suojata internetin protokollapa-

ketteja tunnetuilta ja tuntemattomilta tietoturvahyökkäyksiltä.

Rivero (2018) on koonnut kaikkien aikojen kymmenen suurinta tietorikkomusta taulukoksi, jossa ne esitellään suurimmasta pienimpään rahallisen menetyksen mukaan tapahtumavuosineen.

Yritys	Summa ja vuosi
1. Yahoo	3 miljardia (2013)
2. Marriott	500 miljoonaa (2014–2018)
3. Adult FriendFinder	412 miljoonaa (2016)
4. MySpace	360 miljoonaa (2016)
5. Under Armour	150 miljoonaa (2018)
6. Equifax	145,5 miljoonaa (2017)
7. eBay	145 miljoonaa (2014)
8. Target	110 miljoonaa (2013)
9. Heartland Payment Systems	100+ miljoonaa (2008)
10. LinkedIn	100 miljoonaa (2012)

Taulukko 1. Kaikkien aikojen 10 suurinta tietorikkomusta (Rivero 2018)

Internetin infrastruktuurin hyökkäykset voidaan luokitella seuraaviin neljään eri luokkaan: DNS-kaappaus (DNS “hacking” attacks), reititystaulujen myrkytykset (Routing table “poisoning” attacks), pakettien väärinkäsittelyt (Packet “mistreating” attacks) ja palvelunestohyökkäykset (Denial of Service (DoS) attacks) (Chakrabarti ja Manimaran 2002).

Abomhara ja Køien (2015) mukaan hyökkäys voi tapahtua monella eri tapaa, joista yleisimpiä kyberhyökkäyksiä ovat: fyysiset hyökkäykset joissa muutetaan laitteistokomponentteja, tiedusteluhyökkäykset joissa järjestelmiä käytetään luvattomasti ja kartoitetaan palveluja tai haavoittuvuuksia, ja palvelunestohyökkäys eli DoS, jossa hyökkäyksen tarkoitus on saada koneen tai internetverkon resurssit tavoittamattomaksi. Lisäksi on myös pääsyhyökkäykset, joissa luvattomat henkilöt pääsevät internetverkkoihin tai laitteisiin joihin ei ole oikeutta mennä, sekä yksityisyyden hyökkäykset, jossa yleisimpiä hyökkäystyyppejä ovat: tiedonlouhinta, verkkovakoilu, salakuuntelu, seuranta, sanakirjahyökkäykset, verkkorikokset, tu-

hoisat hyökkäykset sekä valvonta- ja tiedonkeruuhyökkäykset teollisuuden ohjausjärjestelmiin (SCADA).

3.3 Kyberrikosten kustannukset

Mattila (2020) on selvittänyt, että vuonna 2018 tietoturvayhtiö McAfee ja ajatushautomo CSIS ovat arvioineet kyberrikollisuuden maailmanlaajuisiksi kustannuksiksi 600 miljardia euroa, joka on noin 0,8 prosenttia koko maailman vuotuisesta bruttokansantuotteesta. Kyberhyökkäyksen kohteeksi joutuneet suuryritykset joutuivat maksamaan viime vuonna arviolta keskimäärin 4,6 miljoonaa dollaria (n. 3,8 miljoonaa euroa), joka on yli 50 prosenttia enemmän kuin vuosi aiemmin. Yksi suurimpia ihmiskunnan haasteita seuraavien kahden vuosikymmenen aikana tulee olemaan tietoverkkorikollisuus, sillä kyberhyökkäykset ovat maailman nopeimmin kasvava rikollisuus, jonka koko ja kustannukset tulevat kasvamaan. Taloudellisten seuraamusten uhkaa ovat lisänneet Euroopassa GDPR-lainsäädännön mahdollistamat sanktiot yrityksille tietoturvan laiminlyönneistä, jotka koskettavat niin suuria kuin pieniäkin yrityksiä.

Tietoverkkorikollisuuden vahingot tulevat maksamaan globaalisti 6 biljoonaa dollaria vuodessa vuoteen 2021 mennessä. Teknologian kehitys on tärkeää talouskasvulle, mutta samalla se on myös johtanut lisääntyneisiin kyberhyökkäyksiin. Verkkokauppa, mobiilimaksut, pilvipalvelut, Big Data ja analytiikka, esineiden internet, tekoäly, koneoppiminen ja sosiaalinen media, lisäävät kyberriskiä käyttäjille ja yrityksille. Verkkokaupoissa on ollut saatavilla jo usean vuoden ajan hakkerointityökaluja ja -sarjoja verkkohyökkäyksille, henkilöllisyysvarkauksille, haittaohjelmille, kiristysohjelmille ja muihin pahoihin tarkoituksiin. Hinnat alkavat niinkin alhaisesta kuin 1 dollari, joka tekee pääsyn kyberrikollisuuteen lähes ilmaisen kustannuksiltaan (Morgan 2019).

MTV–uutiset (2018) kirjoittaa kyberhyökkäysten määrän kasvaneen etenkin Yhdysvalloissa. F-Securen toimitusjohtaja Samu Konttisen mukaan Yhdysvallat, Venäjä ja Kiina ovat aktiivisimpia kybertiedustelussa ja siellä on normaalia verkkorikollisuutta, joka voi pahimmillaan lamauttaa infrastruktuuria. Tietoturva-asiantuntija Petteri Järvisen mukaan on todennäköistä, että myös Suomessa tullaan näkemään yhä enemmän kiristyshaittaohjelmia. Nykänen (2020)

kirjoittaa artikkelissaan kuinka kiristyshaittaohjelmia tehtaillaan yhä ammattimaisemmin, ja niiden olevan pelottavin tietoturvauhka tällä hetkellä. Esimerkiksi Bulgariassa toimii rikollisia, jotka päivätöikseen suunnittelevat ja toteuttavat kyberhyökkäyksiä, eikä lainsäädännön voimin olla kyetty kyseisissä maissa asiaan toistaiseksi puuttumaan. Vahingot voivat olla hyvin suuria kyberhyökkäyksen kohteeksi joutuneelle.

4 Kybermaailma - yhteiskunta ja tekniikka

Limnéll, Majewwski ja Salminen (2014) mukaan on erittäin tärkeää varautua uhkiin ja pyrkiä suojautumaan niiden negatiiviselta vaikutukselta, joka toteutuu parhaiten laittamalla kyberturvallisuuden perusasiat kuntoon, kaikkien tietoisuutta ja toimintakykyä lisäämällä sekä pitämällä tietoturva ajan tasalla. On myös tunnistettava kyberturvallisuuden haasteet ja reagoida niihin, sillä se on ainut keino suojautua mustilta joutsenilta, eli tunnistamattomilta kyberuhilta. Kybermaailma kehittyy ja muuttuu jatkuvasti, joten on mahdotonta pysyä täysin ajan tasalla sen kanssa.

4.1 Yhteiskunnan haasteet hallita globaalia internetiä

Valtiolle ei ole helppoa vaikuttaa kybertoimintaympäristössä, sillä siihen sisältyy ainakin kolmenlaisia haasteita, joista ensimmäinen haaste on Singerin ja Friedmanin (2014) mukaan se, että valtio ylläpitää byrokratiaa ja on siksi hidas, joten se ei kykene vastaamaan kybermaailman hektisyyteen kovin helposti, jossa hyökkäykset tapahtuvat ilman ennakkovaroituksia. Isot strategiset päätökset ja lakimuutokset vievät aikaa ja niiden sisältö on voinut jo vanheta siinä vaiheessa, kun ne lopulta valmistuvat (Jansson ja Sihvonen 2018).

Toiseksi valtio joutuu myös alati pohtimaan puolustuspolitiikkaansa ja kansainvälisen yhteistyön mahdollisuuksia muuttuvassa digitaalisessa ympäristössä. Siinä missä fyysisessä maailmassa on helpompaa osoittaa missä menevät maiden väliset rajat ja niitä puolustavat sotavoimat, voivat valtiot suvereniteetin ollessa uhattuna asettaa toisensa kauppasaartoon tai muihin pakotteisiin, kun taas kybermaailmassa ei välttämättä vastustajaa tunneta, tai hyökkäyksen taustalla voi olla jokin muukin toimija kuin valtio. Kyberrikollisuus on globaali, joten se on valtioille yhteinen uhka, joten rangaistusten asettaminen vaikeutuu. Kansainvälinen yhteistyö ei kuitenkaan jakaudu tasa-arvoisesti eri maiden kesken ja vaikka kansainvälisestä yhteistyöstä puhutaan paljon, kybermaailmasta puuttuvat kansainväliset standardit, joiden puitteissa kyberturvallisuutta toteutetaan (Jansson ja Sihvonen 2018).

Kolmas valtion haaste kybertoimintaympäristön toimijana on kysymys valtion oikeudesta määrätä yksityisen sektorin toiminnasta, sillä Choucri ym. (2014) mukaan kybertoimintaym-

päristön perusarkkitehtuuria ylläpitävät ei-hallinnolliset elimet, eivät valtiot. Singer ja Friedman (2014) mukaan Internet Engineering Task Force (IETF) kehittää internet-standardia ja -protokollia, jonka toiminnalle teknistä tukea antaa Internet Engineering Steering Group (IESG), joka on yhteistyössä Internet Architecture Boardin (IAB) kanssa. Nämä taas vastaavat toiminnastaan Internet Societylle (ISOC), joka valvoo avoimen lähdekoodin laillisia oikeuksia. Sen lisäksi internetissä on myös muita oleellisia osia, joita tarvitaan sen toimintaan, kuten nimipalvelu, josta on vastuussa Internet Corporation for Assigned Names and Numbers (ICANN), joka jakaa ja hallinnoi verkkosivujen IP-osoitteita (Jansson ja Sihvonen 2018).

Hallamaa (2019) kirjoittaa globaalin nimipalvelujärjestelmän olleen pitkään Yhdysvaltojen hallinnassa, joka ärsytti varsinkin Venäjää ja Kiinaa. Nimipalvelujärjestelmä siirrettiin verkkotunnuksia hallinnoivan kansainvälisen ICANN-järjestön alaisuuteen, joka oli Venäjän ja Kiinan mielestä muutos oikeaan suuntaan, mutta maat toivoivat että nimipalvelujärjestelmä siirrettäisiin YK:n alaisuuteen, jolloin vaikutusmahdollisuuksia olisi enemmän. Venäjä näyttää nyt keskittyvän oman internetin rakentamiseen kansainvälisen nimipalvelujärjestelmän vaikuttamisen sijaan ja Venäjän hallinto onkin ilmoittanut tavoitteekseen reitittää 95 prosenttia internet-liikenteestä paikallisesti ensi vuoteen mennessä.

4.2 Kiinan suuri palomuuri

Ensimmäinen lähetetty sähköposti vuonna 1987 liitti viestinsä mukaan Kiinan koko maailmaan. Muutaman vuoden kuluttua siitä, maa sai ensimmäisen internetliittymän ja vuonna 1996 säädettiin ensimmäinen sensuurilaki, jonka jälkeen kaikkien IPS- osoitteiden tuli olla valtion hyväksymiä. Tuolloin oli rakenteilla jo internetin käyttöön liittyvä mittava sensuurijärjestelmä, jota kutsutaan Kiinan suureksi palomuuriksi (Great Firewall) (Airaksinen 2020), joka tunnetaan myös nimellä GFW (Anderson 2012). Se on serveri, jonka tarkoitus on estää pääsy ulkomaalaisille verkkosivustoille, joita hallitus pitää epämieluisina (Airaksinen 2020).

GFW salaa kaikki kansainväliset linkit ja tarkastaa liikenteen havaitsemalla yhdyskäytävän läpi kulkevat arkaluontoiset avainsanat syvä pakettitarkastus- tekniikalla (Deep packet inspection). GFW toimii pääasiassa kolmella eri tekniikalla haitallisten tietojen estämiseksi: IP-

esto (IP address blocking), DNS (Domain Name System) injektio (DNS injection) ja TCP-nollaushyökkäys (TCP RST) (Anderson 2012).

Kiinan käyttämää internet- suodatusjärjestelmää pidetään yhtenä maailman kehittyneimmistä vastaavanlaisista järjestelmistä. Verrattuna muiden valtioiden vastaaviin ponnisteluihin, Kiinan suodatusjärjestelmä on laaja, pitkälle kehitetty ja tehokas. Se käsittää useita oikeudellisen sääntelyn ja teknisen valvonnan tasoja. Siihen osallistuu lukuisia valtion virastoja ja tuhansia julkisia ja yksityisiä henkilöitä. Se sensuroi useilla menetelmillä lähetettyä sisältöä, mukaan lukien verkkosivut, verkkolokit, online-keskustelupalstat, yliopiston ilmoitustaulujärjestelmät ja sähköpostiviestit (Bambauer ym. 2005). Kiinan palomuuri on rakennettu lähinnä propagandatarkoitukseen, ja siitä ovat vastuussa Kiinan yleisen turvallisuuden ministeriö, joka tekee sensuuripäätökset ulkomaisesta materiaalista (Airaksinen 2020).

Sensuroituja tai osittain sensuroituja sosiaalisen median sivustoja ja sovelluksia sekä hakukoneita ovat tällä hetkellä esimerkiksi Facebook, Twitter, Snapchat, Instagram, Youtube, Pinterest, Tinder, Google ja Yahoo. Kiellettyjä viestisovelluksia ovat esimerkiksi Facebook Messenger, Whatsapp ja Telegram. Myös uutisia ja informaatiosivuja kuuluu kiellettyjen listaan, kuten New York Times, The Economist, CNN, BBC ja englanninkielinen Wikipedia. Palomuuri estää myös sovelluksien latauksen, osan VPN- yhteyksistä, sähköpostit ja pikaviestit (Airaksinen 2020).

Kurenmaa (2020) on selvittänyt että Pekingissä sijaitsee Kyberavaruuden hallinto (Cyberscpace Administration of China CAC), joka on virasto, jonka tehtävä on valvoa, sensuroida ja hallita Kiinan internetiä. Kyberavaruuden hallinto uudelleenarvioi tietyin aikavälein kyberavaruutta tai tekee erilaisia puhdistuksia tiettyihin aiheisiin keskittyen. Sensuuria kiristetään esimerkiksi protestien vuosipäivien lähestyessä. Kiinan hallituksen Cyberspace Administration of China CAC (2020) sivuilta löytyy vuoden 2020 kesäkuun ensimmäinen päivä alkanut tarkastus ja siihen liittyvät toimenpiteet.

Kiinan maakuntiin perustettiin ensimmäiset internetin poliisiryhmät valvomaan internetin käyttöä 2000-luvun alussa ja internetin valvonta työllistääkin kymmeniä miljoonia kiinalaisia. Kiinan valtio on arviolta estänyt pääsyn yli 500 000 verkkosivustolle ja viimeisten vuosien aikana Kiinan hallinto on säätänyt uusia rajoituksia estämään internetin vapaata käyttöä

lakien ja määräysten muodossa, joista monet rajoitukset antavat Kiinan hallitukselle yhä paremmat mahdollisuudet puuttua heille vahingollisen materiaalin julkaisemiseen. Sensuuritoimille on käytetty yleisesti perusteluna pornografian julkaisemisen vastaista taistelua. Suurten nettirajoitusten takia maan tärkeimmät palveluntarjoajat ovat kiinalaisia, esimerkiksi hakurobotti Baidu, sosiaalinen verkosto Renren, verkkokauppayritys Alibaba ja Twitter-tyylinen mikroblogi Sina Weibo, joka on Kiinan suosituin mikroblogipalvelu (Airaksinen 2020).

Kiinan kyberturvallisuuden strategia koostuu neljästä pääteemasta:

1) Hallita internetin sisältöä ja luoda sinne positiivista energiaa

2) Taataan yleinen kyberturvallisuus ja suojellaan tietoinfrastruktuuria

3) Luodaan laitteille ja ohjelmille Kiinan oma ja itsenäinen tekninen alusta, joilla kontrolloidaan internetiä Kiinassa

4) Lisätään Kiinan kansainvälistä roolia internetin rakentamisessa, hallinnassa ja toiminnassa.

Kiinasta on tarkoitus kehittää kybersupervalta. Strategisen suunnitelman takana on nykyinen presidentti Xi Jin- ping ja hänen toimensa oman vallan ja kommunistisen puolueen vallan vahvistamiseksi. Positiivisen energian luomisella internetiin pyritään siihen, että kansalaisilta halutaan positiivista internet- keskustelua, unohtaen negatiivisiin epäkohtiin takertuminen. Tärkein osa tätä positiivisen energian -kampanjaa, on luettavissa rivien välistä vaatimus siitä, ettei kritiikkiä saa esittää valtiota kohtaan (Airaksinen 2020).

4.3 Venäjän RuNet

RuNet on venäjänkielinen, itsenäinen ja suhteellisen suljettu online-ympäristö, joka perustuu myös "venäläiseen toimintatapaan", tarkoittaen esimerkiksi suvereniteettiin, riippumattomuuteen lännestä ja "digitaalisen itsemääräämisoikeuden"palauttamiseen (Ristolainen 2017). Myös Huhtanen (2018) toteaa, että tutkijoiden mukaan Venäjä pyrkii digitaaliseen suvereniteettiin, joka tarkoittaa valtion kontrolloimaa ja kansallisen turvallisuuden takaavaa verkkoa. Länsimaisessa ajattelutavassa internet taas perustuu avoimuuteen ja datan vapaaseen liikku-

vuuteen.

Venäjän hallitus on viime vuosina kiristänyt merkittävästi Venäjän tietotilan valvontaa ja hallituksen lisääntyvä aktiivisuus tekee RuNet- verkosta entistä venäläisemmän ja myös valtiollisemman, sillä valtio valvoo internetiä rajojensa sisällä ja sensuroi tai tukahduttaa Venäjän tietotilassa liikkuvan tiedon. Sen lisäksi venäläisiä kannustetaan pysymään "kansallisen verkon"puitteissa, jolloin tietotilan muotoilu saa aikaan luonnollisen ja itsensä saavuttaman eristämisen (Ristolainen 2017).

Venäjän hallinnon näkökulmasta RuNet on Venäjän lainsäädännön alainen tietoverkko, joten valtion turvallisuusviranomaiset valvovat sen liikennettä. Venäjän turvallisuuspalvelu FSB valvoo internetliikennettä niin sanotun Sorm-järjestelmän avulla ja venäläiset operaattorit on velvoitettu auttamaan FSB:tä verkkovalvonnan järjestämisessä. Gossopka on toinen keskitetty verkkovalvonnan väline Venäjällä, joka on FSB:n parhaillaan kehittämän järjestelmä, jonka tarkoituksena on tarkkailla keskitetysti verkkohyökkäyksiä ja auttaa puolustautumaan kriittisiin verkkoihin kohdistuvia hyökkäyksiä vastaan (Huhtanen 2018).

Kun Venäjä valmisteli valtiollisen informaatioturvallisuusdoktriinin päivittämistä, se listasi myös mahdollisia uhkia vuodelle 2016, joihin kuului esimerkiksi se, että ”valtiot käyttävät teknologista ylivaltaansa taloudellisten ja geopoliittisten etujensa ajamiseen kansainvälisessä informaatioympäristössä”, jolla tarkoitetaan esimerkiksi kahta jättimäistä amerikkalaisyritystä Applea ja Microsoftia, jotka korostavat Yhdysvaltojen valta-asemaa verkossa. Venäjä on myös jäänyt kehityksessä jälkeen ja se, että on toisten kehittämästä teknologiasta riippuvainen, koetaan uhkana. Venäjä on kokenut olevansa liian riippuvainen muista myös internetin ja sen rakenteiden suhteen ja kokee internetin olevan uhka, sillä Venäjää voidaan vahingoittaa sen kautta (Halminen 2019).

RuNet on Venäjän hallinnolle vaihtoehto amerikkalaisvetoiselle läntiselle internetille ja siihen onkin kehitetty esimerkiksi omat venäläiset sosiaalisen median palvelunsa, hakukoneensa ja sähköpostipalvelunsa, jotka ovat yksityisten yritysten omistamia, mutta yrityksillä on läheiset yhteydet Venäjän poliittiseen hallintoon (Huhtanen 2018). RuNet:ssa on hyvin kehittyneitä ja erittäin suosittuja hakukoneita, kuten Yandex ja Rambler, sosiaalisten verkostojen sivustoja, kuten Vkontakte, Odnoklassniki, LiveJournal, Moi Mir ja ilmainen sähköpostipal-

velu, mail.ru (Ristolainen 2017).

Venäjä on suunnitellut jo vuosien ajan oman RuNet- verkkonsa irrottamista globaalista internetistä, johon on otettu mallia esimerkiksi Kiinan palomuurista ja Iranin eristetystä halal-internetistä (Hallamaa 2019).Tietoverkkosodankäynnin tutkijoiden mukaan Venäjä voi päästä globaalista internetistä riippumattomaan omaan nettiinsä suhteellisen pienin kustannuksin, sillä siihen on jo olemassa sopivaa teknologiaa. Tämä tapahtuu käytännössä siten, että Venäjä pakottaa omien verkkojen reitityksen tapahtuvan Venäjän alueella. BGP- reititysprotokollaa (border gateway protocol) ja ohjelmallista verkonhallintateknologia SDN:a (software-defined networking) käytettäisiin oman verkon sulkemisen apuna Puolustusvoimien tutkimuslaitoksen tietoverkkosodankäynnin asiantuntijat ovat päätelleet, että mahdollisessa kriisitilanteessa Venäjä saa suhteellista etua suljetusta ja valtion valvomasta internetistään (Huhtanen 2018).

Venäjä on jo kopioinut oman version internetin nimipalvelujärjestelmästä, eli DND- järjestelmästä, joka ohjaa verkkoliikenteen oikeisiin IP-osoitteisiin. Nimipalvelujärjestelmää hallitsemalla Venäjä voisi määrittää, mihin osoitteisiin sen alueelta on pääsy. Tämän avulla saataisiin myös hankaloitettua anonyymina toimimista verkossa ja estää lisäksi ulkopuolelta tulevan liikenteen venäläisille sivustoille (Hallamaa 2019).

RuNet- verkon runkoyhteydet ovat lähestulkoon kokonaan viiden yhtiön hallussa. Kaupungit venäjällä on yhdistetty valokuitukaapelein, mutta esimerkiksi satelliittiyhteyksiä on myös käytössä. Tärkeät yhdysliikennepisteet internet- liikenteelle ovat pääosin Länsi-Venäjällä ja Siperian rautatien varrella. Venäjän viranomaisilla on RuNet- verkon lisäksi käytössä omia verkkojaan, kuten esimerkiksi Venäjän federaation valtionverkko ja Venäjän asevoimien verkko. Noista asevoimien verkko perustuu Venäjän puolustusministeriön ja teleyritys Rostelekomin verkkoihin. Sotilasyksiköillä on omat palvelimensa ja reitittimensä, joista ei ole yhteyttä yleiseen internetiin. Dataa välitetään valokuitujen, satelliittien ja radiolinkkien kautta ja ilmeisesti käyttöjärjestelmä on ainakin alemmalla tasolla Astra Linux, sillä pyrkimyksenä on lännestä riippumattomaan teknologia- ja ohjelmistokehitys (Huhtanen 2018).

Heinäkuussa 2016 hyväksyttiin terrorismin torjuntaa varten kaksi liittovaltion lakia (nro 374-FZ ja nro 375-FZ), joita julkisissa keskusteluissa kutsuttiin "Yarovaya-laiksi- yhden aloitta-

jan nimellä. tarkistusprosessista ja liittovaltion lain myöhemmästä hyväksymisestä. Liittovaltion laki nro 374-FZ asettaa muun muassa teleoperaattoreille tiukkoja vaatimuksia, jotka koskevat verkon välityksellä lähetettyjen sekä virallisten että käyttäjien tietojen varastointia kuuden kuukauden kuluessa lähetyspäivästä. Teleoperaattoreiden ja riippumattomien lähteiden mukaan liittovaltion laissa nro. 374-FZ vaatii valtavia investointeja ja valtavia kustannuksia. Muutokset, jotka antavat hallitukselle valtuudet velvoittaa teleoperaattorit pitämään kirjaa käyttäjien puhelinkeskusteluista, SNIS-palveluista ja käyttäjien Internet- liikenteestä kuuden kuukauden ajan, tulevat voimaan 1.7.2018. Samanaikaisesti tarkistusten perusteella nämä tiedot on säilytettävä yksinomaan Venäjän alueella. "Yarovaya-lain"säännöt voivat johtaa palvelujen hintojen vakavaan nousuun ja sitä myöten kaikkien pienten ja keskisuurten teleoperaattoreiden katoamiseen (Uglov 2017).

Yarovaya-laki ja internet- sivustojen estojen laajentaminen Venäjällä eivät olleet riittäviä käyttäjien turvallisuuden varmistamiseksi. Digitaalitalouden kansallinen hanke, johon on tarkoitus käyttää 1,1 biljoonaa ruplaa valtion budjetista, sisältää aloitteita lapsille tarkoitettujen internet- sivustojen suodattamiseksi, viestintäpalvelujen ja jopa IoT- laitteiden asiakkaiden tunnistamiseksi, sekä kotimaisten virustorjuntaohjelmien pakollinen asentaminen uusiin henkilökohtaisiin tietokoneisiin. Toimenpiteiden päätavoitteena on rikollisuuden torjunta, sillä lainvalvontaviranomaisten on ymmärrettävä, kuka on tietyn tilin takana laittomien toimien yhteydessä. Jotta voit käyttää Internetiä ensimmäistä kertaa sen kautta, sinun on ilmoitettava puhelinnumero, johon on teoriassa passitiedot ovat sidottuna. Lisäksi hieman yli kolmen vuoden kuluttua viranomaiset odottavat ottavansa käyttöön valvonnan teini-ikäisten käyttämälle verkkosisällölle. Venäjällä olisi 31. joulukuuta 2021 mennessä otettava käyttöön järjestelmä Internet- liikenteen suodattamiseksi, kun lapset käyttävät tietoresursseja. Järjestelmä maksaa valtiolle 140 miljoonaa ruplaa ja hankkeen toteuttajina toimivat Roskomnadzor, tele- ja joukkoviestintäministeriö, sisäasiainministeriö ja FSB, ja vastuullinen päällikkö on Roskomnadzorin varapäällikkö Alexander Pankov (Zhukova, Novyi ja Tishina 2018).

4.4 Internetin pirstaloituminen

Maailman talousjohtajat kokoontuivat Sveitsin Davosiin keskustelemaan neljännestä teollisesta vallankumouksesta eli tuotantojärjestelmien digitalisaatiosta kaksi vuotta sitten. Tapaamisessa nousi esille huoli siitä, että internet, joka on luonut talouskasvua vuosien ajan, saattaa mahdollisesti pirstaloitua valtioiden ja yritysten toimesta pienemmiksi alueiksi. Maailmanlaajuiseen tietoverkkoon on tällä hetkellä kytkettynä noin kymmenen miljardia laitetta joiden määrä kasvaa entisestään ja nyt vaarassa on talouskasvu joka perustuu tähän kehitykseen, jos kaiken tämän perustana oleva internet murenee pienempiin osiin (Hallamaa 2018).

Maailman talousfoorumin ohessa julkistettiin raportti internetin fragmentaatiosta, jossa internetin pirstaloituminen jaetaan kolmeen osa-alueeseen: Tekninen pirstaloituminen, valtiollinen pirstaloituminen ja kaupallinen pirstaloituminen. Tekninen pirstaloituminen sisältää internetin infrastruktuuriin liittyvät asiat, jotka saattavat haitata laitteiden yhteen toimivuutta ja datapakettien liikkumista. Valtiollinen pirstaloituminen käsittää kaikki valtioiden toimet, jotka haittaavat tai estävät pääsyn internetiin ja kaupallinen pirstaloituminen sisältää kaupallisten toimijoiden toimet, jotka haittaavat tai estävät internetin käytön. Siinä missä tekninen pirstaloituminen käsittelee itse internetin pirstaloitumista, niin valtiollinen ja kaupallinen pirstaloituminen käsittelevät pirstaloitumista internetissä (Hallamaa 2018).

Venäjällä ja Kiinassa pirstaloituminen näkyy internetpalveluissa, sillä näillä mailla on internetpalveluissa kaikki keskeiset omat kansalliset versionsa niin hakukoneista, yhteisöpalveluista kuin keskustelupalveluistakin. Pirstaloitumisen uusimpana muotona on tiedon ja informaation pirstaloituminen. Presidentti Putin esitti joulukuussa 2019 että Wikipedia tulisi korvata vastaavanlaisella venäläisellä sähköisessä muodossa olevalla tietosanakirjalla, jonka tulisi hänen mukaansa sisältää luotettavaa tietoa, joka on esitetty hyvällä ja modernilla tavalla. Myös Kiina on jo keväällä 2017 esittänyt ajatuksen korvata Wikipedia digimuodossa olevalla kiinalaisella ensyklopedialla. Näyttää siltä että internetin hajoaminen tai pirstaloituminen on väistämätöntä. Monelle diktatuurille vapaa tiedonvälitys ja tiedon saaminen on uhka, jonka vuoksi internet tulee muuttaa nationalnetiksi, jossa valtaapitävät voivat pitää tiukassa kontrollissa tiedonsiirtoa, palveluita ja tietosisältöjä (Lehto 2020b).

Euroopan hybridiosaamiskeskuksen Haavoittuvuudet ja resilienssi- verkoston johtaja Jukka

Savolainen toteaa, ettei ole tekninen asiantuntija, mutta internetin rajaaminen tai sulkeminen ei ole teknisesti kovin mutkikasta, vaan pikemminkin yksinkertaista. Siinä tietoliikenne ohjataan kulkemaan yhdessä maassa sijaitsevan palvelimen kautta. Surreyn yliopiston tietojenkäsittelyn professori Alan Woodward kommentoi BBC:lle, että Venäjän koe on yksi askel kohti internetin hajoamista. Myös kyberturvallisuuden työelämäprofessori Jarno Limnéllin mukaan niin Suomen kuin EU:n olisi syytä varautua siihen, että seuraavien vuosien aikana maailmanlaajuiset tietoverkot muuntuvat tai jopa hajoavat valtioiden tehdessä niistä irtiottoja, joten olisi tärkeää pohtia Euroopan ja Suomen kesken, mitkä olisivat niitä ratkaisuja joita voisimme eurooppalaisten kesken käyttää. Sillä juuri nyt näyttää siltä, että internetin hajautuminen maailmalla vain voimistuu (De Fresnes ja Brännare 2019).

4.5 EU:n oma kybermaailma?

Vielä vuonna 2014 ajateltiin että eurooppalainen verkko olisi vaikea toteuttaa ja lisäksi kallista sekä vaikeaa. Eräänä vaihtoehtona olisi luoda tietynlainen Euroopan oma intranet, johon ei olisi pääsyä mantereen ulkopuolisilla, mutta Merkel ja Hollande korostavat internetin avoimuuden merkitystä, joten tähän tuskin ollaan ryhtymässä. Tuolloin Saksan liittokansleri Angela Merkel sanoi myös, että Euroopan olisi syytä ryhtyä kehittämään omaa tietoverkkoaan, eli eräänlaista eurooppalaista internetiä, joka Merkelin mukaan mahdollistaisi paremman tietosuojan, kun viestejä ei olisi tarvetta kierrättää yhdysvaltalaisten palvelimien kautta (Heikkilä 2014).

Nykyään palvelimia on keskitetty Eurooppaan ja Google (2021) sivuston mukaan Suomesta löytyy Googlen yksi palvelinkeskus Haminasta ja muualta Euroopasta löytyy Alankomaista, Irlannista, Tanskasta ja Belgiasta Googlen palvelinkeskuksia. Lisäksi myös GDPR on tiukentanut yritysten tietoturvamäärityksiä, joka on tuonut paljon muutoksia esimerkiksi henkilötietojen käsittelyyn. Your Europe (2021) sivuilla mainitaan että henkilötietoja siirrettäessä EU:n ulkopuolelle, niin tietojen mukana on siirryttävä yleisen tietosuoja-asetuksen tarjoaman suoja. Eli, yrityksen viedessä tietoja ulkomaille, on yrityksen varmistettava jonkin seuraavista toteutuvan: EU pitää EU:n ulkopuolisen maan suojaa riittävänä, yritys toteuttaa asianmukaiset suojatoimenpiteet, kuten erityisten lausekkeiden sisällyttäminen EU:n ulkopuolisen henkilötietojen tuojan sopimukseen tai tietojen siirto perustuu erityisiin perusteisiin

(poikkeuksiin), kuten henkilön suostumukseen.

Jos GDPR- asetusta ei noudateta, valvontaviranomaisilla on mahdollisuus antaa huomautuksia tai määrätä hallinnollisia sakkoja. Hallinnolliset sakot määrätään kunkin yksittäisen tapauksen olosuhteiden mukaisesti 58 artiklan 2 kohdan ja sen alakohdassa tarkoitettujen toimenpiteiden lisäksi tai niiden sijasta. Sakkojen suuruus on enintään 20 000 000 euroa, tai neljä prosenttia yrityksen edeltävän tilikauden vuotuisesta kokonaisliikevaihdosta sen mukaan, kumpi näistä on suurempi (Digiturvamalli 2017).

5 Johtopäätökset

Kaikista lainsäädännöistä ja kyberrikollisuuden ehkäisevistä toimenpiteistä huolimatta, uutisista saa jatkuvasti lukea uusista tietoturvahyökkäyksistä, tietovuodoista, lunnasvaatimuksista ja yhä kehittyneimmistä haittaohjelmista sekä viruksista. Kaikki uudet tukahduttamisyritykset ovat vain reikien paikkailua. Kun yksi reikä saadaan tukittua, on jo odottamassa monta uutta reikää. Siitä syystä ei voida jatkaa nykyisellä linjalla, vaan täytyy luoda rinnalle uusi turvallinen kybermaailma.

Rikolliset ovat siirtyneet kybermaailmaan ja kyberrikollisuus laajenee entisestään, kun taas tietoturvan asiantuntijoita ei ole riittävästi. Kybermaailma on jatkuvasti alttiina niin virusten, haittaohjelmien ja identiteettivarkauksien kuin myös fyysisen maailman ongelmille ja kyberrikollisten hyökkäyksille. Kyberrikollisuuden kustannukset ovat suuria ja tulevaisuudessa ne tulevat entisestään vain nousemaan.

Kiinan suuri palomuuri on rakennettu lähinnä propagandatarkoituksessa, kun taas Venäjän RuNet- verkon rakentamisen ja kehittämisen tarkoituksena on enemmänkin pyrkiä lännestä riippumattomaan asemaan ja onkin vahvoilla mahdollisen kriisitilanteen sattuessa. Eurooppa voisi ottaa mallia Venäjän ja Kiinan kybermaailmoista suunnitellessa omaa kybermaailmaansa, huomioiden kuitenkin omat tarpeet ja rajoituksensa.

Euroopan oman kybermaailman rakentamisen viive vaikuttaa johtuvan siitä, ettei uskalleta ottaa sitä askelta eteenpäin peläten mahdollisia konflikteja muiden maiden kanssa. Globaali internet on ollut yrityksille taloudellisesti tuottavaa bisnestä, joten rahahanoja ei helpoin perustein haluta laittaa kiinni. Myös erottelu globaalista internetistä voi tuntua haasteelliselta ja työläältä, eikä siihen jakseta pureutua, vaan mieluummin laitetaan rahaa nykyisen järjestelmän suojaamiseen siitä huolimatta, että se on loputon rahareikä kyberrikollisten tullessa yhä taitavimmiksi ja nokkelimmiksi.

Globaali internet pirstaloituu ja EU:n onkin syytä varautua maailmanlaajuisten tietoverkkojen hajoamiseen ja pohtia eurooppalaisille sopivia ratkaisuja tulevaisuutta varten. Aiheesta ei ole tehty suoraan tutkimuksia, vaan aihetta hahmoteltiin keräämällä aiheesta sivuavia tutkimuksia ja tietoja, joiden perusteella tehtiin päätelmiä ja tulkintoja.

Tutkimuksia tarvitaan kybermaailman rakentamisen kustannuksista sekä siitä, lisääntyykö kyberturvallisuus oman kybermaailman avulla ja onko sillä vaikutuksia kansainväliseen yhteistyöhön. Tutkimuksien avulla saadaan parempi näkemys siitä, olisiko Euroopan oman kybermaailman rakentaminen hyvä ratkaisu. On syytä myös perehtyä syvemmin siihen, kuinka EU:n oma kybermaailma saataisiin teknisesti toteutettua ja lisäksi on tärkeää pohtia, olisiko syytä rakentaa Suomelle oma kriittinen infrastruktuuri EU:n kybermaailman rinnalle, jolloin kriittisimmät tiedot olisivat vain oman valtion suojissa.

Lähteet

Abomhara, Mohamed, ja Geir M Køien. 2015. “Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks”. *Journal of Cyber Security and Mobility,* 65–88.

Airaksinen, Tiina H. 2020. “Sensuuri, kielletyt aiheet ja tieteellinen julkaiseminen Kiinassa” [kielellä suomi]. *Tieteessä tapahtuu* 38, numero 2 (huhtikuu): 3–11. ISSN: 0781-7916.

Anderson, Daniel. 2012. “Splinternet Behind the Great Firewall of China: Once China opened its door to the world, it could not close it again.” *Queue* 10 (11): 40–49.

AT&T. 2015. *What Every CEO Needs to Know About Cybersecurity, Decoding the Adversary.* Saatavilla WWW-muodossa, https://www.business.att.com/content/dam/attbusiness/reports/decodingtheadversary.pdf/, viitattu 31.3.2021.

Bambauer, Derek E, Ronald J Deibert, John G Palfrey, Rafal Rohozinski, Nart Villeneuve ja Jonathan L Zittrain. 2005. “Internet filtering in China in 2004-2005: A country study”. *Available at SSRN 706681.*

CAC. 2020. *Kyberturvallisuuden tarkistustoimenpiteet.* Saatavilla WWW-muodossa, http://www.cac.gov.cn/2020-04/27/c_1589535450769077.htm, viitattu 3.4.2021.

Chakrabarti, Anirban, ja G Manimaran. 2002. “Internet infrastructure security: A taxonomy”. *IEEE network* 16 (6): 13–21.

CNN.com. 2001. *Key homeland security deputies appointed.* Saatavilla WWW-muodossa, http://edition.cnn.com/2001/US/10/09/rec.homeland.defense.posts/, viitattu 21.2.2021.

De Fresnes, Tulikukka, ja Stina Brännare. 2019. *Venäjä kokeili netin sulkemista muulta maailmalta – asiantuntijat: Kyse on informaatiotilan hallinnasta ja sotilaallisesta pelotteesta.* Saatavilla WWW-muodossa, https://yle.fi/uutiset/3-11134570, viitattu 21.2.2021.

Digiturvamalli. 2017. *GDPR: Vastuu ja seuraamukset.* Saatavilla WWW-muodossa, https://fakta.digiturvamalli.fi/kategoria/oikeussuojakeinot-vastuu-ja-seuraamukset, viitattu 19.4.2021.

Europe, Your. 2021. *Milloin yleistä tietosuoja-asetusta sovelletaan?* Saatavilla WWW-muodossa, https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_fi.htm#shortcut-6, viitattu 3.4.2021.

Google, palvelinkeskus. 2021. *Tutustu palvelinkeskustemme sijainteihin.* Saatavilla WWW-muodossa, https://www.google.com/intl/fi_fi/about/datacenters/locations/, viitattu 3.4.2021.

Hallamaa, Teemu. 2018. *Kiina estää tehokkaasti tiedonkulun, Venäjä uhoaa perustavansa oman internetin: Hajoaako internet osiin?* Saatavilla WWW-muodossa, https://yle.fi/uutiset/3-10226579, viitattu 21.2.2021.

———. 2019. *Venäjä aikoo testata internetistä irtautumista tänä keväänä.* Saatavilla WWW-muodossa, https://yle.fi/uutiset/3-10641041, viitattu 21.2.2021.

Halminen, Laura. 2019. *Voiko Venäjä irrottaa itsensä internetistä ja meneekö koko verkko silloin rikki? Asiantuntijat vastaavat.* Saatavilla WWW-muodossa, https://www.hs.fi/teknologia/art-2000006099267.html, viitattu 4.4.2021.

Heikkilä, Annastiina. 2014. *Eurooppalainen internet – ratkaisu tietoturvaongelmiin?* Saatavilla WWW-muodossa, https://yle.fi/uutiset/3-7098548, viitattu 21.2.2021.

Huhtanen, Jarmo. 2018. *Suomalaiset tutkijat: Venäjän valmistelut muun maailman internetistä irrottautumiseksi eivät olekaan propagandaa.* Saatavilla WWW-muodossa, https://www.hs.fi/kotimaa/art-2000005736787.html, viitattu 1.4.2021.

Hutchins, Eric M, Michael J Cloppert, Rohan M Amin ym. 2011. *Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains.* 1:80. 1. Academic Conferences Limited.

Jansson, Saara, ja Tanja Sihvonen. 2018. “Kyberturvallisuus valtiollisena toimintaympäristönä ja siihen kohdistuvat uhkat”. *Media & viestintä* 41 (1).

Kriz, Danielle. 2011. “Cybersecurity principles for industry and government: A useful framework for efforts globally to improve cybersecurity”. *2011 Second Worldwide Cybersecurity Summit (WCS)IEEE* 11:1–3.

Kurenmaa, Tom. 2020. *Tiedonvapauden erot: Suomi, Kiina & Yhdysvallat.* Haaga-Helia ammattikorkeakoulu Oy.

Lehto, Martti. 2020a. *Digitaalisen kybermaailman ilmiöitä ja määrittelyjä: Kyber on kaikkialla.* Jyväskylän yliopisto.

———. 2020b. *Hajoaako Internet?* Saatavilla WWW-muodossa, https://www.upseeriliitto.fi/sotilasaikakauslehti/4_2020/hajoaako_internet, viitattu 8.3.2021.

Lehto, Martti, Jarno Limnéll, Eeva Innola, Jouni Pöyhönen, Tarja Rusi ja Mirva Salminen. 2017. *Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi* [kielellä suomi]. Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja, 30/2017. Suomi: Valtioneuvoston kanslia, helmikuu.

Limnell, Jarno. 2014. “Kyber rantautui Suomeen” (marraskuu). https://doi.org/10.13140/RG.2.1.1559.8162.

Limnéll, Jarno, Klaus Majewwski ja Mirva Salminen. 2014. *Kybermaailma.* 1. painos. Jyväskylä: Docendo.

Mattila, Juri. 2020. *Kyberrikollisuus yleistyy ja Suomi kompuroi tietoturvassa – osaamispula jarruttaa kehitystä.* Saatavilla WWW-muodossa, https://www.etla.fi/ajankohtaista/kyberrikollisuus-yleistyy-ja-suomi-kompuroi-tietoturvassa-osaamispula-jarruttaa-kehitysta/, viitattu 11.4.2021.

McAfee. 2016. *McAfee Labs Threats Report.* Saatavilla WWW-muodossa, https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-dec-2016.pdf/, viitattu 31.3.2010.

Minchev, Zlatogor. 2016. “Cyber Threats Identification in the Evolving Digital Reality”. Institute of Mathematics / Informatics Bulgarian Academy of Sciences.

Morgan, Steve. 2019. *2019/2020 Cybersecurity Almanac: 100 Facts, Figures, Predictions And Statistics.* Saatavilla WWW-muodossa, https://cybersecurityventures.com/cybersecurity-almanac-2019/, viitattu 11.4.2021.

MTV–uutiset. 2018. *F-Secure varoittaa: Verkkohyökkäysten määrä kasvaa rajusti – "Kaikkia hyökkäyksiä ei pystytä torjumaan".* Saatavilla WWW-muodossa, https://www.mtvuutiset.fi/artikkeli/f-secure-varoittaa-verkkohyokkaysten-maara-kasvaa-rajusti-kaikkia-hyokkayksia-ei-pystyta-torjumaan/6931786#gs.c0i64b, viitattu 18.4.2021.

Nykänen, Maria. 2020. *Kiristyshaittaohjelmat ovat pelottavin tietoturvauhka, linjaa asiantuntija – "On tahoja, jotka tekevät kyberhyökkäyksiä päivätöinään".* Saatavilla WWW-muodossa, https://www.mtvuutiset.fi/artikkeli/kiristyshaittaohjelmat-ovat-pelottavin-tietoturvauhka-linjaa-asiantuntija-on-tahoja-jotka-tekevat-kyberhyokkayksia-paivatoinaan/7882004#gs.vlur6v, viitattu 8.3.2021.

Ristolainen, Mari. 2017. "Should 'runet 2020'be taken seriously? contradictory views about cyber security between russia and the west". *Journal of information warfare* 16 (4): 113–131.

Rivero, Nicolás. 2018. *The biggest data breaches of all time, ranked.* Saatavilla WWW-muodossa, https://qz.com/1480809/the-biggest-data-breaches-of-all-time-ranked/, viitattu 1.4.2021, suomennos minun.

Sanastokeskus. 2018. *Kyberturvallisuuden sanasto.* Saatavilla WWW-muodossa, https://www.tsk.fi/tiedostot/pdf/Kyberturvallisuuden_sanasto.pdf, viitattu 21.2.2021.

Sauer, Tim. 2020. *Hacking the Internet: How BGP paves the way for attackers.* Saatavilla WWW-muodossa, http://sauert.com/documents/bgp.pdf, viitattu 25.4.2021.

Turvallisuuskomitea. 2013. *Suomen kyberturvallisuusstrategia.* Saatavilla WWW-muodossa, https://turvallisuuskomitea.fi/wp-content/uploads/2018/05/Suomen-kyberturvallisuusstrategia-ja-taustamuistio.pdf, viitattu 21.2.2021.

Uglov, Ivan Valer'yevich. 2017. "Ways of realization of the"Yarovaya Law"requirements in telecommunications". *T-Comm-Telekommunikatsii i Transport* 11 (7).

Valtioneuvosto. 2012. *Suomen turvallisuus- ja puolustuspolitiikka 2012 Valtioneuvoston selonteko.* Saatavilla WWW-muodossa, https://vnk.fi/documents/10616/622970/J0512_Suomen+turvallisuus-+ja+puolustuspolitiikka+2012.pdf/b534174a-13bc-4684-beb0-a093be30ce2a/J0512_Suomen+turvallisuus-+ja+puolustuspolitiikka+2012.pdf?version=1.0&t=1422011065000, viitattu 30.3.2021.

Zhukova, Kristina, Vladislav Novyi ja Yulia Tishina. 2018. *RuNet za stenoj: Kak nacproekt 'Cifrovaâ èkonomika' povliâet na pol'zovatelej interneta.* Saatavilla WWW-muodossa, https://www.kommersant.ru/doc/3773489, viitattu 20.4.2021.